DECENTRALISED.CO's

YEAR in REVIEW

2023

Hey there,

I created this PDF (*using screenbreak*) figuring it would be easier for people to read when disconnected from the internet. Feel free to print it, sync to your kindles and share in circles that you may find it interesting.

For those receiving this copy for the first time - the following is a series of articles published on Decentralised.co over the course of 2023. We are a newsletter covering the intersection of technology, finance and the gradual decentralisation of the web.

You should sign up for our newsletter at Decentralised.co if the writing interests you.

I have added a total of 37 articles into the PDF. It should take you about 10 hours in total to read all of it. The articles are not in a chronological order so take on it one chapter at a time. Or go through specific titles that interest you. I have added articles that have been behind our paywalls for readers that are not on our paid list as a way of saying thank you for the love and support over the year.

The articles have been exported in their raw format from the newsletter. So you will see the occasional ad or references that are specific to the day. I have kept these intact as the PDF is an export of our existing body of work and not a book. Maybe, that is something to work on in the years to come.

Hoping to find answers to tougher questions in 2023,

Joel John

Contents

11

A New Internet

Joel John
decentralised.co

25

Value Accrual

Joel John
decentralised.co

35

The Narrative Wedge

Joel John
decentralised.co

44

Volatility As A Service

Joel John
decentralised.co

58

Mapping The New Internet

Joel John
decentralised.co

72

Mapping The Data Landscape

Saurabh
decentralised.co

83

The Royalty Wars

Joel John
decentralised.co

94

On Aggregation Theory And Web3

Joel John
decentralised.co, 23 Mar 2022

103

Payment Pipelines

Joel John
decentralised.co

116

The Data Wars

Joel John
decentralised.co

121

Token Mergers

Saurabh
decentralised.co

126

Bugs In The System

Joel John
decentralised.co

133

How To Take Over A DAO?

Saurabh
decentralised.co

139

Two Worlds Blending

Saurabh
decentralised.co

144

Gaming is a spectrum

Saurabh
decentralised.co

150

Blurring Lines

Saurabh
decentralised.co

156

Cynical Optimism

Joel John
decentralised.co

164

The Advertisers Are Coming

Siddharth
decentralised.co

170

Soul Bound Tokens

Joel John
decentralised.co

175

Bearproof Treasuries

Saurabh
decentralised.co

182

Retention in Web3

Joel John
decentralised.co

187

The Modular Experiment

Saurabh
decentralised.co

192

Using Telegram for Distribution

Joel John
decentralised.co

199

The Funding Environment

Joel John
decentralised.co

207

Token Bound Accounts

Joel John
decentralised.co

214

Revisiting The Metaverse

Joel John
decentralised.co

220

Keeping it Stable

Joel John
decentralised.co

226

It is All Derivative

Saurabh
decentralised.co

232

The Interface Dilemma

Joel John
decentralised.co

238

Zero to One

Saurabh
decentralised.co

244

On dYdX

Saurabh
decentralised.co

250

Matching Engines

Joel John
decentralised.co

258

Beyond Consortiums

Joel John
decentralised.co

265

Stress Testing

Saurabh
decentralised.co

270

Passport Please

Joel John
decentralised.co

276

Blast From the Past

Saurabh
decentralised.co

282

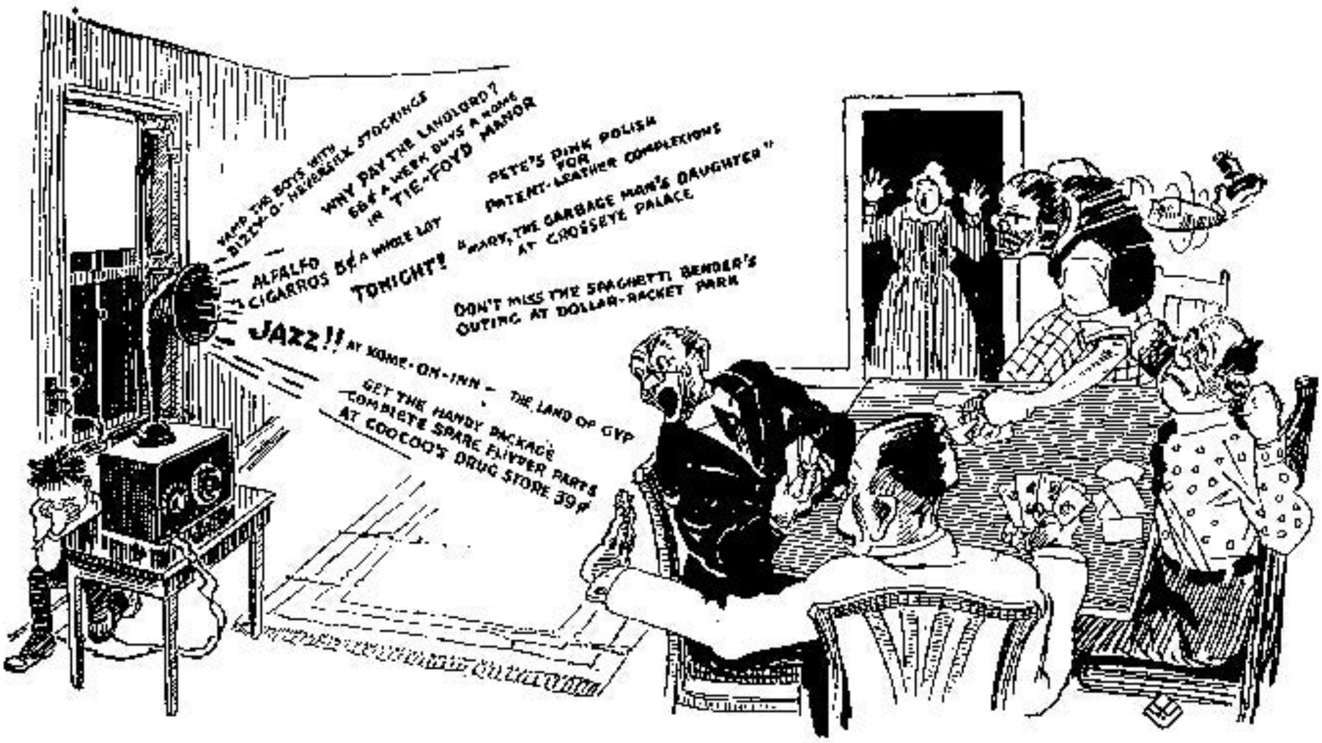
The L2 Paradox

Saurabh
decentralised.co

Joel John
decentralised.co

A New Internet

On Web3 Primitives & Social Networks


VAMP THE BOYS WITH BIZZY-O-HEVERSEK STOCKINGS
WHY PAY THE LANDLORD? 68¢ A WEEK BUYS A HOME IN TIE-FOYD MANOR
PETE'S PINK POLISH FOR PATENT-LEATHER COMPLEXIONS
ALFALFO CIGARROS B¢ A WHOLE LOT
TONIGHT! "MARY, THE GARBAGE MAN'S DAUGHTER" AT CROSSEYE PALACE
DON'T MISS THE SPAGHETTI BENDER'S OUTING AT DOLLAR-RACKET PARK
JAZZ!! AT HOME-ON-INN - THE LAND OF GYP
GET THE HANDY PACKAGE COMPLETE SPARE FLIVVER PARTS AT COOCOO'S DRUG STORE 39¢

Hey there,

Today's newsletter was co-authored by Sid - who is ironically, taking a well deserved break far away from social networks. Somewhere in the hills in Himalayas. We have been brainstorming about what the state of the internet looks like & whether web3 primitives have a role to play in its future over the past few months. This piece, is by no means a market-map. It barely mentions any tokens. It is not a case for absolute decentralisation of everything on the web. Instead, what it addresses are the incentives & reasoning behind social networks emerging the way they are today. Along the way, I break down how we may have a new vision for the internet and the creators on it through the rails blockchains enable. This is a long read that may take close to 40 minutes. You may need coffee. But I hope you take the time to read through, criticise or build upon what you read.

Drop me an e-mail if you have strong thoughts post reading this. I would love to feature them to our readers.

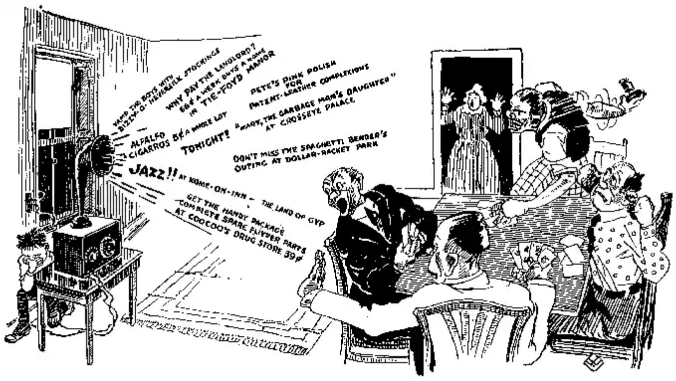
In 2020, when the pandemic lockdowns kicked off, I began spending an incredible amount of time on Clubhouse. I racked up a nice audience spending an hour every morning talking about what is going on in crypto. Everybody was working remotely; people were stuck at home, and much like AI today, DeFi and NFTs were the hot new thing. However, Clubhouse went from being valued at $3.4 billion to the app nobody talks about anymore in no time.

There is a myriad of reasons. The novelty faded off. People simply did not have the time to be online, plugging into conversations all the time. Or there were better conversations to be had in person. One could argue Twitter Spaces simply replicated Clubhouse for many users. But looking back on it, there's a valuable lesson for anybody building an audience online.

You are only as good as your link to a social graph is. And your social graph is only good as long as it can be maintained and evolved. This is the difference between a city (like NYC) and an in-game community where the possibility of a social graph vanishing is very real. Physical, social graphs tend to stay stickier when compared to the ones we form online.

Surveilling Social Graphs

This challenge of being only as good as your social graph was learned by telephone operators a hundred years before social networks like Clubhouse. During the advent of the telephone, it was common for independent telephone operators in communities to tie a telephone to speakers and communicate. Much like podcasts a century later, people would speak on the telephone, broadcasting across villages in real-time. Think of it as a primitive radio.


VAMP THE BOYS WITH DIZZY-O-HEVERSILK STOCKINGS
WHY PAY THE LANDLORD? 66¢ A WEEK BUYS A HOME IN TIE-FOYD MANOR
PETE'S PINK POLISH FOR PATENT-LEATHER COMPLEXIONS
ALFALFO CIGARROS 6¢ A WHOLE LOT
TONIGHT! "MARY, THE GARBAGE MAN'S DAUGHTER" AT CROSSEYE PALACE
DON'T MISS THE SPAGHETTI BENDER'S OUTING AT DOLLAR-RACKET PARK
JAZZ!! AT HOME-ON-INN - THE LAND OF GYP
GET THE HANDY PACKAGE COMPLETE SPARE FLIVVER PARTS AT COOCOO'S DRUG STORE 39¢

There were campaigns against advertisements on the radio as early as 1922. The image above is from Tim Wu's book - The Master Switch.

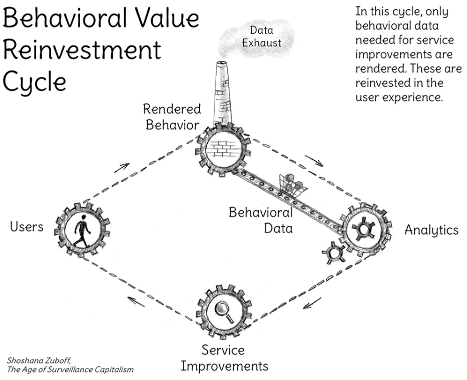
As larger players like AT&T and Bell took over telephone lines in the United States, these smaller telephone networks and their primitive podcasts vanished because running private, niche telephone networks was no longer sustainable. This is a chapter that we will see repeatedly as we traverse the emergence and eventual death of multiple social networks in this piece.

The emergence of a new network – like railways, telephone or internet – and new communication mediums have one thing in common. They unlock entirely new methods of collaboration. The Enlightenment era and the Arab Spring were both powered by people who found new ways to express themselves. But as we have seen, new communication forms do not establish themselves overnight.

They undergo a period of evolution and mutation before acceptable behaviour on these platforms is defined. For instance, you would not behave on Reddit as you would on LinkedIn (I'd think). And to set these ground rules and play the great social game, a social graph is needed.

But what even is a social graph? Put simply, it is the network of people and their relationships on an emergent platform. A social graph can be formed outside a digital native platform, like a university. Or it can be powered through algorithmic discovery like on Twitter. A graph can be public, where you can see who interacts with whom.

Or, in the case of dating apps, there can be closed, 1:1 graphs where the platform can charge you to display you to more individuals. But before we understand why social graphs matter, we must understand how targeted advertisements on the internet evolved to their current state.



In this cycle, only behavioral data needed for service improvements are rendered. These are reinvested in the user experience.

Shoshana Zuboff, The Age of Surveillance Capitalism

Figure 1: The Behavioral Value Reinvestment Cycle

From Shoshana Zuboff’s - Age of Surveillance Capitalism

Monetising Eyeballs

Shoshana Zuboff in *The Age of Surveillance Capitalism,* refers to user interactions on platforms like Google as behavioural value surplus. Historically, a firm had limited resources that it had to employ immediately to produce the goods it sold you. Or it paid ridiculous amounts in storage fees. A pencil manufacturer had to ship pencils. Ford's car factories had to sell cars. They could not endlessly stockpile the timber or rubber for the process.

With the advent of the internet, however, this equation changed. A player like Google or Meta could keep your data for a decade until it could be monetised for their benefit. I could go to Facebook now and download all the cringe texts I may have sent my crush back in 2011 (and so could you).

Much like I often nerd out about how blockchain data can be parsed for better consumer targeting on this publication, Google's team considered using sensors to capture user data as early as 2000. They noticed that grabbing data from wearables and in-home sensors could help create a better user profile suited to a person's needs. At the time, little did they know that we would be carrying watches that could do ECGs around the clock or that half of the world's mobile devices would be powered by an operating system powered by Google (*Android*). There was a new resource in town. User data was available in surplus. The mechanisms to monetise it were not.

In the early 2000s, most dot-com projects were what AI websites are today: an abundance of inbound traffic with little or no business model. You could license your search engine to a larger corporation or sell sponsored ads like Yahoo did. We try that here at the blog too – and as anyone would know, a bear market is the worst time to sell ads. So Google had to find a different way of selling ads altogether.

Instead of allowing people to bid on and list ads based on their assumptions about what the audience would click on, the data scientists at Google could measure and predict which ad would best suit which person. Instead of a brand's ad manager working on assumptions, you had data scientists targeting users, allowing the brand to see a clear RoI on each click from Google.

The perfect storm was in place for the evolution of the web. A business was realising the possibility of generating and storing a resource (user data) with next-to-no marginal costs and had the pipelines (targeted ads) to monetise it. All that was missing, in the style of most venture-backed companies, was a mechanism to scale it. This is where social graphs came to play.

Quoting from the book (yet again)

> *At that early stage of Google's development, the feedback loops involved in improving its Search functions produced a balance of power: Search needed people to learn from, and people needed Search to learn from. This symbiosis enabled Google's algorithms to learn and produce ever-more relevant and comprehensive search results. More queries meant more learning; more learning produced more relevance. More relevance meant more searches and more users*

See the bit about 'more users'? One of the strongest on-ramps for more users was the network effects of new-age networks like Facebook and Twitter. Social graphs serve two purposes. Firstly, they took the internet from a weird niche technology where you had LimeWire or AOL to the cool thing kids spoke about at school. Secondly (and more importantly), it gave the Internet a business model.

More users effectively meant you had a critical mass which could be divided and sold all kinds of goods. Users belonging to similar social graphs could be bucketed and served similar content. This became the basis for the algorithmic feeds in which we currently find love, jobs, giggles, despair & hope.

As a creator, one spends time on platforms like Twitter or Facebook today as they are the means for distribution This occurs because these social networks have a never-ending appetite for content that feeds into a relevant social graph and keeps users engaged. If a community of fintech fanatics were constantly given content from crypto influencers, they would eventually be outraged and depart the platform.

Similarly, if my Web3 content were shared with an audience subset who hates it, my incentives to create content would drastically decline. Platforms play a critical role when targeting relevant audiences with content based on the data they have on users. The longer platforms can keep a user hooked, the more ads they can sell and the more data they can gather. As they hoard more data, the more relevant their ads get. This process is an infinite money-printing machine for all intents and purposes.

In Web2 networks, the social graph is the moat. If you allow users to interact with a graph via third-party applications, your chance of capturing user data diminishes. After all, the user then won't be on a product that you control. If users can simply port their network of friends and family to a different application, they will have no incentive to return to yours, either.

We don't have a shared protocol for social applications that work at the scale of Meta or Twitter because of how incentives are structured for existing behemoths. A Web2 product with open social graphs opens itself to competition and declining revenue. Both of which may not be a desirable outcome.

Composable Social Graphs

Centralisation of social networks in the gilded age of platform censorship also comes with risks. A recent article on The Verge sums up the question everyone has been asking amidst Elon Musk's antics on Twitter and the United States' desire to rein in TikTok's growth.

An excerpt reads as follows:

> *But if our current social system were decentralized, you'd be able to post a picture on Instagram, and I could see it and comment on it in the Twitter app. Your friends could read your tweets in their TikTok app. I could exclusively use Tumblr, and you could read all my posts on Telegram. Different apps would have different strengths, weaknesses, moderation policies, and creator tools. Still, you'd have the same followers and follow the same accounts no matter your platform. There would be no 'Facebook friends' and 'Twitter followers.' The social graph and the product market would split completely.*

What they are describing is the composability of a social graph at scale. A mechanism for users to access their network across applications in formats they deem best. What would that look like? Many applications that emerged after the early 2000s have not yet had a standardised protocol. There is SMTP for e-mail. There is DNS for resolving domain names. There is RSS for articles.

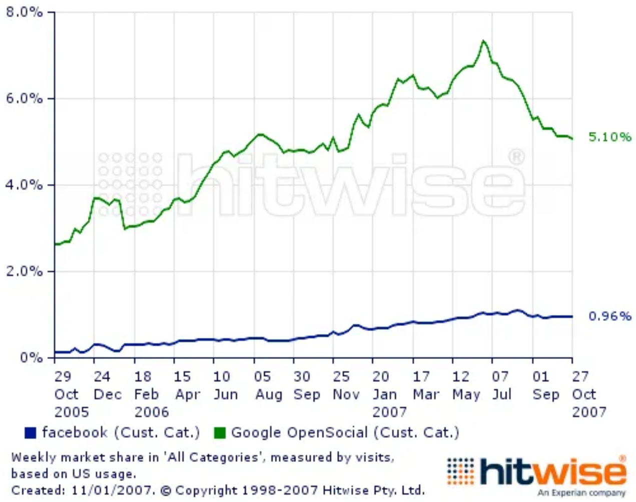
But what if you wanted to send vanishing images across Snapchat, Whatsapp and Instagram? What if you could have Twitter content with proprietary algorithms tweaked to your preferences? Or what if there were a version of Instagram that did not force you to watch reels?

Control is lost without a protocol for social graph maintenance and portability. Users can no longer determine how and what they consume. With RSS feeds, the user is in control. But with Twitter, Elon Musk and his minions are in control.

The solution to such a situation was proposed as early as 2007. OpenSocial was a collaboration between multiple large social networks to create a group of APIs that would allow platforms to replicate a user's social graph elsewhere. For users, it meant not having to worry about adding friends again with each new network they joined. For platforms, it meant not having to compete against the network effects of an incumbent. Everyone's winning, right?

Well, not really. As we all know, platforms have walled off social graphs today. The product was initially used by Orkut only and eventually saw over 350 million users. Legend has it that Google onboarded several social networks like Friendster and Myspace under an NDA, then broke the news to Facebook and forced Facebook to join.

For a moment, this strategy worked, as the graph below shows. By late 2007, OpenSocial's network of applications had five times Facebook's traffic. In 2008, there were 350 million users on the network, but by the 2010s, it became clear that an open graph was not what the internet desired. Much like Libra in 2022, a group of large organisations working as a nonprofit tend to be beaten by smaller incumbents that can move at speed.



Weekly market share in 'All Categories', measured by visits, based on US usage.
Created: 11/01/2007. © Copyright 1998-2007 Hitwise Pty. Ltd.

Facebook dominated in a few years as it had cracked a critical mass of users. Which they managed to do by becoming an open platform third-party developers could deploy applications on. In the early days of social networks, people were not coming to them for content alone. Applications were a huge part of the draw towards them. Remember Farmville? The firm behind it (Zynga) grew on the network effects that came on a platform like Facebook. Each action you took in the game propagated across your social graph, which meant more friends to play with.

During the early days of social networks, applications empowered platforms to grab attention while user-generated content slowly emerged. Posting outrageous comments on the internet was a habit yet to be formed. The dopamine hits from the like, and retweet buttons had yet to be discovered. However, this trifecta – of powerful applications, network effects and distribution that came with a social graph – enabled social networks to establish themselves by 2010.

In hindsight, all the things we have been exploring in Web3 are aspects the internet has already tinkered with. Social graphs being portable? Done. Applications embedded with your identity? Yeah, I tried that. How about a single protocol that multiple applications can interact with? Boring.

There is no novelty in these new approaches, but the technical layer to enable them did not exist in the past. **That change in infrastructure - from server-side, centralised ownership by monopolies to blockchain-based decentralised ownership by users is what is "new" about Web3.** OpenSocial's last update was in 2013. Nobody I know has access to their Friendster or Myspace social graph today. You cannot build or ship applications on top of Twitter like you once could. Blockchains may meaningfully change that equation.

Yield Farming Human Attention

Siddarth Jain had a beautiful metaphor to paint here. When a tree in the jungle dies, it has continuity, contributing to the growth and sustenance of other trees that come long after it. When a community on the internet dies, there is little that it passes on to what comes after it. Going back to how I started this piece, Clubhouse went from the app we all started our mornings with to one nobody cares about anymore.

As I write this, Naval's Airchat is making the rounds on Twitter. I am excited about it because it uses AI to allow people to converse in their native languages. I would love to host our readers worldwide, speaking in their own languages as the app goes live. But when we start on Airchat, we start with a blank slate – a non-existent social graph.

Lens Protocol offers an alternative to this situation. The essence of their offering is simple. You have a social graph linked to your identity, which a wallet owns. The wallet lets you sign into a suite of apps, each serving a different purpose. In a hypothetical example, that would mean subscribers of this blog would also be able to opt-into seeing things I post on an Instagram-like feed or short-form short content like what's on Twitter instead of separately signing up for each.

This protocol approach for human attention is new in Web3. It has worked for NFTs with SeaPort and DeFi liquidity, as we saw with Uniswap. But can human attention be shared across applications if captured in a protocol like Lens?

I don't quite know, but there are benefits to doing so. It considerably empowers competition in social networks by reducing the entry barriers to creating new social networks. Founders could focus time on the application itself instead of bootstrapping a user base.

In such an instance, you could own your network of friends, but you would reach out to them and post content through a third-party application. Nikita Bier shared a modular approach to enabling social networks on Twitter recently. I presume he is not much of a fan of Web3, but the elements he has covered as "Reusable" are precisely the things that can go on the chain.

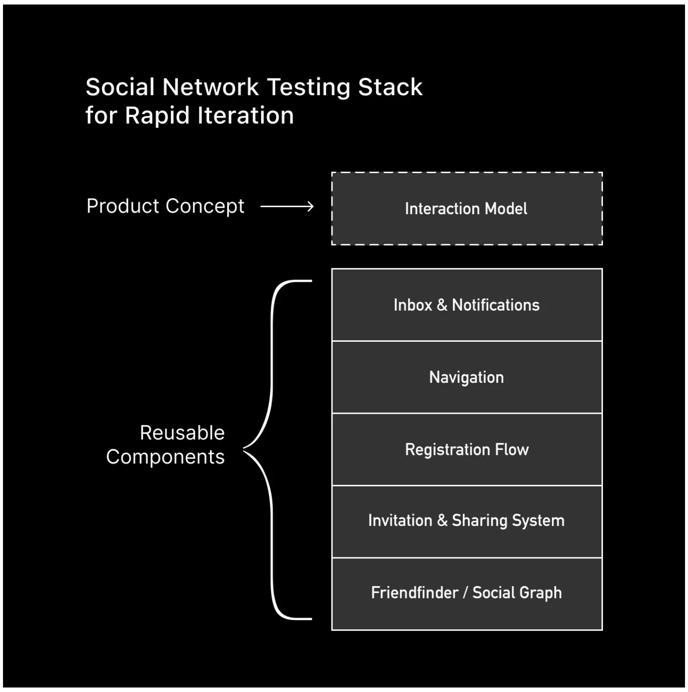


Image is from Nikita Bier's twitter.

As Lyn Alden pointed out in this post, we have had open money for quite some time. But open social networks have not yet scaled substantially. Part of the reason for this is that there is a clear lack of business models. When social networks like Facebook took off in the mid-2000s, years of perfecting the advertisement-driven model had already occurred.

The means of monetising Web3 social products is not entirely clear. Now, there are a few distinctions to make here. Firstly, decentralised social networks have existed for a while with no tokens. Mastodon, Nostr, and Bluesky are all functional products without tokens. I don't quite believe that tokens are the holy grail for the future of social networks.

Secondly, decentralisation brings challenges that might not be solvable with things as they are. Data must be stored in a decentralised social network in a P2P network like IPFS or Filecoin. That incurs costs along with it. Even if these costs are minuscule, they will discourage many users. Furthermore, no clear models exist for discovering content or algorithmically targeting users if the content is entirely on-chain.

Discovery today happens through products with huge moats on on-chain data analysis, like Nansen or Covalent. Lets ignore for a moment the fact that content is different from transactional data. They incur costs while parsing and categorising content that emerges on-chain. Who bears those costs? This ignores the fact that in such a model, a service provider can still tweak the algorithms to suit their agenda, leaving the user little choice regarding what kind of content they consume. So, we end up making the same mistakes all over again.

(*I am skipping through a lot here about where user data will be stored and the privacy benefits such a model could bring users. We will speak about it in another piece.*) .

What I'm trying to get at is the following:

1. Decentralised social networks have existed for a while. Humans are creatures of convenience. The incentives of distribution and discovery are far more efficient in Web2 native products. And there are no upfront costs to the customer. It is why much of the social graphs we know exist in walled, centralised social networks today.

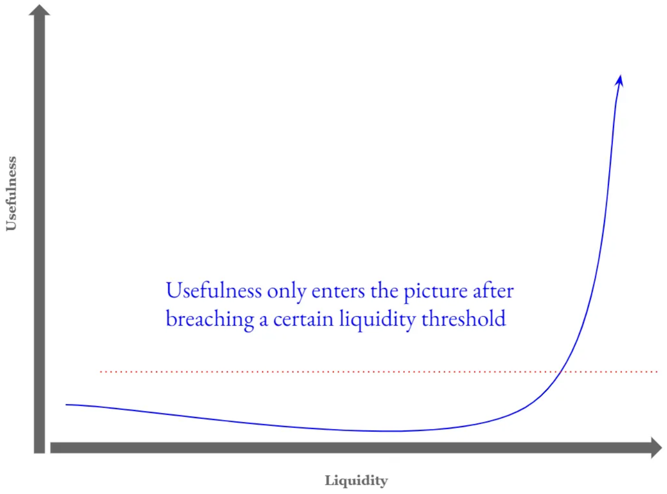
2. Slapping tokens alone won't compensate for the early-stage liquidity of human attention because, unlike NFTs or capital in DeFi projects, attention can't be parked on a product. When a user parks $1,000 in Aave,

the transaction may take 10 minutes. You cannot give away tokens and expect users to spend 1,000 hours on a social network. This is the reason why most social networks in Web3 die really quick deaths. (*Remember Steem?*)

Embedded Social DApps

So what exactly is the point of Web3 social networks? Is it just fugazi for the sake of issuing tokens and pretending as though we are at the precipice of a new internet? Or do these primitives hold promise? One way to think of it is through the lens of what @mhonkasalo mentioned in this post.

Applications require a threshold amount in liquidity to become relevant. In Uniswap's case, it is capital locked. In the case of Mirror or Lens, it is the number of people creating content and engaging with it. At its crux, compared to Mastodon or Nostr, a token-based network can have drastically better chances of bootstrapping initial liquidity to become relevant.



From Mhonkasalo’s Substack post.

This is not to discount the possibility of airdrop hunters posting spammy content and engaging with posts for the sake of an airdrop. If you think of it, somebody like Ben Thompson (of Stratechery) or Packy (from Not Boring) has very little incentive to move to a new Web3 native platform. Their audience base is strongly embedded in their mailing lists and Twitter.

But for a new creator building an entirely new audience base, tapping into a community of airdrop hunters on Lens could be a powerful strategy. **Token networks help distribute social graphs like those on Lens from 0 to 1.** One instance of a creator scaling along side a platform is that of Bill Bishop. He was one of Substack’s first writers & scaled his newsletter substantially alongside the growth of the platform.

The challenge, becomes how you retain a community after you reach threshold levels – say 10,000 engaged members on an app. This is where Web3's DApp ecosystem elements come into play. Remember how I mentioned that applications like Farmville were crucial in kick-starting large audience bases on social networks?

Applications and social networks in Web3 will have a symbiotic relationship in that neither has seen a substantial user base as they stand. But what if you could trade a token based on what an influencer you follow mentioned? Or collect an article as an NFT directly from your feed? Interfaces to enable this already exist but they are spread across applications.

Much like how Facebook empowered a generation of applications built on it to tap into their privately held social graph, Web3 DApps will be able to use emergent social graphs on protocols like Lens. The missing “bridge” here is a client layer that can enable that transition.

I am hinting at the composability of social graphs and DApps coming together. In such a case, a user could consume content and trade assets, collect

NFTs, or reward creators directly without the platform taking on the risks of any of these actions. You could source liquidity from Uniswap, OpenSea, or Mirror to perform these actions.

The platform could charge a small fee (say 0.1%) for bringing together the protocol and the user on every transaction. This may seem far-fetched, but consider that Metamask alone has enabled some $3 billion in volume for swaps of assets on it. Once you have a user base, you can embed financial applications of all kinds.

This open interaction of social graphs and open-access applications is at the crux of what will empower Web3 native social networks to be a thing. As things stand today, we have isolated islands. We trade on Uniswap, often making questionable decisions alone. We track DAO activity on products like Snapshot, wondering who else is involved, and then proceed to read through Mirror and support our favourite writers by collecting their articles. Each of these is an isolated interaction in Web3. And humans don't like sitting around alone too long.

Nobody knows which of their friends are playing which cool Web3 native game. Crypto and Web3 today is either a cut-throat, PVP game where there is only a few winners or an isolated, single-player game where you hold your assets with your dear life. The technology to enable cooperative multiplayer games are here in the form of DAOs.

But our platforms rarely ever make use of them. Think of a large crowd, putting together all the components you need to make a rocket. Then piling it behind a truck. And pushing it across town physically. All the while screaming "WAGMI" and scrolling through Twitter to see if Ethereum is a security according to the SEC. That is what we have been doing with some of these primitives.

My argument is not that Web3 native social networks will become new hotbeds for Twitter influencers to find more unknowing prey for their hot new meme coins. Genuine creators can monetise their work and empower communities to tap into it. For instance, we routinely have readers translate our work to Mandarin or Vietnamese. I love it when people take our content and make their own derivatives of it.

People often ping me and ask permission to do so to avoid drama if someone calls them out on a translated piece. One way Web3 could solve for this simple conundrum is if a person could mint a NFT (on Mirror) for the pieces we write & then upload their on NFT as a derivative of our work to the same collection. (*Sidenote: For the moment, I have no plans of issuing more articles as NFTs, but I'll soon be compiling all the translated works I see on the website).*

Establishing relationships on-chain for creative work lends credibility to both the original article & the derivative, without stealing the limelight from either creators. Simple, but effective provenance. But what about the money?

I have been thinking about the commercial elements of being a creator. We have been testing a paywall for some of our archived pieces at Decentralised.co because Substack does not allow you to make content (free) subscriber-only. Naturally, we've had people paying for content in the past few weeks despite the paywall message that reads, 'Please don't pay.' (*No, seriously, don't pay just yet.*) I'll share more on what's planned at another point, but here's how the math works very crudely.

For a creator on TikTok to make $60K, they would need 100 million views every month consistently for a year if their only income source was ads. A newsletter charging $20/month to hit the same figure would need ~250 subscribers. Nas pointed out that the numbers may be slightly off, but the underlying point remains.

Free content often gets excellent distribution, but the monetisation mechanisms don't exist in a way that empowers creators that focus on smaller niches. We have seen Web3 offer an alternative through royalties in NFTs. The idea is that a creator can make an asset (like a painting) once, and every time the asset is traded, they get a portion of the royalties. I don't think that model scales, as most artists without distribution may be unable to use it.

Communities as Networked Economies

What would occur instead is that communities formed around a creator would pool resources to support that creator. In a Web3-native social network, artists would simultaneously distribute their content (gathering eyeballs) and have a subsection of power users 'collect' it as we do with articles on Mirror today. These power users, in turn, could gather and coordinate much like a DAO.

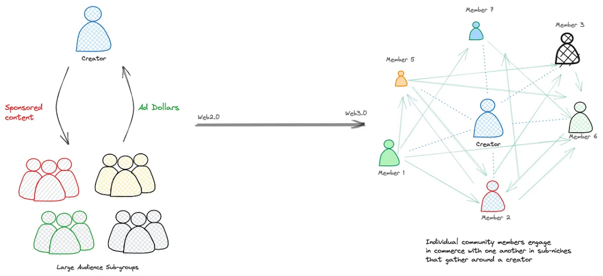
When a creator releases a new product, the subscribers who have collected works from the person could be the first to access it. These feedback loops of incentivising community members who proactively contribute would enable micro-communities for creators. This would be when a creator could benefit from the economic activities of people they have brought together. Creators, would be the founding fathers of new digital cooperatives.

I believe this is the future of the creator economy for a reason. Creators have expanded to businesses to add to their revenue stream. The most commonly cited celebrity brands are Ryan Reynold's involvement with Mint Mobile and Aviation Gin. But before that, Rihanna had Fenty Beauty, Jay Z had Rocawear, and MrBeast had his burgers. Historically, a creator's revenue stream was only their artwork. Modern-day creators expand on their brands to capture more value for themselves.

But a creator may not be the best person to expand into a new product line. For every celebrity with a billion-dollar acquisition, countless influencers have launched a brand and failed. Even having a shot at launching a brand requires one to reach a certain scale and size.

Protocols like Lens allow any third party to query the number of likes or retweets a post has received. An application could then be built that curates only members who have received a certain amount in on-chain engagement to reach out to one another. Naturally, the challenge with such a system is that it would incentivise individuals to spam for engagement. But with strong moderation, such a curated social graph could be compelling if applications are built on top of it.

I try to explain what the transition would look like in the image below. With due apologies to the readers from mobile devices - the model below shows how a web2.0 influencer would differ from a community curator in Web3.0. Blockchain-enabled payment rails would enable creators to enable member-to-member commercial interactions. The green lines on the left side indicate payments between members, and the blue dotted ones towards the creator indicate potential royalty payments.


Creator
Sponsored content
Ad Dollars
Large Audience Sub-groups
Web2.0
Web3.0
Member 7
Member 3
Member 5
Creator
Member 6
Member 1
Member 2
Individual community members engage in commerce with one another in sub-niches that gather around a creator

For instance, someone could build a version of the Producthunt and bootstrap community members from what we have at Decentralised.co. A third party could build an Angel List or a syndicate DAO – and query our community for the most engaged VCs and founders. Both of which are a possibility today.

This composability of social graphs is missing on today's internet. When we run ads, we pay Google or Meta (or this blog's authors) to mention a venture to a smaller audience subset. However, the human mind works because we have effectively blocked out advertisements from our periphery. The average person sees about 4,000 to 6,000 ads on a given day. We consume without paying active attention, and human attention has evolved to ignore advertisements because it is a cognitive load we did not ask for.

Composable social graphs can fix this by allowing people to buy a new product. For instance, if a new game is launching and they wish to tap into the Decentralised.co community, all that is needed is to list them on the Substack. Users can then choose if they wish to interact with their product. **This switch — from the platform determining what is best for a user to one where users can select products based on their preferences — is the fundamental promise of what a Web3 social network can offer.**

You can always argue that this seems far-fetched and unnecessary, but experimentation is the crux of what made DeFi and NFT so powerful. When centralised product managers run a platform like Instagram or Twitter, you have no say in how the product evolves. You could also argue users should not have a say in how a product evolves - but I think it is different when it comes to social networks. When users are the ones driving the growth of a platform, there needs to be a balance of power between shareholders and stakeholders.

Community-driven content networks have existed as long as the internet has. Wikipedia is a powerful example. What Web3 brings to that equation is the probability of financialisation and user ownership. Would the contributors of Wikipedia like to have a say in how the product evolves? I would think so.

Reaching large numbers of users (scale) has long been the primary incentive on the internet. As I wrote earlier, people write on Twitter instead of Mirror because the distribution is on the former. **However, if we change the incentives to ones where people are no longer the product, we can form the basis for a better internet — one that does not involve creating content to spur emotions.**

It may seem far-fetched to think of a social network involving payments, but Twitter already charges $10 for premium subscribers, and the internet has ample instances of a community going from free consumers to paid ones.

In India, most of my generation used to torrent content in the late 2000s because products like Netflix or Spotify were not around; even if they were, these platforms would not accept our debit cards. However, a shift has occurred over the past decade. As an increasing number of Indians came online, and the payments network within the country evolved, we had what could be considered an economy of scale. Paying for access to watch the latest movie or cricket matches became commonplace as paying the amount was easier than bothering with the illegal route. Convenience is the ultimate sales pitch if your consumer does not have to break the bank to make a decision.

Capitalising on content on the internet has been restricted to an elite few that have reached scale. Web3 native social networks allow creators to change the equation by offering new alternatives to monetise their social graphs.

Looking through this lens, we will soon have digital native nation-states. Balaji Srinivasan's work looks at the other end of this equation—a time when a digital commune can perform functions that a conventional state does. I argue that creators will be founders of micro-nations oriented towards niches before that transition occurs.

They will not collect taxes or issue identity verification documents like the government today, but they will be crucial in establishing and growing entirely new industries. This may seem far-fetched, but consider that Satoshi and Vitalik Buterin are the founding fathers of their digital economies. Their ownership of Bitcoin and ETH represents the value they generated in creating new financial paradigms.

Power to The User

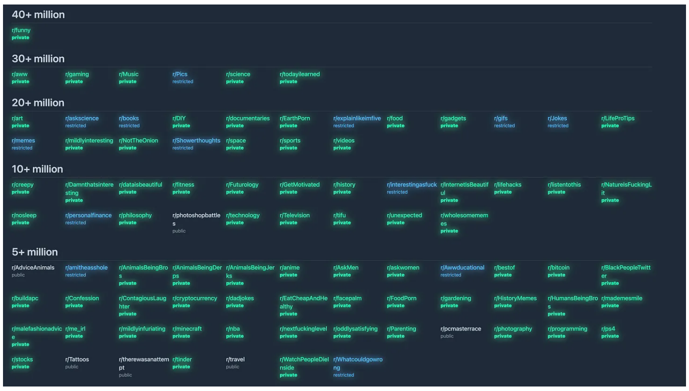
Erik Hoel is one of my favourite writers on Substack. In a recent post, he argued that a new social network's emergence is unlikely and not worth pursuing anymore. As we scale, we reach what he calls a '*Semantic Nadir*' – a tendency to take things in the worst possible way. *Did you post something about how much you like burgers? Someone on the internet will see this as a call to war against vegans.*

He believes that as human networks scale, our tendency to gossip or lash out at one another grows. The internet can curate the worst of what humans are capable of and present it to you overnight.

He is right in his argument so long as we presume that distribution (alone) is the key incentive for social networks. My argument is that incentives can be restructured altogether. However, before this occurs, there will be a period of transition. This will be when users can tweak the algorithms to suit their preferences.

In such a system, the social graph would not be user-owned, but the algorithms that determine what is shown to the user can be tweaked by the user. This may seem far-fetched, but platforms like JoinColumn* are already working towards this vision.

One place where the internet is already seeing the power of communities and users is Reddit. APIs that power external mobile apps on Reddit saw a substantial surge in pricing. The change will affect everyone from behemoths like OpenAI, which may be using data from the platform, to smaller mobile apps.



40+ million

r/funny private

30+ million

r/aww private
r/gaming private
r/Music private
r/Pics restricted
r/science private
r/todayilearned private

20+ million

r/art private
r/askscience restricted
r/books restricted
r/DIY private
r/documentaries private
r/EarthPorn private
r/explainlikeimfive restricted
r/food private
r/gadgets private
r/gifs restricted
r/Jokes restricted
r/LifeProTips private
r/memes restricted
r/mildlyinteresting private
r/NotTheOnion private
r/Showerthoughts restricted
r/space private
r/sports private
r/videos private

10+ million

r/creepy private
r/Damnthatsinteresting private
r/dataisbeautiful private
r/fitness private
r/Futurology private
r/GetMotivated private
r/history private
r/interestingasfuck restricted
r/InternetIsBeautiful private
r/lifehacks private
r/listentothis private
r/NatureIsFuckingLit private
r/nosleep private
r/personalfinance restricted
r/philosophy private
r/photoshopbattles public
r/technology private
r/Television private
r/tifu private
r/unexpected private
r/wholesomememes private

5+ million

r/AdviceAnimals public
r/amitheasshole restricted
r/AnimalsBeingBros private
r/AnimalsBeingDerps private
r/AnimalsBeingJerks private
r/anime private
r/AskMen private
r/askwomen private
r/Awwducational restricted
r/bestof private
r/bitcoin private
r/BlackPeopleTwitter private
r/buildapc private
r/Confession private
r/ContagiousLaughter private
r/cryptocurrency private
r/dadjokes private
r/EatCheapAndHealthy private
r/facepalm private
r/FoodPorn private
r/gardening private
r/HistoryMemes private
r/HumansBeingBros private
r/mademesmile private
r/malefashionadvice private
r/me_irl private
r/mildlyinfuriating private
r/minecraft private
r/nba private
r/nextfuckinglevel private
r/oddlysatisfying private
r/Parenting private
r/pcmasterrace public
r/photography private
r/programming private
r/ps4 private
r/stocks private
r/Tattoos public
r/therewasanattempt public
r/tinder private
r/travel public
r/WatchPeopleDieInside private
r/Whatcouldgowrong restricted

Data from Reddark. Numbers indicate size of the subreddit that has gone private in protest. 8400 of 8800 Subreddits are currently private in what is one of the largest protests in the digital realm.

The change in pricing made it impossible for interfaces to Reddit, such as Apollo, to keep functioning. Multiple large subreddits catering to tens of millions of users have begun going 'dark', which involves setting these pages to private so that users can no longer access the subreddit.

The protest may be somewhat weak unless users leave Reddit in droves. (*At the time of writing, some 8400 subreddits off a total of 8800 has gone private)*. But as platforms like Snapchat and companies like Meta have shown in the last decade, social networks have strong Lindy effects. The longer they have been around, the greater the odds that they will continue to exist. This outcome is because a user faces a high opportunity cost to delete their Facebook or Twitter accounts entirely.

They cannot access the same group of friends elsewhere without much friction. Portable social graphs – like the ones enabled by Lens – offer an alternative where a user can switch out of the platform but still hold on to their network of friends.

Consider it as if social graphs were nation-states and platforms were businesses. It is incredibly hard to switch out of a nation-state entirely, as anyone who has had to move to live elsewhere would know. But a platform with commercial interests should very much be treated as an entity that can be switched at will.

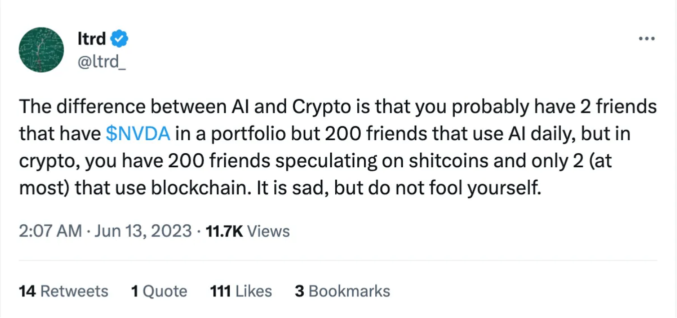
The internet does not give this option to users today. We see aspects of it with text-based applications like Signal and WhatsApp. You can choose to quit WhatsApp entirely and text the same friends on Signal, then realise that only a small fraction of your friend group even uses Signal.

Ultimately, creating a new internet with entirely new incentive structures requires rethinking how the past three decades of the internet have evolved. Presuming slapping token incentives or shiny new buttons would attract users is a bad heuristic. We need creators and their audience bases to rethink how and why we interact with one another on the web and to what extent bits of it can be monetised in ways that don't involve tapping into user data.

A model that protects privacy without distribution may not work. Similarly, one that reaches scale without retention will not work. We will have multiple iterations and narratives in the market as these transitions occur, but it is clear to me that there has never been a better time to attempt to create a truly Web3 native social network for the masses. Humans are creatures of habit. **Changing habits we picked up and perfected over 30 years of consuming free content and disbursing pointless ads will be a slow, uphill batter.**

One of the controversial stances Peter Thiel was infamous for in the early 2000s was his thoughts on how we were in an age of stagnation regarding tech. I'd think the same if I were a VC in that era. (*FWIW, I think the same now, because mentally I am a cynical old man*) In fact, Tascha from Twitter recently had a very similar stance — that crypto has not had anything novel or groundbreaking for quite a while, and until we deliver on it, the markets may not recover.

I echo those sentiments. But I also believe we are looking at the problem incorrectly. Crypto does not lack fund apps or trading products. It does not even have a UX challenge if you consider account abstraction. **It lacks a social graph that can help propagate these products in a way that keeps the consumer entertained and engaged. And that will not happen until we produce social products that provide more than shilling tokens.** We see large-scale, privately held graphs emerge. Layer3, for instance has over half a million users with credible, on-chain activity in their userbase. They are well-positioned to expand into a social network.



ltrd
@ltrd_

The difference between AI and Crypto is that you probably have 2 friends that have $NVDA in a portfolio but 200 friends that use AI daily, but in crypto, you have 200 friends speculating on shitcoins and only 2 (at most) that use blockchain. It is sad, but do not fool yourself.

2:07 AM · Jun 13, 2023 · 11.7K Views

14 Retweets 1 Quote 111 Likes 3 Bookmarks

As the user above pointed out on Twitter, the difference between AI and crypto is in how many people use the underlying technology. One way to inverse the relationship between token holders and product users is by looking at social products where a token is not required to interact with the product.

Much like it took well until the mid-2000s for large-scale, retail-oriented social networks to emerge in Web2, it may take a while to see social networks of scale in Web3. It is a function of time. We have tried, experimented and failed multiple times in the past with social products in the sector. But the difference is that in 2023 the technology to enable such a social product exists. And that gives me hope.

Joel John

Disclosures.

1. *I am a seed-stage investor in Join Column*
2. *Decentralised.co has been actively looking at the Lens ecosystem for investments and dispersed a grant for one venture.*
3. *Entities I am associated with are investors in Layer3*
4. *None of this is investment advice*

Telegram and Pitch Decks

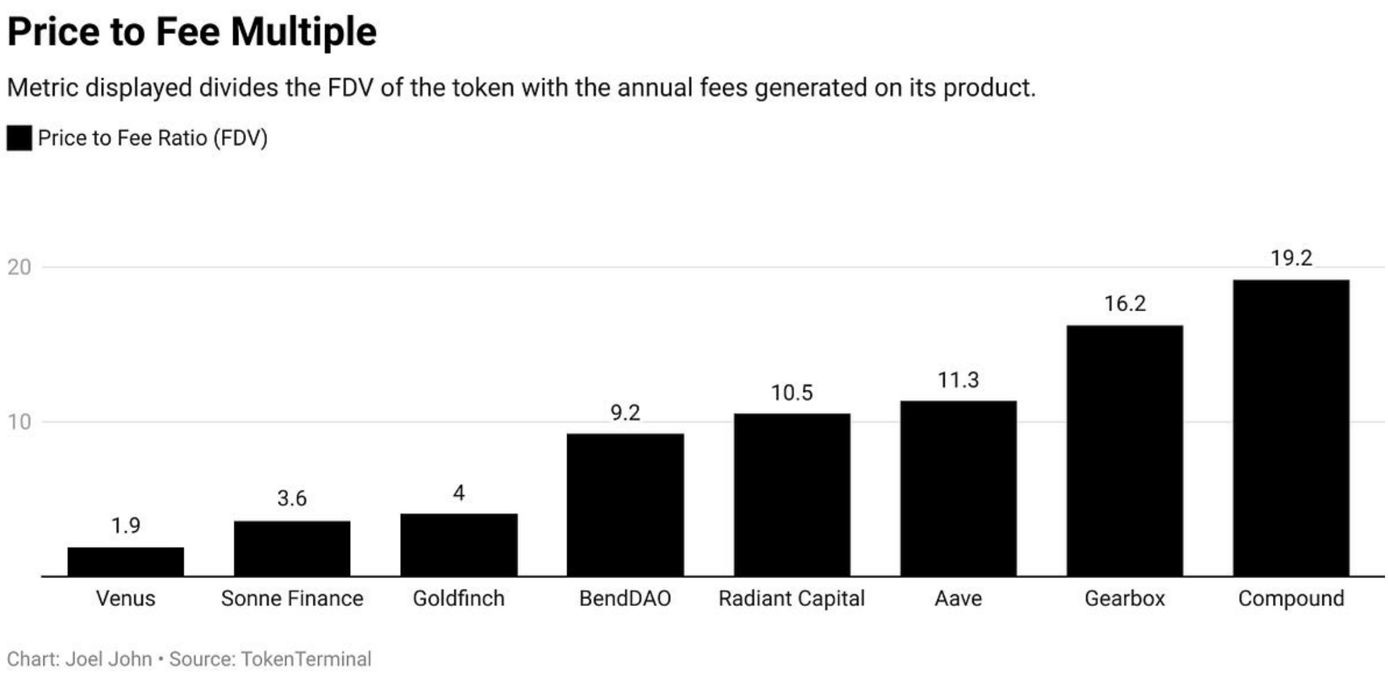
Join in with ±3000+ researchers, investors, founders & overall great human beings. We don't exactly talk much, but it would help you stay close to what we are focusing on & connect with others building cool things.

Fill out the form below if you are a founder building cool things and in the process of raising money or looking for feedback on what you are pursuing. We like the builders.

Joel John
decentralised.co

Value Accrual

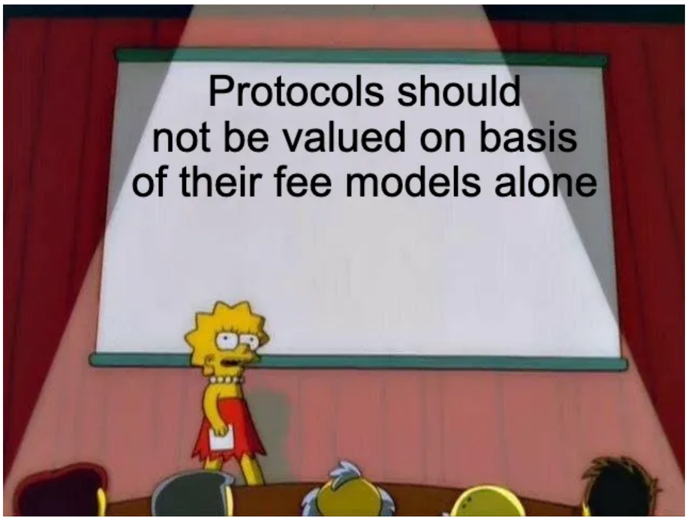
Should protocols make money?



Price to Fee Multiple

Metric displayed divides the FDV of the token with the annual fees generated on its product.

Chart: Joel John • Source: TokenTerminal



Protocols should not be valued on basis of their fee models alone

Hello!

Sid and I discussed the Fat Protocol Thesis a few months back. Much has been written about its validity. For those not in the know, the thesis argues that the value of a protocol will be higher than the combined value of all the applications on top of it. It is an excellent narrative to buy into when a new network is coming to market.

Joel Monegro wrote it in 2016 when ETH's price was a few dollars. There has been much debate around the thesis since then, but if I had to summarize, here's what happened. During bear markets, as value accrues to stable, less volatile assets, it is possible that applications atop a protocol become "worth" more than the protocol itself. A simple place to check this is the value of stablecoins held on top of certain L2s.

During bull markets, given that the underlying infrastructure (an L1 or L2) is an indexed bet on the applications built atop it, money flows towards investments in the infrastructure itself. It drives the underlying asset's price (like ETH or OP) and proves the thesis right.

We figured it was worth revisiting the thesis. Don't worry; we will not be arguing for or against it. A lot of intelligent people have done so over the years. I think it makes little sense to commit to that concept forever. It is called a thesis and not a law for a reason. Today's piece explores "value", how it is captured and why protocols may cancel out one another's growth. It is a bit long, but there are memes along the way.

We'll start with some basic definitions.

Protocols, Platforms & Applications

A protocol is a set of rules followed by participants within a system. For instance, a protocol in the military dictates how people should behave. Diplomats have a "protocol" for how they interact with one another. Think of protocols as a bundle of rules. In the context of machines, specifically computers, protocols have been defined as the rules that specify how data flows. RSS, for instance, is a protocol that defines how information about articles is updated in your client. SMTP defines how emails flow through to your inboxes. You get the gist. Protocols are bundles of rules that are context-specific.

On the other hand, platforms are operating systems, social networks (*like Meta*) or hardware (*ARM/NVIDIA*) that enables a group of protocols to run atop it. When you use Outlook (an application) on Windows, you use SMTP (the protocol) to get data to Windows (the platform). There are no Web3 native platforms that have scaled yet. Solana's mobile devices may have their operating system, which is fine-tweaked to the needs of the industry. Ronin has its app store that allows for the distribution of NFT-enabled games.

HTC's blockchain phone from 2019 came long before Solana's device. Source : The Verge

But when you think of the kind of scale Azure, Facebook, or iOS has, there are no platforms at scale in Web3. (*Quite possibly, because we don't need them yet*). There were multiple attempts to create hardware-enabled mobile devices by both Samsung and HTC in the 2019 cycle, but I assume that with the release of tools like Secure Enclave, the need for wallet hardware-enabled phone devices have declined.

What confused me was the concept of applications that can also be protocols. Take 0x, for instance. Is it a protocol or an application? Matcha is the application. And 0x is a protocol multiple DeFi products can tie into for liquidity. Similarly, OpenSea' has Seaport, their protocol for NFT marketplaces of all kinds to tap into shared liquidity. Do you get the gist?

Because protocols do not find multiple developers on their own in the early days, developers often release an application with it to bootstrap activity.

And there's a reason for this. If you are a standalone application, you stand to be disrupted. OpenSea lost the royalty wars meaningfully to Blur. **But if you are a protocol with multiple applications built atop it, the possibility of complete disruption reduces drastically.**

So if you zoom out a bit, the playbook in the past few years has been relatively straightforward.

- Release an application. Bootstrap liquidity by offering token incentives
- Grow to a point where you can now allow third-party applications to tap into your liquidity.
- Release a protocol which has a governance token.

Compound and Uniswap are both instances of this playbook. It just happens that the core products they released are so powerful that people don't think of the applications built atop the protocol. Products like DeFiSaver, InstaDApp, MetaMask and Zapper send liquidity to these products. But the bulk of user activity happens on the initially released product—the native website of the protocols.

In these instances, the team builds moats in two ways.

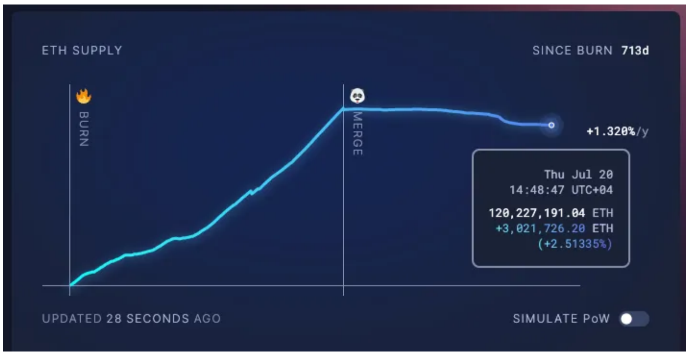
1. First, through distribution, they have by being the most reputed brand in the industry.
2. Secondly, the network effects emerging from multiple applications sending them liquidity.

In other words, applications can evolve into protocols (or platforms) in the digital asset space. As roll-ups make it easier for applications to pretend to be L2s, we will see an increasing number of apps claiming to be protocols for the bump up in valuations they stand to see.

Utility Enters The Chat

During the ICO boom, there was no clear definition of what tokens would be doing. There was a general understanding that they should not be doing things that may turn them into a security, and that's about it. People would tinker with dividends, buy-back and burn (*like Binance*) and governance rights that came with tokens. **The crux of the problem was tying economic value with something minted for no cost.**

Transactional networks like Bitcoin, Ethereum and Ripple can claim that a small amount of the asset is required for transactions. As the number of transactions rises, the base asset (*ETH, XRP*1*etc.*) would increase in value. This is a sound thesis if you have an exponential number of people trying to do transactions. It works because it costs the equivalent of a low-cost Android device to do a transaction on Ethereum if someone is busy minting kitties at the same time you are trying to get money across.



Ethereum has burned over 3.4 million ETH since the merge. OpenSea, Uniswap and Tether have been responsible for nearly half a million of those burned tokens. Chart. from Ultrasound.money

It was a helpful mental framing as many tokens were valued based on the revenue they created from transaction fees. For context, Ethereum's EIP 1559 burns a small portion of the token's supply on each transaction. Thereby, making it a deflationary network. This philosophy works exceptionally well when you are a base layer that derives value partly from the number of transactions you enable.

The challenge emerges when you are not a transactional network but an application. Requiring users to hold your native asset is a hindrance. Imagine if your bank required you to hold their stock each time you took a loan. Or if the server at McDonald's asked you how much of their stock you owned before giving you a burger.

Tying an actual use case with a base asset leads to horrendous outcomes if it becomes a requirement. Exchanges understand this exceptionally well. It is the reason why Binance or FTX (RIP) never required you to hold their tokens for an exchange. They only nudged you towards it with a discount for using their tokens.

Many of what we now refer to as governance tokens are utility tokens in hiding. That is, their utility stems from the idea that they can be used to govern the network itself. Now it is up for debate whether true decentralisation of governance ever occurred in DeFi - but the base assumption is that holding an asset helps voice opinion regarding how a product is run.

For many DeFi projects, it meant being able to change fee variables, assets supported and other random functions involving the treasury. In such instances, a token holder receives no revenue from the product. But the token they hold "governs" a treasury which may get income. So if a product creates a hundred million in fees (*for users*), the argument is that a multiple based on that is relevant when considering a fair valuation. Compound and Aave's multiples align with what we see with listed FinTech companies. Markets are driven by narratives in the short run but return to rationality over time.

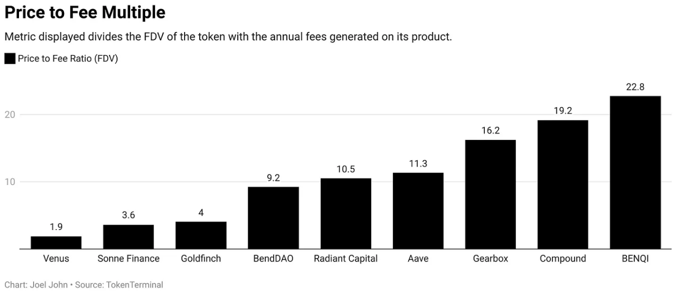


Chart: Joel John • Source: TokenTerminal

Markets are narrative machines that fuel up from time to time. When that happens, platform usage drives valuation less by the fees they generate, and more so by the narratives they can fuel. In simpler terms - **a thousand people noticing ten people are using a dApp can drive the valuation of a token higher than the fees generated from those ten users can.**

This is because, given **the liquid nature of digital assets, there are more capital allocators than users.** For a sense of scale, Compound has over 212k individuals holding their tokens in a wallet outside an exchange. In the last month, ~2k people used compound for a loan. **That 1% ratio, is still a healthy number by Web3 standards.**

Ashwath Damodaran refers to this syndrome as the big market delusion2. A paper written by him in 2019, explores how multiple VCs bet on a similar theme with the assumption that all of their bets will eventually become a winner. We are seeing this in AI these days.

Billions of dollars flow into multiple firms doing the same thing, assuming the market is large enough to sustain all of them. VCs pile on capital in hopes that the startup they have invested in will emerge winner, and have a large enough market share to justify higher valuations. Given the power laws we often see in ventures, many die. We see a variation of this with digital assets.

Individuals overcrowd into trading an asset on seeing a handful of users emerge. Often, the assumption is that utility will continue to rise and match up with where valuations are. Soon enough, a new product appears with a shiny token airdrop. Users flock elsewhere, and valuations tumble as the market reprices the lack of platform usage.

Sidenote: This paper from 2021 studied the ratio between speculative behaviour and platform usage for utility tokens. I won't dive into it in this article as the paper was relatively outdated at the time of writing.

dApps vs Protocols

Cumulative Fees Generated

Data shows the total fees generated (for users, network or platform) over the course of its lifetime

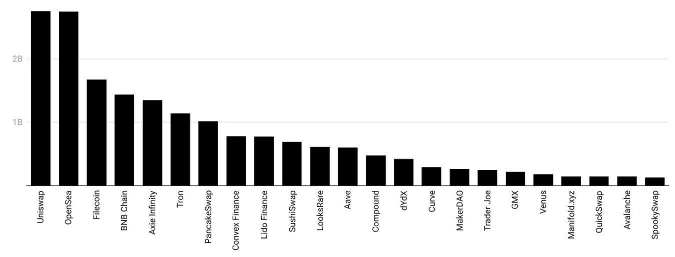


Chart: Joel John • Source: TokenTerminal

Now that we have established some baseline economics around how protocols and applications make money, it is worth looking at which of the two generates more in fees. The chart above excludes Bitcoin and ETH, given their early mover advantages. It also does not include Solana, in case you are wondering. You will notice that apps like Uniswap and OpenSea make considerably more in revenue than the average protocol. This may conflict with the idea that protocols should be valued more than applications, given how value flows downwards (*to the infrastructure enabling it*).

This is where blindly citing fat protocol thesis as a basis for backing new L2s becomes faulty. Mature applications on Ethereum can generate more fees than entire protocols of relatively younger age.

There's a reason for this. dApps tend to make money by capturing a small percentage of the transactions on them. Your fees are proportional to the amount of capital flowing through the product and your take rate. Uniswap and OpenSea have made nearly $2.8 billion because they have a high monetary velocity (*frequency at which assets change hands*) and an enforceable take rate that passes on value to users.

In the case of protocols, enforcing higher take rates as usage increases breaks network effects unless the use case justifies it. Let me explain. It is acceptable to pay the equivalent of a week's income in emerging markets for a transfer on Bitcoin if your life depended on it. Assuming users will be OK with that to play your Web3 game is faulty thinking. Bitcoin's promise of immutability and decentralisation is a feature people would pay a hefty premium for.

The fee rate on Bitcoin is justified by

- The lindy effect of the network
- Its decentralisation and immutability.

But when you introduce something like a stablecoin issued by a centralised source, markets will be repricing what they are willing to pay on protocols. This is why Tron is a hub for stablecoin activity. Here's one way to quantify it. The average USDC transfer on Ethereum last week was close to $60k. For those on Arbitrum, it was down to $9k. And on Polygon, $1.5k. One can debate using "average" as a metric here, but the assumption goes that transactions worth under $100 become possible as fees trend lower. The point I am trying to drive is

- We presume protocols become more valuable as transaction count increases, and costs of transacting increase.
- But the high costs tend to break the network effects of users concentrating on a single network and drive them elsewhere over time.

This is why dApps in emergent chains never see critical velocity to create sufficient fees. When you launch a DeFi product on Ethereum today, you are tapping into the network effects of users that have made their wealth from ETH, ICO boom, NFT boom and DeFi boom alongside the robust infrastructure that allows people to trade, lend and borrow. When you build on the hot new L2, you hope users bridge their assets and use your product. It is like building a business in a new nation-state. Sure, you have less competition, but there are also fewer users.

It's like running the only Starbucks on Mars.
Fun? Possibly.
Profitable? Likely not.

Community as a Moat

We have been thinking extensively about what is a moat in Web3. Because, unlike other industries, most applications in crypto are known for two things.

1. Open-source: you are enabling anyone to replicate what you have built

2. Capital flight: you are allowing the users to leave with their money as soon as they please

Inspite of both these characteristics, Uniswap, Aave and Compound have maintained relative dominance in what they do over the years. Multiple DeFi products have forked Compound and failed miserably in the process. What is the moat for these products?

(Sidenote: Uniswap has begun using licenses that are restrictive in the past few months)

The simplest measure of a moat in the industry is liquidity. If you are a capital-intensive product, liquidity is the amount of money available to facilitate transactions on the product. If you are a consumer application, like a game, it is measured in attention. In both cases, what drives either liquidity of capital or engagement, is a community.

The only real moat in Web3 is a community. And what keeps early community participants retained are capital incentives or product utility.

Exponentially better user experiences like ChatGPT do not require incentives for users to flock to it. Blockchain-enabled applications occasionally produce similar magic. DeFi crossed this chasm in the golden age of AMMs and permissionless lending, coming alive in June 2020. An era, we fondly remember as "DeFi Summer".

A large user base looking to make a quick buck through an airdrop may look like a community. But it is not. It is a "cost" on the network in the long run because the buy-side for the token would have to give them sufficient liquidity if you want to maintain prices. For instance, yesterday, it was revealed that 93% of the tokens held in wallets for Arkham Intelligence moved their token right away. Are the members who sold - community members or a cost on the network?

They can be community members if they strategically buy back in. But as long as they don't need the tokens to use the platform, they have no incentive to buy back in. They can allocate that money to hundreds of other tokens. DeFi products like Compound and Uniswap have a community not just in the form of token holders but also in the thousands of individuals that have kept billions of dollars in their product's liquidity pools.

One can fork their code base, but you cannot replicate the liquidity pool, on a long-enough basis, without building a community with conviction. Capital incentives help retain communities in the long run.

Capital incentives can be tokens given in exchange for performing a function on the network. Those providing storage on Filecoin for instance, receive tokens for their contribution. Being early to networks is another way capital incentives accrue to users. Bitcoin and Ethereum are similar in this regard because their early adopters made abundant wealth by being early and having the patience to hold.

Crypto events are culture-building services with a mix of parties on the side.

The need for capital allocation from users is transcended through shared culture. Bored Apes and the myriad of GMs or WAGMI statements we used to see on Twitter in the last bull run is an instance of this. Culture helps individuals align their identity, and retains individuals longer. There is no quantifiable way to measure culture, but the excitement one sees around EthCC or Solana's Hackerhouses is an instance of this. It gives individuals a mechanism to build, relate and ideate without putting up capital to be a part of the conversation.

Protocols don't run on vibes alone. You need people to build on them. Developers are how culture and capital combine to help develop tools that retain users in the long run. If you think of a protocol as a nation-state, developers build utility that retains users (*citizens?*) on the networks for the long run. Protocols can charge fees, much like highways can charge tolls. **But if they become prohibitively expensive, they will drive users elsewhere**. Looking through this lens, it becomes evident that protocols may not be designed to be making money at all in the first place if the use case is consumer related.

Moats in web3 emerge from users sticking to a network long enough to help facilitate economic transactions in the applications built on top of it. Every network has the same group of dApps replicated with the same code but different branding and sells the idea of "lower transaction fees" alone as a USP. We will soon have fragmented ecosystems with divided user attention. Indeed, capital will flow to it in the short run through exchanges, as users trade, but they will soon be dead towns like EOS.

In the real world, you cannot replicate a nation-state. No mechanism exists to expand the land area within national borders (*without violence or economic alignment*). This is why people are forced to concentrate in hubs, which have historically been ports. London, Mumbai, and Hong Kong - are all similar in this regard. This concentration of people helped drive network effects within the city. Rents surged, but it meant faster groceries and better services.

In the digital realm, users were forced to concentrate in an ecosystem due to a mix of how intellectual property rights work and expanding product suites. Google's launch of their search engine, Gmail (2004), Android (2005), Youtube (2006) have each facilitated our stickiness to that ecosystem. A user signing up for GMail inevitably enters the rest of Alphabet's product suite. Apple and Meta have similar strategies that concentrate users within their ecosystem.

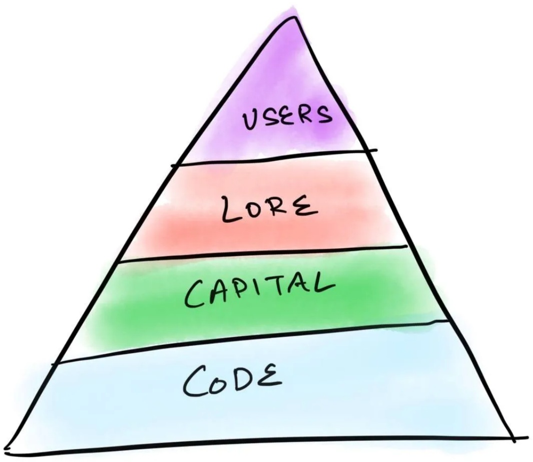
Apple takes it to the extreme by owning the whole stack, from hardware to payments. **Concentrating user bases allows the facilitation of economies of**

scale. There's a reason why I mentioned this - and it boils down to developers.

If I drew a hierarchy of needs for early-stage protocols and dApps, it would look like the image below. You need developers to

- Form the code,
- Based on which capital can be invested into
- To develop a lore
- That attracts users.

Without the code, we are simply running in circles.



This was custom art, hand-drawn by me.

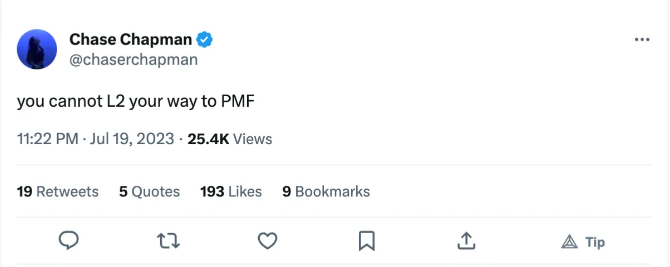
VCs that have been around since the early 2000s emphasise a lot on developers. It is because developer count is a distilled measure of the economic activities that may occur on a protocol. Say you purchased an iPhone for the camera. There's a high chance you end up paying for an app that helps you edit images on the device.

So your initial decision (*the camera*) fuels a secondary purchase (*the app*). With each new app, the ecosystem grows stronger as the suite of products a user can use expands. **The value proposition for buying the device is no longer the camera. It is the entire ecosystem that opens up to the user.**

A variation of this was also evident during the early days of the web. People were not taking subscriptions to the "internet". In their minds, they were getting a subscription to AOL - a group of landing pages summarising what is happening on the internet. But the open internet grew only when people realised they could send e-mails, send cringe texts to their crush from school and get bullied in games from the same network.

Now imagine if 20 different internets were competing, each with their listed equities and their variations of applications with entirely different branding and transaction fees. Consumers would be baffled, and the internet would not be what it is today. That is where we are at with Web3 native protocols.

Value Capture Another Day


Chase Chapman @chaserchapman

you cannot L2 your way to PMF

11:22 PM · Jul 19, 2023 · **25.4K** Views

19 Retweets **5** Quotes **193** Likes **9** Bookmarks

The original tweet is linked here.

Protocols need significant user liquidity to support emergent applications on top of them. Everyone is incentivised to pretend to be the next L2 in the age of roll-ups. But with each new protocol, we fragment the number of users web3 native products can have. There may come a period where users don't know the chain or stack behind their tools. But we are not there yet.

In the interim, wanting every protocol to capture as much fees as well-established dApps may be faulty. The first generation of blockchain dApps was capital-intensive. The next generation may be attention intensive. There are no Web3 games of scale, because we value transactions over great games. The same could be argued for on-chain media too. Blockchains are financial infrastructure by nature. So it is only fair to presume every user would want to transact.

But that mode of thinking is partly what's held the industry back.

All of this made me wonder what even is "value". Tokens, like equities, in-game items and any other liquid asset, will always have a premium. Depending on the crowd's hopes or fears, that premium may sway higher or lower. Speculation - has been a driver of financial markets for atleast eight centuries. And I doubt we will change this aspect of human behaviour soon.

For founders, the message is quite clear. There are two ways you can make money. One is through driving the narrative, even when there is a lack of protocol fees or usage. Meme tokens are a version of this, taken to the extreme. The other is building a dApp that generates fees and commands a reasonable multiple. Aave and Compound have matured to reach that arc. Both, require an incredible amount of work.

The best founders we have seen can drive both narratives and platform usage. Having only one is generally a recipe for disaster. Protocols or applications that offer an unrivalled core utility can have higher take rates due to their stickiness. This is where Peter Thiel's view of "*competition is for losers*" come to play. **The more crowded a market segment gets, the lower the probability of a new entrant being able to command higher take rates or sticky users.** All of this looks at user concentration alone. What about protocol economics?

Joe Eagan from Anagram had a good analogy here. The best protocols have an incentive to behave a lot like Amazon. The marketplace made little to no money in net income for the longest time, but the inherent network effects paid off in the long run. The broadest range of sellers meets the largest group of buyers on Amazon. Any protocol that "*succeeds*" in the long run may have a similar attribute. Exceedingly low fees with the broadest range of applications built on top of it so that users don't have to bridge elsewhere to complete their day-to-day functions. The monetisation could occur through the richness of the data such a protocol would leave on the blockchain. (*That last bit can be debated quite a bit*).

One way this could play out is with a protocol launching without a token. Instead of charging fees for a new native asset, it could charge in dollars. Imagine paying $0.0001 for a transaction, in USDC. Users "reload" their wallets with a dollar after every 10k transactions from a local store. The caveat is that most base chains cannot do this, as their native tokens are needed in their security model, and we don't quite know how such a protocol would make money. Such a protocol could scale exponentially, without users having to fork over large sums of money each time protocol usage surges like you have with Ethereum today.

If we believe that blockchains are infrastructure for transactions, and all of the actions on the internet will become transactions, we may inevitably need low-cost protocols with fixed costs. Or, we may end up with 50 new L2s, each of which sees sky-high valuations, because markets like a shiny new thing. Markets can facilitate both. And that is perhaps the beauty of it. There is room for both utility and speculation.

I'll see you guys next week with some work we are doing on algorithms and identity in the context of Web3 social networks.

Stay safe,
Joel

Telegram, Pitch Decks & Referrals.

Join in with close to 5000 researchers, investors, founders & overall great human beings. We don't exactly talk much, but it would help you stay close to what we are focusing on & connect with others building cool things.

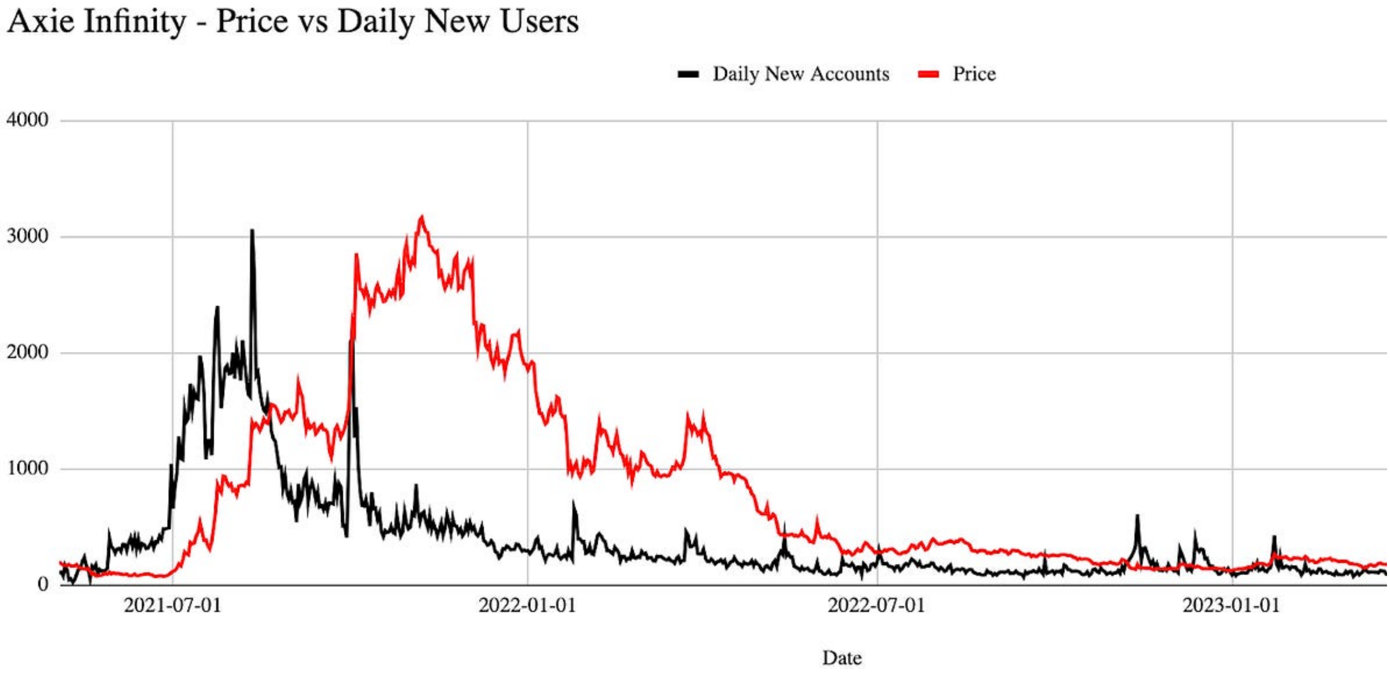
Fill out the form below if you are a founder building cool things and in the process of raising money or looking for feedback on what you are pursuing. We like the builders.

Enjoyed reading this? Consider sharing with a friend for access to premium newsletters we enjoy reading and good karma.

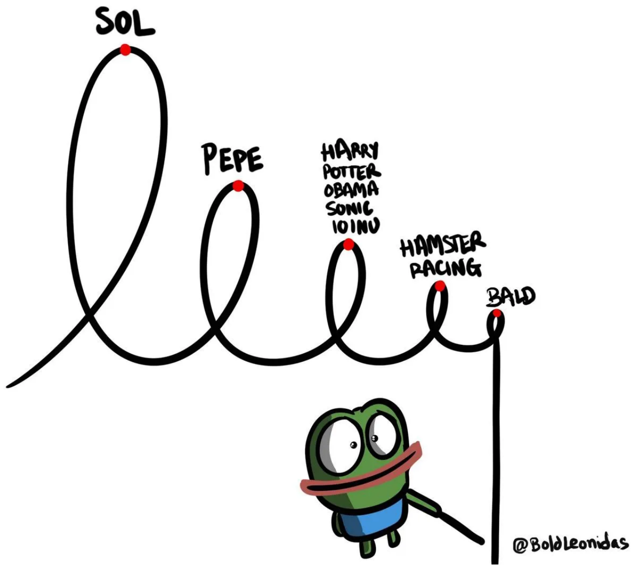
Joel John
decentralised.co

The Narrative Wedge

A field guide to profit and survival.



Hey there!



Art by @boldeonidas on Twitter. Follow him here.

In our previous piece, we explored how value accrues to protocols. A considerable part of "value" is narratives. In today's piece, we explore how narratives evolve, their impact on founder's strategies and blind spots in venture investing.

TL:DR for those in a hurry

1. Token prices often influence venture investing in crypto
2. Narratives driving prices have short shelf lives.
   Ventures take much longer to scale
3. Themes picked by founders and investors based on narrative windfalls can be terrible as attention flows elsewhere by the time products go live.
4. Crypto's original sin is in charging users. Tools like account abstraction may reduce the cost for founding teams to onboard and retain users longer.
5. Strong narratives do not compensate for bad products. Botted metrics do not compensate for the lack of community.

Here's an observation I had over the last week. You could have deployed money into Axie Infinity[1] at the start of the gaming rally, walked away - and returned to more money than most venture investors in Web3 gaming would make. At the bottom, Axie was trading at $0.14. Currently, it is at $6. A 40x return.

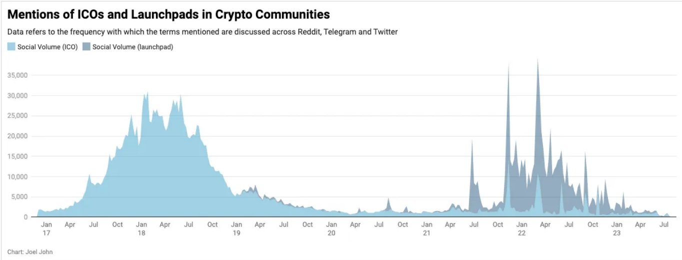
It peaked at a little over a 1000x multiple. The reason is that most seed-stage ventures in Web3 gaming are either not close to liquidity or will likely die before they can raise more capital in the current market environment. I'll explain this further with a chart in a bit.

But there were flaws in my thinking.

1. Seed stage ventures are not supposed to give returns within 18-24 month timeframes.
2. I presumed an investor would have allocated money to Axie Infinity when gaming was an obscure theme nobody cared about.

But the underlying theme remains that you could have deployed money into a liquid asset during the bear market and seen better returns than investing in early-stage venture deals within the theme. This whole conundrum made me think a bit about the risk spectrum within crypto, how attention precedes capital & the blind gaps within venture investing as an industry. This piece summarises my thoughts on how narratives drive money and focus within our industry.

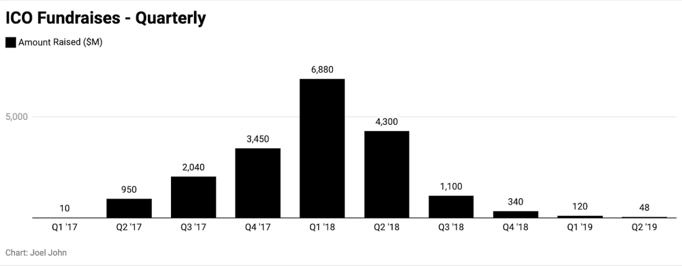
Some numbers before we begin. Close to 1300 of 3500+ tokens being tracked by a data product I use had less than 10 wallets moving their tokens in the last month. Of the 14,000 dApps being tracked by DappRadar, less than 150 had 1k users when I wrote this. As an industry, our attention shifts from one asset to the next in no time. A version of this occurs with our conviction in fundraising mechanisms too. The data below shows mentions of ICOs and launchpads in prominent crypto-native communities over the last few years.



ICOs captured retail attention but eventually gave way to “launchpads” by exchanges—one instance of a narrative evolution in real-time.

If you were around in 2017, you would have thought venture capital is about to change forever. Many startups that raised money in that market are no longer around. Based on your source for the data, crypto raised between $19 billion and $60 billion from retail and institutional participants that year. But the mortality rates of ventures from that cohort of ICOs were on par with what we traditionally saw with ventures.

You can see the result between Jan of 2019 and January 2021—a golden age for venture capital in crypto in the chart above. Interest in ICOs vanished rapidly. Investors saw an opportunity in a brief period where starry-eyed founders no longer had access to retail capital for building. Valuations were at $5 to $10 million for startups. Founders and investors had to return to working together to survive.



Part of what drove founders to switch to raising from VCs was a better understanding of the risks of launching tokens too early. You had to spend time managing the community, doing legal work to stay compliant & tie your net worth to a liquid asset - all while building a company. Founders could wake up 20% poorer because somebody on Discord got annoyed at a comment made by someone on the team and decided to dump all their tokens on an exchange with $10k in liquidity.

Years later, we are back in launchpad season—when exchanges play gods and determine which venture gets millions of dollars from retail participants. While there is much gatekeeping this time, at the very least, they ensure retail has better terms of investing than the billion-dollar valuations we saw in 2017 ICOs.

I took the case of how ICOs gave way to launchpads because there was data on this. Enough years have passed since the ICO boom to understand what happened in hindsight. If you take more nascent themes like DeFi, NFTs or Web3 gaming, you'd see the absolute obliteration of public interest in discussing them.

Unlike ICOs, the story for DeFi, Web3 gaming and NFTs is still evolving.

Dying Narratives

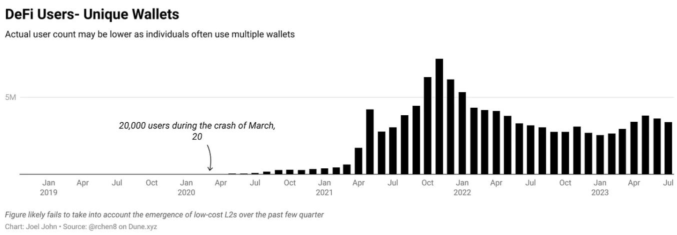
DeFi has gone from a peak of inflated expectations to a slope of enlightenment. There are no new competitors for Uniswap emerging every day. Aave and Compound strongly capture the lending market (for spot, over-collateralised assets). The successive iterations of these products will either be more consumer-facing or institution focused and less obsessed with speculation as a use case.

Robert Leshner's transition of focus to launching a mutual fund (*CeDeFi*?) and Stani's transition to

Lens (*Web3 social*) show how founders that have been around are positioning for the next run.

Google search trends, TVL and user counts are good places to see how attention and capital flow through DeFi. Money on DeFi platforms has dwindled from a high of $160 billion to a low of $40 billion as of writing this.

If you look at the user count data, there's a 50% reduction over the past few months. But it is still up 100 times from March 2020, when the start of DeFi summer was just about to take off.



DeFi Users- Unique Wallets

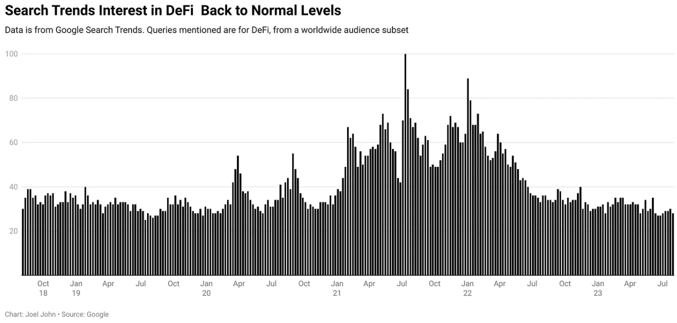
Actual user count may be lower as individuals often use multiple wallets

Figure likely fails to take into account the emergence of low-cost L2s over the past few quarter

Chart: Joel John • Source: @rchen8 on Dune.xyz

In other words, **while there is a reduction in interest and usage, a far higher number of users are retained within these product categories**. However, if you were to look at search trends for the same function, you would witness a very different story.

Interest has gone back to 2018, bear market levels. It is as though nobody cares about the sector anymore. I checked the data for NFTs and ChatGPT - both on similar arcs. Search trends for aliens are on the rise. (*We may need to start investing in alien servicing businesses. Do lmk if you are building anything along those lines*)



Search Trends Interest in DeFi Back to Normal Levels

Data is from Google Search Trends. Queries mentioned are for DeFi, from a worldwide audience subset

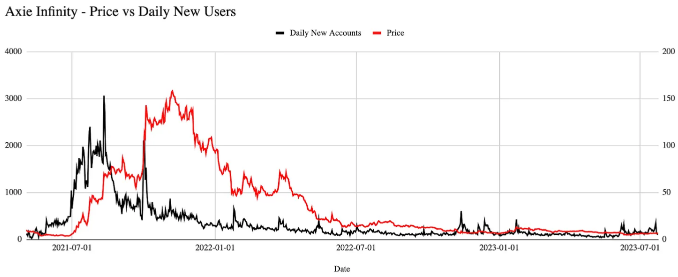
Chart: Joel John • Source: Google

Putting these numbers for DeFi together, I had a few observations to make.

- Narratives pick up steam at the beginning of a bull market.
- These tailwinds usually occur due to technological developments.
- Early entrants in specific sectors produce outsized returns as a function of narratives and usage scaling simultaneously.
- Compound, UniSwap and Bored Apes are each an instance of narrative tailwinds blending with product usage to produce outsized returns for investors.

The challenge is investing in a theme in the middle of a narrative tailwind that may die before it sees enough velocity to attract an enormous enough trove of users. We may need to return to Axie Infinity again to understand what I mean.

Timing Bets Right



Axie Infinity - Price vs Daily New Users

I go back to Axie because it captures several themes quite well

1. It was a listed asset with ~2 years of product development by 2021
2. You could argue it was undervalued at the time.
3. Axie marked the beginning of Web3 gaming as a theme (*and possibly, its decline too*)

If you notice the chart above, there was a huge influx of users to Axie well before its massive rally to $150. On-chain sleuths likely saw the extent to which new users were flocking to the product and priced it well through July 2021.

But by October, when the new user count had begun diminishing, Axie became less of a product and more of an asset. It is a trap all on-chain products are vulnerable to. Hyper-financialisation of in-game assets meant a hedge fund in NY could be paying for someone hustling it out in a game through a guild. The play-to-earn model depended on inbound liquidity for in-game assets. And sometimes, this liquidity came from speculators & institutions.

Venture-style investing in the theme has a six-month lag between July 2021 and January 2022. Many investors watched on the sidelines, forming convictions and writing theses about how the industry would evolve. The same would have occurred with founders realising the difficulty in building DeFi dApps and believing gaming is the next big thing to jump into. Much like many founders today are hopping on to AI.

The real risk is in the 18 months that come after Jan 2022. Do you see how that figure for new users flatlines in the chart above? That's the shrinking of userbases for all Web3 native gaming applications. Tools built at the periphery, like "*Steam for Web3 games*" or "*Reputation for Web3 games*", soon struggled to find users.

This misinterpretation of a short-term price rally for actual consumer demand is a trap multiple founders we see fall into. The risk for the subset of founders is that without traction, it becomes tough to do a follow-on raise in the current market environment.

It is quite possible that the founder was building in the right market at the wrong time. The peril for founders is shutting shop before sufficient attention or capital flows into the category.

As a venture investor, on one end, you would have seen how liquid markets heavily rewarded traders, and on the other, you'd be battling it out with a crew of founders that had hopped on the theme with you. It is not a pleasant experience for anyone involved.

My point is -

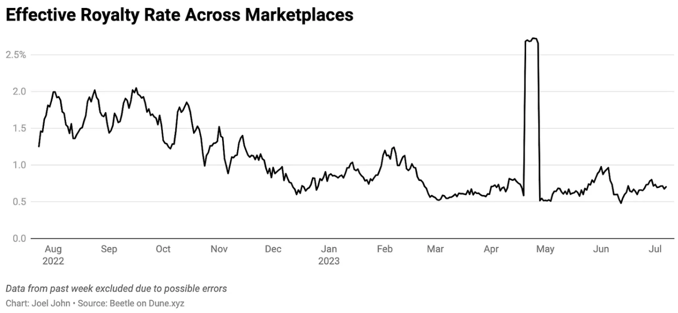
1. Markets often price in narratives in the short run.
2. Given the liquid nature of Web3 investing, liquid assets may provide exits within a quarter.
3. Given the illiquid nature of venture investing, ventures may not have a market to tap into when their product goes live because products take time to evolve.
4. Which often inevitably means a slow death and a gamble on the return of users. Products effectively become a bet on "*the return of a bull market.*"

The exception is when a category scales to have sufficient interested users, and you build something unique. Somewhat ironically, DeFi has crossed the chasm. At 3 million users, founders building in DeFi no longer have to worry about new users entering the market.

They can build for the crowd that is here today and now and have sufficient interest from users as long as they are not producing the 30th iteration of a copycat product.

Crypto-native investors making venture-style bets are either tastemakers or front runners. Either they

have the distribution and influence to birth a new category. Or the foresight to understand there is a whole new sector emerging. If one is to go by price action alone as a driver for emerging theses, the odds are pretty high that they are entering a market very late. It is quite possible that they do not see a meaningful exit unless it is a business that can scale to an IPO or be acquired. Both of which are rare occurrences in token-land.



Follow Beetle on Twitter here.

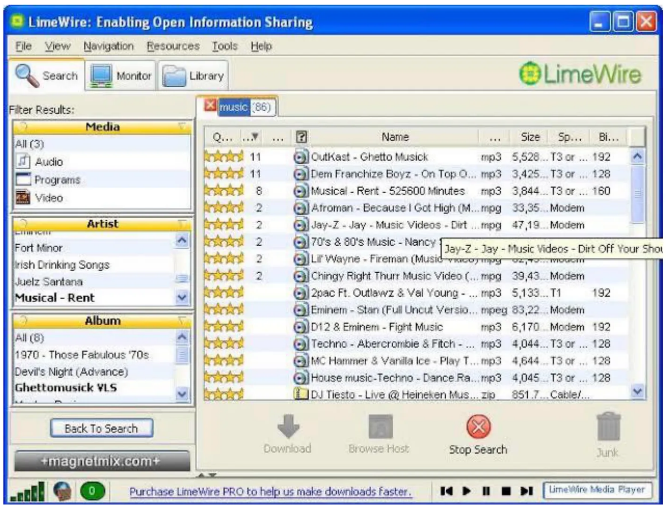
A different way this affects founders is when business models evolve. NFTs, for instance, have gone from an effective royalty rate of ~2.5% to 0.6% in the last year, thanks to the arrival of royalty-free marketplaces like Blur. As of writing this, some 90% of NFTs traded collect no royalties.

In essence, it translates to the complete obliteration of any venture built on the idea that large troves of traditional artists would be coming to the industry, and they, in turn, would need tooling to handle revenue. Countless creator economy ventures had to pivot in the last year as the model shifted.

As with all emergent technologies - chaos, is a way of life in crypto.

Freedom

Let's take a step back and go to the late 2000s. After a long day at school, you hop on Facebook to talk to your friends. YouTube has countless funny videos. Google sends you down rabbit holes about secret, clandestine banking groups. Dispersed across these activities are ads, but you rarely ever pay a penny for any of these things. The internet formed habits before it expected you to pay up.



Q...	...▼	...	?	Name	...	Size	Sp...	Bi...
★★★★	11			OutKast - Ghetto Musick	mp3	5,528...	T3 or ...	192
★★★★	11			Dem Franchize Boyz - On Top O...	mp3	3,425...	T3 or ...	128
★★★★	8			Musical - Rent - 525600 Minutes	mp3	3,844...	T3 or ...	160
★★★★	2			Afroman - Because I Got High (M...	mpg	33,35...	Modem	
★★★★	2			Jay-Z - Jay - Music Videos - Dirt ...	mpg	47,19...	Modem	
★★★★	2			70's & 80's Music - Nancy				
★★★★	2			Lil' Wayne - Fireman (Music	mpg	[illegible]	Modem	
★★★★	2			Chingy Right Thurr Music Video (...	mpg	39,43...	Modem	
★★★★				2pac Ft. Outlawz & Val Young - ...	mp3	5,133...	T1	192
★★★★				Eminem - Stan (Full Uncut Versio...	mpeg	83,22...	Modem	
★★★★				D12 & Eminem - Fight Music	mp3	6,170...	Modem	192
★★★★				Techno - Abercrombie & Fitch - ...	mp3	4,044...	T3 or ...	128
★★★★				MC Hammer & Vanilla Ice - Play T...	mp3	4,644...	T3 or ...	128
★★★★				House music-Techno - Dance Ra...	mp3	4,045...	T3 or ...	128
★★★★				DJ Tiesto - Live @ Heineken Mus...	zip	851.7...	Cable/...	

Jay-Z - Jay - Music Videos - Dirt Off Your Shou

LimeWire opened our eyes to free music.. and malware.

In comparison, Web3's obsession with ownership and exclusivity has driven us to create small pools of users interacting in echo chambers. According to their blog, Arkham Intelligence has over 100k users. Nansen's V2 product crossed 500k registrations today. Dune has one of the largest communities of data scientists in the industry. There's only one thing common between them: a free tier.

The web's genius was making the user not bear the cost of most of our actions. What it received, in turn, was distribution. Web3's great peril is in how much it costs for each interaction. Spending $8 to acquire images on a blockchain doesn't appeal much to users that don't need a community online. Why bother with your $10,000 ape when you have friends on Reddit?

The value proposition of spending $50 to purchase an ENS may not be apparent to users that have owned e-mail addresses for decades, for free. Axie Infinity initially required $1200 to buy NFTs to play the game. The guild model depended on this high barrier to entry. Last year, they released a free-to-play version realising the perils of keeping a high wall to entry.

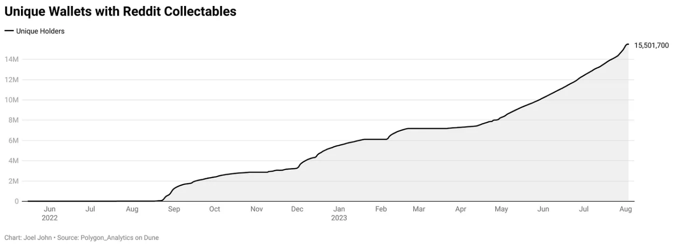
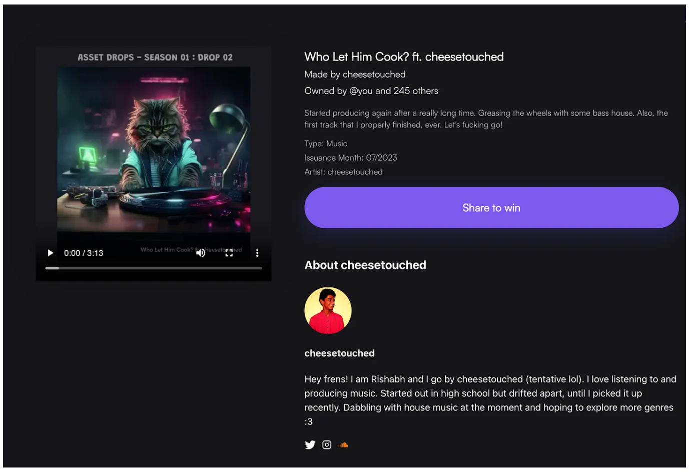

Unique Wallets with Reddit Collectables

Chart: Joel John • Source: Polygon_Analytics on Dune

One place this combination of “Free” and “own” happens quite elegantly today is on Reddit. At 400 million MAUs, the social network is a behemoth. Some 15 million wallets have collected their collectables so far. That is roughly twice the size of DeFi users during its peak month. Accounts with specific ages and characteristics were allowed to buy collectables from Reddit.

In this instance, most users are still on the “free” product, and a small subsection is minting, trading and owning collectables. Distribution is solved through a website that has been live for over 18 years.

A new class of applications has been seeing large users come in through compiling opportunities. Rabbithole and Layer3 fit that mould quite well. Instead of charging users, they give away value to those curious enough to explore new opportunities on-chain. According to tweets from the founder of Layer3, the product has enabled some 15 million on-chain actions for the crypto-curious.


ASSET DROPS – SEASON 01 : DROP 02
0:00 / 3:13
Who Let Him Cook? ft. cheesetouched
Share to win

Who Let Him Cook? ft. cheesetouched

Made by cheesetouched

Owned by @you and 245 others

Started producing again after a really long time. Greasing the wheels with some bass house. Also, the first track that I properly finished, ever. Let's fucking go!

Type: Music

Issuance Month: 07/2023

Artist: cheesetouched

About cheesetouched

cheesetouched

Hey frens! I am Rishabh and I go by cheesetouched (tentative lol). I love listening to and producing music. Started out in high school but drifted apart, until I picked it up recently. Dabbling with house music at the moment and hoping to explore more genres :3

Asset.money lets you collect an NFT in under 10 seconds

This shift in product strategy is already happening. If you visit Beam.eco - you’d see a wallet that sets itself up in less than 10 seconds. Asset.money helps you collect NFTs with less than three clicks. The user does not have to worry about gas costs, on-ramps or setting up wallets. Naturally, there are security trade-offs at play here. They are similar to how e-mail went from everybody running their servers to being hosted on third-party servers run by players like Hotmail and Google.

The Countertrade

Remember the bit where I said venture in crypto cannot be timed on narratives alone? The only way you escape, that trap is by the oldest trick in the book

1. Attract a user base and retain it long enough

2. Accrue value steadily over a long time frame

Some tokens in the industry have managed to do precisely that. Uniswap comes to mind in DeFi. OpenSea has maintained relevance inspite the attack on royalties over the year. The tail end of venture land is a large bet on how and when attention and capital would flow.

The only way to escape an unhealthy reliance on investor or speculator capital is with the purest form of capital all businesses can access. Their customers' attention. As VC funding contracts, more startups (and protocols) would have to return to finding users that care.

The most relevant example I have found of this is Manifold.xyz. The product focuses on enabling creators to mint NFTs with relative ease. Last month, they clocked over $1 million in fees, according to data from TokenTerminal. Glamorous? Possibly not. Relevant in the current market? Absolutely.

What I have found common among many players that do well over market cycles is their early mover advantage. It is a repeated story.

Small teams enter an industry during periods of peak narrative. They see the market drying up slowly. Less than five players are often willing to continue building as competition leaves. When attention and capital do return, they are the ones that are best positioned to scale. Looking through these lens, the themes that large investors are writing off are the ones to be involved with so long as you can survive.

Often, founders get shaken out by a shift in status before a lack of runway takes them down. A while back, it used to be "cool" to be in Web3. It is likely to cringe to mention your work in the industry now. Teams feel the need to cook up their statistics to feel relevant. Too often, we see founders making tall claims through airdrop-fueled bot activity on their products.

For a seasoned investor, these games are often quite evident and send the wrong signals about the team. No matter how good their product is.

Me using Twitter every morning.

For founders, here's a cheat sheet for survival.

1. Understand the difference between a VC betting on narratives and those digging deep into your theme. One of them will be flipping your SAFT. The other could co-author your whitepaper.

2. Being early is a moat in itself. But it could also mean it takes months before someone builds conviction on what you are making. Most of your pitches will be investor education classes. It is a blessing and a curse.

3. Survival is the ultimate flex in a market where all your peers die. Keeping spending to a minimum to survive is often the right thing.

4. Consumer attention often precedes investor capital. It helps to speak to users to iterate on the product before pitching it to investors.

5. It is acceptable to shut down a venture if you do not find PMF in a meaningful timeframe. Life is too short to be employed by your VCs past a point. There need to be more candid conversations around how firms can wind down with the least friction. (*This was hard to write, but it must be mentioned)*.

Given crypto is such a liquid market, investing (time or money) requires understanding whether you are early to a theme, or riding a wave. The trap is often in spending years on a collapsing theme. For what it's worth, I do not believe Web3 gaming as a theme is done for. Its story is still being written by countless founders who still have conviction in the theme. I am trying to figure out chapters of that story myself every week.

The trap is in confusing public market price action with private market investing opportunities. A narrative could be dead by the time a product comes to market. Follow-on rounds may vanish. And consumers may not care. That is an uphill battle many founders will have to fight in the coming quarters.

If you are building, make sure to drop your decks here. We may be able to help.
I'll see you guys next with notes on staking.

Joel

Telegram, Pitch Decks & Referrals.

Join in with close to 5000 researchers, investors, founders & overall great human beings. We don't exactly talk much, but it would help you stay close to what we are focusing on & connect with others building cool things.

Fill out the form below if you are a founder building cool things and in the process of raising money or looking for feedback on what you are pursuing. We like the builders.

Enjoyed reading this? Consider sharing with a friend for access to premium newsletters we enjoy reading and good karma.

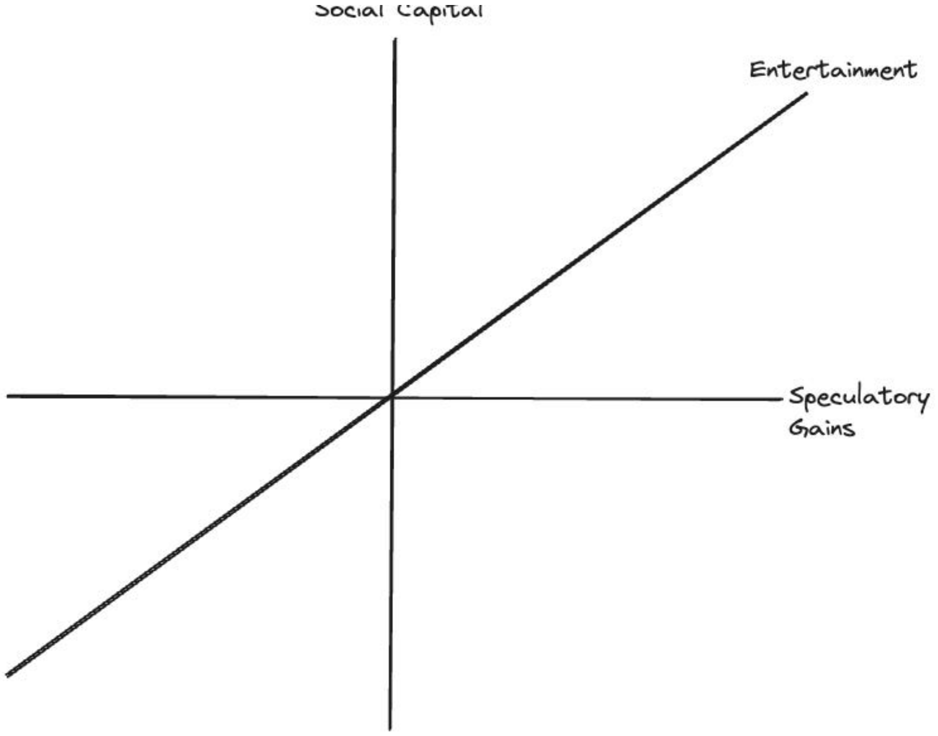
Disclosure

1. Decentralised.co owns a minority stake in Asset.money

Joel John
decentralised.co

Volatility As A Service

On social networks, status and risk in Web3



Skip this Section

Look at you. Quite the rebel. Reading the parts I specifically asked you to ignore. We have a few ad slots left unsold for the next few months. See that white space up there? With our custom-made, hand-drawn, lost stick figure? Yep. That one. It is up for sale. He seems annoyed about us wanting to move him out of there.

We have been writing long forms for some of the brightest people in our industry for over six months. They make decisions at enterprises, build products and allocate money. You know—the movers and shakers of our industry.

Your brand could be seen by people who can be highly impactful for your product. Right now, they are staring at an idle, lonely stickman. I think we could do better than that.

You might wonder - "*How do you even pitch an unknown newsletter to your marketing committee?*" Isn't it safer to go with our larger peers? Nobody looks stupid pitching IBM. We get it. But we have the numbers.

A quarter of our mailing list opens our newsletters within two hours. 42% of our readers would have read it by the weekend. 150 enterprises are part of the mailing list. Over 10,000 people will have read this article over the coming weeks.

And if that doesn't convince you, consider reading the story below. You'll understand what we do and how we differ.

Contact us on Passionfroot for more details.

Hello!

This was initially meant to be a piece for our paid subscribers alone. But it ended up being a long form that I had to get into everyone's inboxes. The e-mail may get clipped in your clients. Click on the read online button above in case that happens. Here we go..

Every once in a blue moon, I think of Archegos Capital. Started by a Tiger cub named Bill Hwang, this firm imploded during last year's stock market pullback. Firms blowing up are nothing new in finance. They happen every once in a while. And people recover from them.

For example, the guys from Three Arrows Capital have been running an exchange while simultaneously dodging Uncle Sam after defaulting on their loan obligations. You get the gist. Funny business is expected in finance.

The bit that makes Archegos interesting is that Bill Hwang had attempted to monetise social capital. He had taken loans from multiple investment banks like Credit Suisse against shares he held. The problem? Bill was using the same shares with numerous firms to open up various lines of credit.

So instead of $100 of equity backing a $80 line of credit, he had $100 of equity, giving him up to $600. You know, good old leverage. It all blew up last year, and the story ended with him being margin called.

What does this have to do with today's newsletter, you ask? Bill Hwang's case is a person using "social" capital to access real money.

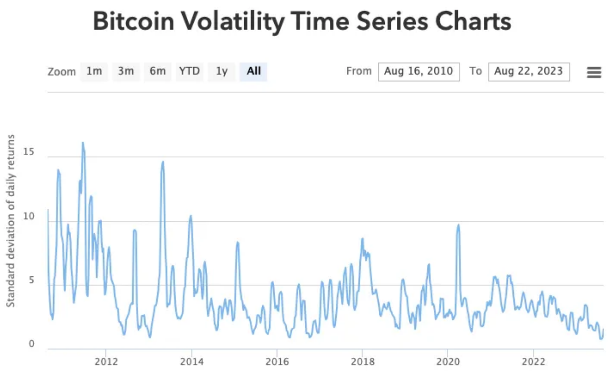
For the longest time, social capital and net worth were separate. The status could be purchased and signalled with money. But constantly talking about how wealthy you are is considered uncool. The media has separated the process of declaring wealth and status.

For instance, the Midas list tells you how rich a VC has gotten. Or the Forbes 30 Under 30 is a list of potential billionaires.

Separating social capital and net worth has historically been important. Rising inequality has often led to political unrest, as many in 19th century France learned the hard way. Political and social order is maintained by accruing influence but never giving it a price.

When markets "price" political power, we call it corruption. Social platforms emerging on crypto today are inverting this relationship in theory. This piece examines why volatility as a service is emerging as a recurring theme across crypto applications and what could be expected from it in the coming years.

But before we do that, consider the chart below. It explains a lot of trends going on within the industry today. Volatility for Bitcoin is at the lowest range it has been since 2016.


Bitcoin Volatility Time Series Charts

Source: Bitcoin Volatility Index

It means most tools and products that see volume during periods of high volatility now struggle to find users. Let me explain

- People have no incentive to borrow one digital asset (*say ETH*) against another (*like Matic?*) if they don't think ETH will outgrow Matic soon.
- Options products see little to no volume if the markets do not anticipate quick volatility within short time bounds.
- Perpetual or decentralised exchange products see volume drying up if traders cannot make money in the short run through trading an asset.

Most products in the crypto space today rely on volatility to be relevant. This is a feature, not a bug. Crypto's core value proposition has been the trustless movement of money over the last decade. And we have delivered on it. The entirety of the DeFi ecosystem was built, grown, and capitalised on during a bull market because of the volatility we were in at the time.

But times have changed, as the chart above makes evident.

Rising interest rates, unemployment, and fatigue of the multiple Ponzis in the industry have translated to a lack of interest in existing product suites. There's a reason for what. During a bull market, traders are incentivised to take an abundance of risk.

Products designed to cater to them see high volume too. But as volatility craters, a market accustomed to being risk-on would find itself bored. Naturally, this pushes users towards where they can discover volatility today. It explains why products pitching volatility as a feature attract the most users off late.

Volatility As A Feature

The chart below shows the number of users on Rollbit over the past few months. The product sees close to 4,000 users on any given day depositing money. For comparison, OpenSea sees around 6,500 users on a given day. This is not to suggest Rollbit is a category leader in gambling. Instead, it reflects how users are flowing from NFTs to high-volatility products.

There are some $46 million deposited on Rollbit as of writing this. The FDV of the token they released is at $800 million, almost 100 times since one year ago

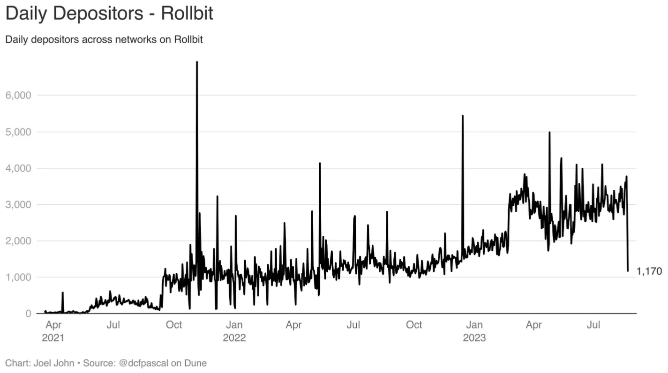
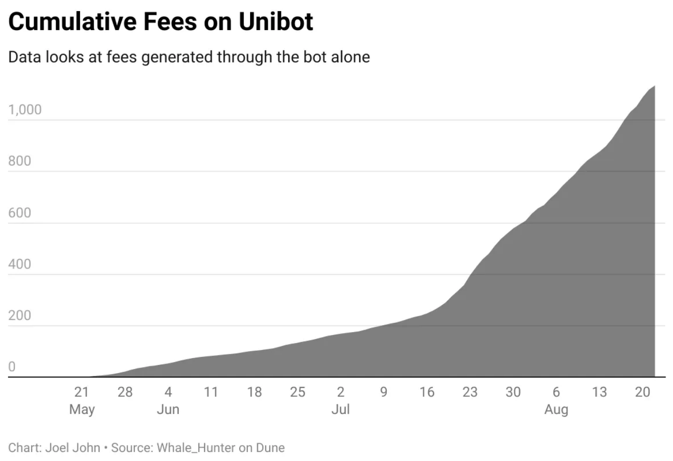

Daily Depositors - Rollbit
Daily depositors across networks on Rollbit

Chart: Joel John • Source: @dcfpascal on Dune

Chart from dcfpascal on Dune

While Rollbit is explicitly a platform for trading highly volatile instruments and gambling, Unibot facilitates users looking to buy the long tail of digital assets. The app's value proposition is quite simple. It bundles setting up a MetaMask wallet, managing its keys, signing into Uniswap, and finding the right pair of tokens for anyone looking to make a quick trade.

The average user on Unibot generates about $2,600 in volume daily; each transaction is around $600. A total of 3,400 users trade through it on a given day. That's a far cry from the numbers we usually see on exchanges, but it has generated nearly $2 million in fees since May of this year.



Cumulative Fees on Unibot

Data looks at fees generated through the bot alone

Chart: Joel John • Source: Whale_Hunter on Dune

Source: Whale Hunter on Dune

Where Rollbit is a casino, Unibot is a tool that facilitates trading low-cap altcoins that usually do not see much volume on a CEX. $PAAL, $DUUBZ, $RAT, $WAGIEBOT - recognise any of these names? Likely not. These tokens have seen the highest volume on Unibot over the past few days.

Unibot is interesting because it ignores a lot of the conventional wisdom in building products in crypto. The private keys are relayed as raw text on Telegram. The product uses a conversational interface instead of the complex ones on Binance. It does not even require you to set up a login! You have to paste smart contract addresses if you are purchasing a token. And yet, it sees close to $5 million in volume daily. A feat that most venture-backed DeFi products struggle to achieve.

Apps are being built with similar philosophies on Telegram. They are aggregating attention and capital. You could easily argue that crypto-native traders spend most of their time on Telegram. Having an interface that combines notifications of new tokens being released with MEV protection and conversational orders would be powerful.

But to me, it sheds light on a different fact. **The pool of money in crypto floating between products is going higher up the risk spectrum due to a lack of volatility.**

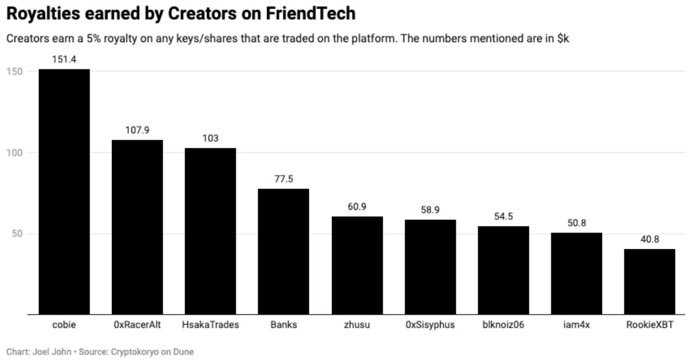
This becomes even more evident with FriendTech. Yes, I have written extensively about them in the past. We will not go into the specifics of why the product is good or bad right now. But here are some statistics that you should be aware of:

- Cobie, the top creator on FriendTech, has made $142,000 in the past week.
- A total of $52 million has gone as an inflow to the product. About $2.7 million in fees has been distributed to users.
- 1.4 million transactions have occurred on the platform across 113,000 buyers and sellers.

(*Yes, I'm branding it as FriendTech, because I don't know what the product's actual name is*).

All of this is on a product that is barely seven days old. FriendTech had ten times the active users Lens Protocol had over the last week. A 100k verified users with Twitter logins, compared to close to 9k on Lens, according to data from Tokenterminal. And as with most social networks, it has its version of emergent power laws.

The chart below shows how much the top “creators” have made on FriendTech over the past week.



Royalties earned by Creators on FriendTech

Creators earn a 5% royalty on any keys/shares that are traded on the platform. The numbers mentioned are in $k

Chart: Joel John • Source: Cryptokoryo on Dune

Chart source: Cryptokoryo on Dune.

There are several things FriendTech got right:

1. The market would have ignored the social app without a backer like Paradigm. The fund gave "signal" value to the product when they tried to onboard influencers.

2. It is becoming obvious there was a round involving influencers for the product. Aligning incentives for individuals with large distribution likely helped with narratives.

3. There is incredible genius in launching the product on Base instead of Polygon (where Lens is currently).

Given its stage and nascency, it is the chain with the most attention. They could have leveraged the Lens social graphs, but they went out and created their own.

Could the product have been built or Arbitrum, Optimism, Polygon - or any other L2? Possibly. But none of those protocols command the attention projects on Base do today. Something the $Bald token rugger knew exceptionally well. Remember these points as we go through the following bits of this article.

Status Meets Capital

There's a reason why I dumped all those numbers on you. Crypto's culture is built on moving money. It makes sense. We built technology that settles ledgers globally and is therefore incentivised to create products that use these ledgers.

What's the best use of moving money if you can't use it for real-life products? Well, you can use it for investments. Compress those investments' growth (or decline) into short cycles, and you have a narrative casino.

Everything is a gamble; the differences are the timelines and odds involved. Crypto works with shorter timelines and worse odds from time to time.

Over the past few quarters, there have been emergent narratives across tokens. NFTs, GameFi, AI, Infrastructure - each quarter brings a brand-new narrative. Part of this is because we like stories.

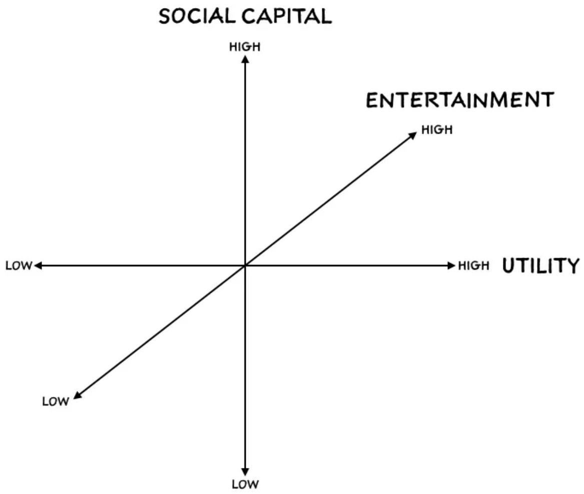
Even when there are no fundamentals to back a token, having a story we collectively believe in helps form conviction in a trade that might eviscerate your net worth. You lose money in a bad trade, but at least it had a strong narrative to back it.

What tools like Unibot, Rollbit, or FriendTech are solving for is this lack of stories and volatility. FriendTech takes it to a different level, likely giving us a view of how Web3 social products could evolve.

Eugene Wei’s “Status as a Service” provides a good framework for how social networks have historically evolved. In the early 2000s, the “intellectually” easy thing to argue was that social networks would become much like traditional social networks. Yet, by some accounts, there were close to 300 social networks of different kinds in the era. Remember Orkut, MySpace, and Friendster?

They all died sad deaths, like many of the altcoins during their rallies in 2017. What made Facebook, Instagram, and TikTok different?

Eugene's article is a masterpiece worth reading - but I'll summarise it in a few points for the sake of this article. But before we go there, take a look at the image below.



According to Eugene, a social network takes off on these three axes. It needs to be high in conferring social capital (status) to individuals posting on it, high on its entertainment (dopamine), and have some form of utility. Quora gives you answers, Pinterest gives you faith in your taste, and TikTok makes you wonder if the future of humanity is worth waiting for.

Each of these apps ticks off all three of the axes mentioned by Eugene.

But how do you confer status in an emergent app? You need proof of work. And the kind of people that can do the proof of work early on in a social network become the "*elite*" on it. TikTok, for instance, primarily leans towards the young because dancing on the application gets you more views than doing a long-form video on YouTube, as Ashwath Damodaran does. It is not that the dean of valuations can't get enough views on TikTok. He may not get as many views as a 20-year-old dancing to the latest tunes on the platform.

The converse is also true. Text-heavy platforms, like Twitter or Substack, confer status to individuals who can write eloquently. Sinocism by Bill Bishop was one of the first publications on Substack. It granted status to the publication more than it did to the author because Bill, at that point, was already a successful writer. Years later, when Packy built Notboring during Covid, Twitter celebrated his writing ability.

Status on social networks is highly contextual, depending on the skills needed to show proof of work. In crypto, speculatory gains roughly translate to "proof-of-work" if you are a trader.

All social networks start as a competition for status between those that can generate proof of work during the early days. Consider Thread's recent launch. I spent half a day on the application thinking Meta's Twitter clone would be a great distribution channel for this newsletter. Much to my disappointment, the product had already broken two core rules mentioned by Eugene.

1. Threads gave status to individuals that were already influencers on Instagram. A product that was built by posting highly-edited photos and entertaining video reels. Users with a large following on Instagram started with more followers on Threads.

2. Given the difference in context, style and content, users on Threads no longer received any meaningful utility from the product. One could go to Instagram to see edited photos. The lack of followers that actual writers saw on Threads meant they had no incentives to

> leave Twitter (or Substack) and start all over in a product dominated by influencers.
>
> The "competition" for human attention on the product did not feel fair and equal for users that were good in the medium Threads was looking to enable.

As I write these words, Threads' active user base is down to 10 million from the 50 million users that flocked to the app during the early days. For people to do the "work," they need verifiable rewards and a fair game they feel like playing. **A social network crosses the chasm of apathy when it has sufficient people putting in the work and an audience base that sees utility in it.**

Web3 native social products have long touted "utility" in the sense that they are claimed to be:

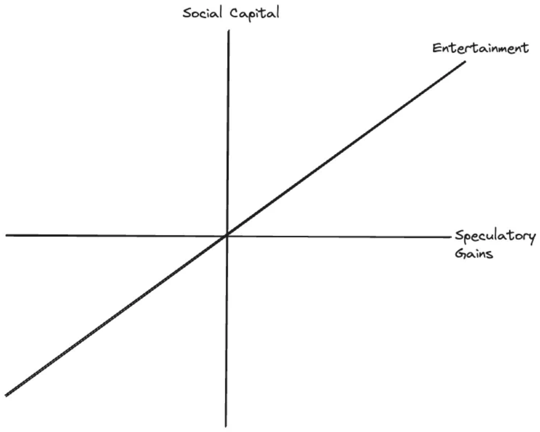
- Composable - users could use multiple clients to interact with or consume content.
- User-owned - in that a handle on Lens Protocol is unlikely to be seized by a centralised company.
- Decentralised - the storage and query layers could be relatively distributed compared to Meta's servers to run Facebook or WhatsApp.

There are other attributes like censorship resistance and immutability at play. Still, I will stick to these three core features because you cannot have retail-scale Web3 social products without moderation. The problem is that these "utilities" do not attract users sufficiently to want to post on a product.

A user posts on Twitter (or Substack) today because that is where the eyeballs are. **Discovery, appreciation, and interaction is the "utility" on Web2 native platforms. Social networks in the traditional world are dopamine machines.** Users are comfortable with their data being exploited by centralised providers because they get many more eyeballs than they would on a decentralised platform.

Creators accept these trade-offs on Web2 in exchange for the scale (of attention) they enable. In the current environment, the only way to switch a creator from Web2 social to Web3 native primitives is if capital is involved. Money is an excellent incentive on its own and is a precursor to social capital.

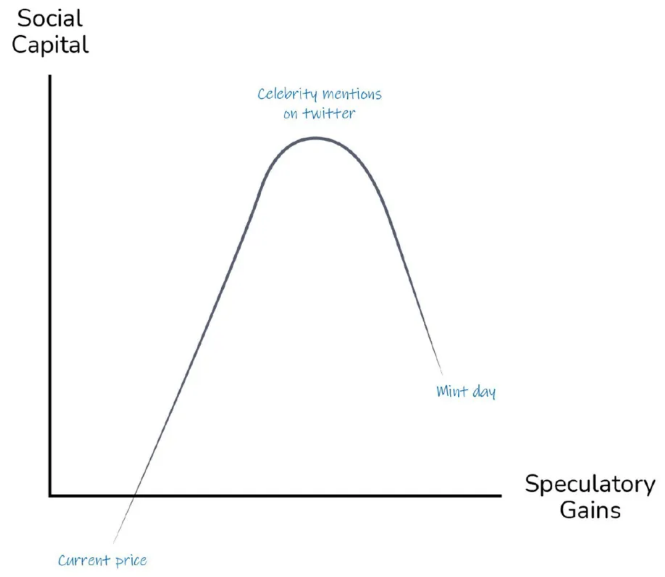
The genius of FriendsTech is replacing the need for "utility" with capital.
If I were to re-do Eugene Wei's axes, it would be like the graph below.



It is fair to suggest crypto is entertaining. We do many things wrong, but entertainment is something we've figured out (especially if financial crime thrillers are your genre of preference). I will remove the entertainment angle from this graph and solely compare social capital and speculatory gains.

DAOs and NFTs follow a very similar arc in their early days. Entrants that can move in early on a product make tremendous speculatory gains, which infers status on them. As the narrative dies, the possibility of making more money on the trade (*through acquiring an NFT like BAYC*) diminishes.

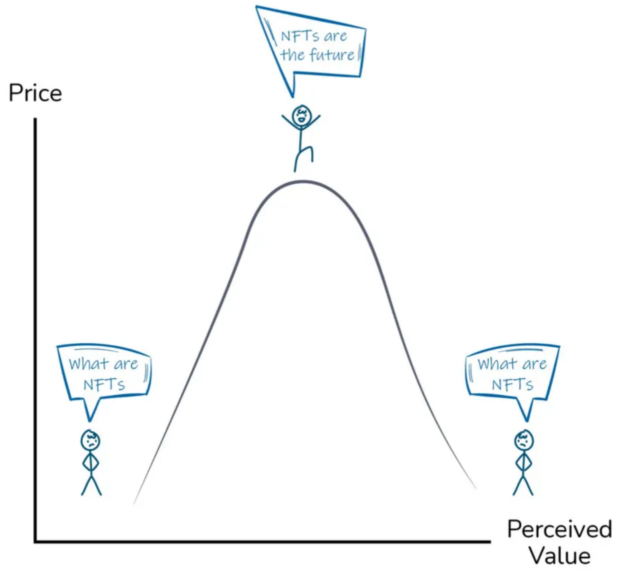
The users that minted BAYC on its launch day had little to no status, but they made the most speculatory gains as they were early. Once the "status" was established through the multitude of celebrities signalling their ownership of the NFT, the profits to be made declined. And buying at peak meant there was only one way the trade could end for you. In losses. The chart would look like something below.



At its peak, NFTs (like Bored Apes) conferred status. Their utility was opening up networks by being part of an elite group of individuals. It either signalled you were resourceful enough to mint an NFT early or rich enough to buy it in due time. Owning an NFT conferred status to you based on who else held it. But as its price collapsed, the "utility" (*in the context of status and social networks*) quickly vanished.

Social networks (like Meta) eventually removed NFTs from their platform because of the negative status associated with the primitives. Bored Apes became synonymous with scammers on Twitter and was no longer a status signal. On the contrary, it became a counter-signal, as evidenced by the countless apes who sold their NFTs (*often at losses*) and reverted to their original PFPs - their faces.

One way to think of NFTs is as primitive Web3 social technology. It mapped out users and gave you a simple social network (or community) depending on who else owned it. The problem these social networks had was that users were aligned with the money they stood to make by holding these primitives. As prices collapsed, the perceived value of being in that social network (of NFT holders) collapsed alongside it—a reverse veblen effect of sorts.



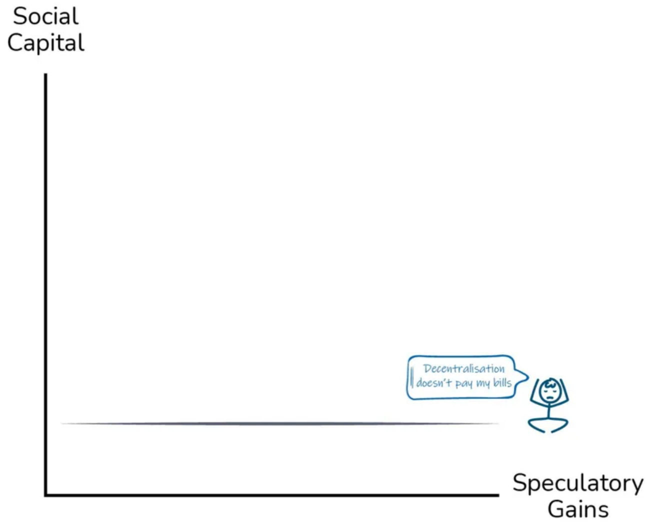
The reverse veblen effect in NFTs occurs when users that previously tied their identity to a JPEG begin disassociating due to its inability to signal wealth or status.

A different class of Web3 social products have avoided this trap by removing (*or limiting*) speculation from their products. The lack of algorithmic feeds mean user don't find you for posting exceptionally great content on platforms like Mirror today. Unlike Substack or BeeHiiv today - most social networks built on Web3 native principals hold on to their idea of neutrality and do not entice creators with any meaningful incentives to switch to them.

This means a user posting on a Web3 social product stands to lose both status and potential gains by any inbound business that comes through the distribution of a product like Twitter offers.

Mirror's genius is in permitting users to issue NFTs and possibly monetise. The challenge is NFTs are one-time sales with limited upside as a creator. You can always hope that royalties from the NFTs will continue to fund you, but that is hypothetical and not a given. So the platform, while rich in features, fails to attract users as it flatlines on the status and speculatory gains unless you are a known creator.

The chart below summarises my thoughts as I post my piece on Web3 native social products occasionally. When a product cannot generate wealth or distribute content - it fails its purpose as a dopamine-inducing machine. Users stick to their existing platforms (like Twitter) instead of bothering with a new one.



A product could be built on a chain that enables a million transactions for next to nothing while permitting users to own, filter, trade, or lend their data. But until the incentives align, users will not flock to it. **Utopian visions of how technology must evolve rarely convert to reality until user behaviours are studied.**

In the past, token communities were "social networks" consisting of individuals with aligned incentives. The product was the token's price. Present-day social networks aim to expand beyond that niche of "token investors."

The more retail audience bases in our products get, the farther we will be from design choices that community members considered normal in the past.

Merging Worlds

Historically, the social graphs you had on-chain never interacted with the social graphs you had off-chain. In Dubai, I prefer not to meet people from work on the weekends because they bring out a different personality in me. And I'd rather not be discussing degen behaviour in my time off. (*I'm NGMI, I know, but it keeps me sane*)

FriendTech explicitly merged a Web2 social graph with a Web3 social product. It used people's Web2 social graphs to propagate itself as the product often tweeted from users' Twitter handles without them knowing.

In doing so, the product managed to do what has historically been the most challenging part of bootstrapping a social network from scratch. Finding friends on a new social network. When you sign up on TikTok, Instagram, and recently Substack, the product asks permission to sync your phone contacts to their servers.

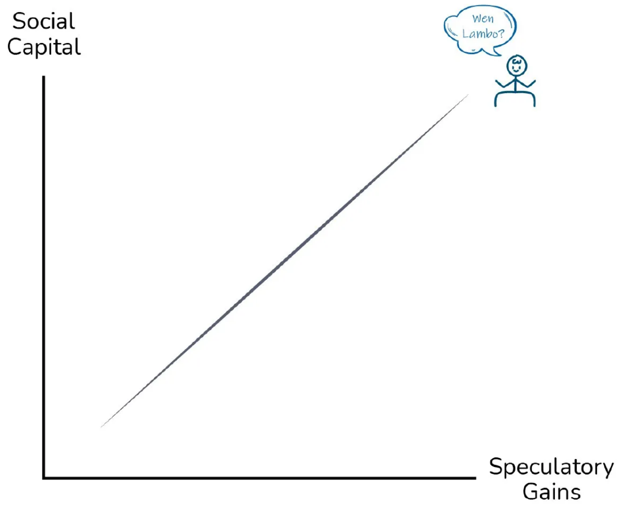
The products then map out the phone numbers to platform users and suggest them as friends to you. WhatsApp took this one step further and permitted you to text users whose phone numbers were stored on your phone.

By merging your off-chain social graph with your on-chain behaviour, the product reduced the “activation” energy a user needed to be hooked on the product. Users are no longer spending time setting up their wallets. One of the first actions you do on the product is ‘buying” your shares, which sets the expectation for what the product lets you do.

From there on, you can use the explore or trending sections to find your friends. These friends, in turn, are notified about you signing up for the product and thus incentivised to buy your shares.

The higher the value of your shares, the more the status conferred on you. What makes FriendTech interesting is that it has put a commercial price that is publicly verifiable for people’s social graphs. It is not about the size of social graphs either. Cobie has close to 740,000 followers on Twitter. 0xRacer, in comparison, has close to 16,000, but the latter has a higher market cap on Friend.

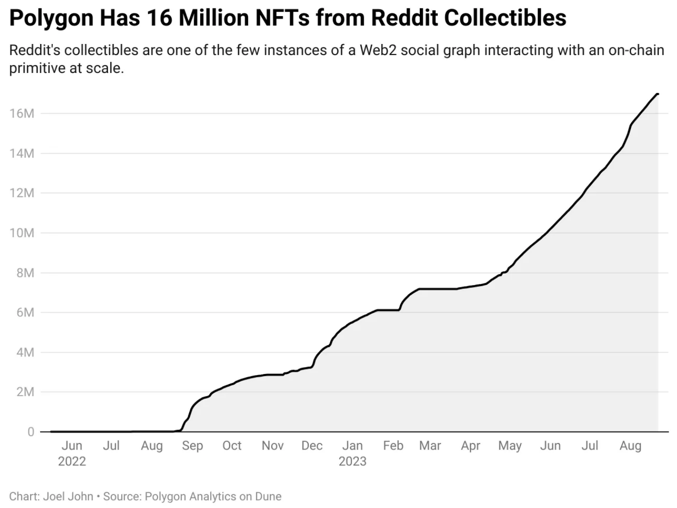
The product verifies the willingness of people to pay for your shares. It is a measure of the desire of your followers to put money where their mind (attention) is—a more distilled measure of popularity. In the age of everyone getting their 15 minutes of fame, creators that can make their $100k of royalties will separate themselves from the rest.



FriendTech is a funnel for translating your social capital into speculatory gains. The graph looks closer to the one below. Historically, it did not mean much outside the crypto realm if you traded altcoins and made much money on them. Web3 social products (like FriendTech) blur the gap between clout (in the real world) and wealth generated from your on-chain behaviour.

Historically, we used to think of the “*on-chain*” world as a limited subsection of wallets. Depending on the category or timelines involved, there are anywhere between 4 million (DeFi) to 15 million (NFTs) users in these product categories. In blurring the lines between social graphs on Twitter and the blockchain, FriendTech has released the proverbial cat out of the bag. (*The last cat was Bitclout, and I know that didn’t end well*).

This “trend” of merging social graphs is not new. Twitter’s integration of NFTs into the product and Meta’s attempt at permitting users to link NFTs to their profiles were variations of blending social graphs. But the one place this has happened quite eloquently is on Reddit. Some 16 million NFTs have been minted on Reddit without spurring a speculatory boom.



Polygon Has 16 Million NFTs from Reddit Collectibles

Reddit's collectibles are one of the few instances of a Web2 social graph interacting with an on-chain primitive at scale.

Chart: Joel John • Source: Polygon Analytics on Dune

The next category of Web3 social products will similarly merge social graphs and hack growth with volatility as a pitch. Mirror can integrate Twitter's graph into the product. Lens (*or products built on it*) can attempt to make it possible to discover your Twitter followers with a Lens handle.

But until an element of speculation drives massive capital inflow, most of these products will (*unfortunately?*) not capture sufficient attention.

According to Eugene, if the product has enough utilities, a social network can sustain itself after users are tired of social capital games. Instagram's integrations of vanishing images (SnapChat) or reels (TikTok) is an instance of a social network expanding its product suite to be relevant after the status games are played out.

The reason why Web3 native social products will have to lean heavily on capital inflow is that these utilities are not built yet. **Volatility is the service until a sizeable social graph to retain users emerges.**

Risky Behaviour

We are a decentralised, user-owned social network with composable social graphs
Can I find a date on your product though

The true litmus test for all social products.

A product on the internet has reached complete maturity only when its users are flirting with one another. It occurs everywhere. From the beautiful corners of YouTube comments to Amazon Reviews and, I presume, even Uber. Web3 native products have not reached a point where there is sufficient user diversity to facilitate making new friends. Instead, we have capital sinkholes that may or may not generate value in the long run.

You can paywall content without crypto. You can run a paid Telegram chat. There is no need for a bonding curve to monetise your content. I doubt any creator needs Friend.tech to be a better creator. Think about it: John Lennon, Beethoven, and Michelangelo relied on elements of finance throughout their careers. But they did not need an on-chain Ponzi scheme to fuel their success. **What Web3 social products will solve is the financialisation of everybody.** Is that a desirable outcome? I don't know.

Historically, you either needed to launch a protocol (like Aave) or run a community (like BAYC) to generate wealth. Web3 social would enable everyone to create money off their social graphs at the click of a few buttons. Given the legal risks, multiple creators with large followings may avoid jumping on the bandwagon, leaving the industry with a curated subset of financial miscreants willing to take on the risks.

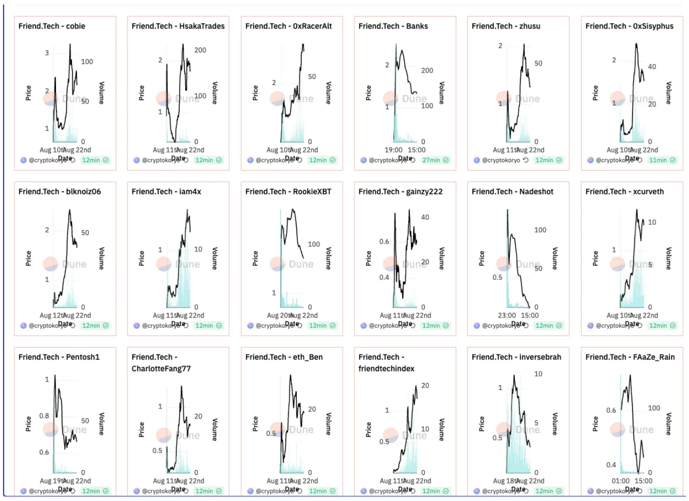
Remember Threads? We could see that with Web3 social quite soon.

This means we will continue to see risky behaviour involving money and reputation with these product categories. NFTs enabled celebrities to issue digital assets and monetise their social graphs. But they also resulted in countless scams. As with all primitives, we will see a period of exuberance, where Web3 native social products are touted as the future of content.

The capital incentives for creators and early adopters would push these financial primitives to users. **But unless we can switch from being an industry of transactional products to one that can enable attention capture at scale, we may be doomed to repeat mistakes of the past.** From a capital allocation perspective, it is becoming increasingly clear that crypto is dividing itself into two broad ends of a spectrum.

On the one hand, when you consider their volatility, you have assets that are becoming similar to hard assets (like gold). They will see cash flow from institutional capital allocators wanting an alternative asset class. On the other hand, you have highly volatile on-chain primitives that are driven by narratives and social graphs.

As for FriendTech, I will remain a sceptic for now. LooksRare, Blur, and many other products have previously humbled me. You start with an optimistic outlook only to see users flock elsewhere once incentives (airdrops) are switched off. As long as an airdrop and royalties are involved, you cannot verify what portion of a product's users are real. FriendTech has an airdrop tab in the product. Creators on the platform are incentivised to distribute to more users because of the royalties involved.



Having a price on access to your favourite creators implies that it may be more entertaining to trade their "shares" than to consume their content. Chart from Cryptokoryo

One of the scariest outcomes that could occur for FriendsTech right now is a reverse network effect of sorts. Presuming a large portion of the userbase goes into losses holding shares of creators, the incentives to stick around engaging with creators tend to diminish. As a creator, making money is terrific. (*Trust me, I know*). You need to pay the bills. But having an audience subset that does not care is punishing in its unique ways. What tools like FriendTech do today is enable users to make portfolios out of social graphs. And portfolios, like many of our crypto-bags, can go deep into the red.

Historically, creators had to compete with other creators for attention. Web3 social products that combine elements of trading with reputation or content will make it possible for creators to no longer compete with a scarce asset—the amount of time people have to give for their content.

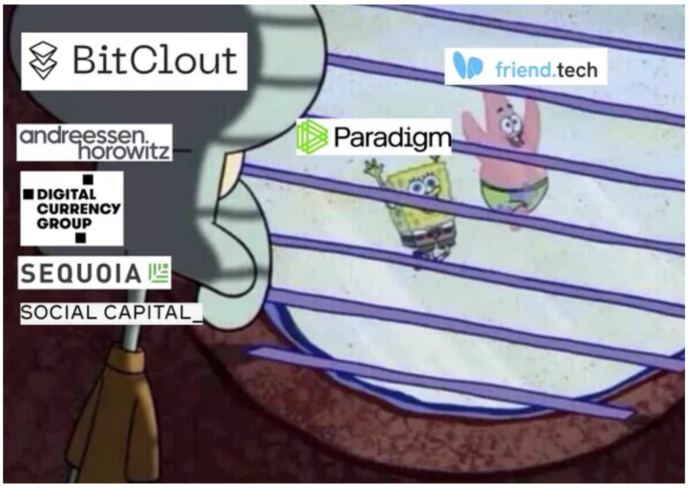
I have my scepticism, but for now, it is becoming evident that volatility is one of the strongest hooks for Web3 social products to come to market.

Here is why. Some 100k signed up to FriendTech over the last week. Those users are looking for risk, not content. You can build great products that target retail participants. But they do not have context on crypto. The only way products can reach sufficient levels of growth to kickstart network effects large enough to onboard retail users is through onboarding crypto-native users and making them rich through product royalties or airdrops.

Whether we like it or not, that process involves speculation. We can ignore it, but people don't care about decentralisation as much as we think they would. They care about what a product can do for them more than the number of PhDs deciding the consensus mechanisms used on a blockchain.

The "pitch" in crypto has been volatility for the longest time. Web3 social will bring elements of volatility and social graphs together. It could enable distilled, collective lunacy. It scares me when I think of how these things could evolve. But as with most technological cycles, I think it may bring back life into primitives like DAOs that have long been ignored.

Until the regulator takes action in some meaningful form, we will continue to see developers blurring the lines between what is acceptable and what is not.



Source: Jason Yanowitz

Ironically, we have iterations of such experiments in the past. Steemit and Bitclout come to mind. The NFT boom was a similar cycle. It would be intellectually dishonest to presume that any capital allocation cycle in a new product category would not repeat patterns from that.

Crypto will have to transition from a "transactional" product to an "attention economy" product to reach the user base the internet has today. The tech stack needs to be able to facilitate use cases that capture our attention instead of our money. Web3 gaming and social networks serve that function quite well. We have no mechanisms to onboard creators with the right incentives just yet.

In 1997, there were some 13 million individuals on the internet. Today, there are 3 billion. The exponential arc of technology humbles the most cynical souls. (*Including me*). Web3 social products are speculative platforms today because we have not figured out how to onboard normal users without making them lose money.

Much of the work that needs to be done for the industry to scale is not in terms of the brand-new L2 or decentralised exchange. It is in figuring out business models that can use the technologies we have already developed. To borrow Janet L Yellen's words: speculation is a transitory feature.

I'll see you next with some work we have been doing on identity products in Web3.

Digging through fish-curry recipes on YouTube,
Joel John

Telegram, Pitch Decks & Referrals.

Join in with over 5000 researchers, investors, founders & overall great human beings. We don't exactly talk much, but it would help you stay close to what we are focusing on & connect with others building cool things.

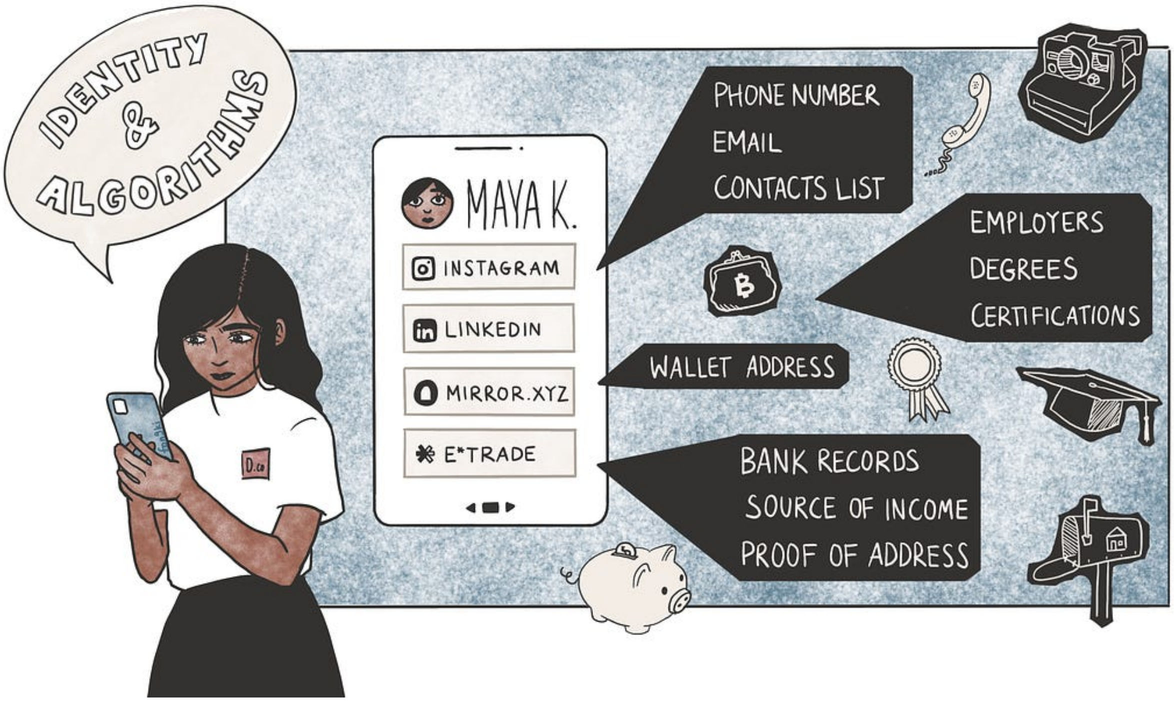
Fill out the form below if you are a founder building cool things and in the process of raising money or looking for feedback on what you are pursuing. We like the builders.

Enjoyed reading this? Consider sharing with a friend for access to the paid versions of our newsletter.

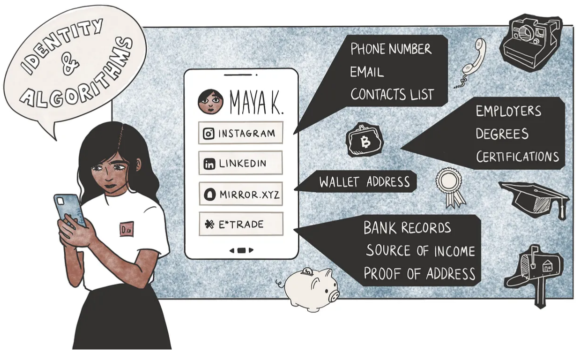
Joel John
decentralised.co

Mapping The New Internet

Identify yourself, anon.



Hello!



Few things before we begin.

1. This piece is written in the first person for easy reading. It would imply that I wrote all of this piece. But much of the groundwork was done by Siddharth. He has been the brains behind some of our best pieces. If you don't follow him on Twitter already, you should.

2. We have been quite active on the paid side of the newsletter. We are ranking #35, right under Jimmy Song, and a few positions away from Laura Shin on Substack in the list for crypto. Here are the things we covered over the last month. Some of it overlaps with today's article.

We have activated free trials if you want to read them without paying upfront. And yes, you can e-mail me for a refund if you decide to cancel but forget to do it on time.

Today's piece begins with setting a baseline understanding of why reputation and identity matter online. We then look at how blockchain networks have historically maintained forms of reputation before understanding the primitives that power verification in the future.

Given the length of this piece, it may break in your e-mail clients. You can read it directly on Substack by clicking the button below.

With all of that out of the way, let’s dig in.

Remember July 1993? Me neither. I wasn't born yet. Neither was Amazon, Alphabet (Google), Meta (Facebook) or X (Twitter). Much like blockchains today, the internet was a phenomenon that was slowly taking shape. The applications needed to onboard and retain users did not exist. Subscriptions to internet services plagued users because of how costly they were. It used to cost $5/hour. The technology was nascent and easy to write off.

"On the Internet, nobody knows you're a dog."
P.Steiner

=

The comic above was published that month by an artist who could not care any less about the technology. According to sources, he had an expiring internet subscription that cost a lot and a deadline to meet. That was all the context he had on the internet. But it captures the state of the technology at the time quite well. The mechanisms to verify identity and reduce bad behaviour did not exist yet.

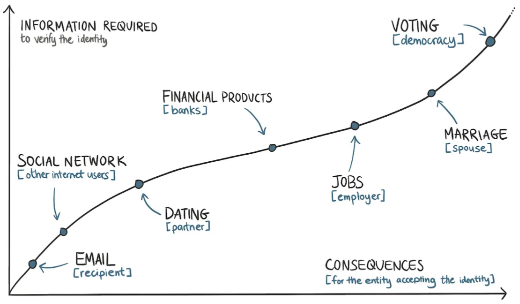
Most emergent networks have this trend in common. It is rather hard to establish who engages with it during their early days. One of Steve Jobs's earliest ventures was a device that allowed individuals to spoof identity on telephone networks.

The evolution of the internet required verifying the identities of individuals. Because the information superhighway (*as Al Gore used to refer to it*) was only valuable so long as it could enable commerce. And doing business in meaningful volumes requires knowing the details of your customers.

Purchasing on Amazon requires your address. Part of the reason PayPal agreed to an acquisition by eBay was the mounting fraud risks on the payments product. For the internet to evolve, trust became mandatory. Establishing trust requires knowing who you are interacting with.

Internet applications collect identity information according to the extent of consequences your actions may cause. It is a spectrum. A simple Google search requires only collecting your IP address. Emailing 100 people would need your email provider to have your phone number. Paying through PayPal would require handing over your state-issued personal identity documents. Regardless of where you stand regarding privacy, it is fair to suggest that applications can scale when the identities of the user base are established.

Large networks like the internet evolve when there is trust in the system. The emergence of different forms of identity instilled trust, and that has been the basis for a more secure, useful internet over the past decade.



The amount of identification documents gathered from a user scales in proportion to the consequences of one's actions in most interactions.

Seen through this lens, it becomes easier to understand why information gathered for each internet interaction is proportional to the possible consequences of one's actions.

Accessing a social network only requires a person to submit their phone number. But for an account that is verified and has massive reach, the social network (like Twitter or Meta) may request additional forms of verification, such as a government-issued identity document. Similarly, banks ask for information on one's employment and source of funds due to the possibility of an online account enabling illicit transactions.

At the absolute end of the spectrum is marriage (*at the individual level*) and a democracy (*at a societal scale*). Assuming rational actors (*which is often not the case*), people gather as much information as they can on a possible life partner before committing to wedlock. The identity of voters often undergoes multiple rounds of scrutiny, as a few thousand fake votes can tip an election to a person who may not be preferred.

Today's piece explores a simple question: **What happens when the forms of identity we use for blockchain applications can evolve?** There are ethical considerations around why they should not evolve. Much of the industry is built on the ethos of relative anonymity and free access. But as with the internet, having additional context on users could be crucial for creating a new generation of applications.

There are two reasons why on-chain identity would become a necessity:

1. Firstly, market incentives continue to drive individuals to exploit protocols through Sybil attacks. Restricting access to users relevant to an application helps improve the overall unit economics of businesses within the industry.

2. Secondly, as applications become increasingly retail-oriented, regulations would require service providers to have additional

information on their users. Placeholder's Progressive Compliance article hints at this.

A simple heuristic to use here is that blockchains, at their core, are ledgers. They are global-scale Excel sheets. Identity products built on top of them are vlookups that filter specific wallets depending on the need of the time.

Networked Identities

The arrival of all new networks calls for the emergence of new identification systems. The passport emerged partly due to the rail networks connecting multiple European countries after World War I. We interact through fundamental identification units around us even when we don't realize it.

A mobile device connected to a cellular device has an IMEI number. So, if you decide to make prank calls, the device's owner could be traced by finding a receipt from when the device was sold. This is in addition to the fact that in most regions, acquiring a SIM card would also require some form of identification.

On the internet, if you use a static IP address, your details like name and address are already linked to your activities online. These are the primary identification blocks on the internet.

The single sign-on button solved one of the biggest hurdles on the web, creating a mechanism for applications to get details on a person's identity without requiring them to fill them out each time. Developers could collect details such as age, email, location, past tweets and even future activity on a platform like X after collecting consent a single click. It collapsed the extent of friction in the onboarding process.

Several years later, Apple's single sign-on button was released with deep integration into its operating system. Users can now share anonymous email addresses that do not divulge their details to the products they sign up for. What is common between all of them? A desire to know more about users with the least effort possible.

The more context an application (*or social network*) has on a user, the easier it becomes to upsell products to them with targeted identities. The basis for what we now call surveillance capitalism is the ease with which firms on the web today can capture users' personal information. Unlike Apple or Google, blockchain native identity platforms have not scaled yet, as they do not have the kind of distribution those behemoths possess today.

Blockchain, native identity primitives, are unique because everyone can access user behaviour details. However, the tools needed to identify, track or reward users based on their past behaviour had not evolved until a few quarters back. More importantly, the products that tie on-chain identity to your real-life documentation, such as passport or phone number, have not scaled yet.

Part of the reason is that the products that require such use cases have not scaled yet. During the days of the ICO boom, Civic was often used to verify the identity of an individual purchasing tokens in a sale. Years later, they transitioned to checking identity on beer vending machines.

For the past few years, the primitives used for identifying users in our ecosystem have been wallet addresses, NFTs and, more recently, soulbound tokens. They serve similar functions as the IMEI number or IP address on the internet. Wallets can be spun up hundreds of times by the same individual, which takes a click of a button. They are similar to email addresses during the internet's early phase. By some measure, in 2014, some 90% of all emails were spam, and one in 200 emails included a phishing link.

We have created elements of identity around a wallet address using its on-chain behaviour. Degenscore and Nansen's categorisation of wallet labels are early instances of what these look like in practice. Both these products examine the historical activity on a wallet and issue a tag.

On Nansen, you can scan a token's holders and find the number of 'smart wallets' that hold the token, the assumption being that the higher the number of 'smart' token holders a product has, the higher the probability of it rising in value as 'smart money' continues holding exposure to it.

NFTs became an instrument for identity through their scarcity. Some 'blue-chip' NFTs in 2021 were limited to several thousand mints. Bored Ape NFTs had a cap of 10,000 in total. These instruments became symbols of identity through their ability to verify one of two things:

1. A person had access to 'alpha' by being early enough to a mint.
2. Or they had the capital to buy an NFT in the market after the mint finished.

An NFT becomes a symbol of value by virtue of who else owns one. Bored Apes were once owned by Steve Aoki, Stephen Curry, Post Malone, Neymar and French Montana. The challenge with NFTs is that they are static in nature and owned by a community. An individual could have accomplished a considerable amount since a Bored Ape's 2021 mint, but an NFT could show nothing to verify that.

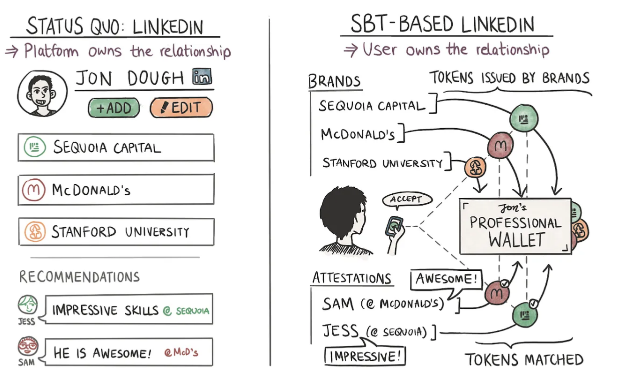
Similarly, if a community develops a bad reputation, that seeps over to the holder of the NFT too. College degrees are similar to NFTs in that both can appreciate or depreciate depending on the actions of other parties involved in holding the instrument of identity. (*In some cases, they are also similar in that their holders tend to hold remorse about the high prices at which they acquired the degree or NFTs.*)

Vitalik Buterin proposed an alternative to the conundrum in his paper on soulbound tokens. Unlike NFTs, soulbound tokens (SBTs) are designed to be non-transferable and require a user to accept them. The crux of the concept is that issuers (*like universities*) could release tokens representing accreditation to wallets from which they cannot be moved. Other token holders from a similar accreditor could attest to the validity of an SBT.

So, if I claimed to work at McDonald's and had an SBT issued to back the claim, a future employer could validate that claim far more quickly than by checking my LinkedIn or CV. I could further strengthen my claim if I had a group of colleagues attest to this claim on-chain with their SBTs. In such a model, my claim is verified by the issuer (*McDonald's*) and through a network of attesters (colleagues) willing to back that claim with their on-chain identities.

Tokens and NFTs are similar in that they are acquirable proofs of status. An SBT's being non-transferable means the wallet that owns it has accreditation that is usually earned[1]. In the above example, a McDonald's attestation may not be easily acquired by going to OpenSea.

But a Bored Ape NFT could be if I had the money to do so. What makes SBTs interesting is the possibility of mixing and matching them to create social graphs. We need to understand LinkedIn's core value proposition to understand what I mean.



LinkedIn, like all social networks, offers status as a service. On its feed, people compete to be the ideal corporate man. The genius of LinkedIn was in being early enough to create social graphs of institutions. I could claim that I studied at Hogwarts with Harry Potter and Professor Dumbledore on the platform in a matter of clicks. The social graph emanated from institutions.

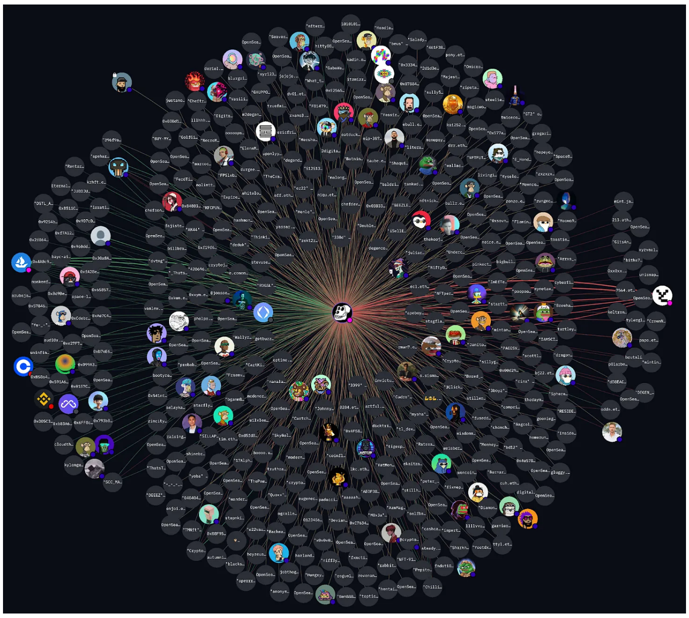
A person's status on the social network depends on the reputation of the organisations they associate with and the relative rank they hold at the place.

In my hypothetical example, the "strength" of my reputation grows with each new organisation I tie my identity to. As long as the network of people within these institutions does great things, my reputation grows with it. It's the reason why we see the PayPal mafia as so significant.

Why does any of this matter? Because today, there's nothing stopping individuals from making false claims on LinkedIn. The social graph is not verifiable or attested, so much so that spies from sanctioned nation-states use it to target researchers.

A network of wallets holding SBTs could be a more decentralised and verifiable social graph. Hogwarts or McDonald's could issue my credentials directly in the above example. SBTs remove the requirement of a platform middlemanning the relationship. Custom applications could be built by a third party querying these graphs, which adds to the value of these credentials.

Owning a Hogwarts SBT could mean I get invited to a local wizard conference. Or it could mean wands at a discount. But it hasn't happened yet. And the reason for it boils down to the number of users. Let me explain using BAYC as an example.



A group of bored apes on the blockchain.

Web3's great promise has been that open social graphs will empower the issuer to have a direct relationship with the owner of an accreditation. But we have that here already. The graph above from Arkham is a visual representation of all the owners of Bored Ape NFTs. But if you had to contact all of them, your best bet would be to export their wallet addresses and send them a text through something like Blockscan.[2]

A more accessible alternative is to go through the social profiles of Bored Apes or their Discord, but it simply repeats the initial challenge we had with identity networks in the first place. Distributing anything through those networks involves centralisation and permission from the management at Bored Apes if you want to reach scale.

All of this brings back a core problem with on-chain identity networks. **None of them have scaled enough to enable network effects yet**. So despite having the theoretical mechanisms to create open, composable social graphs that validate users through tokens, wallets and SBTs, no Web3-native social networks have retained users and grown yet.

The largest 'verified' social graph that exists today on-chain is that of Worldcoin. They claim to have over 2 million users on the network. That is barely 0.1% of users on a traditional Web2 social network like Facebook. Yes, I'm comparing apples to oranges here – but here's the point. An identity network is only as strong as the number of participants with some identity that can be verified.

There is a bit of nuance to be added here. When we speak of “identity” online, it is a mix of things. If I were to break it down, it would be

1. **Identification** - The core primitives that individually identify who you are. This could be your passport, driving license or university degree. They usually verify your age, skill and location-related parameters.

2. **Reputation** - In the context of algorithms like the one on X, it is a tangible measure of an individual’s skill or ability. This is linked to the quality of a person’s content on social networks and the frequency with which an audience base responds to it. In the context of work, it is the graph of entities that pays an individual (or entity) over some time. Where identification is usually fixed at a given point in time, reputation evolves over some time.

3. **Social Graphs** - Consider it the interlink between a person’s identity and reputation. An individual’s social graph depends on who interacts with them and at what frequency. Individuals with high reputations (or social rank) interacting frequently with an individual leads to a higher ranking on a social graph.

As we go through this article, I will use these terms interchangeably as the organisations solving for identification on the internet are not solely looking to validate your passport. Some of them are building portable social graphs. Others want to identify your behaviour on-chain to assign it a score so developers can better identify their users.

As with most things, there is a spectrum of applications even within the realm of identity on the internet.

The Core Primitives

Though anonymity was part of the feature set in crypto, we have had identity checks at the periphery. The bits where on-chain money converts to fiat transfers (exchanges) have historically mandated collecting user information.

Exchanges are the largest existing graph of on-chain persona linked to personal identification documents. But it is unlikely that an exchange (like Coinbase) will roll out an identity-linked product as of today given the conflicts of interest such an action may provide.

Binance's SBT Experiment Has over 850k Verified Wallets

The tokens were offered to users that had verified their real life identity on the exchange.

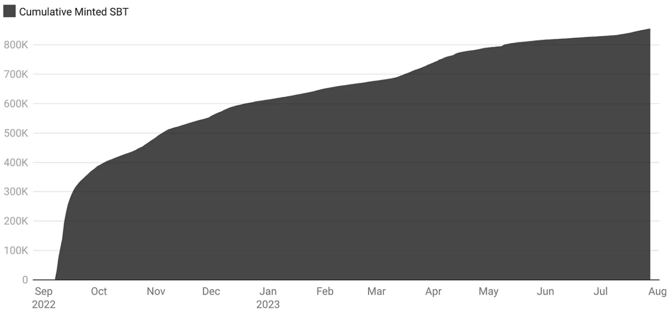


Chart: Joel John • Source: David_C on Dune.xyz

One early instance of an exchange tinkering with on-chain identity is that of Binance's experiments with BABT. Specifically, a Binance account-bound token is the equivalent of a Soulbound Token (SBT) issued on the Binance Smart Chain. The token was offered to users who had done their AML/KYC on the exchange. Over the past year, over 850k wallets claimed a BABT in an early attempt at creating linkages between wallets and real-life identity at scale.

But why bother with it? It helps applications know that a user is 'real'. By limiting access to users who have provided their verification documents (in the form of passports or other regional documents), products enabling access to a handful of wallets can optimise for reducing Sybil attacks and increase the number of real users with minimal effect.

In such an instance, the dApp does not access a user's verification documents. That function is executed by an exchange (like Binance), which may use the APIs of a centralised service provider like Refinitiv. For dApps, the upside is having a verified subset of users who have already proved they are human.

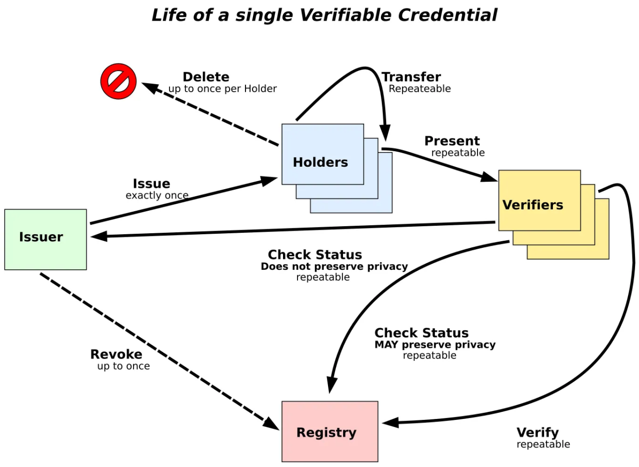
The approaches with which information on a user is gathered and passed on to an app vary depending on the context and resources at hand. There are multiple ways to go about it. Before we get into the models, though, it helps to master a few basic terms. A detailed breakdown of each of these concepts is beyond the scope of this article, but I have attached hyperlinks where relevant for the curious ones amongst our reader base.

Think of it as a design philosophy that puts the credential owner in complete control of their identification documents. In traditional, state-sanctioned forms of identity, a government or an institution is responsible for issuing and validating identification.

When a person hands over their identity documents, like a license for verification, the government's systems must not cut the person off. SSI's core argument is that a person should be in control of (i) management (ii) privacy, and (iii) access to an individual's identity.

An SSI-based identity product can contain multiple forms of identity, such as certificates from their university, a passport, driving licenses and so on. Each of these may be issued by centralised institutions, too. SSI's core argument is that users should control how these details are accessed.

Verifiable credentials are a model of the cryptographic validation of a person's identity. At its core, the model is contingent on three parts: an issuer, a verifier and the credential holder. An issuer (like a university) can issue cryptographic proofs, signed by the organisation, to a credential holder. These proofs are used to back what is considered a 'claim'.

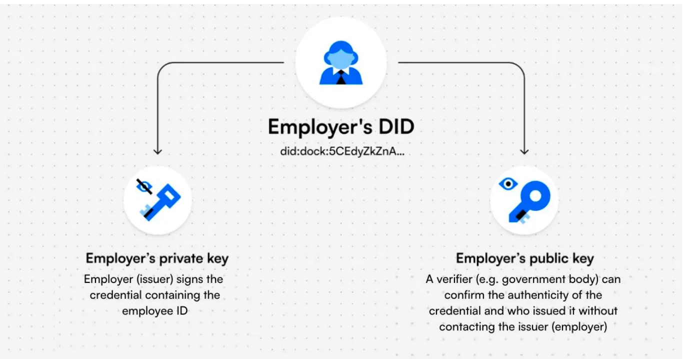


Source

In this context, a claim could be anything, ranging from 'X studied here' to 'Y worked with us for five years'. Multiple claims can be merged to make what is known as a graph of an individual. In the case of a verified credential, the documents (like passports or certificates) are not passed along; only cryptographic signatures from issuers are passed along to validate identity. You can see a live version of such a model here.

Decentralised identifiers (DIDs) are the structural equivalent of a phone number or an e-mail address for your inbox. Think of it as a wallet address for your identification. When you use a platform that requires you to verify your age or geolocation, providing a DID could help the application verify that you fit the parameters needed to use the product.

Instead of manually uploading your passport to Binance, you could provide a DID. The compliance team at Binance can then validate the location of the proofs held by your DID and onboard you as a user.


Employer's DID
did:dock:5CEdyZkZnA...
Employer's private key
Employer (issuer) signs the credential containing the employee ID
Employer's public key
A verifier (e.g. government body) can confirm the authenticity of the credential and who issued it without contacting the issuer (employer)

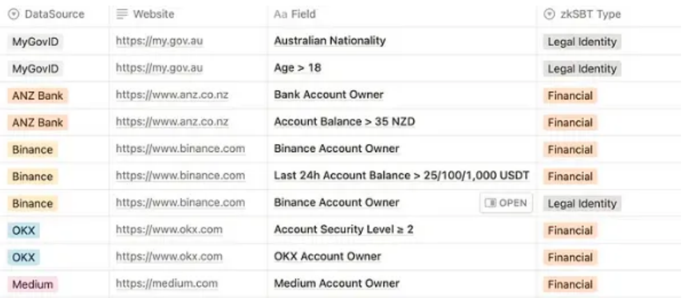
Source: Dock.io

You may have multiple DIDs with segregated identification proofs on each, as you hold separate wallet addresses today. Tools like Dock allow users to hold their identification proofs and authenticate access directly from a mobile app. In this sense, users of blockchain native applications are already accustomed to the flow of signing transactions and verifying the authenticity of an identity request. An alternative approach. An alternative approach to managing segregated forms of identity across wallets is ERC-6551.

Zero-knowledge proofs (ZKP) allow users to prove eligibility without disclosing specifics. Each time I apply for a visa to the UK, I have to provide all my banking transactions for the past quarter. The lack of privacy from a foreign visa administrator going through my banking transactions is not discussed much but it is one of the only ways to get a visa.

Proving you have the funds to travel and return home is a requirement. In a ZKP model, a visa officer could query if a person had a banking balance over a certain threshold for a specific period without seeing all of the person's bank transactions.

This may seem far-fetched, but primitives that do this exist here and now. zkPass's pre-alpha was launched in July of this year, allowing users to provide anonymised personal data (alongside verification documents) to third parties via a Chrome extension.



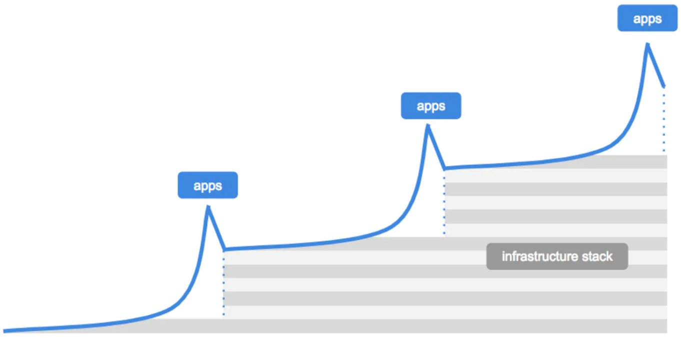
DataSource	Website	Field	zkSBT Type
MyGovID	https://my.gov.au	Australian Nationality	Legal Identity
MyGovID	https://my.gov.au	Age > 18	Legal Identity
ANZ Bank	https://www.anz.co.nz	Bank Account Owner	Financial
ANZ Bank	https://www.anz.co.nz	Account Balance > 35 NZD	Financial
Binance	https://www.binance.com	Binance Account Owner	Financial
Binance	https://www.binance.com	Last 24h Account Balance > 25/100/1,000 USDT	Financial
Binance	https://www.binance.com	Binance Account Owner	Legal Identity
OKX	https://www.okx.com	Account Security Level ≥ 2	Financial
OKX	https://www.okx.com	OKX Account Owner	Financial
Medium	https://medium.com	Medium Account Owner	Financial

A list of data types supported by zkPass' Beta product

The range of application support goes from merely proving your identity via a third-party service provider to proving you have learned specific courses on Coursera. They do not host identity-related documents but query them off websites using HTTPS.

Evolving Infrastructure & Use Cases

I could go on all day about the ecosystem of identity-related applications in Web3. Millions of dollars in venture capital have flown to many developers who have delivered over the past few years. However, we are not building a market map of identity solutions here; I want to focus on what the evolution of these identity primitives means for the internet today. A piece by Dani Grant and Nick Grossman from 2018 on USV's blog gives a good reference for the next phase.



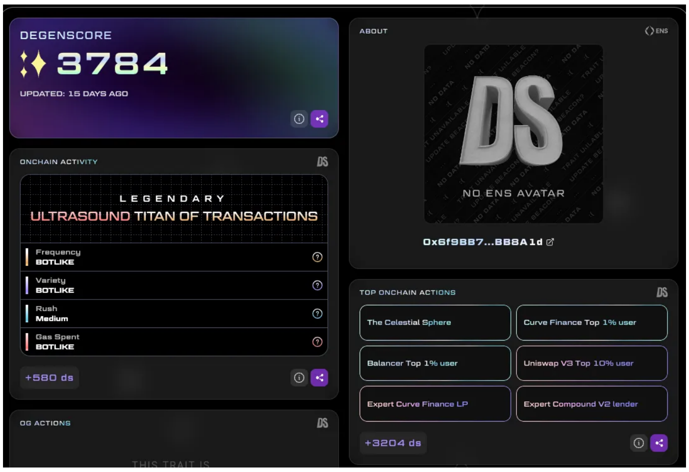
Source: USV

According to them, first comes breakthrough applications requiring better infrastructure. This leads to a point where infrastructure must evolve to support scaling applications. A new generation of applications is then built on this revamped infrastructure layer, and the cycle repeats until a mature market exists – for example, blockchains and NFTs. In 2017, the Ethereum network entirely clogged due to CryptoKitties and came to a standstill.

In 2021, the high price of NFTs justified spending money on NFT transfers. As of 2023, you can send millions of NFTs for less than $100 on Solana, partly explaining why OpenSea has integrated Solana into their product over the years.

Historically, developers had no incentive to tinker with identifying their users. They would have reduced their market size if they had forced users to provide documentation. The law is, in part, what has nudged many developers to implement the identification of users.

Quite recently, Celestia's airdrop for their token, TIA, prohibited persons from the United States from accessing it. The other reason for verifying the identification of users has been to check for Sybil airdrop farmers. In both cases, emergent networks need primitives to prove who is becoming a participant.



DEGENSCORE
3784
UPDATED: 15 DAYS AGO

ONCHAIN ACTIVITY
LEGENDARY
ULTRASOUND TITAN OF TRANSACTIONS
Frequency BOTLIKE
Variety BOTLIKE
Rush Medium
Gas Spent BOTLIKE
+580 ds

OG ACTIONS
THIS TRAIT IS

ABOUT
ENS
NO ENS AVATAR
0x6f9BB7...BB8A1d

TOP ONCHAIN ACTIONS
The Celestial Sphere
Curve Finance Top 1% user
Balancer Top 1% user
Uniswap V3 Top 10% user
Expert Curve Finance LP
Expert Compound V2 lender
+3204 ds

A profile of a user from DegenScore

One of the primitives that has seen substantial adoption in this regard is DegenScore. This product parses a user's historical data to assign them a score. Apps launched on-chain can then enable access to wallets based on the user's score. This strategy restricts people from making hundreds of wallets and attacking emerging products for airdrops.

The product is not an identity verification tool in that it does not check whether or not you have a state-issued document. However, it provides a mechanism for developers to validate if users should have access to their products based on their historical behaviour patterns.

One product that combines off-chain identity with an on-chain wallet is the Gitcoin Passport. This product assigns 'stamps' each time people link a form of identification to their wallet address. The stamps could be given for linking a Facebook account, LinkedIn or Civic ID. Verified credentials are issued from Gitcoin's servers to a person's wallet address. As such, the product uses the Ethereum Attestation Service to bring these stamps online.

What's the point of all this? In Gitcoin's case, it is primarily used for grants. Given that the product matches donations made for public goods, it becomes vital for the product to verify that real users are donating money. The use case for such a product outside Gitcoin is with DAOs. Oftentimes, a single person could split up his or her tokens across thousands of wallets and vote in favour of a decision that benefits them. In such instances, it becomes essential to validate the personhood of a wallet, either through past on-chain behaviour or through linkages with a real-world identity. This is where the Gitcoin Passport is of use.

Naturally, a person will not maintain a single identity in all their applications. It is normal for users to have multiple wallets while using the same product. Consider the number of wallets you may have used with Uniswap. Users also tend to swap wallets depending on the nature of the application they are using.

A separate wallet for gaming, media consumption and trading is not rare. Products like ArcX Analytics combine browser data (like Google Analytics does) with smart contract interaction data from blockchains to help identify users. They primarily target developers wanting to understand the behavioural patterns of their users.

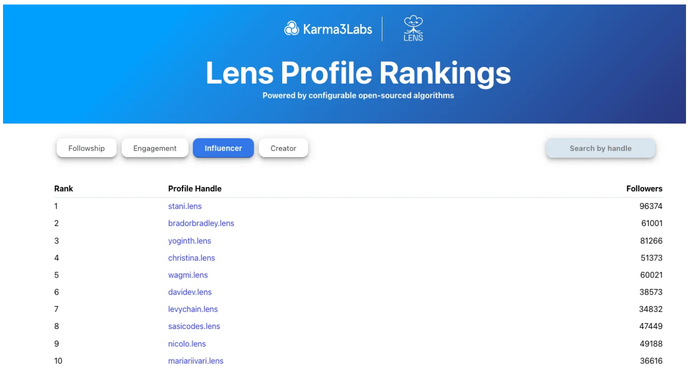
The tools for handling multiple pseudonymous identities have also been evolving in tandem. ReDefined allows users to resolve their e-mail addresses to a certain wallet owned by them. Their API allows developers to create custom resolvers, which means you can have products where a user's phone number resolves to a wallet address.

Why does this matter? It makes building a remittance application like Venmo as easy as a few clicks. A user could upload their contact list (*like one does with Whatsapp*), and a product like ReDeFined could map out all the phone numbers to addresses on-chain.

While writing this piece, I resolved my e-mail address (joel@decentralised.co) to a wallet address. The data on which e-mail is owned by which wallet address is not stored on ReDeFined's servers. They cannot change it without me signing in from my wallet address, as the resolution data (the bits that match an e-mail to a wallet address) is stored on IPFS.

You can link wallet addresses across chains like Bitcoin, Solana or Polygon on ReDeFined. The product checks which asset is being sent by a user and routes the asset to the wallet on a matching chain.

But what if you wanted to identify and rank users across a protocol like Lens? Ranking algorithms for user behaviour have been emerging on Web3 native social networks. In the late 1990s, Google came to be what it is through studying the relative ranking between pages on the internet.



Rank	Profile Handle	Followers
1	stani.lens	96374
2	bradorbradley.lens	61001
3	yoginth.lens	81266
4	christina.lens	51373
5	wagmi.lens	60021
6	davidev.lens	38573
7	levychain.lens	34832
8	sasicodes.lens	47449
9	nicolo.lens	49188
10	mariariivari.lens	36616

From Karma3 ’s ranking page.

Aptly named PageRank, the system gave reputation scores to websites based on how frequently they were mentioned on other websites. Two decades later, as the web has slowly become composable (through Web3 native social networks), we have the same conundrum with wallets. How do you validate a user's "value" on one social network using their activity on a different network? Karma3 solves this.

It helps applications (and users) figure out how to rank a community member within a DAO or see which artist's previous mints were abandoned. As the core unit of identity (the wallet address) is used across protocols, Karma3's product helps rank wallets. So, a user on the Lens Protocol may not have to start from scratch when writing on Mirror.xyz.

Composable ranking gives products a relative advantage to users with high signals on one product when they port over to a different one.

The ability to port reputation has historically not existed on the internet. You could have 100k followers on Twitter, but when you start on Instagram, you start from scratch. This disincentivises large creators from switching over to new social networks. This is partly why, despite their relevance and need, Web3 native social networks have not grown to scale yet. The discovery engines are broken, and the incentives to switch to alternatives do not exist.

In a model using Karma3's products, new social networks do not have to start from scratch when ranking users relatively, solving the cold start problem of attracting good creators early on. Does that mean we will see a multitude of niche-specific social networks emerge? It is well within the realm of possibilities.

So far, we have only talked about individual reputations, specifically about reputation in the context of a person who is active on-chain. But what if you could create composable metadata about firms that could be queried and displayed across outlets? This happens today in a Web2 native fashion. Crunchbase was pulling in details about firms from LinkedIn as early as 2008.

The problem is that nothing stops Crunchbase, in this example, from falsifying data shown by them on a third-party outlet. You can 'trust' the system because, in this hypothetical model, an outlet (like Crunchbase) has every incentive to relay accurate information. However, the corporate entity is not in control.

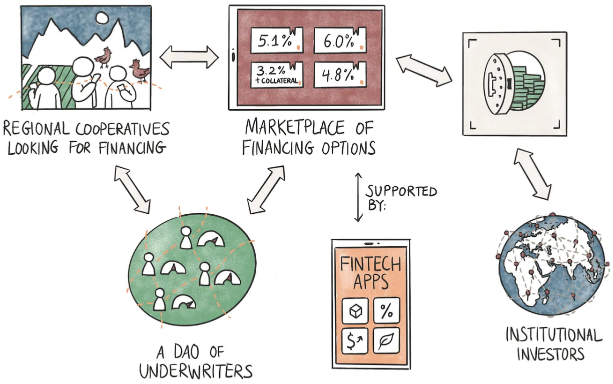
This matters, especially in the context of Web3, as traders often make decisions based on details they find on Messari, CoinGecko or CoinMarketCap. The Grid is creating a network of verifiable credentials for firms. In their model, a firm could use its private key to upload details, such as investors, team members, funds raised, logos and so on, to a sufficiently decentralised network.

Third-party data platforms, such as VCData.site, could query information from The Grid to show it to users. The advantage of such a system is that a firm would not have to go across multiple platforms to update its details. Any time a venture updates its details using verified credentials, it would be reflected on all platforms that query its data.

(*Sidenote: The Grid's founder had previously built a company in the data space and sold it to CB Insights. So I'd like to think he knows what he's doing. Do slide into his DMs on Twitter if the theme interests you).*

Third-party verifiers (like community members) would be incentivised to dispute falsified claims on such a network. It is still theoretical and far-fetched, but the ability to have a unified update on all information related to a venture across all platforms that mention it could be powerful.

But what applications could such reputation primitives enable? A fairly simple instance could be loans in the context of real-world asset (RWA) lending.



The flow above shows what that could look like in practice. Grameen Bank has made a reputation for being the go-to bank for cooperatives in the emerging world. Part of the reason is the social reputation attached to a person defaulting on a loan. Cooperatives, consisting of women engaged with SMEs, take loans directly from the bank and keep a rotating line of credit that grows depending on the frequency of repayments.

In the 1980s, when digital identities were not common, offering credit to the underbanked with no collateral was revolutionary. In the 2020s, the model could evolve with the digital primitives we do have.

In the image shown above, cooperatives could provide their data to underwriters that function as DAOs. This data would primarily involve their banking details, the SME's commercial transactions and similar data points from Web2 native products. Tools like zkPass (referred to above) could anonymise and provide the data to underwriters, who then could assess the creditworthiness of the cooperatives and pass on a risk score to a marketplace.

The marketplace could source liquidity from fintech apps or institutional investors looking to generate yields on their idle assets. There are two ways this could work:

1. A fintech app could directly offer loans to cooperatives with credit scores passed on by an external under-writer.
2. An aggregator (or marketplace) could source liquidity from third-party fintech apps or institutional investors and offer loans on basis of the credit scores provided by an underwriter.

In both instances, cryptographic primitives could be used to ensure the privacy for data provided by borrowers. A DAO, run by multiple underwriters, could help facilitate loans faster than a traditional entity if multiple individuals are racing to assess the risks. Lastly, one could presume that using blockchain rails to source liquidity from global markets could translate to better interest rates for borrowers. Our friends at Qiro have been tinkering with such a model.

While the money flow could vary, the 'core' difference is how the underwriting is done and how that score is passed to marketplaces. A cooperative seeking a loan would have to provide their details only once, and they would have the right to protect their personal banking details from third parties that should not have access to them.

Naturally, this is not a crypto product. It is a fintech primitive that uses blockchain technology. The blurring of lines between the two has not historically happened due to regulatory restrictions and the lack of identification on the internet. The nature of applications that can be built on-chain will grow exponentially in sophistication and adoption as the primitives we use to track and identify users evolve.

There are two clear cases where this blurring of lines is already happening. First, with Paypal's integration of stablecoins in the product. Secondly, with MoneyGram releasing a native wallet in their product. We don't entirely know what kind of fintech applications could be built as the next hundreds of millions of users come on-chain.

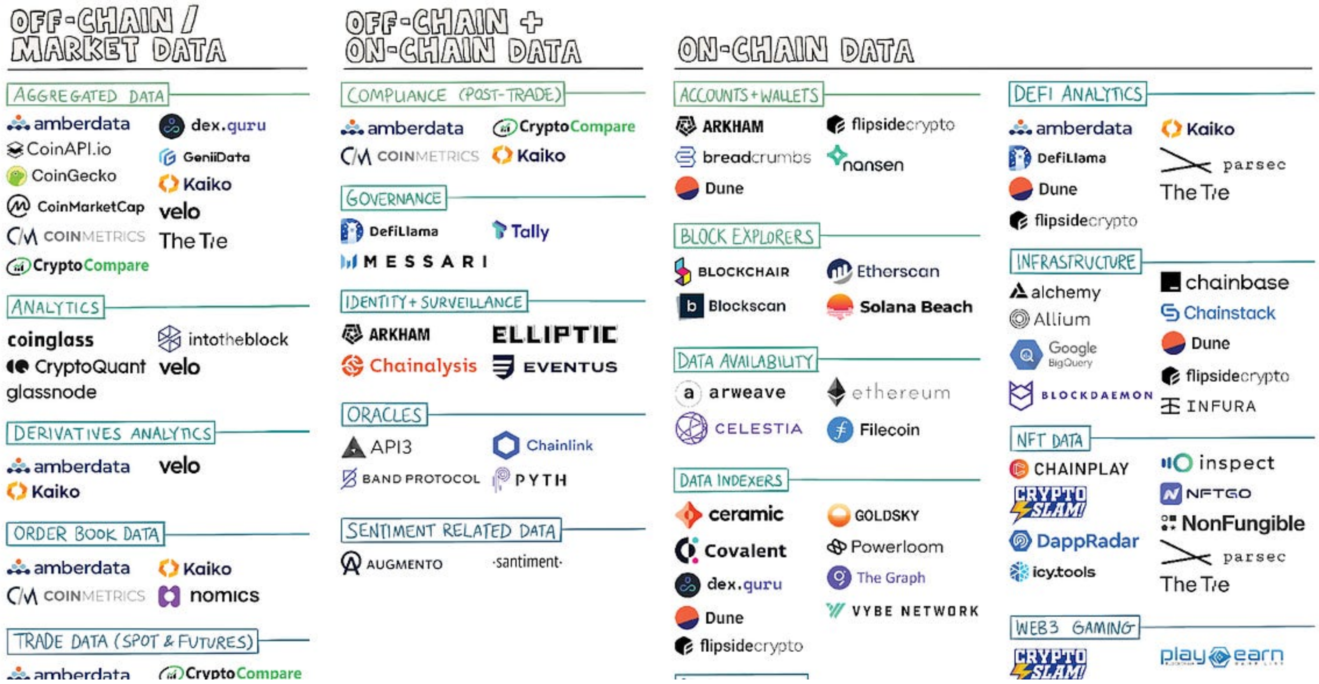
Can't Be Evil

Alexa, play country roads, take me home.

Saurabh
decentralised.co

Mapping The Data Landscape

From Telegraphs to subgraphs.



Today, we updated VCData.site with 350+ funding rounds data from the past quarter. If you are a founder raising in the market, use it as a reference to identify active investors.

Fill out the form below to get in touch with the team if you are building cool things in the current market environment.

The newsletter may break on some email clients due to its length. Click on the view online button in the top right corner to read it directly on the website.

**faster, easier
crypto data**

<v>

Last week, Kraken sunsetted one of the most beautiful products in crypto for tracking price. RIP Cryptowat.ch.

We have been using an alternative that looks prettier and covers more data points. Today's article is written in collaboration with the team behind Velo Data.

Velo Data has slowly become a permanent bookmark in the browsers of the best investors in crypto. Take a look at their product here to understand why. They are also offering free trials to their API if you'd like to be early.

Hey there,

We had written a pre-cursor to this piece on July 18th if you'd like context that goes beyond what's written here.

All living things keep some record. Animals track seasons to understand when to hunt. Rodents and birds store food in unique places. They need to remember where they stored it when accessing it for sustenance months later. Wolves create marks around the perimeter of their territory to signal other animals to keep out. Even trees keep track of time. Every year, a ring is formed in trunks. One can estimate a tree's age based on the number of rings.

Although trees and animals keep track of time, they cannot retrieve or narrate the past. They don't have access to memory. It is what makes human recordkeeping different. Thanks to our communication abilities, we know that Sumerians in Mesopotamia (*3400 BCE*) and ancient Egyptians (*3200 BCE*) used cuneiform writing and hieroglyphics to record information.

Humanity evolved when knowledge could be passed on without requiring the source to be physically involved. We read and enjoy the works of Plato or Socrates long after they are gone because we have the means to store their teachings. Writing was the original AR platform.

Writing from Iran keeping track of grain. Source: *Link*

Where writing left things to the imagination, data helped keep things objective. It reduced the requirement for individuals to store things in their memory. This is partly why some of the oldest human texts involve debt, income, or trade records.

Going Digital

In the post-industrial age, firms built competitive moats to strengthen their market position by going digital with their sales records. One example of this is an Indian company called Asian Paints. Their paint might not be the best in the market, but they control a 50%+ market share of India's $8 billion paint industry.

Why? The easy answer is that it is a household brand, and the company has economies of scale. But how they got there has roots in data. They invested heavily in data collection and processing to optimize their supply chain.

For context, the Asian Paints stock has had a staggering CAGR of 25% over the last 30 years. Backing that growth was an investment in a mainframe computer in the 1970s. The device was more powerful than the ones used at the best research organisations in India at the time. It collected hourly data about the colour and quantity of paint sold across India. This allowed Asian Paints to build a model that predicts paint demand throughout India with 98% accuracy.

This predictive power allowed Asian Paints to capture maximum value, as it could drastically reduce its replenishment time. At the time, the norm for selling goods like paints was to sell it to a wholesaler, who then gave it to a distributor, who would, in turn, sell it to a dealer. The dealer would interact directly with the consumer. The reason for such a complex supply chain was that each party held an inventory of assets and controlled data on the supply and demand for paint.

Mr Choksey - the founder of Asian paints, removed wholesalers and distributors from the supply chain by studying the consumption patterns of the end user and reducing reliance on the middlemen. Through removing the middlemen, Asian Paints captured 97% of the MRP (*3% to dealers)* compared to the 60% captured by their competitors.

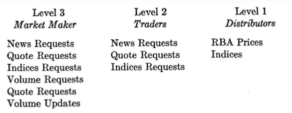
Telegraph extractable value would be frontrunning ticker tapes relayed over the Telegraph.

The transition to digital did not happen overnight. Part of what made data collection interesting was the world of finance and how interconnected it had slowly become. For instance, in the late 20th century, stock market data was relayed over the telegraph using devices like the one above. As early as 1835, traders would train pigeons to carry bits of paper with information about what was happening in Europe. When steamboats carrying goods came within 50 miles of land, the pigeons would fly to designated spots with the information. Traders used to pay up to $500 for each hour in advance they could get the news.

By 1867, traders began competing to optimise how fast information was relayed through the telegraph. A Western Union Employee named E. A Calahan paid over $200k to the NYSE for the ability to send employees on their trading floor to relay ticker data to his clients. One of the individuals working diligently on optimising the system was a young scientist named Thomas Alva Edison. A century later, tools like the Bloomberg terminal would exponentially scale the pace and amount of financial data relayed on any given day.

Moulding Raw Data

Data, like crude oil, has to undergo several steps of refinement before it can be used. Learning how Bloomberg grew sheds light on how the whole data landscape evolved and which process. Bloomberg was not the first attempt to use technology to improve trading and reporting mechanisms. NASDAQ used Bunker Ramo terminals to disseminate information and place bid/ask orders. However, relying on erstwhile telephone communication networks meant that scaling this model would always be challenging.



Level 3 *Market Maker*	Level 2 *Traders*	Level 1 *Distributors*
News Requests Quote Requests Indices Requests Volume Requests Quote Requests Volume Updates	News Requests Quote Requests Indices Requests	RBA Prices Indices

Figure 1—NASDAQ services Levels 1, 2, and 3

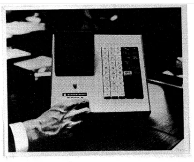


Figure 2—Bunker Ramo Level 1 terminal

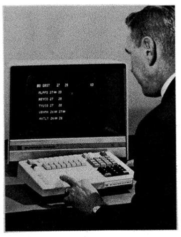
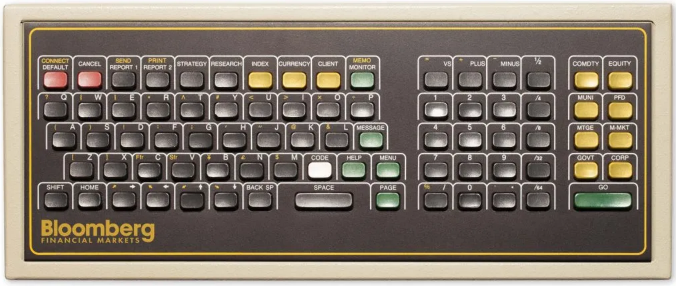


Figure 3—NASDAQ Level 2 and Level 3 terminal

Source – NASDAQ – The Evolution of Automated OTC Trading

In 1981, Michael Bloomberg, a partner at the investment bank Solomon Brothers, got fired with $10 million for his equity when Phibro Corporation acquired the bank. He realised that investors are ready to pay for streamlined financial information with the growing electronification of financial markets from New York to Japan. He started a data services company called Innovative Market System, which was rechristened to Bloomberg in 1986.

Before the internet took off, the Bloomberg Terminal was accessed using The Chiclet. This was connected to the Bloomberg controller via a special cable connected to the local hub via dedicated telephone lines. Bloomberg collected data via data partnerships, news agencies and press releases, proprietary methods like manual data entry and phone-based data collection.



With the internet, the information floodgates opened. Today, Bloomberg procures, processes, and delivers 200 billion pieces of financial information in almost real-time. That is approximately 23 million data points per second. Some of the information available on Bloomberg is public. Data points like companies' financial statements and stock and bond prices can be found on public forums.

But what if you are an oil and gas analyst and want to understand the movement of crude oil containers? You are unlikely to get this information in real-time if you don't subscribe to a data source like Bloomberg. Not all the data on the internet is freely available.

There are typically two constraints for individuals when it comes to data in Web2: permissioned access and a high barrier to processing large amounts of data. Over the years, providers like Bloomberg have built strong enough network effects to source data through their affiliates, which analysts or investors cannot afford to do.

It is better to pay $20,000 to Bloomberg for an annual subscription than to try to source the data from a mix of data platforms that may each have varying pricing tiers. Even if you grind hard enough to get your hands on the data, you cannot process and run analytics in real time without significant infrastructure spending. On the retail end, many platforms that eventually scaled - were data-matching engines.

Think of it this way: Google (*the search engine*) is a data company that offers businesses access to users in exchange for ad dollars. When a restaurant or a newsletter (*like ours*) wishes to target users searching for information on Google, they match supply and demand for similar information. Somebody searching for information on a newsletter specific to Web3 is looking for us. And we are looking for that person. *(I am resisting the urge to plug our referral programme here.)*

Google built a monopoly due to the economy of scale it functions in. Their inventory of users and the number of queries their users make each day remain unrivaled. Google built that position by launching a search engine that had no ads at a time when advertisements were the norm, then through acquiring YouTube and Android, and eventually, through paying peers like Apple to make Google the default search engine. For Apple alone, Google pays $20 billion a year to remain the default search engine on Safari.

Google pays that premium because, at its core, its offering is a matching engine. The matching engine puts users with a need in touch with businesses that have an offering. Most of the web's monopolies are, at their core, matching engines. Amazon matches product sellers with buyers. Instagram matches an audience with creators. These matching engines work because interactions on these products leave rich trails from which context can be driven.

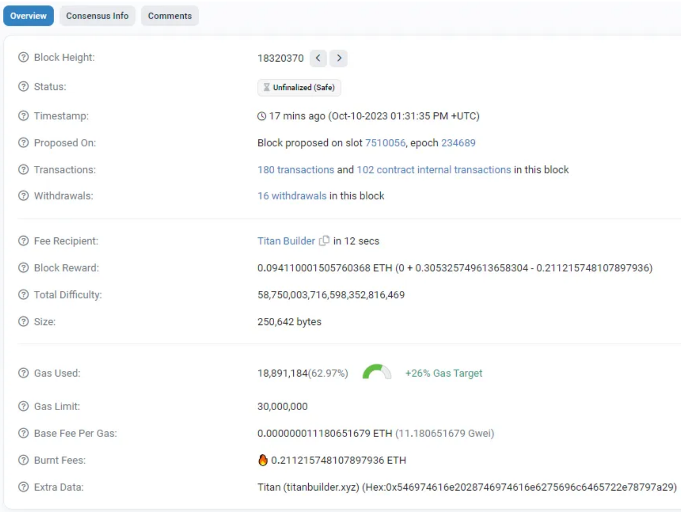
Ben Evans famously wrote in 2022 that there is no such thing as data. Knowing my content, food, or travel preferences is not worth much to a third party. It becomes valuable – for commerce or research – only when it is aggregated or enriched with context.

Context in the sense that my preferences for eating biriyani on a Friday night could be used to advertise biriyani delivery to me precisely when the probability of me buying it is the highest. In the aggregate, comparing the probability of my purchasing with a peer in the same region helps target users better.

Data needs either scale (*in large numbers*) or context to be valuable. Where Web3 and Web2 products have historically differed is in the trails they leave. Only Amazon knows how many Xbox controllers would sell in a given week. But you can see the patterns in which traders buy or sell NFTs on OpenSea on any day. The reason is that each of those transactions leaves a public trail.

Data products in Web3 use those trails to build context.

Blockchains like Ethereum and Bitcoin produce blocks every 12 seconds and ~10 minutes, respectively. Every block contains transactions that change the state of the blockchain. Block explorers like Etherscan capture data related to all the transactions. For example, if you go to Etherscan and see a block, the image below is what you may see.



Overview | Consensus Info | Comments

Block Height:	18320370
Status:	Unfinalized (Safe)
Timestamp:	17 mins ago (Oct-10-2023 01:31:35 PM +UTC)
Proposed On:	Block proposed on slot 7510056, epoch 234689
Transactions:	180 transactions and 102 contract internal transactions in this block
Withdrawals:	16 withdrawals in this block
Fee Recipient:	Titan Builder in 12 secs
Block Reward:	0.094110001505760368 ETH (0 + 0.305325749613658304 - 0.211215748107897936)
Total Difficulty:	58,750,003,716,598,352,816,469
Size:	250,642 bytes
Gas Used:	18,891,184(62.97%) +26% Gas Target
Gas Limit:	30,000,000
Base Fee Per Gas:	0.000000011180651679 ETH (11.180651679 Gwei)
Burnt Fees:	🔥 0.211215748107897936 ETH
Extra Data:	Titan (titanbuilder.xyz) (Hex:0x546974616e202874697461 6e6275696c6465722e78797a29)

Transactions on the blockchain are rich in context. Products like Arkham and Nansen are interpretation engines for researchers to understand what is going on when a transaction occurs.

You can view all the blocks since Ethereum started. But what can you do with this information? Almost nothing. So, you need a way to capture this data in several tables. For example, whenever an NFT contract of a marketplace gets called in a block, the data related to that transaction should be appended to NFT-related tables, or when a Uniswap contract gets called, the related data should be stored in DEX-related tables. (*Dune does this as a service.*)

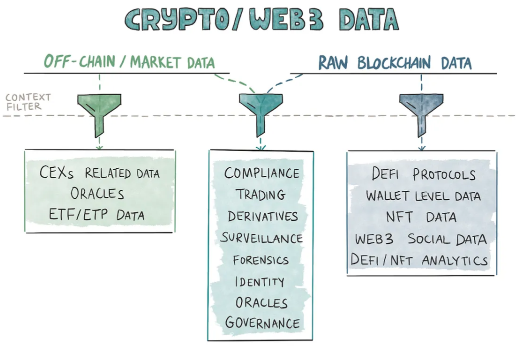
You cannot analyse the raw data without incurring significant infrastructure costs. So, although the data is freely available, you run into the same problems. You rely on external data as an investor or a dApp builder. But your core function is not related to gathering and managing data. Expending resources on essential but non-core activities is not a luxury every organisation can enjoy.

Context Drives Value

For data products, the context around data makes the product unique. Bloomberg applies its financial understanding and transforms data into a form that inventors and traders can easily consume. Websites like Similarweb or research publications like Newzoo use their core competencies to apply social- or gaming-related context to the data they track.

Blockchain native data products differentiate themselves by providing user context through queries that answer questions relevant to specific user subsets. For instance, TokenTerminal computes the economic fundamentals of protocols. Nansen helps market participants label and understand the movement of assets. Parsec queries on-chain data to help traders better analyse DeFi positions.

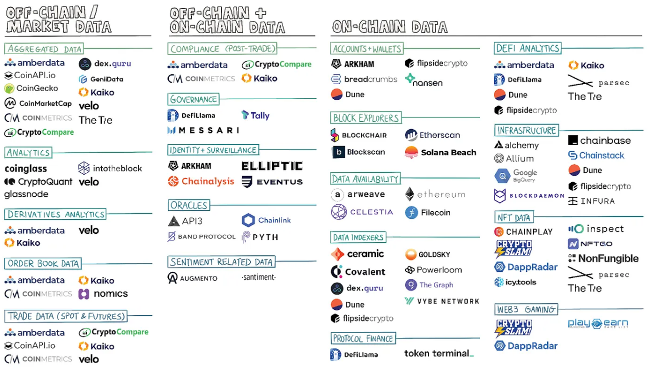
All of these products run off a public good: on-chain data. The difference is how these products present their data, which makes them appealing to different audiences.



The product category split in our industry is based on what data goes on-chain and what information is derived from off-chain sources. (S*ome often use both.*) Data providers use their context filters to create products. Just as Web2 data has its niches, Web3 data companies have built or are gradually building moats using their core competencies.

As such, the founders' backgrounds often dictate the nature of the products released. When a core team has spent significant time in capital markets before crypto, their products tend to imitate Bloomberg, whereas crypto native products look like Nansen. Different products cater to different needs, even when querying off the same data.

For instance, exchanges typically discard data after fixed intervals. They are not in the data business, and storing old data demands additional servers and management. Some data providers, like Kaiko and Amberdata, maintain historical order book data from exchanges. Such data allows traders and investors to build models to test their hypotheses. But if you want to understand which DeFi contracts are getting flushed with an inflow of ETH or stablecoins or analyse the on-chain behaviour of specific addresses or entities, you will need a product by Nansen or Arkham.



Market-map is not representative of every player in every category.

One way to understand how products have been positioned in the markets is through the lens of consumer personas in crypto. These personas can be classified into the following four key categories.

Financial Institutions

Most dollars flowing through crypto-data products come from financial institutions during a bear market. These are big-ticket customers with longer sales cycles and far more complex data requirements. One way to know if a product is oriented towards financial institutions is if a customer must undergo a sales call to determine how much it costs. In the Web2 world, you cannot find how much PitchBook or CB Insights costs. In crypto, you don't know what a product like Chainalysis would cost.

Jokes aside, part of the reason for such a sales process is the hands-on, white-glove service offered by data products oriented toward this consumer segment. These users usually opt for highly granular and frequent data. They require data not only for pre-trade decisions but also for post-trade uses to fulfill compliance and taxation requirements.

For example, they need products that tell them what their portfolio value was historically, help them with tax calculations, and so on. Firms like Amberdata, Kaiko, CoinMetrics, CryptoCompare, and, to an extent, Nansen, serve these customers.

In my experience, only founders with backgrounds working in institutions or teams with large funding rounds have been able to crack open the institutional market for data. The barrier to entry is relatively high here, as would be the case with any enterprise product.

Developers

We often come across the composability feature of Web3, which means that Web3 applications can be interdependent. They could require data from one another. So, they constantly need to read data from each other. For example, a platform like Yearn Finance needs to read data from Aave and Compound, and an NFT aggregator like Tensor needs to read data from Magic Eden and other marketplaces.

But this data is stored across blocks on chains like Ethereum and Solana. Ethereum creates a block in 12 seconds, and Solana does it in 400 ms. Sorting blockchain data into tables and storing it for quick access is a non-trivial task. This is where indexers like Covalent, Graph, Chainlink, and Powerloom come into the picture. They ensure that raw blockchain data is stored in a desired format so developers can fetch it via simple API calls.

An emergent segment in this consumer persona involves tools used to understand user behaviour. For instance, ARCx allows developers to map out off-chain data (like browser behaviour) with on-chain data (like wallet addresses) to capture the demographic information of users interacting with a dApp. They are in a relatively small but relevant niche as they help developers identify who their users are.

Researchers and Publications

Data products in crypto often find distribution by collaborating with researchers and publications. CCData, for instance, is often cited on Bloomberg. Researchers are incentivised to lean back on data products as they help save time and effort when collecting, cleaning, or curating data. Products like Dune have built a moat by building a community of analysts who compete with one another to rank higher on their list.

Publications like *The Block* and *Delphi* showcase dashboards built using data from third-party providers. Here at Decentralised.co, we rely entirely on external data providers as they help keep the team lean whilst using external resources when collecting data.

The challenge with catering to this consumer segment is that smaller researchers may not have the required budget to justify spending tremendous resources to surface niche insights that may be relevant only to a single person. Conversely, firms are well incentivised to spend effort and resources partnering with significant publications like the *Financial Times* as it helps with distribution.

Retail investors

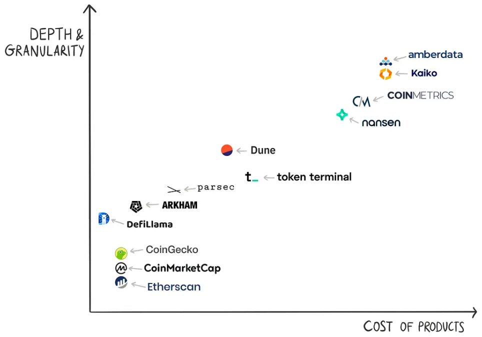
Products oriented towards retail investors usually have lower granularity and frequency of data. But they are highly profitable niches to build in as they see economies of scale. Ten thousand users paying $100 each is a $1-million ARR business in a world where churn does not exist. It is easier said than done, but those economics explain why we have so many retail-oriented crypto-data products.

A large chunk of retail-oriented products are free or supported by ads. For example, a free resource like DefiLlama will not tell you how you can route your order via different exchanges (CEXs and DEXs) to avoid slippage as it does not take order book snapshots, but it showcases information about token unlocks or yield unlocks.

One change in this consumer segment is how the delivery medium opens up a new market category—for instance, Cielo delivers data as notifications through Telegram. It has scaled to over 40,000 users by relaying information in an easy-to-consume fashion for a consumer segment that would rather not deal with desktop interfaces. When done right, even distribution mediums can be differentiators for early-stage ventures. Even in data.

Although the classification blurs at points, data firms can be split into B2B or B2C orientations.

Companies like Amberdata and Kaiko have products that cater to sophisticated actors. These products are more granular (*details in which the data are available*) and frequent (*e.g. tick-by-tick and real-time order book data*), and they satisfy demands like building and testing models, pre-trade analysis, post-trade reporting, taxation, and compliance. Data is provided in a format that allows customers to carry out proprietary analyses and build visualisations to their tastes. These companies typically offer their products behind a paywall.



Cost is generally a function of granularity due to infrastructure requirements, the nature of the clientele involved, and the length of the sales cycle.

The image above maps different products on two axes – depth and granularity vs. prices of products. Please note that these plots are not exact. A few points may be misplaced. The idea is to develop a mental model to think through several products and their standing in the market.

Retail-focused products like Dune or CoinGecko display almost all the data for free. Customers must pay to access some data or if they want data via APIs for running their analyses. For example, you can view all the charts created by several Dune wizards, but they limit how many rows you can download in CSV form. You can download larger CSV files and view private queries as you pay more.

Retail-focused companies tend to have low revenue per customer and few paying customers as a percentage of free users. Compare this with conversion rates for the freemium models of internet companies. Typically, the conversion rate is 2%–5%. A 10% conversion rate would be an outlier. Their playbook is to have as many free customers as possible so that a 4% conversion rate significantly contributes to the revenue. This is what we call the top of the funnel.

So data companies need the top of the funnel to be large enough to generate enough revenue to sustain themselves at a lower conversion rate. Companies can also consider generating revenue from advertisements when the site has many visitors. CoinGecko uses ad revenue as leverage to keep providing most of the data for free.

Over the years, companies have filled spots on both ends of the (*B2B and B2C*) spectrum, leaving some gaps in between. If someone wants to see how order books are changing across centralised exchanges or how the put call ratios, IVs, and skews are changing, there aren't many products that help with visualisations. There is space for a more granular product than the CoinGeckos of the world but less granular than products by pure B2B players.

On Moats

Finding moats in businesses where the raw material is free is not easy. Blockchain data is freely available. There's nothing proprietary in what data you can gather. So, the moats in data businesses are not just based on you having some data that others don't. Instead, they are based on a team's ability to furnish the data in an insightful, consumable format, on time, and without errors.

Many companies claim to have the same data, but the data quality and its presentation differ. For example, many companies claim to have off-chain order book data. However, factors like the number of bid/ask orders, time series length, and the number of available exchanges and pairs differ from provider to provider. Amberdata and Kaiko have the most comprehensive order book data for crypto markets.

Why, though, can only a few providers provide this kind of data? The explanation for where moats emerge in Web3 data lies here.

Talent – At the risk of stating the obvious, when the raw material is free, how you mould it determines the worth of the product. Turning raw data into useful information requires domain expertise in many niches within crypto and traditional financial markets. Teams like Velo Data, with experience in traditional markets, have an edge over others trying to build similar B2C products. Finding talented developers who understand blockchain data structures and have relevant experience in financial markets is rare.

Infrastructure – Collecting and delivering large amounts of data requires infrastructure that doesn't come easily. This kind of operation requires capital and talent. Why is infrastructure a moat? Think of memory pool data. Blocks contain data for confirmed transactions. What about unconfirmed transactions?

Different network nodes *(for example, nodes connected to the same pool*) see different unconfirmed transactions. Running just one node will not give a global view of competing transactions. Maintaining multiple nodes on several blockchains adds to infrastructure costs. Much like with AI *(and content networks in the past)*, the ability to keep hardware costs low whilst scaling will determine the winners and losers in the sector over time.

Network Effects –One can hypothesise that network effects exist in many crypto data products. Take Chainlink as an example. It was one of the first oracles that allowed applications to read data from other applications or chains. It managed to garner the community's support and has one of the strongest communities. Another example is Nansen. Its claim to fame was address labels that allowed it to attribute asset movement to real entities instead of hexanumeric addresses.

Subsequently, it launched features like NFT Paradise and Token God Mode, allowing users to track NFTs and tokens more effectively. Arkham launched a product similar to Nansen's labels, but investment in dashboards and research allowed Nansen to manoeuvre towards enterprise clients and offer products tailored for them. It is worth mentioning that network effects are not possible without the first two points (talent and infrastructure).

One place this works is with indexers. The higher the number of chains a product supports, the higher the probability that a developer would use the product instead of relying on multiple sources. Teams like Covalent have an edge here as they have been optimising the breadth of chains supported for quite some time. But do remember that depth is as important as breadth.

It is too early to say whether any product has a meaningful moat in crypto. We have witnessed early-mover advantages in the grand scheme of things. As categories like Web3 social and the overlap between AI and crypto continue to scale, data products in the industry may grow to be the next Alphabet. But that will be a multi-decade story; we are still in its early years.

Beyond Speculation

Many of the use cases we mentioned for this article look at financial speculation in some form or another. Even the developers using APIs to query data are building financial products. It may seem odd, but blockchains (*as a new network*) follow the same trend the Telegraph and the Internet did.

The arrival of a new medium and the emergence of a new network accelerates financial use cases. With the internet, it took until the early 2000s for people to realise that users could be targeted based on their location. With blockchains, we are still figuring out how to build business models off publicly available data trails.

We have seen one key change in our day-to-day use of these platforms - Dune Analytics embedding AI in their product. Dune provides an SQL-based interface for users to query data off blockchains like Ethereum and Solana. The market for such a product is usually restricted to users who understand how to write SQL queries. They recently began using AI to help analysts generate queries without being SQL experts. It is not as functional as one would hope it to be. But it still is a step towards the future. It may not be long before we ask AI (*like ChatGPT*) to query data off a blockchain and offer its analysis.

One way to think of "data" in the context of Web3 is through the lens of Google Maps. GPS has been around since at least the 1980s. Google put in the work needed to map out the world. In making the overlays for maps available for third-party apps (using APIs), the firm enabled a new generation of applications to be built. Everything from delivery to ride-hailing boomed because a single player specialising in data took on that burden from developers.

Data products in Web3 stand to play a similar role. We don't yet know the exact nature of applications that could be built atop this publicly available resource, but it is becoming apparent that there is an Alphabet-sized opportunity within the data landscape.

Signing off,
Saurabh Deshpande

P.S.- Pressing the like button below helps us with discovery on Substack. I'd appreciate one if you enjoyed reading this.

Disclosures

1. *Founders at Decentralised.co hold exposure to Nansen, Covalent and BitsCrunch.*
2. *Commercial relationships between Velo Data and Decentralised.co go beyond the scope of collaborating on this article.*
3. *We continue to build exposure within data markets as a theme through tokens and equity.*
4. *None of this is investment advice.*

Joel John
decentralised.co

The Royalty Wars

Blurring fee lines.

ASSET MONEY

Today's piece explores how royalties in the NFT markets trend to the lowest possible amount. We have seen Asset.money build a portfolio management app over the months in our community and had the pleasure of collaborating with them for this piece.

*NFT markets in their current form are a lot like the internet before Google. You invest, track and hold portfolios on a mix of apps. If you hold these primitives on multiple chains, you must also maintain wallets on each chain. Asset.money brings it all under a single roof, so you can worry less about losing your assets to hacks and rug pulls. Take it for a **spin here.***

Hey there!

Whenever I reflect on our economy and society, I often realize how similar it is to a large biosystem with small interdependent actors: Workers, small and medium enterprises, banks, customers, and regulators are all individual components of this global organism. When a business (or employee) no longer serves the purpose of the overall system, it is made redundant – either through competition, under-resourcing, or self-interest. For instance, a rational actor who believes their venture or effort is bound to fail would shut it down. This is the definition of self-interest.

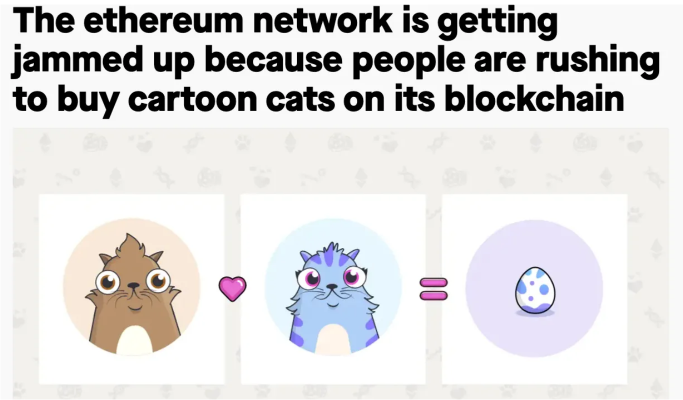
Of course, my idea that markets and evolution have much in common is nothing new. Before Adam Smith's writings on the economy inspired me, they motivated Darwin to become a naturalist and redefine modern biology. I would have loved to nerd out with them about the similarities of how markets and ecological systems evolve! But our time machine remains broken, so that is not what we will do today.

Instead, today's piece is co-authored with Siddharth, who has been nerding out about the future of NFT markets – specifically about an ongoing battle to determine how royalties will be structured for creators in the months to come. But before we do that, let's start by going back a few years.

Gem of a Memory

The year is 2019. We are in the middle of a cold winter. The bear markets made the masses abandon almost all crypto. Not even the nice girl you matched with on Bumble cares about your Bitcoin anymore. DeFi is this weird thing finance nerds did once in an obscure corner of the world wide web. People are excited about getting magical internet money loans for their useless digital tokens. So-called Simple Agreements for Future Tokens (SAFTs) is the most common form of NFTs; these are investment contracts venture capitalists (VCs) invested in with hopes of getting more tokens down the line.

But most founders keep pushing off their token launches, and VCs pretend they want to continue building with the founders while trying to find an OTC buyer for the token agreement. The only meaningful NFT collection people know is a collection of cats that repeatedly clogs the Ethereum network. How fun. The consultants that came in hordes with enterprise and government use cases faded away. People no longer think putting land records on a blockchain is a good idea. And decentralised Uber is nowhere to be seen



The ethereum network is getting jammed up because people are rushing to buy cartoon cats on its blockchain

Cryptokitties were one of the earliest NFT primitives that captured public pysche. Source : Quartz

If you were an NFT marketplace in 2019, you had a real problem. You see, tokens had product market fit thanks to the initial coin offering (ICO) boom of 2017. At that time, users had become used to transferring, trading, and losing their crypto in hacks. But NFTs? Only an isolated group of Silicon Valley bros were talking about them. Even hardcore crypto folks barely bothered with this non-fungible nonsense.

In the physical world, an artist sold a piece of work and made money from it only once. So their earnings were linear, and the artist had to keep producing art to make a living. NFTs allowed art to evolve into financial assets that accrued value for the creator whenever a person traded their art.

How does that work? This is the magical concept of royalties. Let me explain with an example for those that don't follow the NFT markets closely. Assume you purchase an image of a pizza from a guy for $100. The artist makes $100 once. By some draw of luck, a hedge fund manager visits your office tomorrow and decides the beautifully painted pizza is worth $1000. You sell it to the manager for a profit of $900. The artist makes nothing.

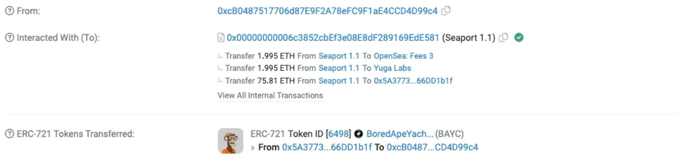
If tomorrow, a friend of the hedge fund manager (*who happens to make a killing speculating on crypto*) notices the work, feels it is now worth $1 million and buys it, the artist gets nothing. Neither do you. Well, you probably get tons of remorse for undervaluing your past asset. But you can't pay the bills with remorse.

Royalties allow a portion of every trade on a piece of work to be transferred back to the artist. This is usually anywhere between 3% to 5%. If tens of thousands of NFTs are released in a new collection, the royalty sum is large enough to support entire teams. There will be hundreds of trades daily thanks to constant speculation on where the price will go. We already see this type of trading behaviour in stock markets. The pizza artist above would have made $50,000 on that million-dollar trade... if he had made it an NFT that pays out creator royalties.

Before you think, *"Oh, this sounds like a classic pyramid scheme,"* explain why it is not. Only the artist earns royalties. The traders in the middle don't earn anything other than the difference in the asset's price. This makes me think it's a good example of the greater fool theory, but I digress.

Over the last few years, this incentive has driven a huge part of the NFT market. We are talking hundreds of millions of dollars in revenue. Yuga Labs (*the creators of Bored Ape Yacht Club*) alone made $107 million in revenue last year.

Consider the image below to see an example of a transfer:



From: 0xcB0487517706d87E9F2A78eFC9F1aE4CCD4D99c4

Interacted With (To): 0x00000000006c3852cbEf3e08E8dF289169EdE581 (Seaport 1.1)

∟ Transfer 1.995 ETH From Seaport 1.1 To OpenSea: Fees 3

∟ Transfer 1.995 ETH From Seaport 1.1 To Yuga Labs

∟ Transfer 75.81 ETH From Seaport 1.1 To 0x5A3773...66DD1b1f

View All Internal Transactions

ERC-721 Tokens Transferred: ERC-721 Token ID [6498] BoredApeYach... (BAYC)

From 0x5A3773...66DD1b1f To 0xcB0487...CD4D99c4

Image sourced from Etherscan

Notice the breakdown of fees above? OpenSea made ~2 ETH, and Yuga Labs made ~2 ETH by selling a Bored Ape NFT for ~80 ETH. Not even a monkey would find that level of recurring revenue boring! The buyer who spent $140,000 for the JPEG of a monkey is (possibly) not buying it for the art alone. There is likely a motive for profit or a desire to speculate on the underlying value. So they are spending money today to sell and turn a profit tomorrow. Everybody's happy as they all stand to benefit beneficially. Until the market decides to evolve.

OpenSea's genius drove the idea that NFTs can enforce royalties and empower creators. Everybody loves empowerment. It is not rational behaviour to argue against someone making a livelihood where there existed none. But here's the problem. NFTs cannot pass on royalties to the end user on their own.

Usually, smart contracts set up by a marketplace like OpenSea pass on the royalty. Why? Because it is impossible to discern a simple transfer from a trade. If 5% were charged on every transfer, users would be dissuaded from simply moving their precious NFTs to a cold storage wallet. So the royalties are generally collected by the marketplace enabling the trade.

But what do you do if a marketplace does not want to enforce royalties to make trading cheaper for users? That is the crux of the problem plaguing the world of NFTs today.

Blurry in the Open Sea

2022 was the year of mutations for the NFT market. Sufficient liquidity and fees incentivised markets to experiment with alternative models. It all started in January when LooksRare released its token. The value proposition was simple. Users would receive tokens in exchange for trading on the platform.

Instead of burning money to build a brand, run ads, and educate users, users could dedicate tokens to govern the platform and receive fees as token holders. There was also a liquid market for the token. At the time, I wrote about the game theory of the platform on Tokenised Marketplaces.

> “*Each of these traders is required to pay 2% to the platform and anywhere between 5% to 10% in royalty to the artist. Effectively, wash traders are doing on the platform to acquire assets at a discount to the spot market.*
>
> *If the platform fee + royalty paid is higher than the price of the tokens rewarded, users will have no incentive to continue trading on the platform.*
>
> *You may think that is dumb, but LooksRare has done ~$11 billion in volume and $220 million in revenue with a fraction of the users OpenSea currently has.*”

At the time, LooksRare captured mindshare because it had a liquid token and OpenSea did not. LooksRare, even had an inferior product at the time. You could barely sort NFTs by price on LooksRare when they launched. Over the year – thanks to the bear market and declining token rewards – the product struggled to build a moat against OpenSea truly.

Management at OpenSea likely realised the threat new-age platforms posed to the firm's monopoly, and it acquired Gem a few months later. At the time of acquisition, Gem was one of the fastest-growing aggregators in the market.

The market had experimented with tokens at this point. It had become common knowledge that incentivising users with tokens to trade on your platform could help improve metrics. But there was one more lever to tinker with: creator fees. Over the year, multiple exchanges began chipping away at creator fees.

DeFi markets provided primitives for the same. SudoSwap, for instance, made it possible to set up pools for NFTs the way it's done in Uniswap. Users could buy into or sell large numbers of a particular NFT by trading against a pool. The platform fees were reduced to 0.5% to be competitive against major players like OpenSea.

Let's say you are a trader looking to buy a Bored Ape NFT like the one we discussed in the transfer above. If you can eradicate the 2 ETH paid to the creator and reduce the 2 ETH paid to the platform, traders will be incentivised to move towards you.

And that is exactly what happened.

An NFT could cost 5% less in certain marketplaces outside of OpenSea. This was a massive cost reduction. All of a sudden, the historic royalty model involving empowering artists collapsed. The dream was broken. And so was the narrative.

The big daddy of the NFT world was fine despite this. Nobody saw the threat from a few hundred traders and their volume, much of which comprised wash trades. Financial incentives powered most of the churn that OpenSea saw. The assumption might have been that as incentives decline, the activity on emerging competitors like X2Y2 will diminish. But beyond a broken dream, the industry was about to wake up to a nightmare in October 2022. A new player with a far superior product oriented towards traders was ready to market. The name? Blur.

Several things set Blur apart:

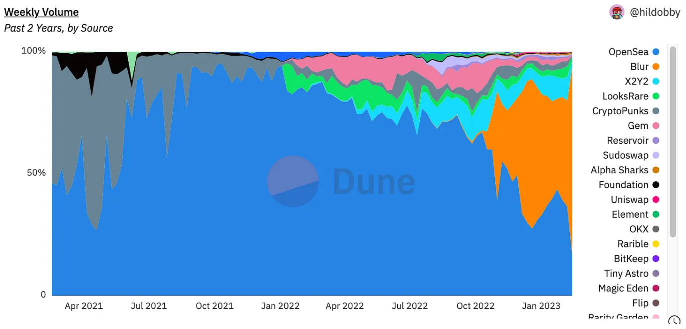
1. First and foremost, they teased users with potential airdrops for adding liquidity on both the bid and ask sides, as close to where the settlement price generally is for NFTs and ETH. This allowed traders to enter and leave the system in droves.

2. Secondly, instead of focusing on retail traders, they pursued high-volume NFT traders. Their product has several complex trading options that traditional platforms do not offer. This was like moving from a spot market for altcoins to a full suite of trading products that satisfies all your professional trading needs.

3. And finally, much like Gem at its launch, Blur integrated a series of charting and data functions into its core product. Suddenly, traders had access to information on historical pricing, depth of the books, rarity, and general volume trends via the same platform they were trading on.

You may think these things don't matter much. But between teasing a token and rolling out a superior product, Blur took ~40% of the weekly NFTs traded on Ethereum. As of February 2023, Blur did ~77% of the volume vs OpenSea's 16% in the same period.

Please note that Blur also released a token, so these data must be taken with a giant grain of salt. Even the token launch had a few innovative elements. The abstracted away the tokens and gave users "boxes". These boxes could hypothetically yield tokens at some point in the future. So nobody knew how many tokens they'd stand to get between October and February. And this drove user behavior.

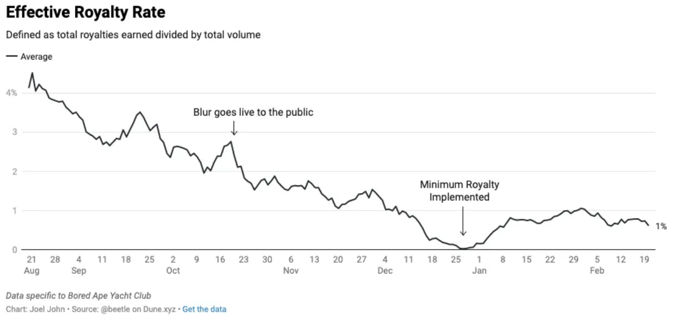


Data from the legendary wizard and overall big brain @hildobby on Dune.xyz

And still, there are two things Blur managed to do in a single quarter. Firstly, it began making the idea that royalties are a necessity vanish into thin air for a brief while. Traders increasingly became comfortable with not paying creator royalties on marketplace trades. When the intent is speculation, paying a creator tax on every trade does simply not make sense. Secondly, Blur eradicated its royalty. Until December 2022, there were no royalties on Blur at all. Since then, they have transitioned to a 0.5% royalty model.

To understand the long-term effects of the launch of Blur, we need to look at what happened to royalties. A user named Beetle released a Dune Dashboard that looks at an effective royalty rate. Beetle defines ERR as the "*total royalties earned across all marketplaces, divided by the total volume across all marketplaces.*" Since marketplaces like Blur initially launched with no royalties, an increasing volume and declining royalty would lower the figure trends. And that is exactly what happened.

The data below looks at the royalty being paid on Bored Apes over some time in the year. It started at under 5% in August because a few marketplaces already offered royalty-free trading. But the trend took off in October. When Blur went live.


Effective Royalty Rate

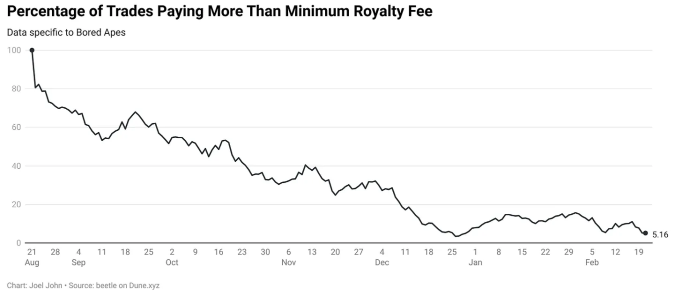
Defined as total royalties earned divided by total volume

Data specific to Bored Ape Yacht Club

Chart: Joel John • Source: @beetle on Dune.xyz • Get the data

Data from 1kBeetleJuice. Follow him on Twitter here.

It is not just the royalty rate that went for a toss. Across marketplaces, the number of trades now creating royalty began trending lower for Bored Apes, as the data below shows.


Percentage of Trades Paying More Than Minimum Royalty Fee

Data specific to Bored Apes

Chart: Joel John • Source: beetle on Dune.xyz

Filters at the Sea Port

If you are a player in the NFT ecosystem, you are now caught amid a major storm. Suddenly, a new player has swept the market, stolen your users and trading volume, and disrupted your business model. For a brief moment, multiple NFT marketplaces took the noble stance of protecting creator income. OpenSea released an operator filter registry. Members were added to the registry if a platform (like Blur) allowed users to bypass creator earnings when the same item would incur creator royalties on OpenSea.

As the months passed, it became evident that the market shifted its view on paying royalties. OpenSea, now home to only a fraction of the volume it once commanded, was forced to remove royalties three days back.

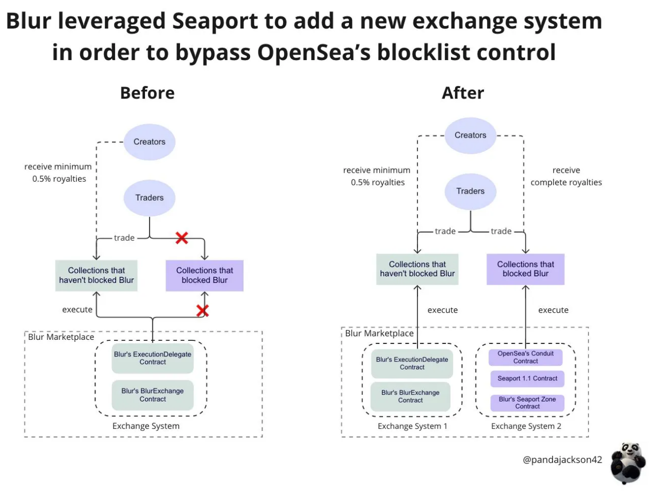
We may need to hire someone to make better memes.

If you think OpenSea was a sitting duck through the whole fiasco, it was not. The platform launched an entire protocol and acquired an aggregator over the year to stay relevant. Seaport, launched by OpenSea in May 2022, was an entire marketplace contract, much like 0x in DeFi. Think of it as a communications protocol that sources liquidity and routes orders across marketplaces. The Web2 equivalent would be APIs listing the same item on eBay, Amazon, and various regional e-commerce platforms.

Why would a marketplace like OpenSea bother with releasing a protocol? They aimed to add new avenues for more people to be onboarded to NFTs.

If the entire market expands and OpenSea continues to be the largest marketplace, they will see more users.

But in a way, this has come back to bite OpenSea. Earlier, creators could simply blacklist Blur and call it a day. Now, whenever a collection blocks Blur, they source the liquidity for the asset through OpenSea's protocol. And there's practically no way to block Blur from going to a protocol and sourcing liquidity for the asset. A user named PandaJackson explains how this worked quite eloquently in a twitter thread.

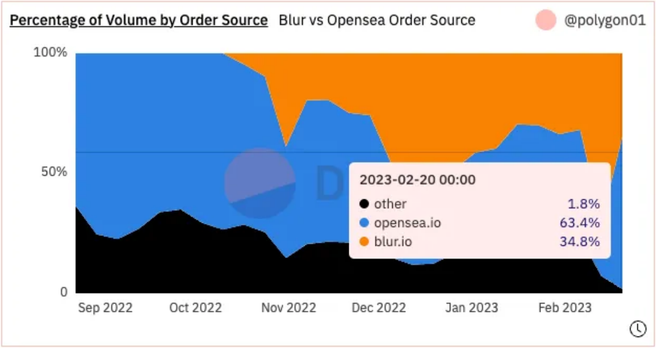

Blur leveraged Seaport to add a new exchange system in order to bypass OpenSea's blocklist control

Before
Creators
receive minimum 0.5% royalties
Traders
trade
Collections that haven't blocked Blur
Collections that blocked Blur
execute
Blur Marketplace
Blur's ExecutionDelegate Contract
Blur's BlurExchange Contract
Exchange System
After
Creators
receive minimum 0.5% royalties
receive complete royalties
Traders
trade
trade
Collections that haven't blocked Blur
Collections that blocked Blur
execute
execute
Blur Marketplace
Blur's ExecutionDelegate Contract
Blur's BlurExchange Contract
Exchange System 1
OpenSea's Conduit Contract
Seaport 1.1 Contract
Blur's Seaport Zone Contract
Exchange System 2
@pandajackson42

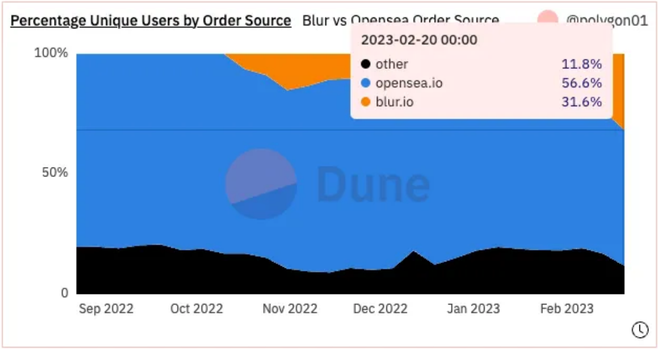
PandaJackson has some great tweets - make sure to follow him here.

Blur did over 4000 transactions for Sewer Passes and circumvented paying OpenSea some $220k in fees. That is a 40% loss in fees. This made a joke of the Blocklist registry as Blur used Seaport to get around the blockade. Even if OpenSea finds a way to block Blur from querying for liquidity from Seaport, it would be antithetical to why they introduced Seaport in the first place.(*Also, Opensea can't make changes to Seaport on a whim*).

You may think this is not a big deal, but considering how order fills and sources have evolved in the last few months, the challenge comes to light.



Sourced via a fork of SeaLaunch's dashboard. Link

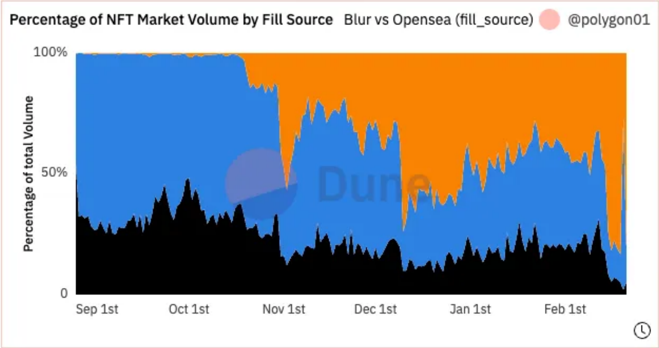


Sourced via a fork of SeaLaunch's Dashboard. Link

The first chart shows the volume percentage by order source, i.e., the marketplace where an order originated. As you can see, when Blur went live to the public in October 2022, they commanded close to 60% of the order source. As of February 2023, it is down to ~21%. This means an ever-increasing number of users have placed orders via Blur's marketplace. This, on its own, is not a big threat. You could place orders from any aggregator, and the liquidity could be sourced elsewhere.

In fact, in the lens of a B2C investor, Blur may pose no real threat to OpenSea. As you can see in the second chart, the bulk of the percentage of unique users is still on OpenSea. A new entrant like Blur cannot replicate their brand equity overnight. **The issue is that Blur has gone from a place that originates orders to a place where users can find liquidity in a single quarter.**

For the data below, Blur is represented in Orange and was doing 83% of the volume for fill-source for 19th Feb. By 20th Feb - it declined to 26%. A massive drop because the initial token airdrops for Blur had just wrapped up.



The next chart above breaks that fact down quite elegantly. Here, fill source refers to the marketplace where the order was fulfilled. If you are an up-and-coming aggregator that is up and coming, you may be a source for orders, but the fill could happen via a third party. When you can complete the bulk of order matching on your platform, you emerge as a stand-alone marketplace. As of February 2023, only about 16% of the orders on Blur are filled using liquidity on OpenSea.

Blur's transition from aggregator to platform is at the core of what threatens OpenSea's future. Losing volume in large tranches to third-party platforms leaves little incentive for marketplaces to maintain high fees. OpenSea moved from releasing a registry to blacklist marketplaces that don't enforce creator royalties to having any fees.

This evolution of the market – from an ecosystem that believed creator royalties are a sacred right and deserve to be protected and enforced across markets to a place motivated by finding unique ways to avoid paying creators – is a real-time representation of how markets evolve. It is also fascinating to realise that within just six months, one single startup convinced the global NFT market that doing away with royalties is rational. Even if it is for a brief period.

Royalties Look Rare

A year back, when we first wrote about LooksRare, the assumption was that releasing a token could upend the NFT markets altogether. The playbook seemed simple. You strip away the take rate (fees) and introduce a token. Teams profit from the token they release instead of any revenue they generate. I was wrong about it because, over the year, the platform trended to as low as ~200 DAUs.

Blur posed a much more significant threat because, compared to the ~11% of volume, LooksRare was grabbing at the time, Blur captured over 70%. The fact that OpenSea had to go from playing with a registry to block marketplaces that don't offer fees to reducing fees to a bare minimum themselves shows the threat Blur poses in the market. So there is some weight and credence to their effort. But will their volume and users stick once the market moves on? It is hard to say.

There are bets on both sides of the matter. One would argue that Blur has a much better product for traders and that the volume would stick with them. A superior product and users "owning" the product through the token will empower them to grow substantially. The other argument is that perhaps this is a temporary blip, and we will be back to OpenSea reigning within a few months. There are a few reasons this could happen.

First and foremost, they have already reduced fees to a bare minimum. So for users that moved elsewhere, if the unit economics were the problem, they can return to OpenSea now. Secondly, with the fee trending to a bare minimum, it is possible that an IPO no longer happens. Especially in the battered tech stock markets we are now. In such a situation, a token is a possibility.

OpenSea does not need to rush into tokenising itself. The angle could be through tokenising assets the firm holds. For example, gem was an aggregator it acquired a year back. Introducing a token to them may be the first line of assault.

And if that doesn't suffice, they could go ahead and tokenise Seaport - the protocol they had launched a year back. Tokenising the protocol and incentivising individual, smaller marketplaces could be a net positive for OpenSea. They could enforce royalties at the protocol level and blacklist bad actors so long as Seaport becomes the standard for trading NFTs.

Much like Ronin today, any protocol released by OpenSea could have a consortium of gaming studios, large NFT issuers and traditional retailers that determine how the shared standard will evolve.

The standoff in the market is a function of two behemoths that have raised enough in venture capital to survive with no revenue for a few years if needed. It affects creators and smaller products that believed the royalty model would continue. Remember how I mentioned NFT royalties could enable user-generated game content markets?

It entirely collapses in the absence of NFTs. Games would be incentivised to run their closed-ended markets to avoid scrutiny from regulators or dealing with app store policies around digital assets.

This also ignores the point that a large portion of what makes NFTs relevant is intellectual property. Yuga Labs or Nike is incentivised to work continually on their NFTs because they see revenue from the royalties. For scale, both firms have made over $100 million each from royalties alone from their NFTs over the last year. Without the model, the incentives to continue working on these primitives vanish—our rush to declare royalties a flawed model may set us back by a few years.

Artists may respond by launching their marketplaces. There are great tools to build one's storefront and issue a royalty mandate on top of it. In that process, the inevitable return to the challenges artists historically had would happen. Gatekeepers and intermediaries take a portion of their incomes. Perhaps, at the crux of all of this is the industry's inability to understand two things.

1. Trading makes up a large portion of the digital asset ecosystem today. The bulk of the money invested and revenue generated comes from financial applications. These applications will continue to trend towards the lowest fees to capture users and volumes.

2. Not all assets are to be traded heavily. At least not as non-fungible instruments. There is very little reason to be trading copyrights of Jay Z's album from 2000 - multiple times in a given day. If the frequency in which an asset is changing hands is low, then the royalty being high makes sense.

We will have entirely distinct user bases. And each will need a different royalty model depending on the asset being traded. One way to resolve the standoff would be for creators to be empowered enough to get their royalties at the protocol level. The market can then determine if it wants to trade it excessively or not. Ironically, inspite of the years of innovation in NFTs, little work has gone towards that effort. Canto's contract-secured revenue allows developers to get a portion of the fee generated by users of a certain DApp. Perhaps, there is a way to tweak it for NFTs.

Back when Jay-Z realised royalties were one of his 99 problems.

The irony of the situation is that this is nothing new. In 2015, Jay Z launched Tidal as a response to music artists making very little from the shift to streaming. Priced at 25 euros, the app failed to scale despite practically every major artist in the US backing it. At one point, the only way to hear specific old Jay-Z albums was to pay for Tidal. And how did that go? Well, the app was ranked over #700 a month from launch. A few year's later, Jack Dorsey from Square acquired it for $300 million.

Our point is, as an artist, you want to optimise for income. But you do not want to do it at the cost of distribution. Even today, artists often optimise for YouTube streaming their work because it counts toward their ranking on the billboard. The moment a platform has substantial attention, it reigns over creators. And there are very little creators can do at that point. If you are optimising for distribution, you make it as easy for your users to discover you. Sometimes, it could be listing on OpenSea. Sometimes, it could be not putting this article behind a paywall.

(*We have no plans of a paywall anytime soon - but shout out and much love to that guy who pledged $200 to this publication over the weekend. You made our day.)*

As I write these words, Blur trades at a valuation of $3.2 billion. Higher than certain protocols. It made us wonder if we are transitioning from the age of fat protocols to value accrual in applications. Teams like the one behind Blur have proven that stand-alone applications can often generate more volume and service more users than entire protocols. There is an emergent playbook here. Launch a marketplace with little or no fees—Incentivise volume through tokens. Pass on ownership to the users via tokens in exchange for their activity on the platform.

In essence, build something people want as opposed to building something people may build on. We have finally reached a stage where product based moats focusing on power users can be a thing.

The authors of this piece do not believe a zero-royalty market is the one that will eventually prevail. As I said at the beginning of this piece, evolution is the market norm. And much like we see in nature - applications will mutate to compete and acquire niche users. A quarter on, it is possible that the hype around Blur will settle down, and we will return to normal. It is also possible that creators stop issuing NFTs entirely, and we sit around with just monkey pictures to show - for all the innovation and development the sector has done over the last three years.

We don't know what will happen. But if we take the wise words of a modern-day rocketship connoisseur & dogecoin maximalist - it is likely that the most entertaining outcome is the most likely one.

We will see you next with some work we have been doing on AI and blockchains.

Beta Testing Szn

1. I dropped two articles as NFTs as an experiment on Mirror a few months back. If you are one of the 50 wallets that acquired the NFTs - you now have access to Gem's V2, Jumper Exchange and Bungee. I may or may not make NFTs out of future articles.
2. Users that had shared their wallet addresses on our Telegram recently were given access to Socket's Bungee exchange beta.
3. We have now taken a referral page live. We are giving away premium subscriptions to substacks of publications we admire and enjoy reading. You can be a part of it here.

We will drop beta access for more in the coming weeks. Join us on Telegram to stay updated on these.

Joel John
decentralised.co
23 Mar 2022

On Aggregation Theory And Web3

Why collapsing the cost of trust and verification is profitable.

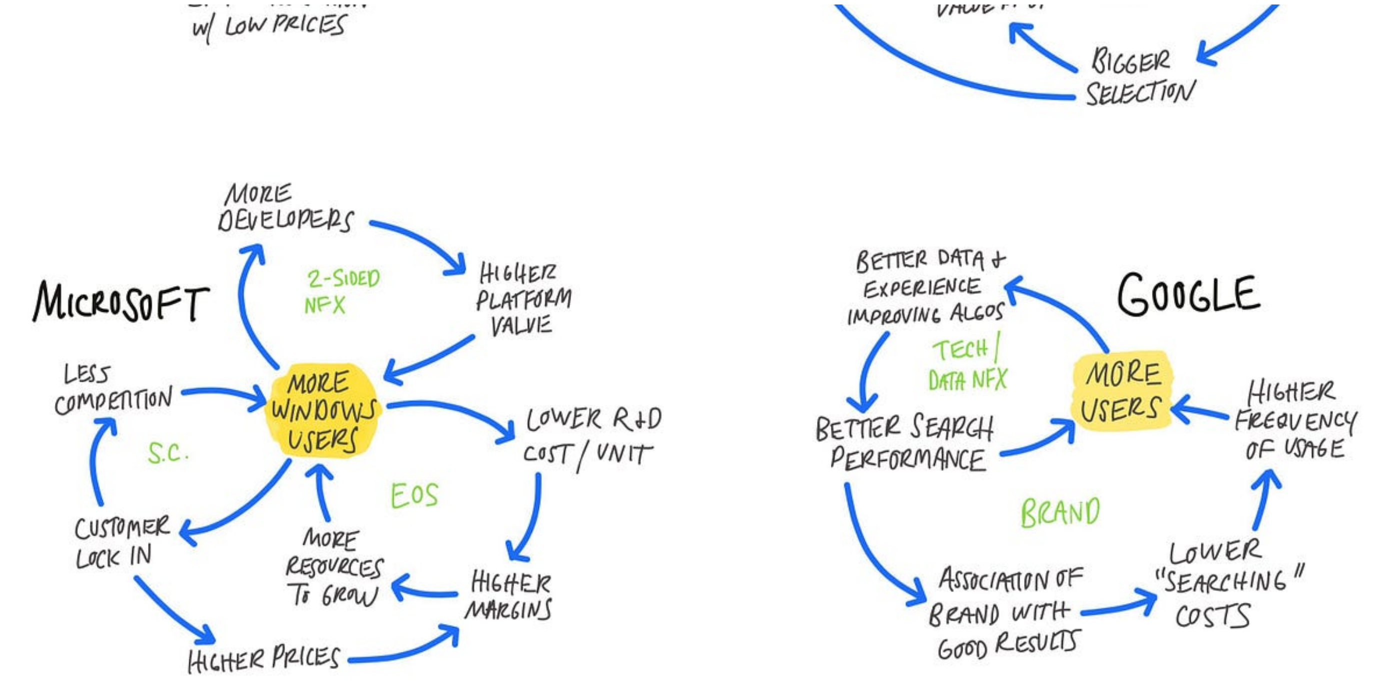


Photo by Shaueel Persadee on Unsplash

This piece was made possible with a sponsorship from Nansen. The platform saves analysts and traders hundreds of hours each month by allowing them to grab network level data with a simple click. No APIs, no going through network scanners or pulling contract addresses. Nansen visualises network level data on user behavior & transactions in a fraction of the time their peers do. Get started with a trial here or simply play with their dashboards here.

Hey,

TL:DR - Me and Krishna from Quantstamp show how multiple multi-billion dollar firms within web3 have been built through collapsing the cost of trust and verification. Drop me an email if you read this and decide on building something cool. We may just be able to put together your seed round 💰

In today's issue, we zoom out a bit and look at Web3 through the lens of Aggregation Theory. It is a bit long, but stick along, and we will break down how we believe the next decade of investing in blockchains will happen.

Ben Thompson first proposed aggregation Theory in 2015 to explain how the Internet has contributed towards the evolution of markets. Ben described it like this some seven years back:

The value chain for any given consumer market is divided into three parts: suppliers, distributors, and consumers/users. The best way to make outsize profits in any of these markets is to either gain a horizontal monopoly in one of the three parts or to integrate two of the parts such that you have a competitive advantage in delivering a vertical solution. In the pre-Internet era the latter depended on controlling distribution.

The fundamental disruption of the Internet has been to turn this dynamic on its head. First, the Internet has free distribution (of digital goods), neutralizing the advantage that pre-Internet distributors leveraged to integrate with suppliers. Secondly, the Internet has made transaction costs zero, making it viable for a distributor to integrate forward with end users/consumers at scale.

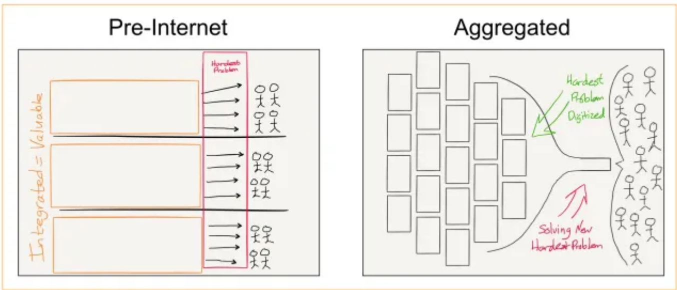


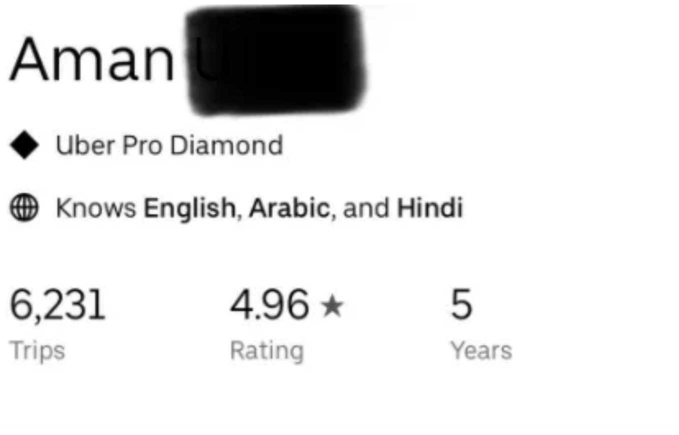
Image from Ben Thompson's original piece from 2015

We believe the theory deserves a revisit from the lens of someone working in Web3. We have seen behemoths like Ramp, Stripe and Spotify being built through the collapse in the price of distribution and collecting payments. But how does it apply to Web3 firms? We propose that in addition to collapsing the cost of collecting payments, blockchains can reduce the price of verification and trust. This enables the creation of multi-billion dollar entities that were historically not possible. The new era of blockchain based aggregators also help drive innovation at the protocol layer, and enable a new business model: Hyperfinancialization-as-a-Service. But before we go there, let’s break down Aggregation Theory for our readers that have not been following Ben Thompson.

Bringing Markets Closer

Here's a breakdown of Uber through the lens of Aggregation Theory. Historically, the vendor (supplier) <> buyer (demand) relationship was hyper-local and had a cap on the number of customers a driver could potentially have. This is why they could get away with treating you terribly. There were limited choices on who could possibly offer a ride. The supply side was messy in that it had minimal signs of reputation, suffered from ineffective pricing in many cities and was unpredictable. Uber came along and organised the supply side.

It was a curated subset of users whose reputation was verified and tracked on an ongoing basis instead of one comprised of random drivers. Think about the information you get each time you request a ride. You know how many times the person has picked people up, the driver's average rating, and the exact amount you can expect to pay.



Aman [redacted]

◆ Uber Pro Diamond

🌐 Knows **English**, **Arabic**, and **Hindi**

6,231	4.96 ★	5
Trips	Rating	Years

Part of what drives value to aggregators is the data they hold on the supply side.

Why did this shift from taxi unions to in-app drives happen? Because Uber controls the supply side through their app. Users looking to book a ride prefer the convenience of remotely hailing a cab instead of waiting out in the streets and being rejected by random taxi-men. This model works because the internet allows Uber to scale globally from their comfortable offices in San Francisco or wherever the new hip place to build a venture is.

It also enables Uber to collect payments and take a fee-cut for themselves without relying on regional partners to do that for them. The rise of digital money accelerated Uber's adoption. If we were still paying for our rides predominantly in physical cash, it is unlikely that Uber would have been a thing.

The largest firms on the internet today can be linked to aggregation theory. AirBnB, Deliveroo, Spotify, Steam, Amazon and Twitter have each upended messy markets through the power of the internet. Aggregators accumulate so much value because they can organise what are typically large, chaotic markets. Newspapers? You had thousands of them opining differently, often with inaccurate sources. Your feeds replaced them.

What about renting a house in a small town for a few months? Airbnb made it "okay" to live in a stranger's home. Customers trend towards these aggregators as they can expect the same level of service, quality and standards with a very varied list of vendors. You get the safety of a familiar platform and optionality that spans the entire market. Going back to my Airbnb example, users know that they can register a complaint with the website to get a refund if a booking goes wrong. Amazon? The refund almost happens instantaneously.

Aggregators enable vendor reputation and moderation. You can look up reviews when you buy something on Amazon. In exchange, they take a cut of the transactions that occur on them. As a platform goes digital, the frequency of transactions tends to increase. This allows aggregators to run with much lower take rates than the cost of physical experiences**.** Why? Because the cost of delivering a digital good (like movie streaming) is a fraction of what a physical experience (like a flight) would take.

Users can only take one flight at a time. During the same flight - you may see a user streaming multiple movies. Or if they are like us, they may buy numerous altcoins or NFTs they will regret purchasing as soon as they get off the flight. Hopefully, you have a good sense of what aggregation platforms are and how they scale. Now let's return to Web3.

Collapsing The Cost of Trust

Much like the internet collapsed the cost of distribution and collection of payments, publicly verifiable blockchains have collapsed the cost of verification and trust. Practically all of the enormous businesses we see in the context of Web3 are built on this principle. Blockchains make it possible for anyone to query and verify if a digital good being sold is genuinely from the source it claims to be. There is no counter-party risk for digital consumption goods like NFTs that are sold through a blockchain-enabled platform because verifying a smart contract ensures you are getting the exact good you are paying for.

What does this signify for those running aggregators in Web3? It means it costs a fraction of what it does in Web2 to verify and trust vendors when it comes to sales of digital goods. When Netflix or iTunes initially launched, they had to spend months or years negotiating contracts to ensure they could go to market with a large enough inventory of digital goods that would attract users.

Even today, Netflix spends some $16 billion on producing content in-house based on their users' data. As the size of these aggregators scaled, they became the best place for digital consumption goods to be sold. After a decade's worth of work, owning the distribution gives them that advantage.

Some interactions are not possible in Web2 aggregators because of the inherent friction introduced by siloed databases and data that is not open. For example, you cannot browse for property listings through Zillow, and subsequently make an offer on it and move on to refinancing the asset all within the same platform. You would have to go to another venue like Figure, and run through their various compliance and onboarding procedures that are unique to each platform.

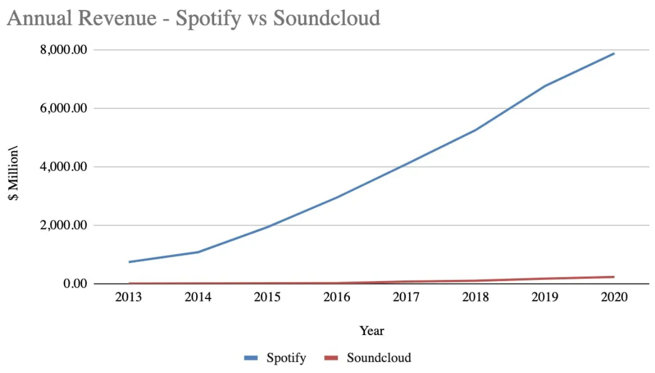
It also makes it much harder and more expensive for developers of other applications to easily tap into your aggregation and build new interesting services on top. On-chain identity, data and verification standards can solve for this, and enable Web3 aggregators to be much more efficient than their Web2 counterparts.

In stark contrast, OpenSea does not spend much worrying about the licenses. They can almost instantaneously verify that a third party's NFT comes from a legitimate source and track how it moves across its userbase. What about Uniswap?

So long as the user accurately adds the token's address, there is no need for human involvement in verifying if a token being traded on it is legitimate.

Blockchains abstract away the verification layer and collapse the cost incurred. Does trust command a premium on its own? I think it does. Let's consider a few instances where a platform owns the commercial rights and compare with one that does not. Music would be a good theme so we go with Spotify and Soundcloud as examples.

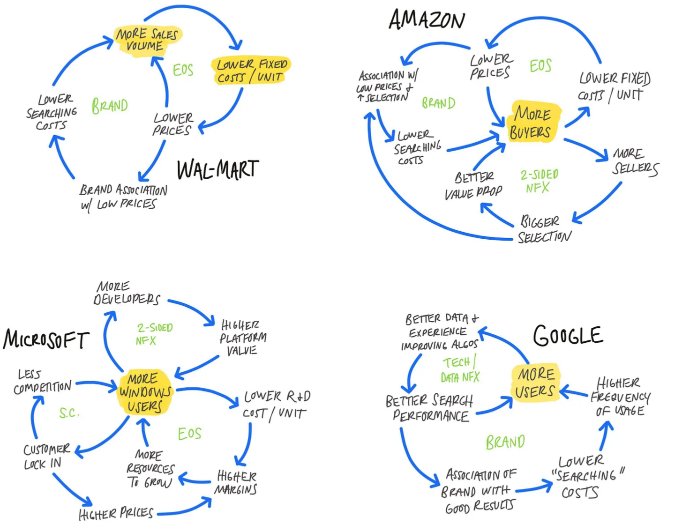
One has been the go-to platform for streaming music worldwide, while the other is occasionally used to find something motivating to listen to at the gym. Soundcloud, by all means, is an incredible business, given its focus on community and enabling new artists to be discovered. But if seen purely through the lens of revenue generated, you will see how the two businesses differ.



The two businesses have different ways of operating. Spotify claims to have 406 million monthly active users of which some 180 million are premium paying. They have a margin of some ±25%, so you can discount the $9 billion annual revenue you figure in the chart below. But even when accounted for that, you will notice that the revenue for Spotify is a massive multiple of what Soundcloud holds.

Part of why this is the case is that Soundcloud requires volume in terms of user streaming to scale on ad-driven revenue. But if all of the users are on premium platforms, why would they come to Soundcloud? This is a phenomenon you can see across product categories.

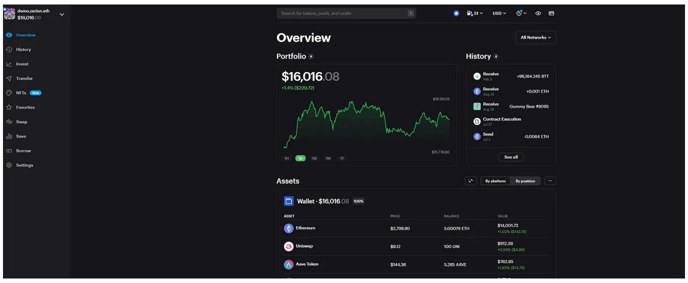
Amazon as a standalone platform commands more in e-commerce volume than Shopify storefronts do. Steam - the storefront for games - takes in more revenue than individual gaming studios. Why? It boils down to customers choosing stores with the maximum optionality and minimum amount of friction. **The greater the number of choices, the higher the possibility that commerce concentrates on an avenue, making it easier for the platform to offer more optionality while keeping costs low thanks to the scale of the operation**. This is the flywheel of modern commerce. Max Olson did a great job at visualising how these work on Twitter a while back.



Web3 is interesting because it changes the unit economics of verification and trust. Historically, aggregators would acquire intellectual property rights for the most desirable digital consumables. As we will see in a piece soon, in emerging markets like India, holding the streaming rights for Cricket paved the way for television networks to scale. Blockchains have enabled platforms to prove provenance and authority of issuance from anyone on the web at a fraction of the cost.

This means the expenses incurred in legal fees and time spent through bureaucracy is now replaced with on-chain verification, identity and verification. This principle will be at the crux of what makes aggregators in Web3 massively influential. Don't believe me? Let's look at some of the aggregators within the ecosystem today and how they use blockchains to their benefit.

Aggregation in DeFi



ASSET	PRICE	BALANCE	VALUE
Ethereum	$2,799.90	5.00079 ETH	$14,001.73 +1.02% ($142.15)
Uniswap	$9.12	100 UNI	$912.36 +0.54% ($4.96)
Aave Token	$144.36	5.285 AAVE	$762.95 +1.93% ($14.75)

Zerion is a wallet interface focused on enabling users to track their portfolios. The product currently tracks NFTs, allows swaps, and gives users a look at how all the tokens in their wallets are performing. Interfaces like those offered by Zerion are quickly becoming the "home page" for DeFi. They allow users to interact with a complex host of apps without going outside the interface of a single website. In addition, these interfaces eliminate the high risks of phishing, losing keys and signing the wrong smart contracts by allowing users to interact with them directly through their interface. They help users access functions like lending through curating protocols, and also drive innovation at the protocol layer by offering more choices to customers that offer them competitive pricing and features. It would be safe to suggest that assets worth a few billion dollars are managed through Zerion's interface.

How much of that risk is with Zerion? None. They don't custody the assets and they don't manage the smart contracts. Instead, they are responsible for embedding each of these protocols into the product to create a super-app. According to a recent press release, they interface with some 50,000 assets across 60 protocols. Comparables like DeBank, Frontier and ImTrust have been at the forefront of enabling more retail participants to find their way around the complex Web3 ecosystem.

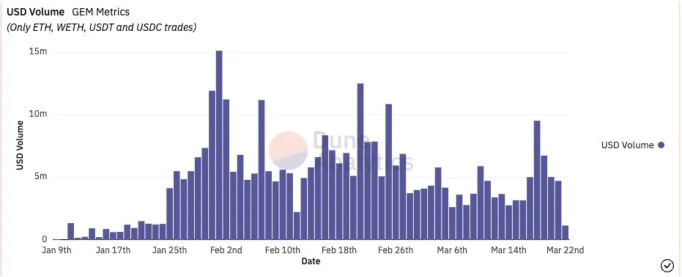
How? They reduce the trust barrier required to use an app as an end-user assumes that the interface creators have already exercised due diligence. Secondly, they enable new apps to be discovered far more smoothly than through complex web of information platforms like Twitter. Lastly, and most importantly, they combine the ability to club multiple DeFi DApps in a single interface. They have also begun integrating on-ramps and tax software as users' needs in the industry evolve.

I have taken Zerion as an example here as it is a centralised entity that acts as an interface to plug in with multiple defi DApps. However, aggregation in DeFi runs beyond that. Here are some examples :

Orderflow - 1inch and Matcha.xyz allow users to find the best price for assets that need to be traded without going to individual platforms. They do not custody the assets used for trading themselves but seek liquidity from third-party platforms. Matcha has taken this one step further by integrating a request for quote model in the product. They have done about $42 billion in cumulative volume across ±900k orders so far. This feature allows centralised market-makers in the back end to quote prices for large order sizes, thereby bringing the experience closer to what a centralised exchange like Binance can offer.

Yield - The holy grail for DeFi has historically been the ability to provide yield. The large risk lending or decentralised exchange platforms have is potentially getting hacked. But what if you could build interfaces that allow users to deploy capital in pools while not necessarily holding the assets yourself? Rari, Alpaca and Yearn Finance do just that. Rari alone has deployed $922 million through Fuse pools for a sense of scale. Instadapp takes this one step further with its user experience. The product allows users to manage debt positions or deploy assets into yield-bearing pools using a single interface. They manage around $5 billion worth of assets across the likes of Maker, Compound and Aave through their interface.

Aggregation of The Metaverse



NFTs are interesting from the point of view of aggregation. You have a digital good with transaction finality and on-chain provenance of intellectual property. Please don't curse me. I will explain it without the jargon. Given that users cannot reverse blockchain transactions, a user buying an NFT almost certainly does not have to worry about losing what they purchased to fraud unless the NFT itself is a duplicate.

They can also verify that it is coming from the right source almost instantaneously. Unlike traditional art markets, you can almost instantly see what the floor price of an NFT is and who its past owners were. These make NFT aggregators incredibly powerful in terms of how they can interact with market participants.

Consider Gem, for instance. The aggregator itself holds none of the NFTs listed on the platform. They use Dune to give analytics to their users. Once you click on a collection, the interface allows you to bid on listings directly in Opensea and LooksRare. Now, this is where this gets even more interesting. Aggregators like Gem become the place for price discovery as users are essentially discovering and tracking their portfolios and bidding through them.

In the future, they'll also cover features that blur the lines between DeFi and NFTs through lending and automated inventory management. The traditional art or physical market have some of the previously mentioned constraints relevant to Web2 aggregators that prevent them from offering these services at low friction and cost. In addition, some of the other verticals like Gaming and Metaverse do not even have historical analogs - **Web3 aggregators will be the first to support and enable efficient markets in those categories of digital assets.**

Over time, they can be influential enough to determine which NFT set gets "discovered" as essentially what they are accruing is the market's attention. How much is that attention worth? I don't know yet, but it is valuable enough to have driven $400 million in volume through the platform alone. Gem is also influencing the market share of the underlying NFT marketplaces themselves. Because users are marketplace agnostic and will buy and sell assets wherever there is a favorable bid/ask. For example, LooksRare's market share on NFT volumes went up in relation to OpenSea since gem was launched.

For an idea of how quick aggregation can scale, consider this tweet below from Vasa flexing the number of platforms Gem shows NFTs today from. *Sidenote: He's a great guy. You should follow him*

We believe that aggregation of NFT linked assets will happen thematically. For instance, Parcel allows individuals to bid on real estate linked NFTs. Similarly, there will be separate marketplaces for gaming linked NFTs. There are gaps in the market for sports, music and film-related NFTs. Part of the reason for this is that the thematic focus on asset types allows founders to curate communities around them. It creates an initial flywheel for enabling transactions through the platform itself.

Aggregating Data Markets

We have discussed how aggregation theory in the context of Web3 creates entirely new marketplaces. Web3 linked aggregation models work because they focus primarily on digital assets. One sector that can be considered more "digital" than tokens and NFTs is that of data markets.

Data markets in Web3 are attractive because:

- all data sets offered can be queried and verified instantaneously by a third party
- they directly embed with multiple third-party apps and therefore scale exponentially
- the cost of adding each new chain typically tends to decrease
- the delivery of the product (data) is instantaneous
- the cost of maintaining the network infrastructure is outsourced in the case of protocols

You can break this sector down into two variations. One of them offers the end-user direct access to the data through charts and queries that present the information in a consumable way. These are centralised businesses like Nansen or Dune. Nansen built a business by focusing on the interface. Their centralisation aspect pertains to the labels on 100million+ wallets and the chains they index. Users themselves don't create the queries. The team at Nansen handles these, but once the queries that pull the data are made, they can be replicated across chains. So the unit cost for expanding to each new chain trends downwards. The initial investment is in labeling and setting up queries that lookup the top holders, smart contracts or wallet interactions on each chain.

Where Nansen excels in giving users pre-defined queries without any hassle, Dune wins by giving an infrastructure on top of which anyone can query. Nansen has constructed their moat based on their extensive work built around labeling over 100 million wallets. On the other hand, Dune has built a moat through its extensive userbase that fights tooth and nail to be at the top of its leaderboard.

It would be relatively easy for a third-party platform to replicate the data Dune holds today, but good luck replicating the community members without an active incentive system. Both platforms are unique in that they can (i) sell data digitally, (ii) do so in an almost instantaneous fashion and (iii) have limited marginal costs in expanding the number of chains they support. There are protocol-based peers in the sector.

Covalent, Graph, Pyth and Chainlink are protocol-based alternatives to the same model. Each of them supports DApps across the ecosystem and respond to millions of queries on a routine basis. Protocols at the data layer are even more fascinating because they don't necessarily own the hardware infrastructure to make these data sets available. Instead, the indexing of the data set is done in third party infrastructure, which is incentivised through the protocol's native tokens. In a traditional data venture, the cost of running infrastructure eats into the firm's profitability. In the case of protocols, the perceived "value" of the network increases with each new node that hosts data on these networks as the possibility of the entire data network going down diminishes.

The Next Decade of Aggregation

Let's revisit the core argument of this piece before we wrap up. **We believe that blockchains will enable an entirely new category of markets that are able to verify on-chain events instantaneously. This will collapse the cost of validating intellectual property at a massive scale and thereby create new business models.** Present-day Web3 aggregators provide interfaces that show on-chain data and allow users to interact with smart contracts from multiple platforms. They don't own the risk of custodying these assets and typically do not bear exponentially higher costs for supporting additional networks. Covalent and Nansen are able to generate exponential value through adding each new chain - which is usually a linear expense.

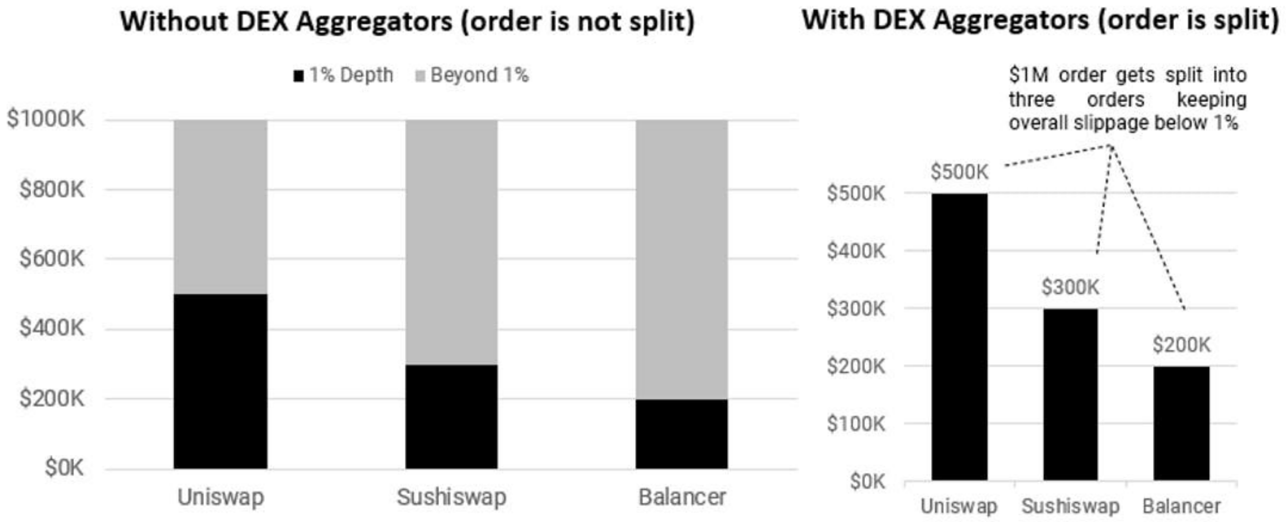
The core proposition of Web3 aggregation over the next decade will be in streamlining large, messy processes with multiple counterparties in systems with low trust. One instance of this occurring has been AngelList. The platform has structurally collapsed the amount of friction involved in putting together a venture round through combining legal, banking and LP management in a single interface. How much is that worth? Around $4 billion as per their latest round. Large, messy markets with multiple moving parts are hard to aggregate at scale unless you have time or capital. AngelList took roughly 8 years to build its monopoly, while Uber had to raise some $25.5 billion to become today's behemoth. I believe blockchains will collapse the unit economics around this and hyperfinancialise the process. **Clubbing the eradication of inefficiencies in what has historically been long, chaotic processes with incentives that allow people to profit them can be a powerful mix.**

Disclosure : The authors of this piece own significant exposure to a number of ventures mentioned above.

Joel John
decentralised.co

Payment Pipelines

Embedding the future of Web3 native payments



Hey there,

Today's issue is a sponsored newsletter written in collaboration with Paraswap. The decentralised exchange aggregator has enabled over $48 billion in volume since 2020. We use the piece today to explain the concept of a transactional aggregator, the need for embedded finance products & what the future of aggregation looks like.

Mounir - and the kind team at Six Degree Labs helped us with much of the analytics and internal expertise we needed to write for the piece.

While they had access to the piece (for informational accuracy), they did not edit the analyses we did over the past few weeks. As always, mentions of a project are not endorsements for their tokens. With all that out of the way, let's dig in.

Tldr - for those in a hurry.

- *Using DeFi instead of custodial exchanges for executing trades is usually cheaper for larger order sizes. Liquidity aggregators like ParaSwap are critical for DeFi infrastructure since they simplify trading order execution.*

- *To differentiate itself in the aggregator landscape, ParaSwap has been taking steps to grow the institutional side of the business by onboarding market-makers and other partners like wallets and lending platforms, allowing them to reach a point where 2/3rd of the volume comes from SDKs that are embedded in third-party applications.*
- *But that's not it! To build a sustainable moat among aggregators, ParaSwap must go through creative destruction of itself. Web2-based FinTech companies offer interesting case studies where aggregators built moats with ancillary services that enhance the value proposition of the core service.*
- *The fee for core services such as routing and splitting trades is a race to the bottom. ParaSwap may evolve into an embedded finance platform—offering services like trading all DeFi primitives from one interface.*

GM!

A year ago, in Aggregation Theory and Web3, I claimed that blockchain native projects can supersede their traditional counterparts, as the former reduce the cost of verification and trust. Few places have seen the power of this concept as well as DeFi and NFTs. The example I gave at the time was of tokens.

When you swap ETH for USDC on Uniswap, you don't worry about the 'authenticity' of the USDC you receive, as long as the right smart contracts are involved.

Part of what I missed at the time was the relevance of the goods being sold digitally. Amazon and Netflix are aggregators, but their marginal costs for adding to their inventories are not zero. Amazon incurs shipping costs on each sale. Netflix has to pay third-party studios for content or create this in-house.

In Ben Thompson's view, an aggregator (in the digital world) has a few avenues where costs creep in. Efficient aggregators manage to avoid all these. As per his post from 2017, aggregators incur zero marginal costs on the following:

- *The cost of goods sold (COGS), that is, the cost of producing an item or providing a service*
- *Distribution costs, that is, the cost of getting an item to the customer (usually via retail) or facilitating the provision of a service (usually via real estate)*
- *Transaction costs, that is, the cost of executing a transaction for a good or service, providing customer service, etc.*

Blockchain-native DeFi aggregators fit this definition quite well because

- You can pass on the cost of capital or goods to the user, using token incentives, as Blur and 1inch did
- There are nearly no costs incurred by aggregators for passing on the final good (an NFT or token) to the user
- The user bears the gas costs and it generally trend to zero with the arrival of L2s

One can always debate whether token economic incentives are a cost to the protocol. Take the case of Uniswap – was the airdrop they offered a cost to the protocol or a mechanism to generate $6 billion in collective value for all stakeholders?

That debate does not fit here, so we will skip it for now. But I wanted to refresh your memory on the matter for a different reason: to introduce the concept of a **transactional aggregator**.

Building further on Ben Thompson's work (and my piece from the last year), **a transactional aggregator is one that holds zero risk for the liquidity it offers by sourcing it from a third party with no fees for doing so.** Unlike Amazon or Netflix, transactional aggregators can scale infinitely by tapping into liquidity from external platforms. No marginal cost is incurred (by the platform) in supporting larger orders.

Note: I wondered for a while if Stripe and Plaid are transactional aggregators. In my understanding, they are data aggregators tracking the flow of capital via third-party payment networks (Visa, ACH, SWIFT). The settlement of payments itself does not happen via Stripe or Plaid.

They have the benefit of scale from focusing on a traditional asset like fiat, but they are still dependent on a third-party network's willingness to work with them. In the case of open-source, networked-capital platforms (like Uniswap), there is rarely a choice of blocking out a third-party aggregator plugging into it.

We may need a conventional example to explain why this matters. Let's take Charles Schwab and Robinhood – both instances of zero-fee stock trading platforms.

They hold large pools of user capital that are often isolated. If a user had to do a block transaction of a million shares of Apple – like Steve Jobs did here in 1997 – they would go through an investment banker or a specialised service handling such transactions. You have a central party that takes these orders, assumes the risks on their own books, and sells them over time.

In the case of Web3 native pools of capital, like the liquidity pools on Uniswap, any third party can build an application that taps into that pool of money.

A developer can build an app that taps into multiple pools of liquidity to absorb an order without ever interfacing with the developers of stand-alone, external AMMs like Uniswap or Sushiswap. A variation of this was evident in the early days of Blur and Gem.xyz, too. **Networked pools of capital, running on smart contracts enabled by public, permissionless ledgers can rarely dictate who interacts with them.**
(*I understand how little sense the last sentence would make to someone outside this industry. Apologies to them.*)

The lack of liquidity for the tail end of assets was beginning to creep up on spot exchanges like Uniswap, right as DeFi summer took off. Given how these systems work, users can trade $10k of smaller altcoin within a 1% price difference. But what if they wanted to sell $100k worth?

You have a problem. This is where a transactional aggregator like ParaSwap comes in. However, before I discuss how it all came together and what its future looks like, it serves to understand what ParaSwap does today.

New Engines Under The Hood

Here is a quick breakdown of some financial jargon before we go further.

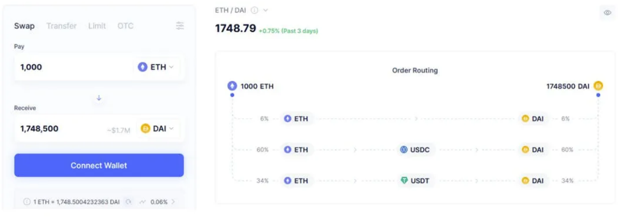
1. Liquidity is the amount of capital (dollars or ETH) available on an exchange against which you can trade. If you have a token priced at $10, with a liquidity of $1, what you may really have is ~$1.5 or $2 and not $10 because you won't be able to sell all those tokens at $10. Where did all your money go?

2. This is where you meet your friend 'slippage' for the first time in the markets. If nobody is willing to buy your token at $10, you will now have your order to sell settled at a new, lower price.

3. For illiquid assets, this could be 10%–20% lower, depending on how many people wish to buy the asset. Last year, FTX imploded partly because the risk assessment team there seemingly didn't know how these concepts work.

   That difference - between the price you wanted and what you got, can be defined as slippage.

Keep these terms in mind as we navigate the following few examples. The image below shows what happens when a user tries to sell $1.75 million worth of ETH for DAI on ParaSwap.



Pay
1,000 ETH
Receive
1,748,500 ~$1.7M DAI
1 ETH = 1,748.5004232363 DAI 0.06%

ETH / DAI
1748.79 +0.75% (Past 3 days)

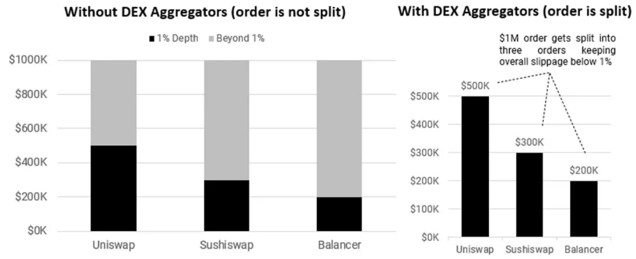
Order Routing
1000 ETH → 1748500 DAI
6% ETH → DAI 6%
60% ETH → USDC → DAI 60%
34% ETH → USDT → DAI 34%

A screenshot from Paraswap

In the above hypothetical example, instead of sending the token down to a single exchange where there may be only $500k waiting to buy the asset without slippage, a transactional aggregator could break down that order and send it to multiple exchanges. You may still not get the $1.75 million you hoped for, but you could get close to it depending on the number of exchanges plugged into the aggregator. The image below examines how an order of $1 million worth of ETH would be split up to reduce slippage.

You may wonder why users wouldn't go to Binance to sell their tokens. The fact is, for the vast majority of the tail end of assets – in the absence of multiple market-makers – liquidity on CEXs and DEXs is very low. Even selling $100k of tokens can collapse price substantially for tokens with smaller market-caps. You may be able to sell $100k of ETH without price slippage, but the moment it scales to $1 million, you are losing money to slippage.

That assumes you are comfortable parking a million dollars in an exchange (like Binance) after last year's FTX fiasco.



An alternative for users is using decentralised exchanges like Uniswap, Sushiswap, and Balancer. But that assumes the user will bother looking at prices at multiple exchanges, then click the sell button within milliseconds of selling on each exchange and somehow calculate the right amount to be sold on individual exchanges to receive the maximum hypothetical returns.

In the example above, a player like ParaSwap routes the order across multiple decentralised exchanges, assuming the price should not fall below 1% while the transaction is being conducted. The two charts show how much of the asset can be sold before the price moves. This is where you can see a transactional aggregator at play.

- The three exchanges (Uniswap, SushiSwap, and Balancer) can put the capital in their liquidity pools to use through large orders coming from ParaSwap.

- ParaSwap does not incur marginal costs from sourcing liquidity or routing trades across platforms.

- The user minimises costs incurred in transacting across multiple exchanges while avoiding the counterparty risk that comes with a centralised alternative like Binance.

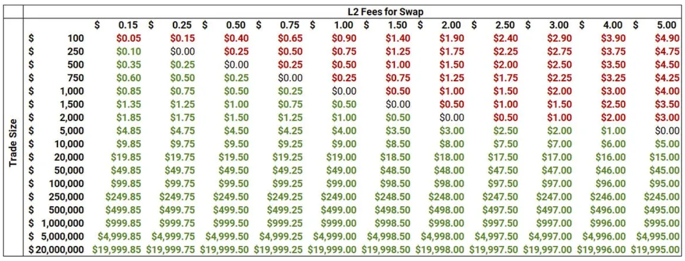
A component drives marginal costs even lower in this equation: the emergence of L2s. In particular, they reduce the on-chain costs to a point where centralised exchanges begin looking inferior. While centralised exchanges charge a percentage fee on every trade, gas fees remain consistent regardless of the trade size.

That is, the marginal cost of trading on a DEX does not necessarily scale with the size of the order involved, presuming there is sufficient liquidity. This is the one part of crypto-economics that is being massively discounted.

When the marginal cost of each transaction trends to nothing, we'll see a whole new class of applications. For now, we are trying to merely catch up with certain centralised businesses that are crucial to the industry. We did the math on how it works for centralised exchanges.

From a purely economic perspective, trade size and gas fees remain the two major factors in deciding whether to use a centralised exchange or DEXs on either base layers or L2s like Arbitrum.

The following table shows how beneficial it is to trade on a DEX on Arbitrum compared to Binance.



Trade Size		L2 Fees for Swap										
		$ 0.15	$ 0.25	$ 0.50	$ 0.75	$ 1.00	$ 1.50	$ 2.00	$ 2.50	$ 3.00	$ 4.00	$ 5.00
	$ 100	$0.05	$0.15	$0.40	$0.65	$0.90	$1.40	$1.90	$2.40	$2.90	$3.90	$4.90
	$ 250	$0.10	$0.00	$0.25	$0.50	$0.75	$1.25	$1.75	$2.25	$2.75	$3.75	$4.75
	$ 500	$0.35	$0.25	$0.00	$0.25	$0.50	$1.00	$1.50	$2.00	$2.50	$3.50	$4.50
	$ 750	$0.60	$0.50	$0.25	$0.00	$0.25	$0.75	$1.25	$1.75	$2.25	$3.25	$4.25
	$ 1,000	$0.85	$0.75	$0.50	$0.25	$0.00	$0.50	$1.00	$1.50	$2.00	$3.00	$4.00
	$ 1,500	$1.35	$1.25	$1.00	$0.75	$0.50	$0.00	$0.50	$1.00	$1.50	$2.50	$3.50
	$ 2,000	$1.85	$1.75	$1.50	$1.25	$1.00	$0.50	$0.00	$0.50	$1.00	$2.00	$3.00
	$ 5,000	$4.85	$4.75	$4.50	$4.25	$4.00	$3.50	$3.00	$2.50	$2.00	$1.00	$0.00
	$ 10,000	$9.85	$9.75	$9.50	$9.25	$9.00	$8.50	$8.00	$7.50	$7.00	$6.00	$5.00
	$ 20,000	$19.85	$19.75	$19.50	$19.25	$19.00	$18.50	$18.00	$17.50	$17.00	$16.00	$15.00
	$ 50,000	$49.85	$49.75	$49.50	$49.25	$49.00	$48.50	$48.00	$47.50	$47.00	$46.00	$45.00
	$ 100,000	$99.85	$99.75	$99.50	$99.25	$99.00	$98.50	$98.00	$97.50	$97.00	$96.00	$95.00
	$ 250,000	$249.85	$249.75	$249.50	$249.25	$249.00	$248.50	$248.00	$247.50	$247.00	$246.00	$245.00
	$ 500,000	$499.85	$499.75	$499.50	$499.25	$499.00	$498.50	$498.00	$497.50	$497.00	$496.00	$495.00
	$ 1,000,000	$999.85	$999.75	$999.50	$999.25	$999.00	$998.50	$998.00	$997.50	$997.00	$996.00	$995.00
	$ 5,000,000	$4,999.85	$4,999.75	$4,999.50	$4,999.25	$4,999.00	$4,998.50	$4,998.00	$4,997.50	$4,997.00	$4,996.00	$4,995.00
	$ 20,000,000	$19,999.85	$19,999.75	$19,999.50	$19,999.25	$19,999.00	$19,998.50	$19,998.00	$19,997.50	$19,997.00	$19,996.00	$19,995.00

The sensitivity analysis uses fees for a swap on Arbitrum and compares it with fees on Binance (0.1% of the trade size). Green indicates that it is cheaper (by the amount) to trade on a DEX on Arbitrum versus Binance, and red indicates otherwise. For example, if an Arbitrum DEX is used to swap $20k worth of tokens when the fee is $2, it is $18 cheaper than the fee on Binance (*the fee on Binance will be $20,000*0.1% = $20*).

An added advantage of DEXs is they are non-custodial: Users are always in control of their assets. We have come to value this after what has been going on with centralised exchanges over the past year.

After EIP-4844 goes live, L2s will incur lower costs while posting data on the L1, increasing the L2 throughput by at least an order of magnitude. EIP-4844 will implement a transaction type to hold a' blob' data space. Note that since moving to proof of stake, Ethereum has separate consensus and execution layers. The blob space only persists on consensus clients. (*We are writing about all the EIPs you need to be aware of in the next newsletter*).

Data inside the blob is not visible to the Ethereum virtual machine (EVM) and incurs only storage costs. Unlike data in regular blocks, this data is only available for a certain period. The absence of EVM dependency and execution costs yields significantly cheaper transactions (*1%–10% of fees before 4844 goes live*).

For now, there is evidence that the DEX volume has shifted from L1 to some L2s. For example, the share of Arbitrum in the DEX volume has increased from ~1% to ~14% in one year versus a drop from ~70% to ~57% for Ethereum.

How It Began

Mounir started working on ParaSwap by himself. He had been building on verticals in transportation and data since at least 2007. So this was not his first foray into entrepreneurship. In 2017, he sought to create an alternative to the decentralised exchanges of the time.

His focus was on improving UX. But during those early days, users needed deeper order books, not an easier interface. And protocols like Kyber and 0x were better positioned for this.

Mounir was working alone with a single external freelancer. He realised that instead of competing against every DEX that was seeing liquidity at the time, he could build a single aggregator that sent the DEXs all orders. Most of the aggregators that existed at the time were more like portfolio managers.

A single interface showed you the value of your assets and the price at which they could be sold at multiple exchanges. However, none of these routed orders the way an aggregator in DeFi does today.

ParaSwap took a few months to build its product, and the company launched in September 2019. At this point, the startup was funded by Mounir's freelance income as the company was not generating enough revenue to sustain its expenses. One of the smart things the firm did during those early days was embedding deep in communities to acquire users. Mounir was a contributor in a chat with some 3000 members at the time.

It is where he found his initial users. But there was no explosive growth just yet. What he had very a subset of users that loved his product and a vast majority that did not care.

By March 2020, DeFi summer was about to kick off. Still, the crash in the market meant no investors were willing to write a cheque. With Compound launching its token in July, the sentiment in the market changed. ParaSwap received commitments worth three times as much as they were in the market to raise.

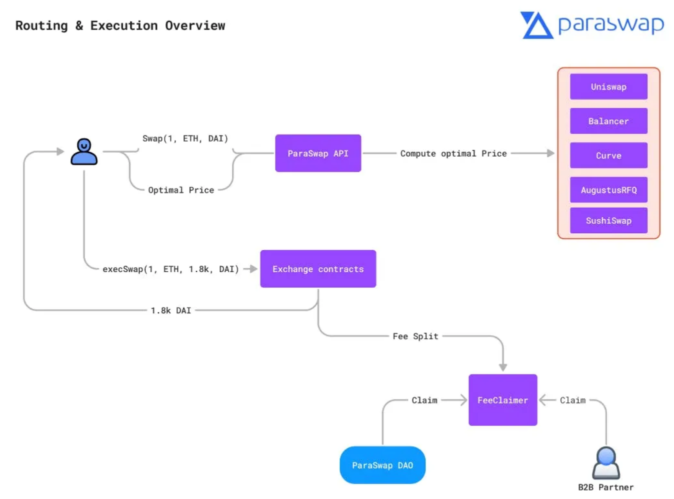
The firm went from just Mounir and a freelancer to having over 15 people in months. I think there's a lesson for founders raising in the current bear market. Sometimes, most of achieving 'success' in venture land is surviving long enough for markets to turn. We also saw this variation with Sky Mavis, the studio behind Axie Infinity.

Part of what helped Mounir navigate those months (in 2019) was his continued tinkering until he found PMF. He survived long enough for sentiments on the product to change. If a founder moves on to something else (like AI), the person would not have the context to build on when sentiments eventually change. ParaSwap evolved from the hundreds of conversations with fellow founders and users that helped build context about market needs.

The current ParaSwap model has a single function: provide large volume exchange transfers and the best pricing possible. ParaSwap has a pricing aggregator that sources prices from DEXs and off-chain pricing (*RFQ, or request for quotes, from the likes of 0x*). Although this appears simple, it's not always the case. Constant pool imbalances in DeFi mean there is always room for finding better rates for users.

For example, say a user wants to swap USDC for ETH. The straight path from USDC to ETH may not yield the best rate. USDC to sUSD to ETH is likely more optimal when the user wishes to perform the swap. So ParaSwap continuously checks for the best possible route, which may not always be the shortest.

Now, say the best route can only accommodate part of the order, necessitating the execution of the rest through the next best paths. Sometimes pathfinding requires splitting the order into multiple chunks. Once the best possible rate is displayed and the user agrees, the swapper contract executes the swap.



From ParaSwap's documentation

But how does any of this even make money? Structurally, ParaSwap's customers want to move large batches of one asset to another. These can either be institutions or third-party DeFi applications like wallets. One may not think of these as such, but Robinhood and PayPal, for instance, are one of the largest custodians of digital assets.

ParaSwap drives growth by embedding itself as a thin layer among applications that help users interface with digital assets. Say a wallet like Argent wishes to enable someone to swap $100K worth of tokens. Argent itself does not want to bother taking the risks of facilitating a swap. They embed a player like ParaSwap to fetch the best prices and enable an exchange for the user.

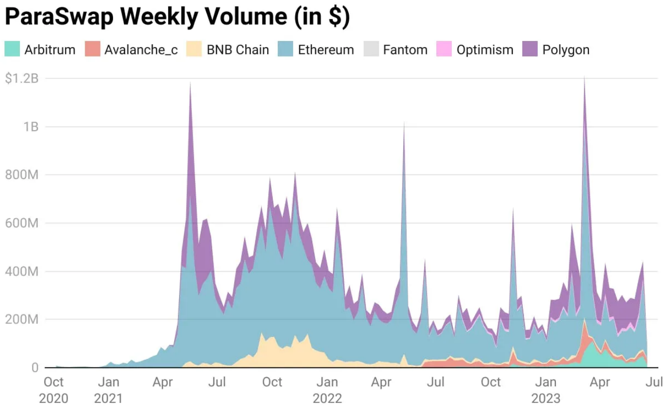

ParaSwap Weekly Volume (in $)

Chart: Saurabh Deshpande • Source: Dune (@sixdegree)

On its own, these standalone integrations may not mean much. But with the growth of the ecosystem of applications using ParaSwap as a thin layer for facilitating swaps, the volume that goes through the product also grows. One place where you may have unknowingly already used ParaSwap is Aave. When you take a loan and swap the asset on Aave, the product uses ParaSwap to facilitate that transaction.

But what portion of ParaSwap's volume comes from businesses? As it stands, 2/3 of the volume on ParaSwap is from external sources. That is, the orders come from SDKs that are embedded in third-party applications. Keep this stat in mind, as we'll be revisiting it shortly.

Here is a summary of the economics at play:

- When wallets like MetaMask and Argent use ParaSwap for their built-in swaps, they charge a fee to the user. Although these wallets get to use ParaSwap's services for free, ParaSwap takes 15% of the fee these wallets charge their users. ParaSwap has over $2M in annualised fee revenue in 2023 compared to 1inch's $2.24M and CoW Protocol's $5.56M.
- When a user initiates a swap, the expected amount of the asset is displayed to the user. If more than the expected amount comes back to the user due to more inefficiencies (created in

the time between the swap being initiated and executed), ParaSwap keeps half of the excess amount.

For example, if a user goes to swap $100 in USDC to USDT and sees a quote that said they would receive $99.75, but the smart contract returns $99.90, ParaSwap would keep the extra $0.15.

Such pricing inefficiencies are rare for smaller transactions but frequently occur when swaps are conducted for large sums.

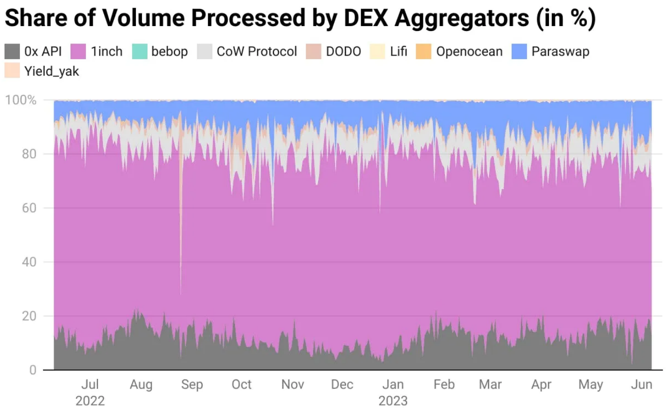

Share of Volume Processed by DEX Aggregators (in %)

Chart: Saurabh Deshpande • Source: Dune (@sixdegree)

DeFi aggregators are evolving from competing to having a clear pecking order. 1inch, for instance, has maintained a clear lead, controlling 60% of the market for multiple months. Given how power laws work, aggregators are forced to expand towards newer markets. In our view, the market has evolved over the past year in response to FTX going down.

If regulatory scrutiny continues focusing on centralised, spot exchanges like Binance, the volume will trend towards their decentralised peers like Uniswap. That window of opportunity for DeFi may emerge in the coming months.

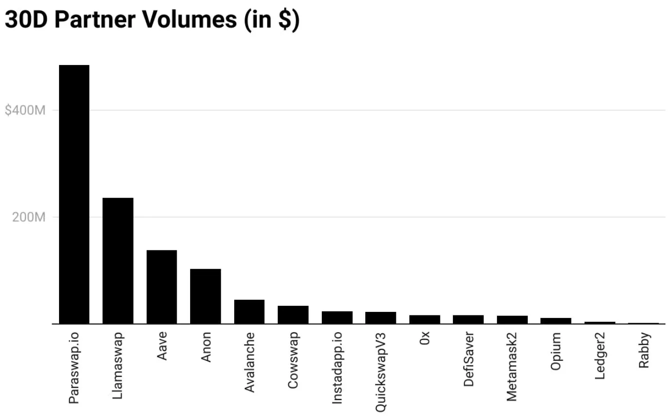
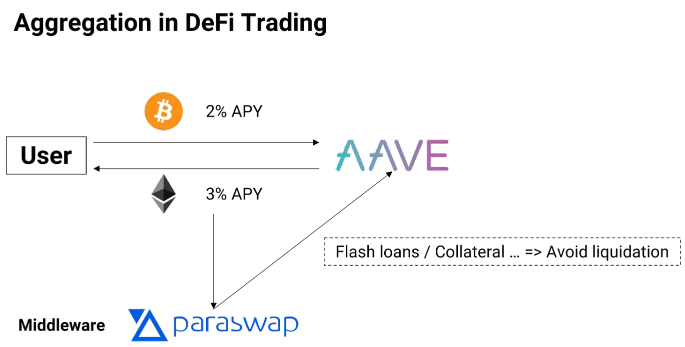

30D Partner Volumes (in $)

Chart: Saurabh Deshpande • Source: ParaSwap Dashboard

For ParaSwap to maintain relevance and evolve to absolute dominance, it must consider a different way of approaching users altogether. Many of these approaches are replicable by 1inch, but based on our observations, **aggregators do not differentiate themselves with infrastructure alone. They also offer services such as analytics or user behaviour data.**

Web2 applications stick with an aggregator due to all the additional offerings it can offer. We have seen a variation of this with Li.Fi aggregating bridges. Teams embedding their offerings are not coming for the bridges alone but for the value-added services they offer.

Looking through this lens, we believe that ParaSwap will evolve from being an aggregator (*and thus competing with 1inch*) to focusing on embedded models of driving volume. It may seem far-fetched, but remember, 2/3rds of ParaSwap's volume comes from external sources today. Currently, 57 businesses rely on ParaSwap to enable users to transact.


Aggregation in DeFi Trading
2% APY
User
AAVE
3% APY
Flash loans / Collateral ... => Avoid liquidation
Middleware
paraswap

Aave's integration of ParaSwap shows what true composability using SDKs in DeFi looks like. It takes collateral from a user's debt position, converts it, and repays the loan, all without the user ever having to leave the app. This is what the future of ParaSwap looks like.

Embedding the Future

To understand why embedded forms of finance will be required going forward, we need to go back to the early 2000s, when eBay was taking off. At the time, to make payments meant, you placed an order online, sent a physical cheque to the seller, or transacted manually through a bank.

This meant that confirming an order might take weeks, the cheque might be bounced, or users would lose interest because physically going to the bank might be inconvenient. PayPal solved this by offering a simple payments page that could be embedded directly on eBay. All of a sudden, users were not going elsewhere mid-transaction.

This may be the norm in the age of Apple Pay, but consider how Web3 interactions work today for the tail end of assets. We presume that users will go to Uniswap, convert ETH or stablecoins to the required token, return to the platform, and continue their transactions.

I believe wallets and service providers will begin embedding exchanges in their apps directly. On its own, this is not a big deal. You can embed Uniswap or a third-party decentralised exchange with relative ease. But a single SDK that looks at all the permutations and combinations an asset can flow to acquire the best price? That's where ParaSwap will kick in.

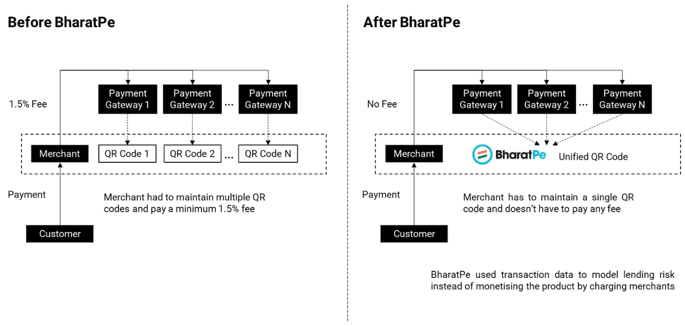
This story has played out in finance earlier. A relevant example is that of BharatPe.

November 8, 2016, was pivotal for India's digital payments industry. The Prime Minister announced demonetisation - a point in time when the currency people held at home (as notes) was no longer valid. While local businesses like Kirana stores (the mom-and-pop stores in India) that dealt in cash were reeling from the shock, digital payment companies rejoiced.

In 2016, India had just over 12.5 million Kirana stores. Due to the shock to the cash system, moving to digital payments was the way forward. Wallets like Paytm and PhonePe began acquiring customers in the region, but UPI - the payment system used, was not widely adopted yet.. Two other problems hindered the widespread adoption of digital payments:

- The biggest was every payment processor, or wallet operator worked in silos. That is, everyone had a unique QR code. This meant that the shop owners would have to install multiple QR codes if they were to accept money from numerous wallet providers.

- While the transaction was free for users, every payment processor charged at least a 1.5% fee to the merchant. This meant the merchants' bottom line would get further hit in profit-starved businesses. For example, for an Rs. 1,000 (~$12) purchase where the typical margin was Rs. 100–150 (~$1.2–$1.82), the shopkeeper would have to pay Rs. 15 (~$0.18) as commission to the payment gateway.



Merchant had to maintain multiple QR codes and pay a minimum 1.5% fee

Merchant has to maintain a single QR code and doesn't have to pay any fee

BharatPe used transaction data to model lending risk instead of monetising the product by charging merchants

Enter BharatPe. Started in Mach 2018, BharatPe utilised one of the most critical features of the UPI stack – interoperability. **Merchants would now only have to use one QR code regardless of which payment gateway or processor the user was using.** BharatPe installed these QR codes nationwide (with over 5 million merchants onboarded).

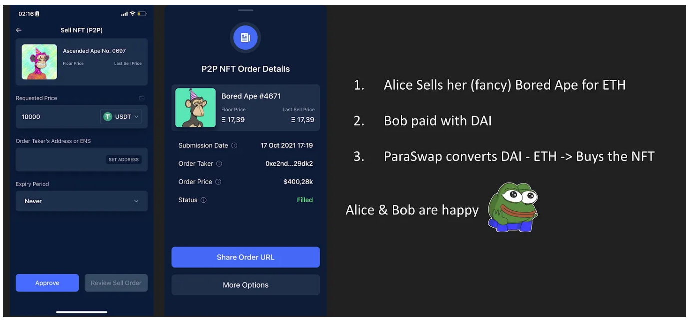
This took care of the first problem mentioned above. Having worked at Grofers (an online grocery delivery startup in India) as the CFO, Ashneer Grover realised charging commissions to merchants operating on razor-thin margins was not the way to scale the business.

Although merchants were not happy with paying commissions for payments, they were more than happy to pay interest on short-term loans they would require for their businesses now and then. Despite micro, small, and medium enterprises being vital elements of the Indian economy, private banks were reluctant to extend loans to them due to the lack of collateral or documents.

BharatPe used data from its QR codes for risk management to start offering loans to merchants without requiring collateral. This took care of the second problem mentioned and created a source of revenue despite offering critical services for free.

Now we won't go into more examples of fintech behemoths forming out of embedded finance being a thing, but we see a variation of this happening live with ParaSwap and NFT markets today. For instance, a user wishes to sell their NFT for DAI, and a different user wishes to pay with ETH.

ParaSwap makes that exchange happen with one click, which means, in the future, there will be no ETH-, SOL-, or Matic-based NFT markets. Products like games, fintech apps, or DeFi platforms can embed a single SDK from ParaSwap and enable transactions in any token. The challenge here for ParaSwap would be to expand to bridging assets – a feature they do not currently offer.



Ascended Ape No. 0697
Floor Price
Last Sell Price

Requested Price
10000 USDT

Order Taker's Address or ENS
SET ADDRESS

Expiry Period
Never

P2P NFT Order Details

Bored Ape #4671
Floor Price Ξ 17,39
Last Sell Price Ξ 17,39

Submission Date 17 Oct 2021 17:19
Order Taker 0xe2nd...29dk2
Order Price $400,28k
Status Filled

1. Alice Sells her (fancy) Bored Ape for ETH
2. Bob paid with DAI
3. ParaSwap converts DAI - ETH -> Buys the NFT

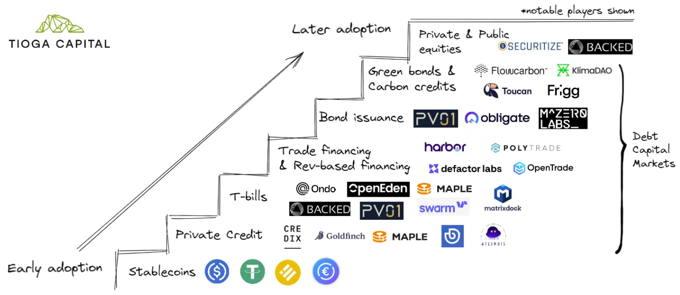
Alice & Bob are happy

A breakdown of how Paraswap enables NFT markets from internal documentation.

Users do not flock to DeFi instead of exchanges because of the former's lack of options. Today, you cannot do margin, options, spot trading, and lending through a single interface in DeFi. Even when the apps exist, there are no market makers facilitating volumes. One avenue for ParaSwap to expand into would be to be the financial backbone routing liquidity for all kinds of primitives in crypto. Today, they focus on spot assets. But what's stopping them from making debt positions tradable?

The challenge most stand-alone options or insurance products face today is volume. Around 30,000 wallets interact with ParaSwap daily. Offering an interface where users can purchase these instruments through ParaSwap is the lowest-hanging fruit. And it is likely that its peers, such as 0x Protocol and 1inch, follow it when that does happen.

But how do you build moats in such a system? Regulatory provisions in traditional payment rails like ACH or Visa make the entry barrier high. In open-source monetary networks, anybody can emerge and compete. As stated earlier, the way forward is for ParaSwap to front-run new product categories. What would those categories be? The image below offers some clues.



The range of assets supported by DeFi has barely scratched the service. The image above is from Tioga's Substack.

One of the directional bets ParaSwap could take at this point is to focus on institutional clients. An RFQ-based product built by ParaSwap allows exceptionally large orders ($10 million+) between verified, compliant counterparties to trade with one another. In such a system, ParaSwap does not have to worry about providing liquidity for trades but offers the interface for routing orders.

In such an instance, the moat will come from the number of large institutions that follow on to such a product. We have verified that the team onboards several market-makers to focus on such a product. Liquidity begets liquidity. The more the number of institutions onboarded to such a system, the higher the probability of other institutions joining.

Another direction is to look at niche assets that have not yet found a large enough market. One of them is RWA assets. Aave and MakerDAO realised the limits of over-collateralised lending with on-chain assets and expanded to off-chain instruments focused on institutions. ParaSwap could theoretically look towards offering infrastructure that settles bonds and t-bills between counterparties that know one another. In both instances, the assumption is that there will be a market for

- Institutional clients leveraging DeFi or
- Newer instruments are coming to market, as we saw with NFTs in the last cycle

Creative Destruction and Moats in Networks

It helps to see how other industries have evolved to learn how the newer ones may evolve. The payments industry has three key players – banks, payment networks, and payment aggregators.

- Banks are where users hold their funds. Wallets in Web3 play this role.
- Payment networks like Visa and MasterCard provide infrastructure and networks for processing transactions between different stakeholders like merchants or card issuers. They are similar to a blockchain a payment takes place on.
- Payment aggregators allow merchants to accept payments from multiple payment networks.

The likes of Visa and Mastercard make money by charging a transaction fee. Visa owned 60% of the payments network space, followed by Mastercard (25%) and AmEx (10%). **The network effects of payment networks are a difficult entry barrier** to overcome for other new entrants; therefore, it is difficult to disrupt incumbents and change practices like charging a transaction fee.

Payment aggregators like Stripe, PayPal, and Square allow merchants to accept payment via payment networks like Visa. But they have not launched a direct competitor to Visa or Mastercard.

Unlike payment networks, aggregators earn revenue via integration or setup fees which cover the cost of merchant onboarding and value-added services. **The point is aggregators facilitated more activities instead of just connecting different payment networks. Over time, their value-added services are what attract customers.**

The further a business moves from the consumer, the lower its probability of setting the price. ParaSwap's current challenge is addressing the obsession with an SDK-based approach to growth. This obsession can reduce its ability to capture value for itself. The only way to change that equation is through driving volume.

Amazon can renegotiate its pricing with vendors due to the volume it offers. Blur changed how we thought of NFT royalties because of the volume they drive. If ParaSwap can command a substantial share for emergent DeFi primitive volumes (like options or insurances), chances are high that it would be able to set a higher fee for itself in exchange for product discovery.

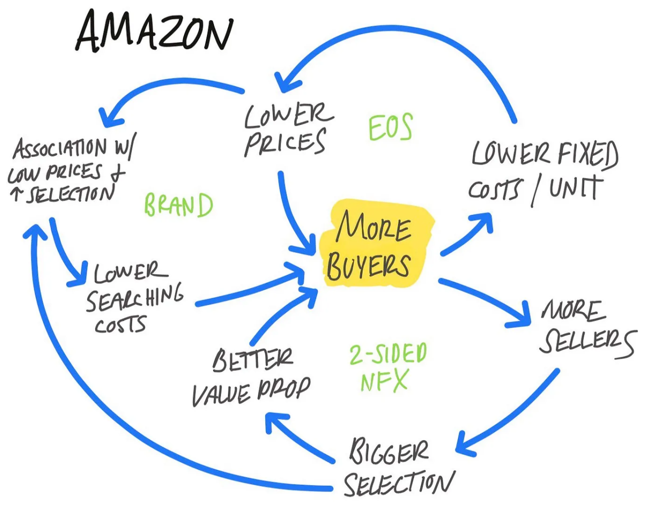
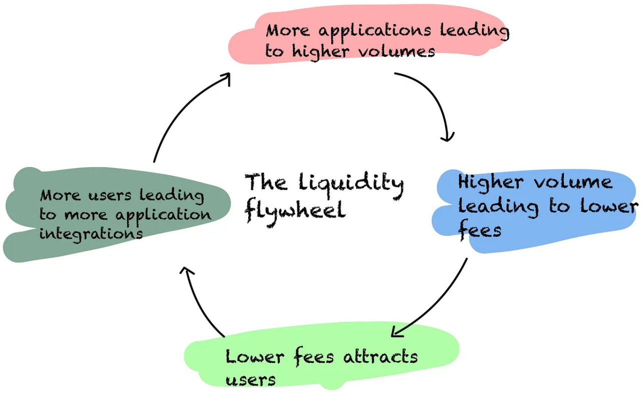


Image from Max Olson

Creating a moat through pricing alone does not happen in open-source money networks. What may happen is - if a single aggregator can plug into multiple products (like wallets, Dex, and AMMs), it may be able to facilitate the movement of liquidity across all of them. In turn, it could offer better pricing for users. By default, that should mean users would have an affinity for products powered by a service provider.

In such a system, ParaSwap's growth is contingent on its ability to onboard service providers and applications whilst using its token to incentivise the behaviour of users through products it is embedded in. Instead of users trading on ParaSwap, even a wallet that uses an SDK embedding could be given rewards or incves.


More applications leading to higher volumes
Higher volume leading to lower fees
The liquidity flywheel
Lower fees attracts users
More users leading to more application integrations

This creative destruction of the self, where ParaSwap evolves from being a standalone price aggregator to a multi-asset, thin embedded protocol servicing multiple products, is where the opportunity lies for ParaSwap. In that pursuit, they may have to integrate (or build) bridges and data layers for better price feeds.

The way I see it, their focus on business applications is likely the way to build a moat. More applications can translate to higher trading volume. This, in turn, should help them reduce fees & lower fees, and should help attract more users. We will slowly start seeing applications built on Ethereum take a page from the ecosystem playbook most L1s have been perfecting over the years.

It may seem far-fetched. But consider that when Blur launched, much of its orders occurred elsewhere. As user behaviour changed and threshold liquidity was reached, the marketplace switched to settling orders in-house. ParaSwap is already at a point where it can absorb and close out orders without sending them elsewhere.

The moat is not in pursuing the supply side more but in building the demand side. The demand side comes only through more users, wanting to use more on-chain instruments from more DeFi platforms at the lowest price possible. It is almost as though DeFi primitives will have to do with financial instruments, what Amazon did with consumer goods.

That is the challenge that lies ahead for Mounir and the team.

Disclosures

1. *I am an investor in LiFi - one of the bridges mentioned above.*

Telegram and Pitch Decks

Join in with ±4000+ researchers, investors, founders & overall great human beings. We don’t exactly talk much, but it would help you stay close to what we are focusing on & connect with others building cool things.

Join the community

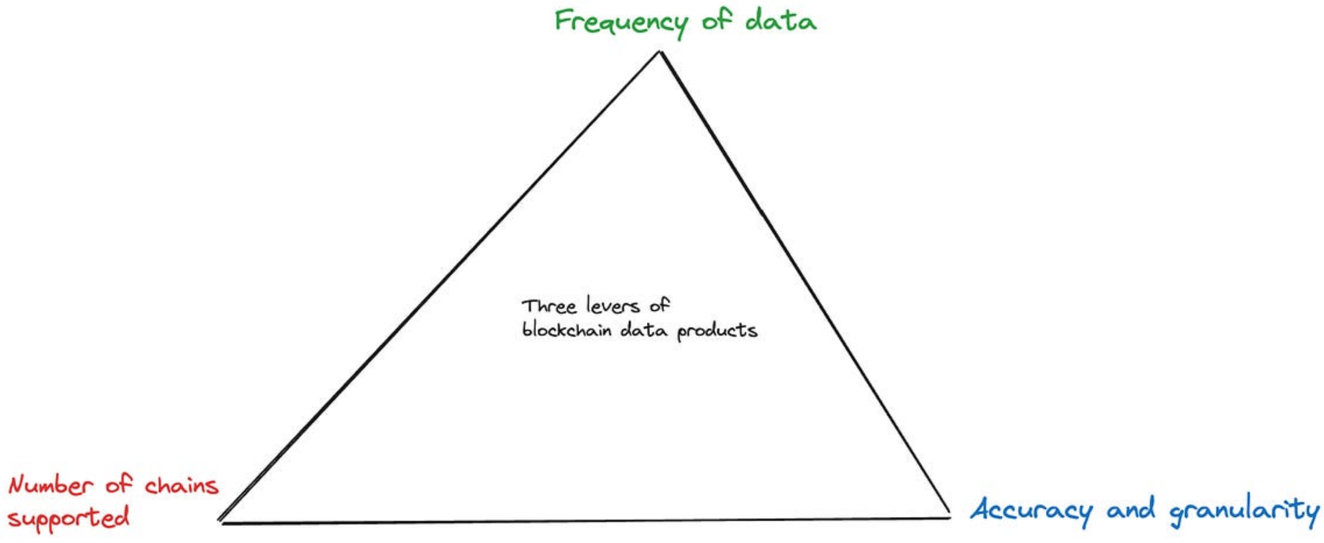
We have been actively deploying money & advising a small crew of founders. Contact us through the form below to go 0 to 1 with your early-stage venture.

Form for founders

Joel John
decentralised.co

The Data Wars

Building monopolies off public goods.

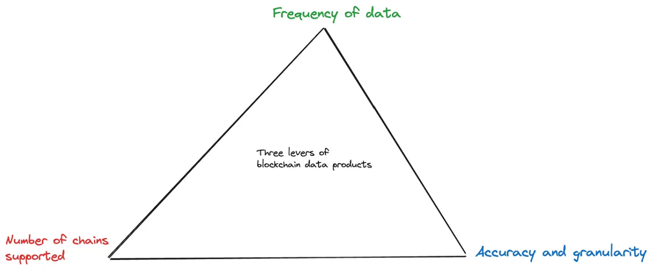

Frequency of data
Three levers of blockchain data products
Number of chains supported
Accuracy and granularity

Hello there!

This is issue three (3/8) of the beta version of our paid newsletter. Do send in feedback if you think there is something we can improve on.

Last weekend, I grimly realised that building monopolies off goods that should be public is no longer possible. For instance, the monopolies on packaged water have already reached scale, and you can't compete with them anymore. I'm not sure I want to cross the ethical lines of selling packaged air. But one asset that is accessible to everyone and generates wealth is blockchain data. You can query it off Etherscan, run your own node, or print copies of every transaction on the blockchain ledger and keep it at home.

I recommend you not try the last one for environmental reasons, but here's the point. Blockchain data is free, publicly accessible, and constantly being produced, yet there's a billion-dollar ecosystem built around it – $10 billion if you include publicly traded tokens. Nansen alone was valued at $750 million in their latest round. So, how can firms take a public asset and profit from it?


Frequency of data
Three levers of blockchain data products
Number of chains supported
Accuracy and granularity

Data products in Web3 have three levers they can tinker with. It is rare to see a product that combines all three extensively as each requires a different specialisation.

Data vendors like Nansen, Arkham and Santiment are visual layers atop blockchain data. They index (store), query and display public data. When you subscribe to these products, you effectively pay for their ability to visualise on-chain situations. Nothing's stopping people from visualising the same things as their competitors, so consumer prices for data products in Web3 are usually a race to the bottom. In this regard, blockchain data differs from privately held data at monopolies like Alphabet or Meta.

Only the guys at Facebook can peer into user data and uncover insights like 'you did this cringe thing 12 years back' in your notifications. With blockchain data, everyone can do that. (*Imagine notifications for all the regrettable purchases you have made through Uniswap or OpenSea.*) Jokes aside, data is weaponised through using it for product insights that retain users for longer amounts of time, often causing them to feel more miserable. The algorithmic feeds we see on YouTube or Twitter come from such data.

During bull markets, the value proposition for a person spending $1,000 on a data subscription is quite easy. If they have a portfolio of $100K, having a slight edge that generates a 1% outperformance in their portfolio justifies the subscription. In a bear market, when these traders are (possibly) liquidated, that subscription is the first to go out the window. Therefore, consumer-faced data products are challenged by a lack of moats and revenue that sways with volatility in the market.

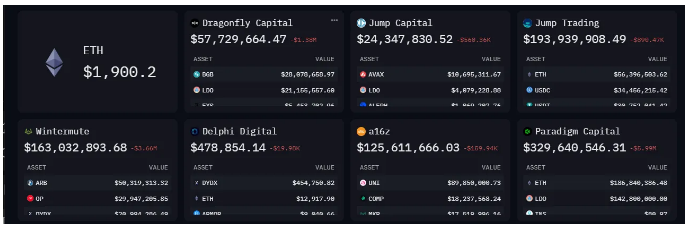
This is part of why we see many VCs rush to back API vendors focused on blockchain data. The revenue these firms have is more predictable and sticky when they focus on selling to other businesses. Often, those contracts can be yearly, so the effort and time taken to make a sale is justified for the period during which it brings in revenue. What, then, is the plight of a data product being sold to customers?

We have been thinking of this internally. The following is a brief mental model on how data products have been differentiating, the opportunities we are seeing and the challenges that lie ahead.

Labels as a moat

How do you differentiate when everyone is building visualisation layers atop the same data? You bring your own elements to interpreting the data. Nansen pioneered the model in 2020 when they launched labels atop their product. Instead of noticing that somebody moved one million of your favourite DeFi tokens to the exchange, you could now see that the person moving them is the seed-stage investor of the tokens. And since Nansen was the only player with that data, users flocked to Nansen at scale.

This was a strong enough moat for a good two years. Nobody had a similar offering until Arkham released its product mid-last year. With its token due for listing on Binance in the coming weeks, Arkham has solved token distribution. But the company has also changed the model quite a bit. Instead of using ML/AI (*or whatever new voodoo magic the data scientists are into*) to label the wallets, they simply crowd-source it and incentivise users with a token. The stranger part is that Arkham has no expenses here for rewarding users. The token is a made-up asset that finds value from speculators on exchanges



ETH
$1,900.2

Dragonfly Capital
$57,729,664.47 -$1.38M

ASSET	VALUE
BGB	$28,078,658.97
LDO	$21,155,557.60
FXS	$5,453,702.96

Jump Capital
$24,347,830.52 -$560.36K

ASSET	VALUE
AVAX	$10,695,311.67
LDO	$4,079,228.88
ALEPH	$1,069,207.76

Jump Trading
$193,939,908.49 -$890.47K

ASSET	VALUE
ETH	$56,396,503.62
USDC	$34,456,215.42
USDT	$30,752,041.42

Wintermute
$163,032,893.68 -$3.66M

ASSET	VALUE
ARB	$50,319,313.32
OP	$29,947,205.85
DYDX	$20,904,286.49

Delphi Digital
$478,854.14 -$19.98K

ASSET	VALUE
DYDX	$454,750.82
ETH	$12,917.90
ARMOR	$9,040.66

a16z
$125,611,666.03 -$159.94K

ASSET	VALUE
UNI	$89,850,000.73
COMP	$18,237,568.24
MKR	$17,519,096.16

Paradigm Capital
$329,640,546.31 -$5.99M

ASSET	VALUE
ETH	$186,840,386.48
LDO	$142,800,000.00
TNS	$80.07

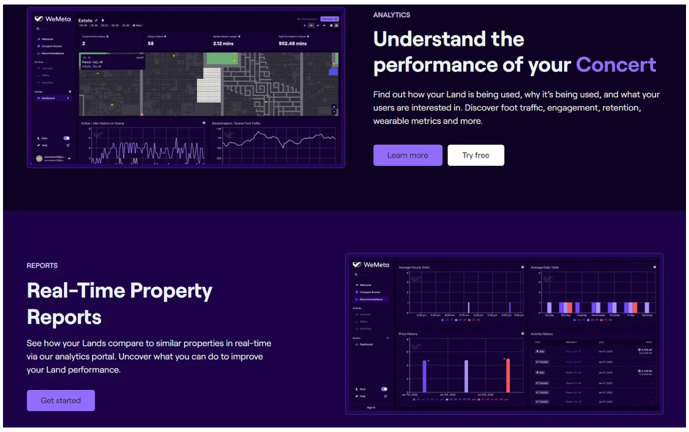
Arkham's genius was in clubbing together multiple wallets held by the same fund and allowing users to see aggregate data on what a fund may be doing.

Since Arkham does not have a paid subscription product (*like Nansen*), the bulk of the value generated (*for investors and founders*) will come from the token. Presuming Arkham sells the token at a meaningful valuation, the dollar figure of those sales may far exceed the cash flows a subscription product sees.

So what's next? Since labels may no longer be the strong moat they once were, firms may expand to offering context for a given transaction. Let me explain.

Context as a differentiator

The primary consumers of blockchain data products in subscription models are traders or funds investing in digital assets. Soon enough, that subset may change into gamers, musicians and, well, real estate developers. Last year, during the metaverse boom, I came across data platforms using AI to predict possible land price surges in Decentraland using user activity metrics. I would presume a large chunk of those businesses have now had to wrap up, given the lack of activity. But the tech was real — and well ahead of its time.



ANALYTICS

Understand the performance of your Concert

Find out how your Land is being used, why it's being used, and what your users are interested in. Discover foot traffic, engagement, retention, wearable metrics and more.

REPORTS

Real-Time Property Reports

See how your Lands compare to similar properties in real-time via our analytics portal. Uncover what you can do to improve your Land performance.

Wemeta.world was one of the startups offering metaverse analytics during the boom phase of the last few years.

As sectors like gaming and music take off on-chain, we may see a new class of analytical products that surface insights that are highly contextual and relevant for a new audience subset. One place we have seen this *(in our deal flow*) is with products focused on giving retention and consumer data about dApps. Say you have a dApp that is a competitor. You can realistically map out every wallet address that uses it, filter it to show the top 1,000 users and see how engaged they are in a 30-day period. All that data is there on-chain.

But as a founder, you likely don't want to spend 10–15 hours cleaning up all that information. A new class of analytic tools may soon allow teams to map out wallet addresses to Twitter handles, making it easier for marketing departments at B2C dApps to target customers considerably better. In each of these instances, the moat comes from a firm's ability to interpret on-chain data and provide it in a context-relevant way for the teams consuming it.

The asset is not the data but the IP that enables interpreting these on-chain events. This makes me believe the next unicorn in on-chain data won't be focused on trading but will be an enabler of B2C use cases.

On-chain feeds and perspectives

We have spoken to at least three teams building algorithms-as-a-service for Web3 content. The premise is simple. As on-chain content explodes, users will need services that curate and surface the way we see on Lens or Mirror today what is trendy and interesting. There are multiple ways to do it. You can check whose content is being collected on Lens the most, create a social graph that verifies a wallet's social signal based on the other wallets interacting with it or check the smart contract interactions it has had.

Would you rather follow Sequoia's wallet or be the first person to have interacted with YFI's wallet? (*I don't quite know the answer to that. But here's a random trivia: as I write this, there's a $750 bounty on Arkham for sharing all of Sequoia's wallets publicly.*)

There are multiple ways to go about it, but in my view, services that help users tweak, iterate or develop their own algorithms to consume on-chain data would be key contenders in the next market cycle. These products would enable users to see when their favourite artists or writers have issued content they can collect or use for access to events.

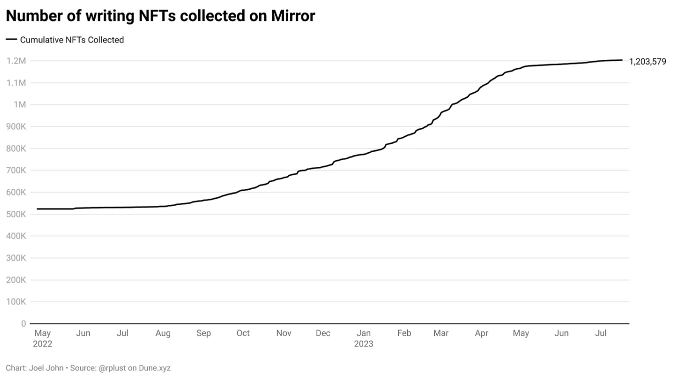

Number of writing NFTs collected on Mirror

Chart: Joel John • Source: @rplust on Dune.xyz

The number of writing related NFTs on Mirror have crossed over a million in the past few months.

There are two ways this can evolve: users may log into their content clients and pick and choose algorithms best suited for them, or users may want to tweak the algorithms to their own preference from multiple platforms. Think of getting the best content from Twitter, Instagram, YouTube and so on in a custom client that curates content based on your preference.

It is a far-fetched, utopian vision for now, and we are still figuring out how the firms in our deal flow will figure out distribution. However, there's a different way to look at data products, and that is through perspective.

Let me explain what that means with an example from Saurabh. A user trading at a decentralised exchange needs exact data on the price and time at which they sold (or acquired) an asset. All such data is needed for the taxman; however, none of it is available today with precision on subscription products like Santiment. The reason is quite simple. All such products are built from the perspective of a trader looking to gather data on the usage of a decentralised exchange. Not of that of a consumer looking to export their own data as you can from an exchange like Binance. (*Saurabh's note: Some of these products exist today but are restricted to enterprise clients*).

It is not what is on-chain already alone that matters. Data that is waiting (*and competing*) in memory pools of different node networks is also critical from a sophisticated trader's perspective. Data providers that run nodes across various providers and help aggregate their mempools are of immense value to those trading in size. We have not yet seen firms specialising in that kind of data scale to size just yet.

There are a new crop of data products solving for perspective when it comes to DeFi. But if you extrapolate the concept to more nascent themes like gaming or music, you will see that the bulk of them barely consider what is needed by a user that is not looking to speculate would want. It is quite possible that creating discovery graphs of on-chain music is not a profitable endeavor, and the TAM for that is less than a thousand users as of today.

But until that tooling evolves, we may be running around in circles with data in a few ways

1. API providers will compete with one another on pricing and lose B2B clients to one another as they race to the bottom on price;
2. B2C-focused (*primarily traders*) products will struggle to generate subscriptions in a bear market and see the opportunity that emerges with issuing tokens; and
3. Those focused on emergent themes (*metaverse, gaming, music*) will struggle with a small TAM.

These are all battles worth picking if you have a long-term bullish thesis on Web3 as an industry. In the last cycle, one of my favourite analytical teams closed shop in March. Had they stuck around a quarter more, it is quite possible they would have been worth a few hundred million.

As with most things in life, the outcomes for on-chain data products are neither predictable nor consistent. All you can do is turn up and build.

Signing out to turn up and build (*err write*) our long-form for this week.

Joel John

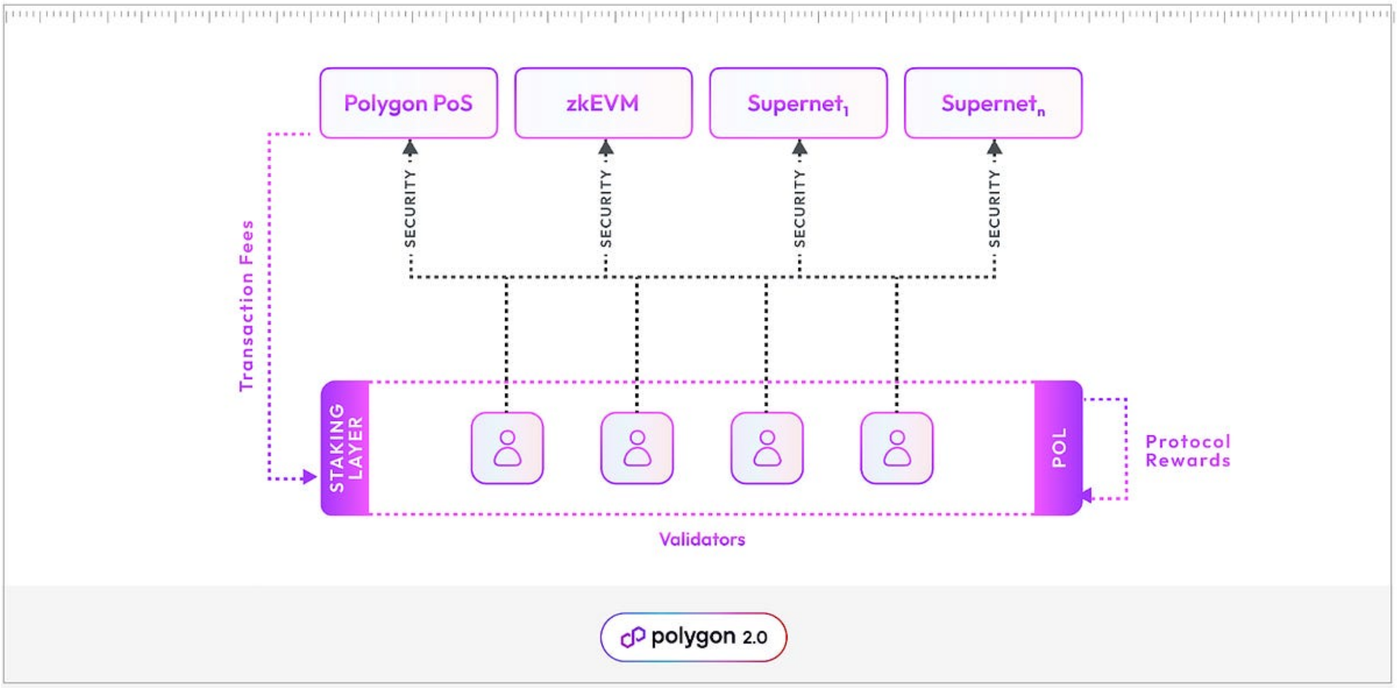
P.S. I could not delve into the dynamics of data networks with tokens (like Covalent), but that will be for a long form in the coming weeks.

1. *I am an early stage investor in Nansen.*
2. *I was an early stage advisor to Covalent.*
3. *We are looking at multiple data-protocols as Decentralised.co for both commercial partnerships and active investments.*

Saurabh
decentralised.co

Token Mergers

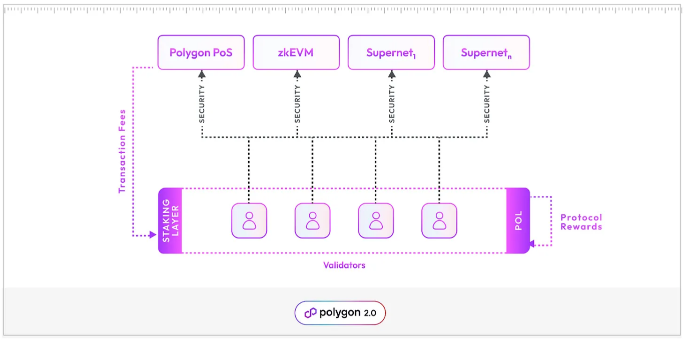
Maybe we need investment banks for these.



Hey there!

It seems to be a merger (*rebranding*) season in crypto. Earlier in July, Polygon announced a new token, POL, due to its architectural overhaul. The old MATIC token will be swapped in a 1:1 ratio to POL. The Polygon ecosystem is currently home to multiple chains such as Polygon POS, Polygon zkEVM, and Supernets.

The new architecture allows validators to vote on multiple chains. The image below summarises how they think of it.



Source – Polygon

The architecture demands an upgrade of the token contract since all these chains can now be staked in one place and used to validate on multiple layers. The new ticker is also a rebranding exercise to signal significant changes in the ecosystem

It is not just a technical change but also an organisational restructuring. Before this, Polygon had completed two significant acquisitions,

- Hermez Network ($250 million) and
- Mir Protocol ($400 million) to expand its zero knowledge (ZK) capabilities.

These mergers got us thinking about general mergers and acquisitions (M&A) activity and how it applies to the cryptoasset industry.

Let's begin with an understanding of why mergers occur in the first place. The goal of any enterprise is to create value for its stakeholders. Companies typically do this by selling products or services, but sometimes they merge with or acquire other companies. **The logical reasoning behind a merger is that the value of the whole is greater than the individual parts of the two or more companies merging together**.

During periods of market turbulence or consumer apathy, firms are incentivised to merge to reduce competition and increase margins on the remaining customers. Fewer resources are spent on battling for the same consumer subset. An early instance of this on the internet was between X and Confinity.com - which eventually became known as Paypal and was acquired for $1.5 billion in 2002 by E-bay.

Consolidation leads to better unit economics and value accrual for shareholders. It seems a win-win for most parties except consumers with limited choices and employees who often get laid off in such processes. A different way mergers occur is when a dominant player acquires multiple smaller ones because of their ability to have better unit economics. Standard Oil's steady acquisition of oil companies leads to the firm owning 90% of the market in the US. AT&T played a similar move with telecom networks in the 1920s.

Now for the fun stuff.
How does any of this apply to crypto?

M&A In The Age of Digital Assets

There are two kinds of M&As we see in Web3. First is that of centralised firms acquiring other centralised firms. The other is networks partnering to co-build a new narrative. We have not yet reached sufficient levels of market maturity to support a network acquiring a centralised business.

Amberdata's acquisition of Genesis Volatility (GVol) is an example of a good acquisition in the crypto industry. Amberdata is an institutional data provider with many capabilities. But they lacked sophisticated options for market analytics. GVol had built its product in the options analytics niche. Since Amberdata's existing institutional clientele requires options analytics, integrating GVol into its offerings was not difficult. In this instance, the firm seems to be expanding its product suite to retain users longer.

Binance's acquisition of CoinMarketCap (CMC) can be seen as a product extension and user acquisition strategy. Since Binance is primarily a B2C company, CMC acts as the top of the funnel for the exchange. Although CMC didn't have robust monetisation methods, it was among the applications with the most number of users.

OpenSea's acquisition of the NFT aggregator Gem in April 2022 has proved ineffective. Almost a year after the acquisition, OpenSea unveiled OpenSea Pro, a platform aggregating NFT marketplaces for traders. This was supposed to be OpenSea's answer to Blur, but the delay has probably forced OpenSea to cede a lot of ground.

A part of the reason can also be because the user is forced to go to a different website, pro.opensea.io, instead of opensea.io. The latter doesn't show any listings from other marketplaces, whereas Blur, by default, shows all the listings and has the power of incentives to ensure that Blur listings often give the best prices.

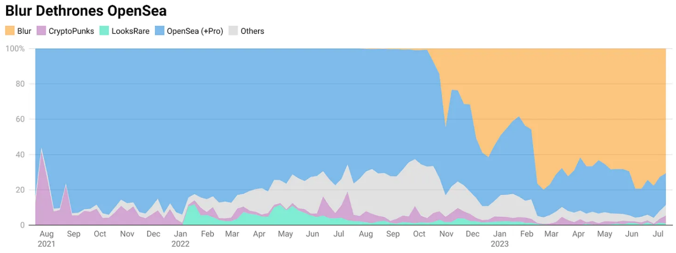


Chart: Saurabh Deshpande • Source: Dune (@hildobby)

(*Caveat: Part of what may have made the acquisition outcome bad may have been OpenSea's inability to release a token without exposing themselves legally. When you have a valuation of $13 billion, you do not want to do anything that may affect it or the probability of an IP)*

When it comes to tokenised networks, mergers are a bit more tricky because you have a very diverse set of decision-makers, each with very different views on how a merger should look.

1. Founders - Founders of protocols or applications with tokens expose themselves to heightened volatility (and possible depreciation) of the tokens they are entitled to.

2. Investors - May have less of a say in what the new merged token should do. In fact, they may even sell in response to a merger and push prices lower.

3. Holders - Cultural mismatches between two networks with live tokens would mean it takes a while for people to align around what are shared goals.

And so, if you look historically, there's only been two kinds of mergers

1. A centralised fund takes over an almost dead network and rebrands it into something new for the narrative. Omisego's rebrand into Boba fits that bucket.

2. A liquid token takes over a centralised entity with IP and tech and merges it internally for the narrative. Polygon has been exceptionally good at this.

The common theme? Narratives. Yearn Finance went on an M&A spree in late 2020. It merged with protocols like Cream Finance, Pickle Finance, Acropolis, and Hegic. The goal was to collaborate with these protocols and expand Yearn's offerings.

These were not token mergers but the cooperation of developer resources of these protocols. Since tokens were not involved, the total value locked (TVL) is probably the best metric to judge whether Yearn benefitted. Yearn performed better than its peer yield aggregators and led the pack in TVL terms. Narratives can meaningfully drive actions. **And sometimes, in crypto, that's all mergers are about. Driving narratives, which can drive actions.**

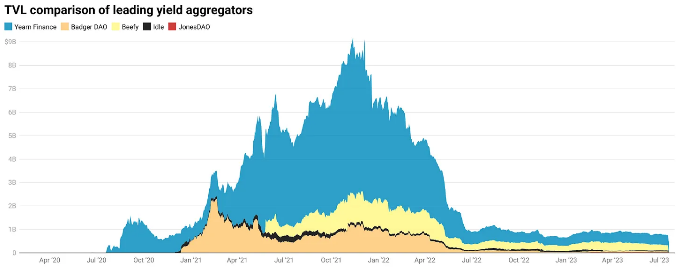


Chart: Saurabh Deshpande • Source: DefiLlama

Crypto has seen a fair share of M&A, but there's often an added motivation of rebranding involved. For example, why does the token need a new name when Polygon wants to upgrade the MATIC contract? Remember ETHLend? Aave, erstwhile ETHLend, started as a peer-to-peer lending protocol for ETH and ERC-20 tokens. Later, the protocol was upgraded to the current pooled capital model and rebranded to Aave.

Strong brands attract a premium because they signal quality. As a result, building a brand is always one of the objectives for companies or projects. But at the same time, brands also get a bad rep.

Our minds somehow seek comfort in associations while navigating the world around us. It is difficult to change those associations quickly. So, instead of changing, it is often easier to create new associations. For some reason, my first reaction to Matic is *"the Ethereum sidechain that just about worked when other scaling solutions were not ready"*, but when I hear Polygon, it is *"an ecosystem that aims to scale Ethereum with zk rollups at its core"*.

The people developing the network are the same, but the messaging has changed as they pivot to better technology. M&A or organisational restructuring often allows teams to change branding and create new associations with their brand. We want to retain strong brands; if the older ones are weak, we want to move to stronger ones.

There are a few attributes that make these kinds of mergers interesting.

1. If the merger is paid for in the native asset of the network, the costs incurred are not borne by management or investors as in traditional mergers. It usually happens from the network's treasury or minting of new assets.

2. Minting a new asset (like POL) helps retain traders' attention in the market, especially at the beginning of a new market cycle. Too often, networks are not pivoting in their strategy but simply rebranding their core story for the new cycle.

3. If two large networks merge, it could possibly mean more users. But the incentives are generally not aligned, as I explained earlier.

All of this made us wonder what would even be the ideal merger!

The Dream Merger

A mental model for identifying merger targets

Networks with live tokens have only one good reason to merge. It is about the community. As we covered in our article yesterday, communities can be a moat if done right. Looking through this lens, a merger would require community members of multiple protocols to wonder why they are competing against each other for a limited user base. This questioning is unlikely to happen as everyone's incentives are aligned with tokens. One way to build a wedge here would be through service providers like Reverie or Gauntlet.

Currently, these are businesses that operate as service providers for DAOs. But given sufficient capital (*by an external hedge fund?*), they could be the ones proposing networks with little usage merge. The first task for such a venture would be to identify networks with huge treasuries that can benefit from more users.

Currently, multiple DAOs from the early 2018 era hold treasuries that are in the millions. Many of them often see "raids" asking for the ETH to be distributed among token holders. Instead of being targets for such raids, what they should be doing is merging with products that have large user bases and limited treasuries. Keeping the theatrics of such decentralised mergers aside, there is a need for firms that can assist and advise on such collaborations. It would require an intermittent party that can align VCs, traders & founding teams for such mergers.

This is, of course, a hypothetical example that requires an imaginary market participant. A clearer use of mergers would be to improve the efficiency of capital locked up in different DeFi products. For example, the product will significantly improve if a perpetual futures protocol like dYdX merges with an options protocol like Ribbon.

Why? Capital efficiency is the Achilles heel of DeFi. Currently, Ribbon doesn't understand dYdX positions and cannot use them as collateral. But when they merge, an ETH long on dYdX can be used as collateral instead of new ETH to open a covered call position on Ribbon. The capital efficiency such a product brings does not exist elsewhere. (*It does on centralised exchanges, which is why traders often stick to them instead of a decentralised alternative*).

Additionally, sophisticated traders are used to creating their strategies combining futures and options. So both protocols can sell the new product to the union of their customer base. There is a lot of work to be done when it comes to mergers. In the past, none of it could occur because the tooling (for DAOs) or the environment (in the market) was simply not there.

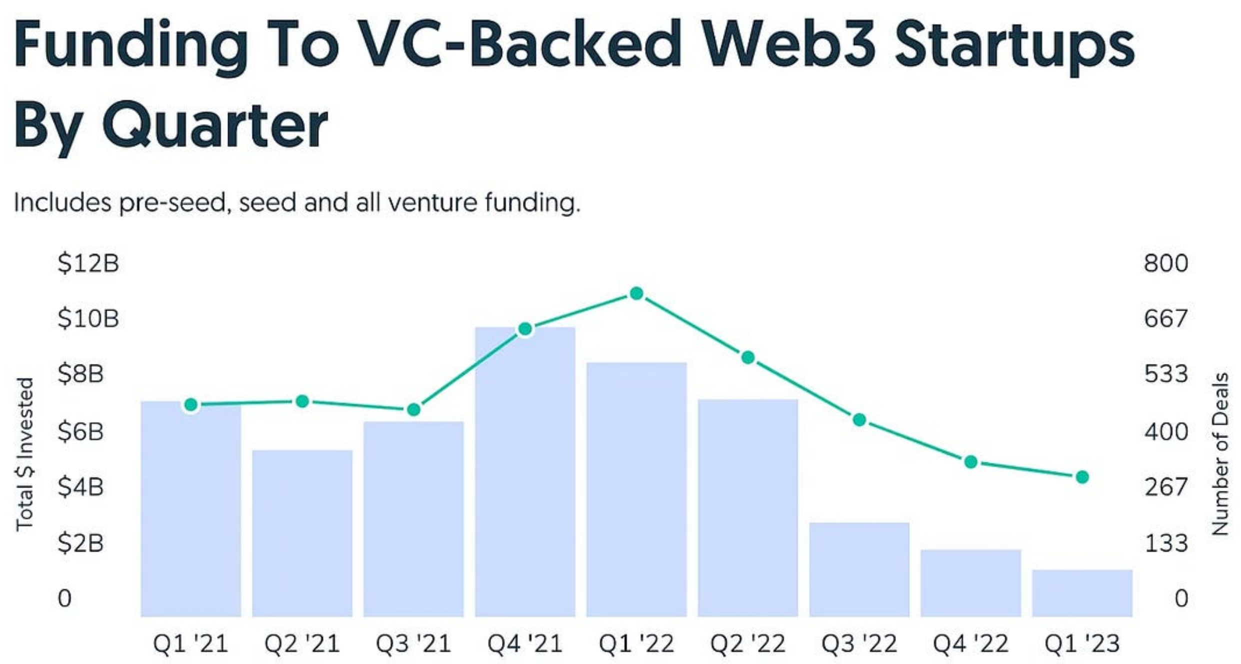
With suppressed prices and next to no customers, many teams in the industry may well consider merging to improve their odds of survival.

Off for the weekend,
Saurabh

Joel John
decentralised.co

Bugs In The System

On capital allocation, hard problems & incentives



Hey there,

I have been writing about the state of venture capital in Web3 since 2019. In all my years of writing, the data has driven the story. When you don't understand the meta-game of what is going on, the numbers define how you see the world. The current cycle gives me time to think and reflect on what is happening. This piece summarises some of my observations.

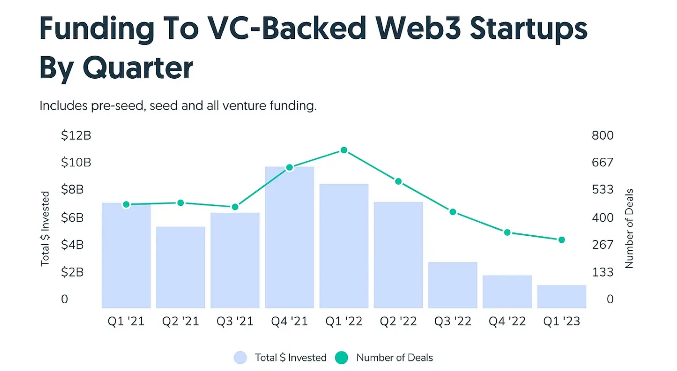
When you study funding data, there are two patterns you would see

1. Capital allocators are reducing the amount of money that goes into the industry. (Contraction)

2. There is an aggressive piling of funds into the sector. (Expansion)

This expansion and contraction of money flowing into any industry is a feature, not a bug. People outside the sector often misconstrue it as the collapse of investor interest. But there's usually more than what meets the eye.

Last week, it was revealed that partners at Sequoia, focused on crypto, are exiting the firm. The announcement came alongside their crypto fund slashing 65% in size. Similarly, Polychain's latest fund ($350 million) is a fraction of the billions they used to deploy. The data below from Crunchbase is a good outlook on how the frequency of deals and the amount of money have reduced over the past few years. Long story short - the data shows that in terms of money allocated, we are in the worst quarter since Q4 2020.


Funding To VC-Backed Web3 Startups By Quarter

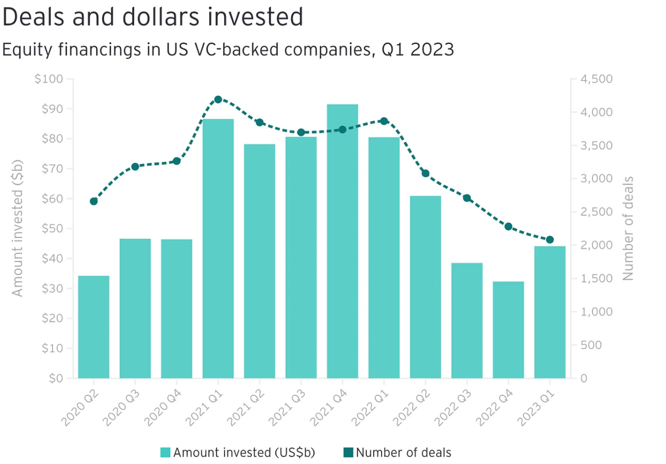
Includes pre-seed, seed and all venture funding.

But is that the case? It is unfair to make that claim without considering two broader points.

1. Firstly, the stress on the US banking system in Q1 of this year forced multiple ventures to see their lines of credit vanish. In turn, they had to raise money urgently from their existing investors to avoid bankruptcy. The trickle-down effect of that is diminishing venture frequency at the early stages.

2. AI, VR and AR as themes are far more capital intensive in terms of money allocated to research and hardware. For instance, Meta has spent at least $100 billion in cash on their VR initiatives. Similarly, some 40% of all patents filed by Apple have been in relation to their Vision Pro device. Nascent categories take tremendous amounts of time and capital to become "retail-ready".

But inspite these broad trends that have driven massive sums of money into AI-specific deals, if you overlay the amount and frequency of deals that have occurred in venture as an asset class, you will see an overlap with what is happening in crypto. The chart below from EY uses data from Crunchbase (yet again). So it becomes easier to see the pattern.


Deals and dollars invested

Equity financings in US VC-backed companies, Q1 2023

Now I don't mean to force fit a narrative here, but here is one way to look at it through the lens of yields. Asset classes like venture and digital assets (what we know as crypto) generally tend to produce beta. If the S&P500 is expected to generate 10% in return, a top-performing VC fund may have a return of ~19%.

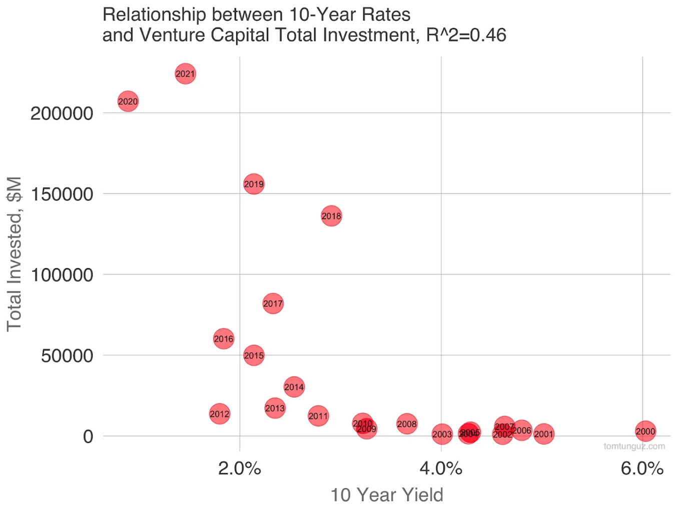
An asset like Bitcoin may produce anywhere between 40-50% annualised. Surely, these assets have more returns, but it also involves more risk. The challenge emerges when yield rates rise. The capital flowing towards risk-on investments tend to reduce because you could create high returns with a fraction of the risk.

Tomasz Tunguz studied the correlation between yield rates and venture capital investment frequency in 2021. Here's the crux of the story from his article.

"Here's the bottom line: as interest rates increase, we should expect venture capital investment to

regress. When the cost of capital is low and yields on cash are small, investors seek greater risk to attain a return. As the risk-free rate on Treasuries increases, market forces should engender enough friction to pull venture investment from the stratosphere into the troposphere or below."

It may sound too theoretical, but the piece had a chart proving his point.



The data above is slightly dirty because

1. Venture as an asset class has grown over the last two decades. The rates could have remained high, and the money going into VC could have stayed just as high.

2. It fails into account the evolution of emerging sectors (like AI, blockchains, and greentech) that require more capital than dot-com ventures of the early 2000s.

Keeping that aside, it becomes evident that the low-interest rate environment of 2020 and 2021 created an interim phase where capital allocation to venture boomed. If you take that peak of $200 billion going into the asset class and take any period after, you will see a decline. Because pandemic markets were a unique condition that simultaneously created a perfect trifecta for ventures to absorb money.

Here's how it played out

1. More people were using digital products due to the lockdown.

2. Ventures were showing hyper-growth due to point 1 and thereby commanded higher valuations.

3. At higher valuations, the tendency to raise more increased to compete with peers in the market and become a dominant player.

The headlines we keep seeing on repeat are designed to induce emotion and are generally not insightful. A different way to interpret this as the culmination of two factors.

1. An excess of liquidity entering the market thanks to stimulus from the government

2. The limited number of startups could meaningfully absorb large amounts of capital investments.

The reason we see market contractions often has more to do with industry maturity than investor conviction. During downturns, industries have a period of consolidation. Said consolidation can be of both technology and users. Without a down-trend, there would not be a period of developers & early adopters tinkering with a new category. That early phase of next to no users is where products evolve for a bull-cycle.

This is why both DeFi and NFTs as a sector took off after the bear markets in 2018. Few things convey this message and OpenSea's userbase chart from 2019.

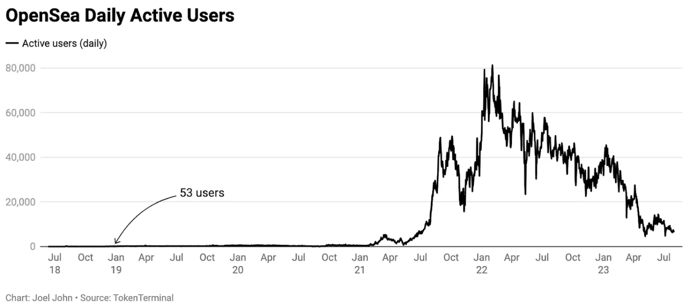


Chart: Joel John • Source: TokenTerminal

OpenSea had a 90% decline in DAUs, but that figure is still up 100x from the last cycle. The media often ignores this fact conveniently.

OpenSea was valued at a peak of $13 billion. It is up to debate whether the valuation is justified, but if it weren't for the bear markets in 2019, there wouldn't be time to sufficiently iterate on the product for the retail users that came in large troves in 2022. MakerDAO, Binance & Uniswap could make similar claims, given all of them grew during a bear cycle.

An even better parallel to draw here is Google and Amazon. The search engine was initially a PhD dissertation by Sergey Brin and Larry Page. Facing the challenges of a lack of advertisement models for search engines, the two set out to sell Google to Excite in 1999. But no parties were willing to buy it, even for $750k. 24 years later, Alphabet is the behemoth we know it to be. Similarly, Amazon dropped 90% since listing during the dot-com bubble. Both ventures have become crucial infrastructure for the Internet today.

Sidenote: Here's a brilliant Ted Talk by Jeff Bezos from 16 years ago comparing the internet to electricity.

All of this paints a rosy picture and does not address the crux of the problem blockchain native ventures have today: A lack of users that pay meaningful fees being retained long enough.

Incentives Rule Everything

Most blockchain ventures we see have a pathway to liquidity in the form of tokens. As Sid often likes to say - ventures are hard to build once a token becomes the product. The DNA required to keep a listed token afloat at high prices & the one needed to retain users that generate fees for a platform are quite different.

What we often refer to as "venture funding" in crypto is, sadly, liquid market investing (*into tokens*) with lock-ups. Since the liquidity event for most blockchain ventures is tokens, there is often little focus on retaining users for the longer run or building a business the traditional way.

Our focus instead is often on

1. Weaponising airdrops for short-term accrual of users
2. Driving narratives with the users and
3. Issuing a token that ties back to that narrative.

When a narrative becomes the product, the business becomes a collection of stories. And stories, on their own, cannot accrue value on a long enough timeline. Eventually, it creates a prisoner's dilemma, where everyone's incentivised to have their tokens vested and sold at the highest price possible.

As I write this, Curve's founder's $168 million worth of tokens is facing a liquidation cascade as he chose to take a loan against it instead of selling it. He had taken the loan to acquire two mansions. This is not too different from a Web2 founder selling secondaries. It is even more transparent, but the time to liquidity is the difference.

A founder can expect meaningful liquidity within a few years in blockchain-native ventures. This means the incentives to stick around building decline rapidly for investors and founders. Last I checked, you cannot build a generational firm within two years.

(*Ironically, Hopin, the example I linked above was also launched two years back*).

When everybody is incentivised to prop up the quickest narrative, the focus on building long-term businesses shifts. It is the reason why we woke up to Twitter influencers talking about $bald (*some meme token that went to zero*) over the weekend instead of discussing what blockchains can be used for. **We are sitting on world-changing infrastructure, battling our instincts to trade meme-tokens and gamble with on-chain Ponzi schemes. In effect, the industry is the biggest marshmallow test there could be.**

Hard Problems

I believe this dichotomy makes investing in Web3 native firms an exciting opportunity. Most of the founders we see can be filtered out once you assess

1. Technical depth
2. Ability to sell
3. Possibility of sticking to the venture for a long enough time frame

It is rare to see the three coming together. Why does any of this matter? Because there are opportunities at the periphery that remain untapped. We made and abundance of noise around DAOs, yet two years later, there are less than 70k active voters (over the last six months) on the three largest DAOs. Smaller ones, have less than 100.

It is hard not to observe how primitives like DAOs and smart-contract-based equity allocations could make a meaningful dent in the lives of thousands of startup employees worldwide. Why isn't there a Deel or Carta that runs on-chain? The discourse is less focused on what the world needs and more obsessed with what seems intellectually intriguing.

While intellectual pontification can drive Twitter clicks, it rarely accrues large user bases the way a thoughtfully designed application can. In other words, we trade real users and meaningful revenue for traders' attention. The business model is less predicated on what a venture can do today and more so on what it can enable a decade later. (*FWIW, all early-stage investing is on the basis of what can occur in the future. The difference is, with crypto, you can have the incentives (or liquidity) here and now).*

A natural extension of this is what we have been noticing with Real World Assets (RWA) as a theme within crypto. There is some ~$3 billion in RWA-linked assets on-chain—less than 0.1-0.05% of the actual market size. If you treat blockchains as financial infrastructure enabling real-life use cases instead of gambling on-chain, you could build meaningful companies that make a dent in the universe. But the incentives are not stacked up to do so.

One way this translates to capital allocators is with how capital raises for protocols far supersedes money that goes into consumer applications. We often see teams struggle to raise money even while building products at par with the Venmos of the world as capital allocators are far incentivised to deploy to protocols that may have tokens down the line. Often, investors have a simple line of thinking.

- A protocol with a token could go up 100x on listing ($20 million to $2 billion)
- An application without a token has a meager chance of surviving, let alone being a unicorn.

This problem usually translates to a lack of capital flowing into applications. It could mean users don't have good experiences when coming on-chain. That, in turn, translates to protocols lying unused. In essence, we create a self-destructive flywheel that primarily runs on narratives. Naturally, there is no instant fix for this. One of the ways this has fixed itself in the past is with a new crop of investors emerging.

If you read Sebastian Mallaby's Power Laws - it becomes painfully evident that **a new crop of investors usually leads the pack when an emergent sector formalises**. Sequoia's Don Valentine started the firm when the traditional investors of the 1970s failed to fill the need for capital felt by tech founders of the time.

Tiger Global and Softbank's Tech funds emerged during the mid-2000s to fill the gap left by PE funds unwilling to invest in growth-stage ventures. One place I witnessed this was with Tiger's Lee Fixel leading a $1 billion round for the first time in an Indian venture named Flipkart. It changed the landscape in India as we knew it and set the stage for over 108 unicorns to come from the market in the following decade.

Closer to crypto, Paradigm, Pantera, and Polychain have filled that gap. But because crypto has shorter life cycles (as an asset class), the pace at which a fund evolves to be the size of a PE fund is much faster. All three funds I mentioned handle billions of dollars, and the desire to build alongside early-stage organisations that can absorb smaller sums of money while facing years of uncertainty may no longer exist. This leaves an opportunity gap for new investment funds to capitalise on.

One way this "*gap*" emerges is with large venture funds that traditionally operate outside crypto. Analysts at the firms often pattern-match through the same lens they use in other sectors when analysing deal flow that goes to partners or investment committees. By the time these funds build a network (for deal flow sourcing) and acquire the skill sets to deploy actively, the whole market cycle will have played out. This is partly why their entry often marks the top and departure marks the bottom.

The winners in crypto in the next cycle will not differentiate themselves by the size of their funds alone. **Startups need three things to go from 0 to 1—capital, distribution and secrets that stem from insights or research. We have an abundance of capital in the market today.** The opportunity is with distribution and insight. A new class of investors have been addressing those problems specifically.

Operators, researchers and media houses are well-optimised to solve for insight and distribution today. Robot Ventures (*by Tarun Chitra and Robert Leshner*) & Bankless' $30 million fund are two instances of this. Paradigm's focus on research is another example of a fund building a differentiator through sectorial expertise. Work by Dan Robinson combined with the firm's capital helped fuel what we eventually came to know as DeFi

To make a long story short - there isn't a lack of capital in digital assets. What we have instead is a mix of factors at play.

1. There is a broader contraction in capital going into venture capital.
2. The market needs time before it can mature enough to take more capital.
3. Incentives are skewed for allocators to sit on the sidelines when it comes to ventures that may take forever to create a return.
4. And there may be opportunity costs in not deploying directly into liquid assets.

All of this ignores the internal friction at large organisations that were historically deploying. How do you meaningfully create conviction at an investment committee once the venture you deployed so heavily into is exposed for fraud? These are things that take time to resolve. And unless those wounds heal, it is unlikely that we see the same players (*of the last cycle*) lead massive rounds in crypto.

For the moment, here's what I do know. Technical innovations are occurring in the industry that are worth backing. We are at a very 0 to 1 phase when onboarding users interested in tools that do not involve speculation.

And for what it's worth, to borrow how Steve Jobs would have put it: **we are nowhere near having made a dent in the universe**. These factors leave me bullish on what can still be built, scaled and exited. If you are building in the industry, leave your decks here—we (really) like the builders.

I'll see you guys later in the week with a long form on narrative cycles & the psychology behind capital flows.

Joel

Saurabh
decentralised.co

How To Take Over A DAO?

Asking for a friend.

Hello!

This is the last of the beta versions of our paid newsletter. We will be announcing this to the broader community on Tuesday. We may or may not have some goodies for readers that have sent in feedback.

Source: Berkeley

Physicists claim that about 13.8 billion years ago, our universe was condensed in an almost infinitely dense spot. Today, the observable universe has over a trillion galaxies, each with billions of stars on average.

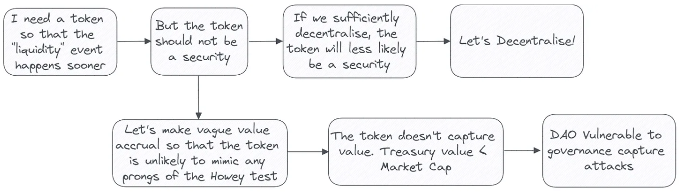
In much the same way, projects start with a few members who control and steer it initially, then gradually add more members to reduce power concentration with each member. Projects seek what Jesse Walden calls progressive decentralisation.

But why decentralisation? Sometimes, it is self-evident as it is with Bitcoin and Ethereum. You want more minor participants to understand whether they independently get what's due to them. You want people to be able to run light nodes on everyday computers. But in many cases, the motivation for decentralisation is different and quite apparent to those who see through the (*frequent*) layers of nonsense.

When a project is "*sufficiently decentralised*", its token is (*claimed to be*) less likely to be termed a security. And why do you need a token? The more decentralised you appear to be, the lower your perceived risks from legal actors. One challenge with "*not being a security*" is ensuring your token captures no value. Dividends? Not allowed. Fee shares? Nope. Often, not even a claim to the IP rights of a product.

It is one of the reasons why we don't flick the fee switch in favour of UNI token holders. Because if we do that, UNI holders have a reasonable expectation of profits to be derived from the efforts of others. That is one of the criteria of the Howey test used to determine whether an asset is a security.

The easiest way to get out of this is to have the token as a utility token (*think casino chips)* or a governance token.


I need a token so that the "liquidity" event happens sooner
But the token should not be a security
If we sufficiently decentralise, the token will less likely be a security
Let's Decentralise!
Let's make vague value accrual so that the token is unlikely to mimic any prongs of the Howey test
The token doesn't capture value. Treasury value < Market Cap
DAO Vulnerable to governance capture attacks

The reason why there isn't a connection from "Let's decentralise" to "DAO vulnerable" is because we presume a truly decentralised venture would not be as vulnerable. But that is often not the case

A DAO working properly does not always translate to price action as their tokens are not designed for value capture. During the ICO boom, many projects raised money in ETH. Years later, their treasury ballooned to be worth hundreds of millions - due to appreciation of ETH's price. In bear markets (*like the one we are in right now*), the value of these governance tokens falls quicker than the value of assets like ETH or BTC. This results in treasury value being higher than the value of circulating tokens or the market cap of the governance token.

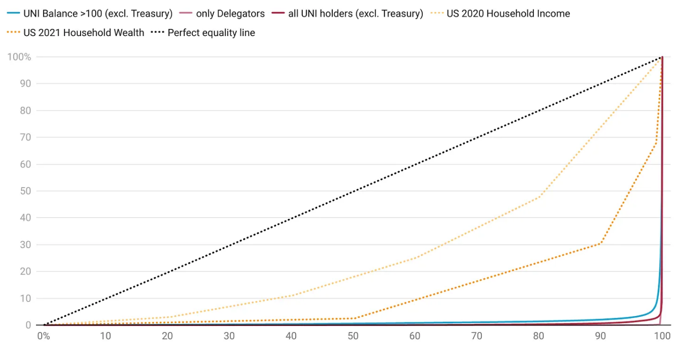
This reminds me of Microstrategy's Bitcoin holdings. The stock itself could prove to be worthless, but the Bitcoin being held by the firm can grow to be of tremendous value in the years to come

In financial terms, the book value of the token is higher than its market value. This is where the governance gets messy. Because the situation creates a divide between token holders and those who control the treasury. Those who control and rely on the treasury for operational expenses are not as incentivised as token holders to increase value going to the tokens.

DigixDAO, Gnosis, Aragon, and Rook were similar in that they faced conflicts because the market value of the tokens was lower than the value controlled by the treasury.

Apathy Everywhere

DeFi tokens have a high gini coefficient. It is a fancy way to say that a few control many tokens. Here’s an example of the UNI token holder pattern. The following chart plots the Lorenz curve for the UNI token and compares it against other curves like US Household wealth.



Lorenz Curve For UNI Tokenholders

Compared to US Household wealth ('21) and income ('20), UNI distribution is significantly unequal

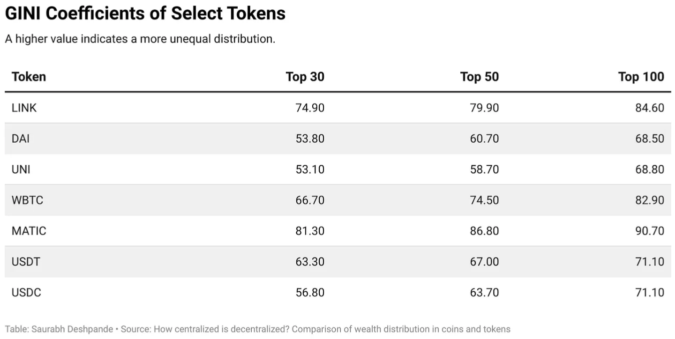
Chart: Saurabh Deshpande • Source: Dune (@web3_data)

Lorenz curve shows how the ownership changes as more population is added. The X-axis represents the population percentage, and the Y-axis represents the ownership percentage. The perfectly equal line shows the distribution in an ecosystem where everyone is an equal owner.

For example, in the case of UNI (*whether it is delegated, holders with more than 100 tokens or all holders*), almost 98% of the holders control less than 10% of the supply.

The top 2% control more than 90% of it.

This paper studied token holding patterns, tokens and coins and found that tokens like LINK and MATIC are significantly concentrated in the hands of a few. The following table shows the GINI coefficients of multiple tokens. 84.6 for Top 100 LINK holders indicates that 84.6% of the LINK are with top 100 addresses.



GINI Coefficients of Select Tokens

A higher value indicates a more unequal distribution.

Token	Top 30	Top 50	Top 100
LINK	74.90	79.90	84.60
DAI	53.80	60.70	68.50
UNI	53.10	58.70	68.80
WBTC	66.70	74.50	82.90
MATIC	81.30	86.80	90.70
USDT	63.30	67.00	71.10
USDC	56.80	63.70	71.10

Table: Saurabh Deshpande • Source: How centralized is decentralized? Comparison of wealth distribution in coins and tokens

Smaller token holders do not feel their vote matter as the top holders will always get their way. So, they don’t bother with voting and keeping up with what is happening with the project. Voter apathy is not a crypto-native issue. In the equities world, retail participation hovers around 28% compared to 90%+ involvement of institutional investors.

Having more skin in the game and being able to impact the outcome drive participation in the governance process.

The voting patterns for three leading DeFi protocols suggest a clear pattern across the board. **More than 90% of token holders do not bother voting**. Quorums for Compound and Uniswap are 4% each and set at a variable for Aave. As of writing this, of the 62 DAOs being tracked by Nansen, only four had active proposals. Only two of those four had more than ten active voters on live proposals. It appears people don’t want to govern.

The token’s price and treasury balances get disconnected over an extended period. Low token prices combined with uninterested voters create a vulnerable combination for DAOs. As risk-free value (RFV), raiders can now target these DAOs by –

- Creating a divide within the community with treasury controllers on one side and token holders on the other.
- And acquiring tokens cheaply to effect any governance outcome.

You get the story. A very small fraction of token holders bother with voting when it comes to governance. When the treasury value is higher than the market cap, it is possible to convince some token holders that liquidating the DAO benefits them since they get more than a dollar for every dollar of their current market value.

The assumption is that on the dissolution of a DAO, the treasury's ETH (*or other asset*) holdings will be distributed to token holders in proportion to how many tokens they have. So activist groups often buy tokens at low prices, then rally other token holders for a dissolution. The difference between the cost to acquire tokens and the ETH received through a dissolution is their profit margin.

The dissolution of RookDAO is an apt example here. Without getting into who was right and who was wrong, here's what happened

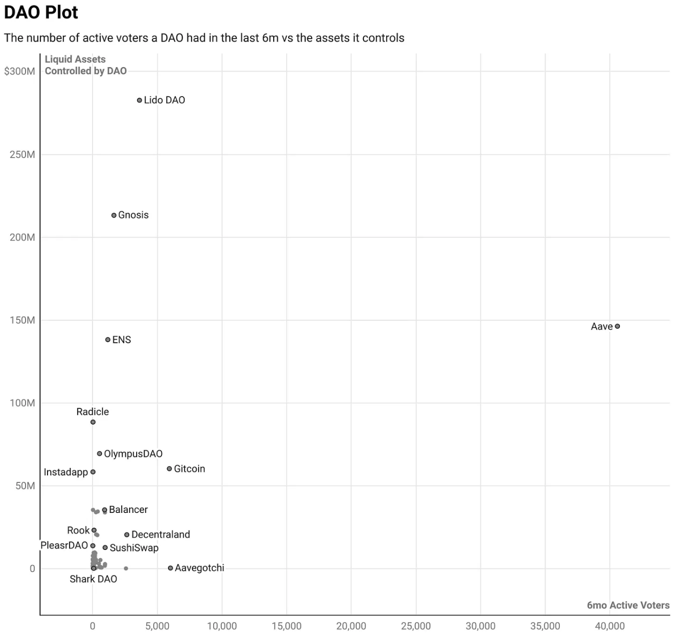
1. Some community members or the RFV raiders thought the DAO was poorly managed. Their points of contention were constant development delays, lousy communication and spendings of the DAO.

2. They started acquiring ROOK tokens from the open market and making their voice heard.

3. Finally, they managed to take over the treasury through governance. A deal was cut. And the DAO was split in two – the new entity with 60% of the treasury and the original entity with 40% of the treasury to be claimed by ROOK token holders.

There has also been an instance where the attacker took a page of LBOs (leveraged buyouts) and attacked Beanstalk using flash loans to drain $182 million.

The following chart shows how most projects had only about 5000 active voters in the last six months. BitDAO and Uniswap, with billions worth of treasury, had 10,000 and 18,000 active voters in the previous six months. All DAOs do not need votes occurring every month, but it highlights the extent to which voter apathy exists.



DAO Plot

The number of active voters a DAO had in the last 6m vs the assets it controls

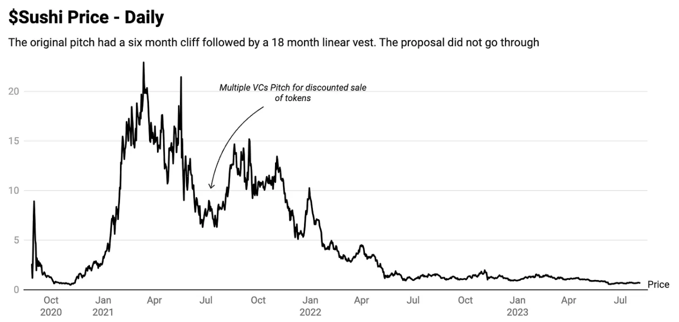
Chart: Saurabh Deshpande • Source: Nansen

Private Interest vs Public Good

A weak community often lacks strong voices that can gather people. It becomes easy to sway votes in a malicious actor's direction. When the community is strong, it has opinionated voices guiding people, much like a democracy. Forming a consensus in support of, or against a critical vote is difficult. One of the ways to create a more robust governance process is to involve more members who understand the market dynamics.

Remember the bar scene from A Beautiful Mind when John Nash corrects Adam Smith? He says *the best result will come when everyone does what is best for themselves and the group.* This would be known as the Nash Equilibrium. Every individual doesn't get what is best for themselves, but the group, as a whole, does better when it acts as per the Nash Equilibrium.

In reality, many individuals don’t care for the group, especially when they are in a position of power. People acting in self-interest is not a ground-breaking realisation. With crypto, it just becomes easier to observe these behaviours.


$Sushi Price - Daily

The original pitch had a six month cliff followed by a 18 month linear vest. The proposal did not go through

An attempt to structure a discounted sale of SUSHI tokens to some of the VCs comes to mind. If you dig up the thread on their forum, you can see that the newcomers could not sway the community's vote. After Chef Nomi (*the pseudonymous creator of Sushiswap)* tried to sell all his tokens and move on, community members scrambled to shed its old image of being "*just another Uniswap clone*".

Some thought that adding VCs who bring expertise in different areas would be a good idea for the growth of the protocol. This would have achieved two purposes.

1. Decentralise the treasury to an extent.
2. Bring additional expertise that the team didn't have.

The deal was to offer a 25% discount to VCs with lockups. But after much debate, it wasn't clear to many community members what they brought to the table, and if VCs believed in the team, why they couldn't buy tokens from the open market just like others. The proposal was eventually withdrawn.

It would have been an interesting transaction considering how the token's price performed in the months that followed as you can see from the chart above

Dissolving DAOs

All DAOs don’t have sad deaths. Some DAOs are created for specific purposes such as buying the constitution. (*Yes, we tried that*). Sometimes the vision doesn’t work out. Or they are no longer needed after a point in time. Failure is not a crime. We have instances of DAOs coming to closure without much drama, even when they are handling millions of dollars.

ICOs during 2016 and 2017 raised significant amounts of ETH. DigixDAO raised ~450,000 ETH to launch a gold-backed token. Digix held physical gold, which was represented on-chain by the DGX token. The DAO’s governance token was DGD. Based on the community’s feedback, a way had to be created for DGD token holders to break away from DigixDAO.

After considering options, the team proposed to dissolve the DAO and distribute ETH on a pro-rata basis of DGD holdings. Due to the team’s bias against dissolving, they did not vote, but the community decided to vote for the proposal, which passed. The DAO was dissolved, and DGD holders could claim ETH from the DAO’s treasury.

As with most things in crypto, DAOs are an experiment. As long as profit motives exist, we will see individuals trying to take over them. In 2021, when Sushi was hot, every VC wanted a piece of it. As prices have cooled down, the focus is on the brand-new narrative. For founders, it is becoming increasingly clear that part of what makes a “token” valuable is how difficult it is to take over its DAO.

One of the things we noticed in writing this piece is the lack of data on proposals, active voters & the amount of capital at risk. The industry has invested billions of dollars into DAOs and tooling around running them. But the most primitive data sets around how decentralised they are, do not exist.

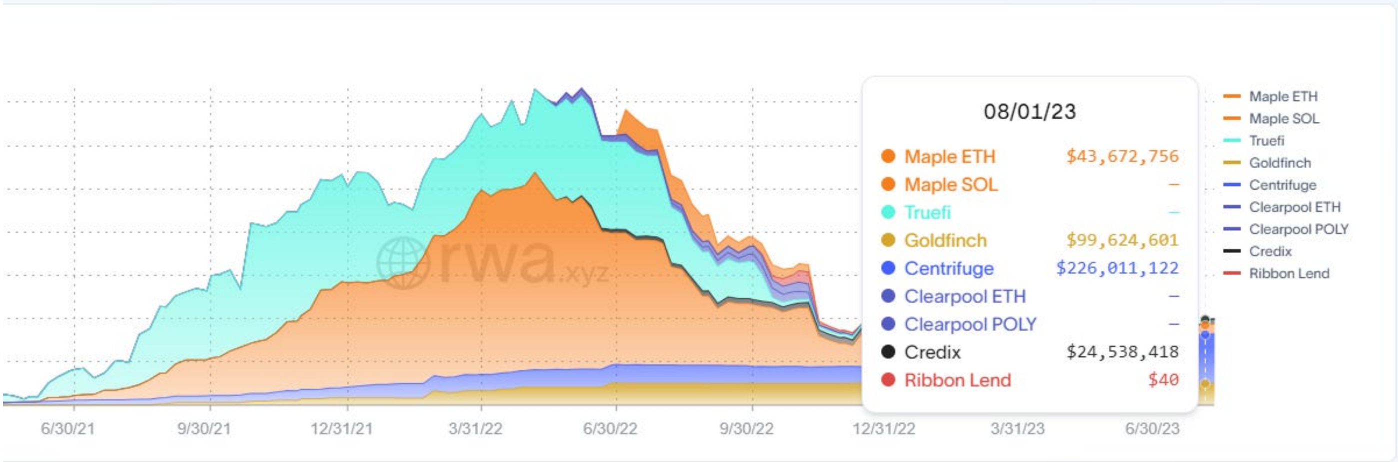
That is something we should work with our data partners on fixing. But for now, we log off for the weekend.

Try not to get wrecked trading altcoins over the weekend.
Touch grass, and find time for hobbies.

Saurabh
decentralised.co

Two Worlds Blending

A (possible) future of finance



Hey there,

December 2017 was a strange time. The ICO boom was coming to an end. And crypto kitties clogged ETH to a point where the market began wondering if they were better off being named crypto-quitties.

A few quiet years and multiple experiments later, Uniswap helped me figure out how to swap assets efficiently without an intermediary. Compound and Aave perfected borrowing and lending on Ethereum. But it was still expensive for everyone to use Ethereum..

Ethereum has 4.5 million monthly active users (MAUs) almost six years later. It pales in comparison with fintech applications. PayPal alone had 433 million MAUs in the first quarter of 2023. So in some sense, we have come a long way.

But there is still a long journey ahead of us if these financial primitives are to make a dent in people's lives.

Risk As a Product

But why is that? Decentralisation brings along with it both good and bad. It can be more inclusive for people of all backgrounds. But it could also be highly predatory for unknowing users. This is why we created a system insulated from the traditional financial world. The “user' in DeFi is almost always comfortable “aping” into a new liquidity pool or “degening” into an unknown token.

Only primitives like swaps, leveraged futures, and borrowing and lending have somewhat achieved product-market fit (PMF) in DeFi. This is because we were able to attract a section of users who embrace risk. DeFi is not ready to take on hundreds of millions of users because it does not solve a meaningful enough problem for them, in an easy enough fashion today. Yes, stablecoins exist. But a large portion of it's volume still comes from traders.

We have built applications for speculators, and they are already here. As we undergo cycles, the number of speculators will keep changing in tandem. Speculation is an everyday use case among all financial products, whether in traditional finance or DeFi. But in conventional finance, some part of speculation is valuable.

For example, when a bank lends to a startup or a mid-size company, they use the credit to produce something useful to people in their day-to-day lives. This is why credit creation is one of the most essential finance primitives. Both DeFi and NFT markets evolved with the arrival of lending products like Compound or Metastreet.

Blurring Boundaries

This tendency of focusing only on speculators is slowly shifting, though. PayPal launched its stablecoin, PYUSD, on August 7. And it will be using Ethereum as the settlement network. PYUSD can be used for P2P payments and fund purchases or converted to other crypto assets. This has mixed reactions because the smart contract allows PayPal to freeze or seize a user's funds.

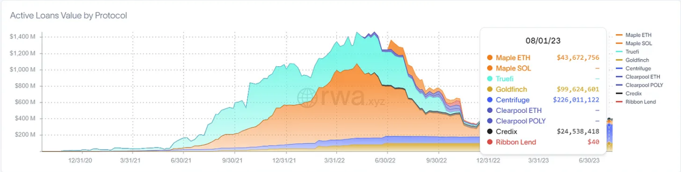
But practically, PayPal is a regulated entity. They have to oblige if they are ordered to stop or freeze certain accounts. The big picture here is not that a large, listed fintech company is releasing a product on a public blockchain. What matters here, is the fact that crypto-native infrastructure seems to have evolved to a point where retail-scale applications can now be built on top of them.

But in case of an exploit, many will desire a point of control that allows the movement of funds to be stopped. Imagine, you lost $10k worth of $PYUSD to a phishing attack. Would you rather have Paypal block that transfer or not? Given Paypal's large consumer base that is not DeFi savvy yet, the token would need to be designed to permit Paypal to blacklist or freeze it if they think something is going wrong. It happens today with Tether and Circle's stablecoins too.

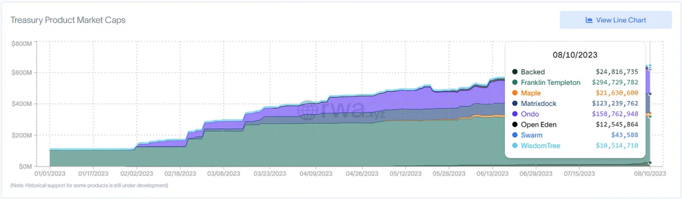
The challenges caused by the blurring of lines - between what happens on-chain and what occurs off-chain is evident with Real World Asset (RWA) loans. The combined TVL of RWAs just crossed $1 billion, according to DeFiLlama. In 2021, we saw prominent players becoming interested in crypto. In almost all developed countries, we were in a zero-interest-rate environment, leverage demand was high, and crypto offered higher interest rates.

The situation reversed when global interest rates rose due to sticky inflation and demand for leverage dropped in crypto. Suddenly, interest rates offered on USDC were lower than the US treasury bills.

When interest in crypto was low and higher in TradFi, MakerDAO saw an opportunity with RWAs. Soon, private credit, treasury offerings, and real estate applications emerged. Protocols like Maple and Ondo Finance started offering treasuries on-chain. Franklin Tempelton started an on-chain fund on Stellar called the Franklin OnChain U.S. Government Money Fund, representing about half of the on-chain treasury offerings.



Source: Rwa.xyz


Treasury Product Market Caps

08/10/2023

● Backed	$24,816,735
● Franklin Templeton	$294,729,782
● Maple	$21,630,600
● Matrixdock	$123,239,762
● Ondo	$158,762,948
● Open Eden	$12,545,864
● Swarm	$43,588
● WisdomTree	$10,514,710

(Note: Historical support for some products is still under development)

Source: Rwa.xyz

But why bring products like treasuries on-chain? You can go to your brokerage portal or call the broker and get treasuries using dollars sitting in the brokerage account. Let's examine the business models of two of the largest stablecoin issuers – Tether and Circle to understand.

When someone wants dollars on-chain, they go to either of the companies and ask them to issue stablecoins by transferring real dollars to company accounts. Once the transfer is confirmed, stablecoins are minted (*sometimes, they are minted based on predicted demand*).

A fee is charged to issue the stablecoins to you. When you are busy using stablecoins on-chain, dollars are still sitting in the bank account of Tether or Circle. They use these dollars to put into short terms instruments such as treasuries, overnight repo, money market funds, and a small portion even in assets like Bitcoin.

They make the bulk of their profits by earning interest from the money in these products. Naturally, when the interest rates are higher, stablecoin issuers make more money. According to Tether's disclosures, their deposits are distributed as shown below. A large part of the cash and cash equivalents are in US treasuries (75%), overnight repo (12%), and money market funds (11%).

Tether Reserves Breakdown (Total $86.8 bn)

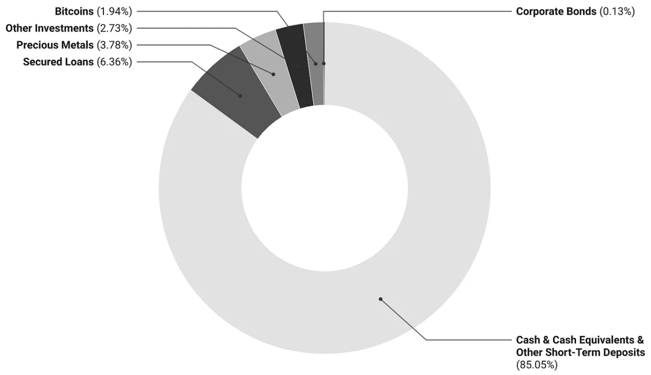


Chart: Saurabh Deshpande • Source: Tether Transparency Report

But when users like you, or I hold stablecoins, the interest is not passed on to us. Markets like Compound and Aave offered returns lower than the US Treasuries over the past few quarters, where interest rates have risen. Bringing treasuries on-chain allows for interest rate arbitrage and may help maintain parity between DeFi and off-chain interest rates.

But does bringing everything on-chain really transform finance as we know it? There are cracks in the system visible already.

Defaults Enter The Scene

When we try to merge the on-chain and off-chain worlds, we will encounter the problems both face. Thankfully, some features of one system will allow us to avoid the pitfalls of the other. For example, the traceability of blockchains makes it difficult for borrowers to obfuscate what they use the capital for. As long as the assets stay on-chain.

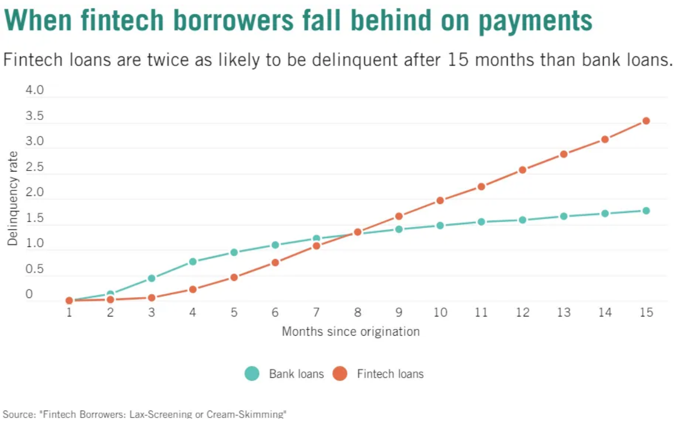
Recently, Goldfinch faced a situation where the covenants of a loan were broken. They were working with a motorcycle financing company called Tugende, which operates in Uganda (*89% of the business*) and Kenya (*11%*). Goldfinch made a loan of $5 million to Tugende Kenya, with October 2023 as the maturity.

In December 2022, Tugende Kenya made a loan of $1.9 million to Tugende Uganda to extend support to the struggling business in Uganda. It meant that the loan-to-value had exceeded the agreed threshold of 80%. You can offer a loan to a business, but very little can be done to determine what the business does with the money you give once the money goes off-chain.

The protocol has a predetermined way of handling defaults by systematically writing down defaults, and the amount will be written off in the next few months according to the schedule mentioned here.

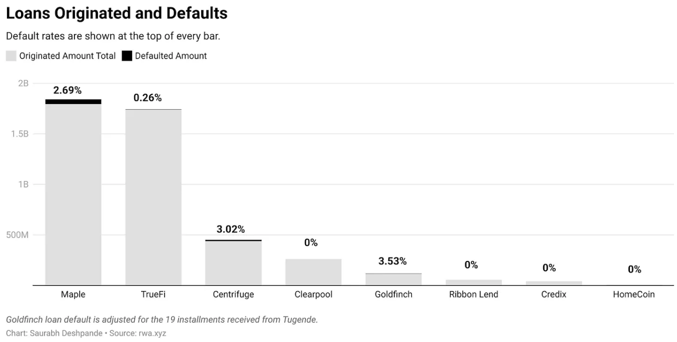
Such incidents are why we need teams that understand how traditional finance works well. Teams with a combination of experience in building in DeFi and conventional finance are much better placed to avoid and manage undesirable situations.

This incident prompted me to examine default rates in traditional finance and other DeFi-based RWA lending protocols. A study published in Harvard's Working Knowledge titled *The Dark Side of Fintech Borrowing* states that at a 3.53% delinquency rate, Fintech loans are twice as likely to face defaults as bank loans.



Source: The dark side of fintech borrowing.

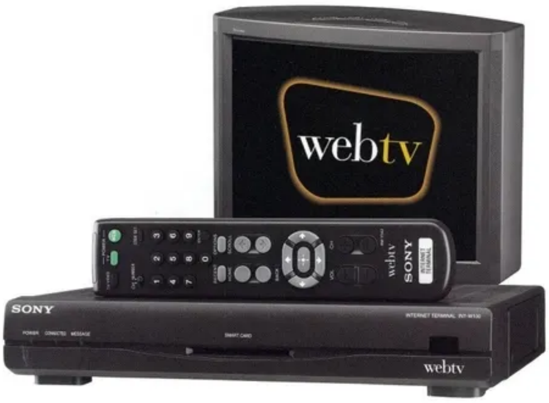
How does this compare with crypto? Although these are early days for RWA protocols, here are some numbers. So far, the default rates are in line with Fintech delinquency rates.



The bars represent originated amount. The figures mentioned above them, represent the defaulted amount in percentage.

Timing It Right

Remember WebTV? Me neither. I had to dig it up as an example. In the late 1990s, WebTV launched an internet-based TV with the hope that people would not want computers at home but would want a TV in their living room. But this was the pre-broadband era with slow dial-up connections and the clunky interface. It never found PMF.



This is where we are with DeFi today. Source

During the 2017–18 boom, many ICOs raised money to solve “real-world” problems. One such ICO was Populous, which wanted to solve issues with receivables with invoice financing. Working capital problems can be life and death for small companies. The infrastructure was far from ready then, and it is no secret that it failed to gain any traction. The graveyard of projects like Populous is a reminder that forcing narratives when the infrastructure is not ready is a recipe for disaster.

We have come a long way since then. Several rollups scale Ethereum. Account abstraction projects are ensuring better UX. There is much more awareness of DeFi. Goldfinch recently announced defifortheworld.com, which incorporates several UX improvements that will allow tradfi folks to use DeFi:

- It uses PassKey for authentication. This is simpler than current ways of using wallets.
- There is no need to write 12 seed words on paper and guard it for eternity. We set up a wallet using our fingerprints through the biometric scanners of our mobile devices.
- It is built on Base (an optimistic rollup by Coinbase) and uses 4,337 style accounts that allow users to pay for gas in assets other than ETH.

Solutions like them show the potential to remove the clunky and daunting blockchain wallet experience and expand the user base beyond those who already use fintech products.

The UX must reach a point where a billion people can use it. We are getting there, but for the industry to evolve, we would need to see crypto-native developers working with the networks and expertise of traditional bankers.

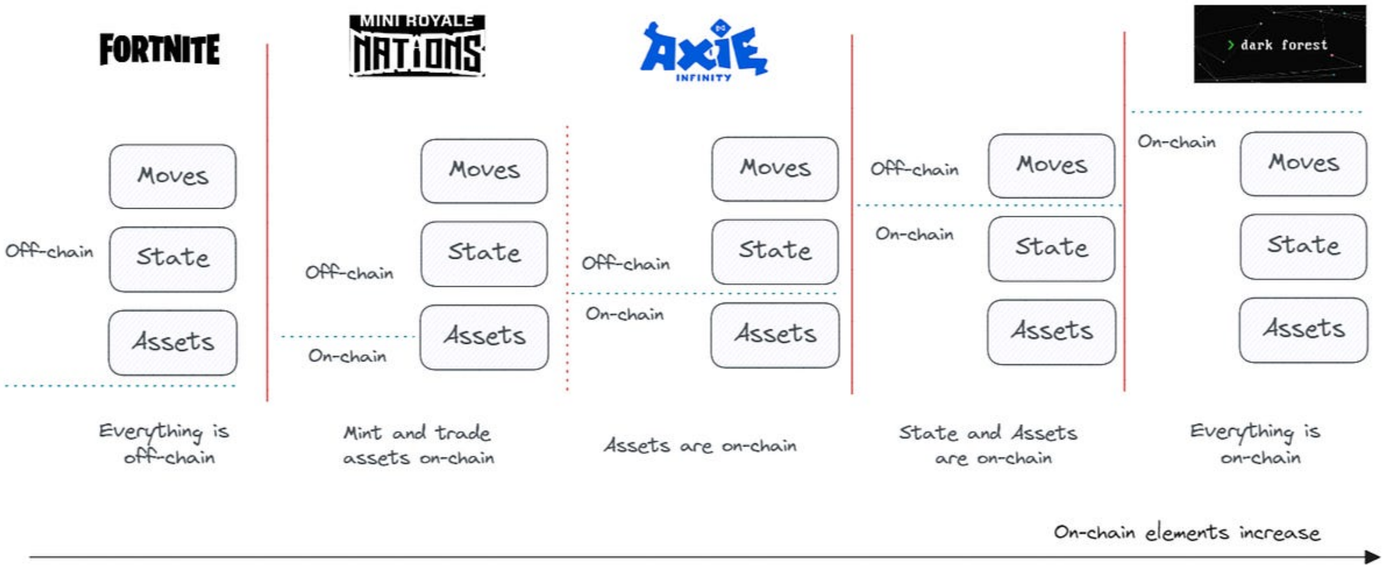
We are seeing a few emerging startups tackling these “transitory” issues and will soon be writing about them in a piece focused on real-world assets.

Signing out to touch grass,
Saurabh

Saurabh
decentralised.co

Gaming is a spectrum

Going from play to earn, to spend to play.



Hey there,

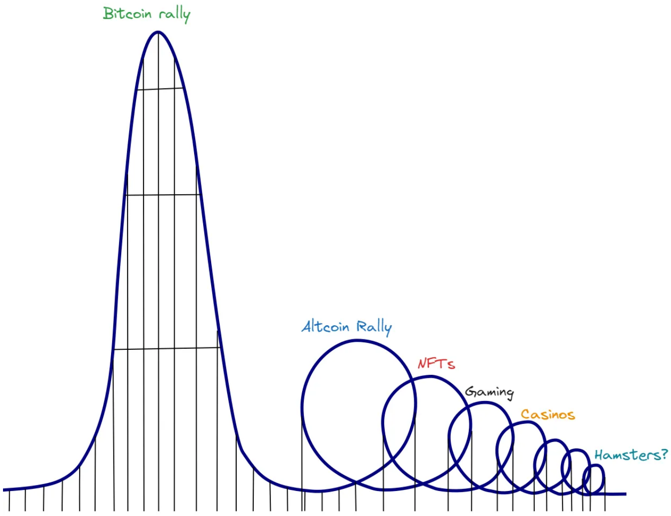
Days like today remind us of how unforgiving bear markets can be. They constantly test how true you are to your thesis. Internally, we constantly debate about the themes that will continue to stay relevant during a market recovery.

Gaming makes an appearance in these conversations quite routinely. It is hard to have a strong view on because of the variables at play. Today's issue looks at how we think the sector will evolve over the coming years.

It's a given that we have to start this article with Axie Infinity as a reference point. At its peak, the game had over 2 million daily active players. This is an achievement, given the industry's size at the time. Turn-based card games have fewer players compared to a first-person shooter. Hearthstone, a card game by Blizzard, has about 200k concurrent players compared to Fortnite, which has 3 million.

Axie did an excellent job onboarding users, but the financial motives at play made it seem like a larger success than it was at the time. Instead of seeing the game as an on-ramp for millions, we built a narrative of potentially helping economies out of poverty with play to earn. The branding transformed it from a cool experiment to an unsustainable digital sweatshop.

At some point, it seemed the game's sole purpose was providing employment instead of entertainment. The short-term success of Axie Infinity paralysed the creativity of all other blockchain game developers for years to come. Nobody wanted to own the crippling responsibility of maintaining livelihoods.



Crypto's market cycles are beginning to look similar to a euthanasia coaster.

Remember the cool Physics experiment where every subsequent bounce is lower when you drop the ball? As an industry, we learn that lesson the hard way with every new narrative. Every bounce since 2021 has been a harsh lesson in the making.

Anyway, the relatively short-lived success of Axie Infinity made me wonder whether it makes sense to have games completely on-chain. To evaluate this, it makes sense to zoom out. Two key observations before we start -

- Games or sports have been integral to our cultures since ancient times.
- Our lives are much more digital than they were a decade ago.

The first will continue to be the case, and the second trend will solidify even more in the coming years. Why do I say that? I work from home in Mumbai with my friends who sit in Dubai. Although collaborating in person is next level, I am perfectly comfortable in this setting. In contrast, my cousins, who are a few years older than me find the notion of working from home quite absurd.

Recently, Joel shared a Bloomberg article that talks about how the scarcity of space has forced Beijing to pilot vertical cemeteries with digital screens instead of headstones. Before Beijing, even Shanghai opened a digital technology cemetery in August 2022. To quote the vice president of Fu Shou Yuan International Group Ltd., a leading funeral technology services provider –

> *The era of putting money just into the purchase of land and the amount of stone for funerals will soon be over. Rather, more money will be spent on science and technology and the emotional experience of cemeteries.*

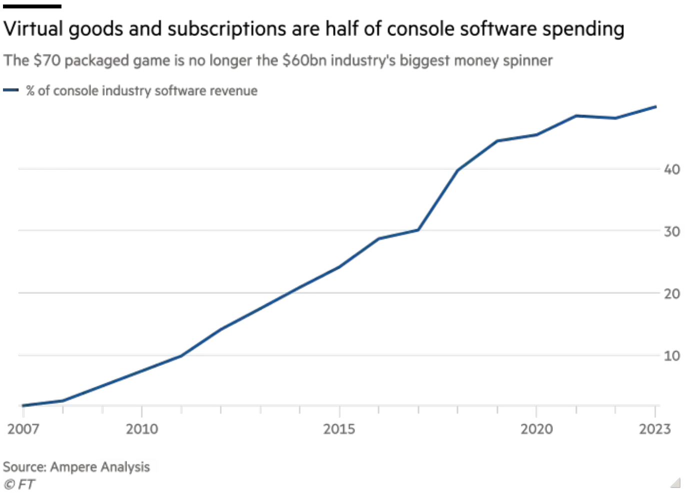
It turns out this has a practical benefit as well. It is far more affordable. For context, digital burials cost 1/3rd of what it would typically cost for burial in cities with high population density. In Japan, a proper burial can cost up to 70% of a person's annual income. Having graves in vertical buildings with digital screens is emerging as a viable alternative. These screens can show a memoir of the person's life using photographs, videos or even tweets if you'd like it to.

The point is, gradually, people are willing to spend more on digital items. And it can be observed in the changing in-game spending patterns. Virtual goods and subscriptions account for over half of the console industry's revenue. The fact that people are willing to spend on buying digital in-game items is reason enough for games using blockchains to exist.

Payments, Storage & Reputation

But why? Ownership. Public, permissionless blockchains (like Ethereum) are permanent records of everything you do. So the "*item*" you purchased in-game may stay with you even if the game shuts shop at some point. This may seem like a weak argument today, as blockchain-native gaming has not grown to a point where people have emotional attachments to the game.

Large titles like Fortnite or GTA 5 have not shut down in recent years. But hypothetically, if and when they do, users would appreciate being able to own the assets in-game so that they can port it to a different client that is community managed. On its own, this is not an investment opportunity. **It is a hypothetical business case that may happen in the future.** As things stand today, consumers don't care about owning their assets as much as about having fun in a game.



Virtual goods and subscriptions are half of console software spending

The $70 packaged game is no longer the $60bn industry's biggest money spinner

Source: Ampere Analysis
© FT

Source: Financial Times

What blockchains enable today is creating a robust financial backbone for games. We explored how this would work for user-generated content in February of this year. Since then, Towns.com and OnCyber have released their version of user-generated worlds. Users can develop and charge other players for gaming in these products. Blockchains are used to collect, disburse and verify payments in these models, while the games, their logic, and assets are primarily kept off-chain.

Mythical Games' Blankos Block Party allows you to create your levels, like shooting arenas and race tracks. You will see practically nothing about blockchains on their landing page. The video below is a marketing teaser from them. It shows how "*blockchain*" games are shedding their addiction to mentioning the infrastructure and selling the application itself to the consumer.

The end user cares little about whether a game is built on a roll-up, Solana or an excel sheet. What they care about, is having the most fun, with the least effort. The dopamine doesn't come easy.

A different way games are evolving to use blockchains is with reputation. If you are a gamer that has spent thousands of hours in games, you would not want to start from scratch in a new game. In theory, applications built on a chain can read each other's state with the help of oracles. This allows composability among them.

So, if a player has crossed 40 levels in Mini Royale, a similar FPS game can allow this user to start from level 10 instead of asking them to go through initial levels that are too easy for their skillset. One way this model could extend is by offering free games to players that have crossed a certain level in a different game. Think of airdropping game keys, instead of tokens.

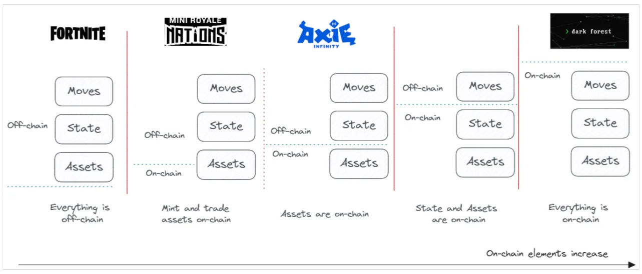
The cost of acquiring highly skilled gamers diminishes rapidly if reputational data goes onchain. Again, this hypothetical scenario may or may not play out in the future. It helps to arrange games on a spectrum to understand which applications may benefit the most from a blockchain in the short run.

The Spectrum

We often hear that over-financialization is the Achilles heel of blockchain games. Although it's largely true, sometimes it adds a different dimension to games. For example, 0Xconglomerate shares that Word3, a Player vs Player (PvP) Scrabble game, introduces fluctuating prices for letters you want to use to play words. The additional constraint on a gaming resource adds a new dimension to the game and makes you more conscious of your moves.

The trick lies in understanding what part of the game is on-chain. For the sake of this discussion, let's break down games into three parts – moves, states, and assets.

- Moves are the actions performed by players
- States are how these actions impact parameters like health or levels
- Assets are collectibles that players earn or buy in games.



The gaming spectrum in Web3 today. Visualised by Saurabh.

The degree to which a game is or should be on-chain depends on factors like the number of player moves per unit of time, whether on not assets can be traded, and so on. For example, for an FPS game, every keystroke constitutes a move. Because the position of a player on the canvas matters in determining how much harm a bullet shot by the opponent can cause, putting all this information on-chain is rather silly.

Having tradeable assets on-chain while managing everything else from the game's local server is a good idea for such games. But think of a game like Scrabble or a strategy game with limited player actions. If the stakes are high, one may record all of this on-chain. If not, the state changes can be recorded on-chain every time the player ends their session.

The kind of data that goes on-chain would vary depending on the nature of the game. Most AAA titles will have the bulk of their IP staying off-chain. Occasionally, there will be assets that a user can own, but it would still require the franchise to continue maintaining the game, its servers and storylines.

Gaming will be a spectrum for the foreseeable future. AAA titles will take years to use blockchains completely. But on-chain games like dark-forest can be developed in a matter of months.

In the immediate future, much of the "*games*" we will see will focus on luck or gambling elements. Their target market will be users from crypto that are no longer entertained by the flat, low-volatile state of the markets. Many will write off on-chain gaming as dumb casinos early on. But it is important to note that many technologies often start looking like toys before they mature enough to onboard retail users.

According to the Blockchain Gaming Alliance's (BGA) 2022 survey, the three most significant challenges to blockchain games are –

1. Onboarding / Accessibility
2. Poor gameplay
3. Players don't readily understand gaming concepts.

Game developers must think deeply about what game components are justified to be on-chain. The first is a UX problem where infrastructure plays a key role. If you think about when CryptoKitties went live, Ethereum was the only place to launch these games. Naturally, transactions were expensive, and it made little sense to have on-chain games.

But since then, several solutions, like rollups, have reduced transaction costs. On the scalability front, three solutions are worth mentioning.

1. Axie Infinity's parent company Sky Mavis built the Ronin blockchain. At the time of Axie's launch in 2019, it would cost $1.2 for a transaction on Ethereum. With Ronin, that expense is down to $0.00027. You can do close to 4500 times more transactions on Ronin for the same amount of money you'd spend to do a transaction on ETH.
2. Similarly, Offchain Labs recently released Arbitrum Nova. Much like Ronin, Nova's transaction costs are under $0.001. Games like Rhascau use Arbitrum Nova to build a better UX for users. The game can finalise balances and settle them much like it would occur with a traditional server-based game.
3. Solana developed state compression, which makes on-chain storage significantly cheaper. It creates a hash of off-chain data and stores it on-chain for validation. The cost to mint a million NFTs on Solana without state compression is ~12000 SOL. With state compression, it is 10.76 SOL.

The easy thing to do in the current market environment is to write off Web3 gaming as an opportunity. The arguments against them are quite simple. Yes, they take years to develop. Traditional studios do not have the skills or conviction to deliver great blockchain native games. And gamers would rather not bother with acquiring crypto or managing private keys.

But investors are likely forgetting the technical leaps we have made in the past few quarters. Transactions are now exponentially cheaper. Transaction signing is slowly vanishing from the user experience. And soon enough, users can store their keys on their iCloud storage.

These exponential improvements make the product far more appealing to the end user. Historically, the speculatory aspects of Web3 gaming are what attracted users. But the tech stack to build a great game, without ever mentioning blockchain or crypto to users, is here, now and today. And it seems as though the market is mispricing this shift.

There is an opportunity to arbitrage the market mispricing these technological shifts that have emerged in gaming over the past few quarters. Investing in them requires understanding which kind of game on the spectrum would grow to prominence at what point in time.

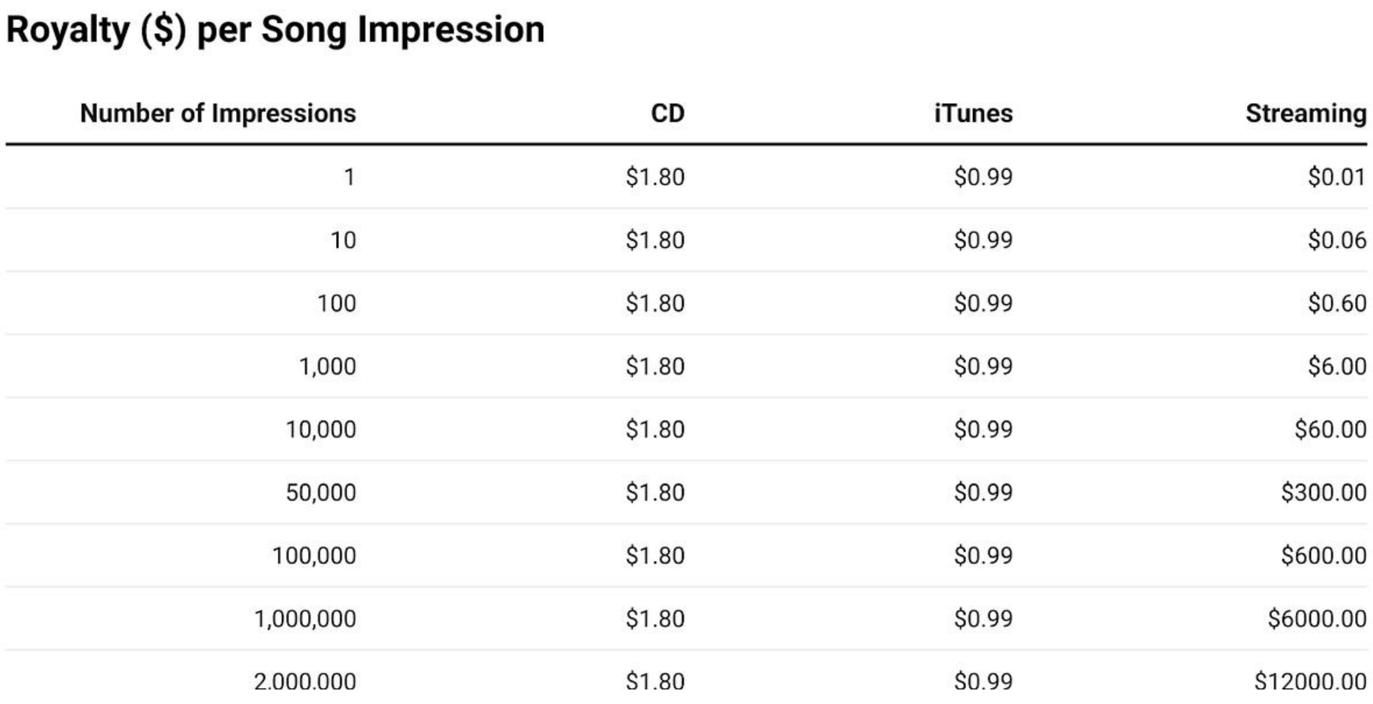
We may be at the early stages of multiple narratives forming within gaming. GambleFi, is, quite possibly, just the beginning of a trend that is here to stay.
More on that in another issue.

Signing out,	Saurabh

Saurabh
decentralised.co

Blurring Lines

What's next in store for NFTs.



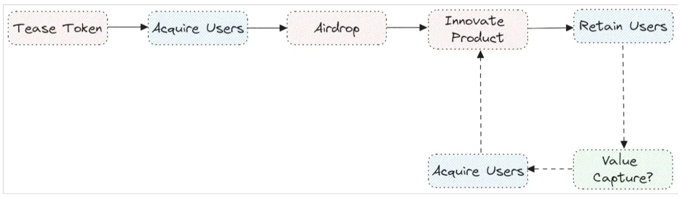
Royalty ($) per Song Impression

Number of Impressions	CD	iTunes	Streaming
1	$1.80	$0.99	$0.01
10	$1.80	$0.99	$0.06
100	$1.80	$0.99	$0.60
1,000	$1.80	$0.99	$6.00
10,000	$1.80	$0.99	$60.00
50,000	$1.80	$0.99	$300.00
100,000	$1.80	$0.99	$600.00
1,000,000	$1.80	$0.99	$6000.00
2.000.000	$1.80	$0.99	$12000.00

Hello!

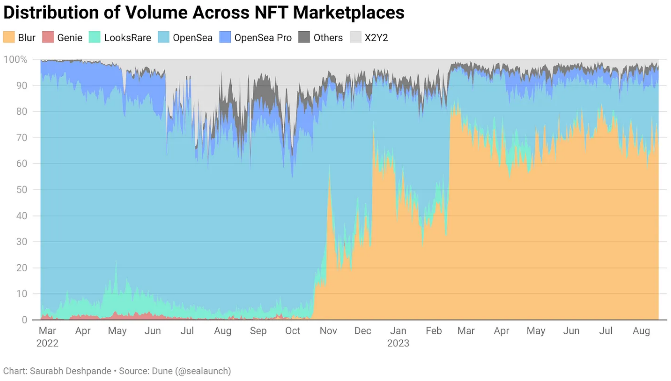
January of 2022 was an interesting time. LooksRare launched with token rewards for NFT traders. Rewards on the platform were a multiple of the fees it used to charge at the time. So, users were incentivised to spend $2 in fees to receive $4 in tokens. As the token price rapidly declined, the interest in trading on the platform evaporated alongside it. The arbitrage had dried up, and with it, the volume.

OpenSea was back as a leader in the business until Blur launched. Blur likely learned from the LooksRare fiasco and avoided releasing the token immediately. Instead, it was released in phases. It looked at user behaviour on their platform and measured activity with a point scale.



Blur's user acquisition strategy

Users were not incentivised to produce trading volume on Blur, which prevented wash trading. A few months after the airdrop, Blur launched a lending product named Blend. By this time, Blur had built a set of core users that stayed for the product and not for the token.



Blur did not focus on incentivising wash trades but managed to attract the bulk of the volume by collapsing the existing fee model around NFTs.

Blur announced its token in October 2022. Airdrop season 1 (*the time users could make themselves eligible for the airdrop*) continued till February 2023. Season 2, which was supposed to end in March and then in May, is still going on as we write this. Continued extension of season 2 means that users or airdrop farmers receive tokens after unlocks for the team and their investors, creating a conflict of interest. Some platform users received no liquidity for their tokens, while team members could sell theirs in the open market.

Until Blur launched, artists could expect to receive a percentage share of each transaction for perpetuity. This meant an artist's income was no longer tied to the number of artworks they produced, but to the frequency with which it changed hands. By removing the royalties paid to artists, Blur made it possible for speculators to trade as frequently as they'd like. NFTs began trading like altcoins. And with it, the NFT markets changed forever.

Show Me the Money

Web3 is undergoing its business model innovation phase. This is an image of Jack Ma from 1999.

We have seen a variation of marketplaces competing for users and volume in the past. Alibaba's Taobao launched in China in 2003. eBay was already well established in China then and had over $2 billion in annual global revenue. Taking on an established player like eBay was not an easy task. At the time, eBay charged users to list products and services.

Instead of directly monetising, Taobao improved users' experiences while buying and selling and, as a result, created ventures around its core product.

- It made listings free.

- It integrated a chatting app that allowed buyers and sellers to connect.
- It introduced Alipay, an online payment system. At the time, online payments were new in China. Alipay formed partnerships with banks, which made payments from buyers to sellers frictionless.
- It integrated ad companies like Alimama, which had a network of thousands of specialised websites that allowed sellers to reach their target audience.

As a result, rivals could barely keep up with the depth and breadth of Taobao's services. By 2010, Taobao had captured 80% of the e-commerce market in China. The takeaway is that sometimes, it is unnecessary to start monetising the core product from the get-go. Building auxiliary ventures can help the core business, and they can be monetised in due time.

Blur is following a similar playbook. Instead of going for direct monetisation, it launched NFT lending. They currently lead in the lending category. The easiest way for Blur to make money is to charge a platform fee for the trading marketplace and a haircut fee to lenders.

Here's the napkin math of how that may turn out.

For the trading side –

- The YTD trading volume on Blur is $6.4 billion. The annualised volume comes to $9.6 billion.
- The volume in 2024 could be $11.52 billion if we presume a 20% growth rate.
- The revenue would be $576 million, assuming a 0.5% platform fee.

For the lending side –

- Within four months of launch, Blur's Blend has a total borrow volume of $1.9 billion, which is ~$5.7 billion annualised.
- Assuming a 20% growth rate, the volume for borrows in 2024 can be $6.84 billion.
- Assuming a conservative 10% interest and Blur charges 10% of the interest earned by lenders, we are looking at ~$68 million in platform fees.

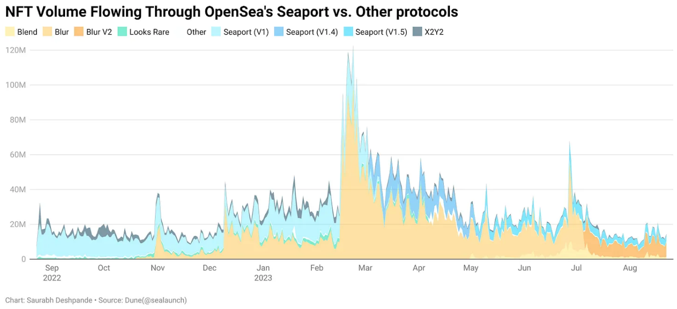
The total earnings for Blur in 2024 can be ~$644 million. Coincidentally, Blur is trading at $642 million FDV at the time of writing – a ~1× multiple on 1-year forward revenue. (*This is not trading advice. Just an observation we made internally*).

Valuing something is more of an art than a science, and the assumptions leading to the conclusion can be wrong. Also, the conclusion here is a function of governance approval for Blur to charge fees from its users. Given that OpenSea already charges a 2.5% fee on all trades, Blur charging a 0.5% fee is not farfetched. They could charge a fifth of what OpenSea charges and remain competitive because the product suite is better.

Creator Royalties

The initial promise of NFTs was that tokenisation would help artists solve royalty issues when it came to their work. This utopian dream was shattered when OpenSea recently announced that it would sunset its operator filter that enforced creator fees. In simpler terms, OpenSea is making royalties optional.

Although OpenSea's move is recent, it acquired the leading NFT aggregator, Gem, in 2022, and Gem always supported optional royalties. Game theoretically speaking, newer marketplaces have little to no incentives to support creator royalties as it eventually adds to the fees the end user pays.



NFT Volume Flowing Through OpenSea's Seaport vs. Other protocols

Chart: Saurabh Deshpande • Source: Dune(@sealaunch)

Blur’s relative dominance in volumes usually translates to a complete loss of royalties for artists behind the collections.

A comparison between how much creators earn via minting vs. royalties is a good way to understand the after-effects of all marketplaces tending towards optional royalties. Although this data is not readily available, according to Magic Eden, the median Solana project made ~6% of its revenue from royalties. For most artists, royalties make up a small component of their revenue. The mint or primary sale is where the bulk of their money is made.

For creators, the incremental cost of creating NFTs is low, and primary sales of NFTs constitute most of their revenue. Much of the NFTs traded in high volumes are usually part of a collection with tens of thousands of NFTs and not one-of-one art pieces similar to those you'd see in the real world.

The pricing power of NFTs depends on who the creator is instead of what has been created. This is primarily why collections like CryptoPunks of Bored Ape Yacht Club can still attract a premium. If an unknown artist issues an NFT today, it'd be valued more for its ability to attract a community than the quality of the art itself.

There are three key stakeholders in the NFT ecosystem today. Creators, marketplaces, and collectors or traders. Out of these, only marketplaces can enforce royalties, but that requires coordination among all the marketplaces. For them, creators are on the supply side, and traders are on the demand side. Will there be any buyers if creators disallow their NFTs from being traded on marketplaces? This is why the most likely scenario is all marketplaces resort to optional royalties.

Like everything else in crypto, NFT markets are also an outlet for speculation. It has become a niche asset class within crypto assets. When the intention to buy is to make a profit, why would you be willing to pay additionally (*in royalties*) to creators for every trade? Free market equilibrium is that creator fees become optional across marketplaces. **Technology is not the answer if we want creators to keep earning fees from secondary trades.** It needs to be a social phenomenon.

We must create a collector base that wants to honour royalties instead of coercing them into paying royalties. The evolution of online streaming and the music industry in the early 2000s offers clues about how this may occur. When streaming platforms launched, indie creators suddenly had a new distribution mode at their disposal. They were no longer at the mercy of TV networks or theatre owners to distribute their shows or movies.

According to Vox, there used to be 80 shows a year across TV networks, and there are now 500+ shows a year across streaming platforms. The number of episodes per show was higher for TV, so the shows ran for extended periods. Commercials during a show were a significant source of revenue.

Streaming platforms removed commercials as consumers were paying for access. The subscription revenue picked up the slack in revenue. Naturally, the nature of shows changed to adjust to the new model – there are now more shows, and the number of episodes is much smaller (*eight to ten episodes per season*). For producers, the economics didn't change much. They usually sell rights to a streaming service for a certain period instead of relying on advertising revenue. But for writers, fewer episodes means less money and the need to find more shows.

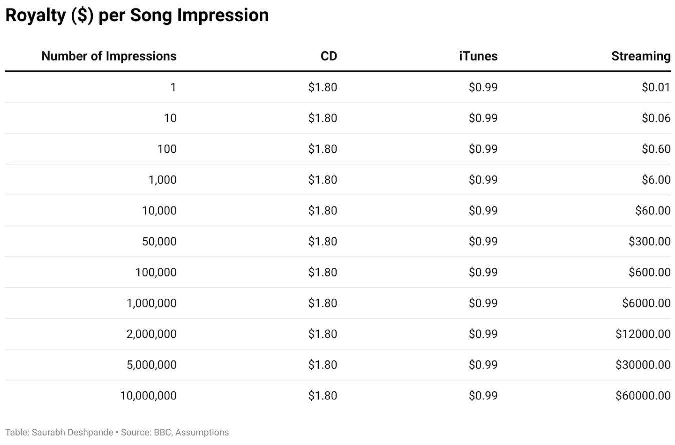
On TV networks, writers get paid every time an episode airs. With streaming platforms, writers get paid a lump sum amount regardless of how many impressions the episode creates. While this paints a gloomy picture, the new model allows more writers. With 500+ shows, the number of writers needed is higher than before. However, the work and pay per writer have gone down.

This is also the crux of the writers' union strike in Hollywood. There is no technological solution to this stalemate. Ultimately, there will likely be a social consensus where all the stakeholders in the creative process are somewhat equitably compensated. We saw a variation of this with music in the early 2000s too.

The music industry went from physical albums or records (pay per album) to iTunes (*pay per song*) to streaming (pay for the streaming service). Physical albums took different forms, like vinyl records and CDs. But, the revenue model remained the same. According to the BBC,

> *About 13% goes to the artists, while 30% goes to the label, with a 17% cut going to the government in the form of VAT (applied at 20% and therefore 1/6 of the purchase price). About 17% goes to the retailer, while the rest goes to manufacturers (9%), distributors (8%) and the spend on administering copyright (6%).*

When iTunes launched, instead of buying the album CD for $18, listeners could purchase individual songs for 99 cents. Records offloaded the entire album on you, although you liked only one song. But Apple's iTunes allowed you to purchase a single track. Records were the full buffet, and iTunes was the à la carte. The Beatles did not sell their albums on iTunes for the first seven years in protest.



Royalty ($) per Song Impression

Number of Impressions	CD	iTunes	Streaming
1	$1.80	$0.99	$0.01
10	$1.80	$0.99	$0.06
100	$1.80	$0.99	$0.60
1,000	$1.80	$0.99	$6.00
10,000	$1.80	$0.99	$60.00
50,000	$1.80	$0.99	$300.00
100,000	$1.80	$0.99	$600.00
1,000,000	$1.80	$0.99	$6000.00
2,000,000	$1.80	$0.99	$12000.00
5,000,000	$1.80	$0.99	$30000.00
10,000,000	$1.80	$0.99	$60000.00

Table: Saurabh Deshpande • Source: BBC, Assumptions

Streaming platforms evolved the business models behind music from being a one-time consumption purchase to an attention economy model. The time spent by the audience on streams mattered more than the number of times a track was purchased.

Around 2008, Spotify entered the market with music streaming services. Before this, the number of times you listened to the song after purchasing it did not impact artists commercially. It changed with streaming. Platforms like Spotify pay artists on a per-impression basis. The typical rate is $0.006 per impression. The table above shows how these three models affect artists' incomes depending on the number of times a track is played. Artists had to evolve with each of these iterations.

What's Next for NFTs

Getting lost in the weeds of royalties is easy, but the point is to try to find where we are headed. It would be criminal to mention NFTs and not bring up Solana, where a lot of the innovations for the primitives are happening.

Affordable transactions on Solana have allowed marketplaces like Tensor to flourish. Seemingly a copy of Blur at launch, Tensor has shown that '*cheap and fast*' can create a distinct product.

Tensor's market-making mode allows traders to place orders that are not possible on Ethereum-based marketplaces.

Market-making orders allow users to sell NFTs incrementally when the price increases and buy when the price decreases. Users can choose what the incremental percentages on either side are. In essence, it provides liquidity for NFTs the way exchanges have it for tokens. This is possible only because users are not spending much for on-chain transactions on Solana.

This change in the fee model is seen with the mint costs on Solana. Compressed NFTs on Solana reduce the cost to mint NFTs by over 99%, which could unlock a new way of using NFTs. Familiarity breeds loyalty they say. Cheap minting costs allow brands to experiment with NFTs constantly and reach their target audiences.

We will see more low-cost, one-time consumption good NFTs. When the cost of minting an NFT is as low as sending an email, brands would be incentivised to issue as many, as frequently as possible. NFTs would become less about trading or speculation and more about the use cases they can enable.

We are already seeing this at Mirror. Our last article was minted over 11,000 times on the platform for a cost of next to nothing. Readers have begun discovering our content through the on-chain footprint of people interacting with the NFTs we released there. In such a model, content discovery occurs less through algorithms and more through what happens on-chain.

The brick phones of the 1980s share a lot in common with Bored Apes from 2021.

The last generation of NFTs looks very similar to the brick phones of the 1980s—High-status, low-utility, and built for the elite. Much like mobile devices, as the cost to mint, trade, and transfer these primitives collapse due to emergent L2s, we will see everyone having a variation of NFTs in their wallet. It would likely not cost tens of thousands of dollars and serve entirely different use cases.

This transition has already happened on the tech layer. You can send millions of NFTs for a couple hundred dollars today. It just happens so that brands don’t know what to do with these primitives in a UI that sparks joy for the consumer. It is only a function of time before NFTs become as common as advertisements on the internet.

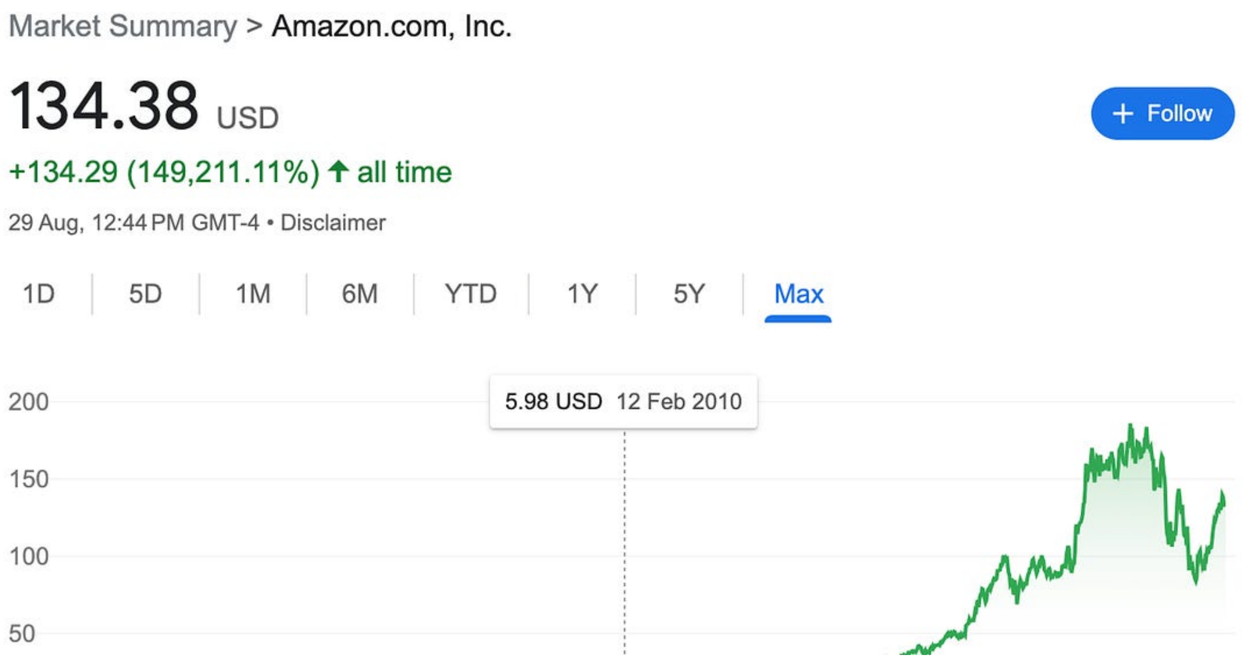
We are working around how NFTs translate to better content discovery engines, but more on that in the coming week.

Signing out to touch grass,
Saurabh

Joel John
decentralised.co

Cynical Optimism

A framework of thought.



Market Summary > Amazon.com, Inc.

134.38 USD

+134.29 (149,211.11%) ↑ all time

29 Aug, 12:44 PM GMT-4 • Disclaimer

5.98 USD 12 Feb 2010

Hello!

I noticed some of our readers have been forwarding our paywalled content to friends and family. I want to clarify that we love people sharing our content and have no issues with readers doing that.

If it helps, ***here's a link you*** *can use for the communities and group chats you belong to. Share everything we write. Ideas are fungible and infinite. And screenshots make terrible reading experience. With that out of the way, back to work.*

My last few articles have been observing the state of the markets as they are today. I observed how narratives drive themes in crypto and followed up with a breakdown of why volatility is a feature in most products. While these articles look at the behaviour of investors today, I'd like to break down a thesis on what the next few years in crypto will look like.

If you go on your Twitter feed, there is a resounding sense of hopelessness. Multiple market-makers have shut down operations, which means liquidity in DeFi applications is relatively low. The only applications making noise are the ones that enable speculation. And despite a decade-long obsession with decentralisation, our killer apps (stablecoins) are largely centralised businesses built on decentralised infrastructure. They are subject to censorship and far from immutable.

In such environments, cynicism is the intellectually easy route. You can be right 9 out of 10 times by simply shooting down concepts. And much like doughnuts, they are highly rewarding in terms of short-term dopamine. We like being right. The cynicism watches out for us by protecting us from potential fraud in the short term. And earns us clout from colleagues in the long term. Win-win, right? I wish.

The problem is while your odds of being right are 90%, that 10% of the time when you are wrong is usually the land of outlier outcomes. So when you are wrong, you could be passing up a potential opportunity to invest in Google, Uber or, as I've learned in my career – Polygon at a $10 million valuation.

I won't make this a post about why cynicism can be costly. Instead, I want to lay a framework of thinking for the next few years. Technologies evolve when a counterculture is formed. That is, early adopters of technology tend to think applications or protocols built using it should work in a certain way.

Eventually, people closer to markets make tools with trade-offs that look strange to early adopters. The new entrants look like the counterculture. As these new entrants build tools to scale, the technology gets adopted, and the early entrants get left behind.

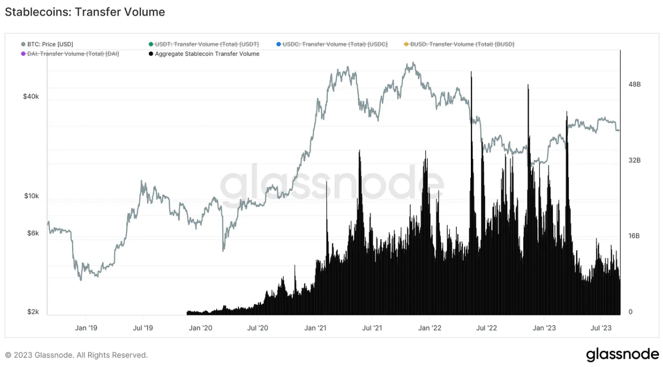
An emergent counterculture (*like NFTs or DeFi*) has not displaced early adopters (*like the laser-eyed Bitcoin bros)* because blockchains enable ownership. The growth of Bored Apes does not diminish Bitcoin's value for a holder since 2011 who purchased drugs and forgot the existence of his wallet up until a few weeks back. Crypto is unique because it has enriched early adopters, regardless of their ability to contribute.

Much like Steve Jobs and Bill Gates commercialised operating systems by licensing them, we will have a point in time with crypto-native applications when the apps that scale go against the ethos of what the industry has stood for.

Let me explain why.

The Killer Applications Are Here

It has been nearly 15 years since Bitcoin's whitepaper was released and almost 8 since Ethereum launched. To presume we are in our infancy as an industry is a good excuse to make when we fail. I think the applications of scale and PMF are already here and now. Consumers do not consider them as useful as Instagram or Amazon due to regulations, product positioning and technological limits. Let me explain.



The graph above shows the aggregate volume moved on any day across stablecoins. We are up from $600 million in early 2020 to $12-$16 billion today.

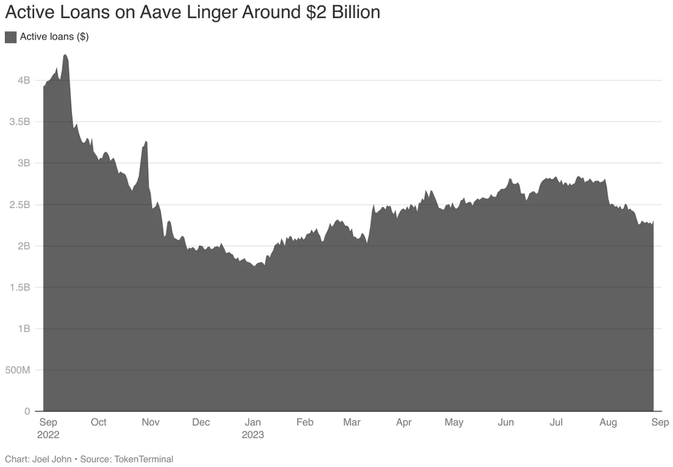
Depending on the statistic you go with, global remittance settlements range between $150 billion to $600 billion on any given day. According to data from Artemis, some $18 trillion have been settled on stablecoins over the past half a decade. The YTD volume for stablecoin settlements is $3 trillion. Surely, the vast majority of it is not retail-focused. If I presume a 1% rate ($30 billion) being retail users and take the high end of remittance volume ($600 billion), stablecoins have covered 5% of the remittance market.

You can scratch all those metrics and argue that they are simply wash-trades between users depositing to exchanges. That could be the case, but consider that the stack enabling large-scale dollar transfers between users exists here and today. USDC on Solana settles almost instantaneously, with transfer costs so low that the developer could pay for all of the user's transactions on a wallet they develop. For scale, consider that some $400k was spent on gas costs for stablecoin transfers just yesterday.

Why, then, haven't stablecoins taken off in the retail psyche? A significant reason is the lack of regulated players. Tether has been controversial, and anybody building applications on top of them stands the risks of USDT going to zero. It may seem like a far-fetched hypothesis, but several yield-as-a-service fintech apps had to close shop last year when Luna collapsed. (*Yes, I'm comparing apples to oranges here.*)

Earlier this year, Circle's USDC temporarily depegged during the collapse of Silicon Valley Bank. While stablecoins are a killer application, no regulatory frameworks exist for trust in these systems. That will soon change with the Monetary Authority of Singapore and the Financial Services Regulatory Authority (Abu Dhabi) issuing frameworks for stablecoins. The emergence of regulatory clarity around stablecoins as an asset will mark an inflexion point where the 'use' of stablecoins will be less oriented around trading and more towards retail use cases such as remittance and B2B payments.

A different place where we have already found PMF is with DeFi. The markets quickly discount the segment because we 'value' it based on how tokens perform. According to DeFiLLama, some $40 billion is spread across DeFi native products in TVL today. If it were a bank, it'd rank somewhere around #40 in the US based on deposits.



Aave has over $2 billion in outstanding loans, while Uniswap processes trades from a million users monthly. The last seven days alone saw over $3.8 million go back to liquidity providers on the product. Are these systems perfect? Far from it. However, they offer a permissionless, censorship resistant, user-owned alternative to the traditional banking world.

NFTs have a similar growth arc over the past few years. Many of us tend to see the ecosystem's growth (or collapse) by measuring the price of NFTs or the frequency with which they change hands. But at a fundamental level, they are tools that verify if the intellectual property being purchased by a person truly belongs to the seller.

It is the equivalent of verifying whether a Gucci or Louis Vuitton bag is an original. Over the past few years, NFTs have done these 'verifications' over 277 million times. Some $43 billion in value has exchanged hands on Ethereum alone in NFT volume. Nobody ever spends time verifying whether an NFT is fake or real. Smart contracts do that job.

Stablecoins, NFTs and DeFi are similar in collapsing the marginal cost of verifying economic activity. I'd written more extensively about this in our piece on aggregation theory. But the broader points to be observed are as follows:

1. Blockchain's core value proposition in the past five years was as a payment enabler. When I send someone $100, the person's balance increases and my balance decreases. Blockchains enforce this in an exponentially more transparent mechanism than banking ledgers.

2. Regulatory choke points meant that historically, the use cases had to be restricted to speculation. But we have improved exponentially within the scope of payments in the past few years.

3. As the regulatory landscape evolves, more retail-oriented applications will launch with an obsession for scale. They will make security trade-offs that look strange to early adopters.

The big mistake most investors would make in the next few years is thinking the current speculatory landscape in crypto is what the technology could eventually enable. The risk we all face is misjudging the timelines with which these changes could occur.

I have an emergent thesis about what could flip the switch. The answer requires us to look at things beyond the blockchains we obsess so much about.

Needs Produce Scale

We struggle to find a 'killer use case' for crypto because we see it as a singular infrastructure that functions independently in a world separated from external linkages. The internet was similar for the longest time, as people used it only for e-mail and chat, while the core subset of users was academia trying to share research.

Founders like Jeff Bezos, Sergey Brin and Travis Kalanick were building links to the real world. Let me explain through the lens of their products.

1. Amazon – It built catalogues of offline products and made them available online.

2. Google – While Google initially indexed the online world, much of the 'value' they built was in enabling individuals to find businesses whose presence was offline up until that point.

3. Uber – It got offline networks of taxi operators to move online.

4. Airbnb aggregated, indexed and curated information on who is open to sharing their house with you. Real estate (or rooms) is an offline product.

In other words, rewards are earned by blurring the lines between offline and online. Social networks (like Meta) are interesting because they have bridged the offline and online worlds. You can sit glued to your screen all day and have a relative sense of what is happening in the real world.

The question we should be asking is not what can be built on-chain but what elements of technology can blend with blockchains to enable applications that can scale.

Uber is an excellent example of how technologies blend to create magical experiences. In 2009, you could walk up to a person in India and ask if they'd like to call a taxi using an iPhone. The iPhone would have cost you $1,000, the internet to run the app would have cost you another $10 (each day), and the taxi might have never come. Mobile devices were a luxury then. It would appear stupid to use a mobile app when you could just ring up a taxi driver.

In 2021, people in cities rarely hailed a cab directly. Uber has built consumer habits to a point where it is strange not to use the app.

(Sidenote: One of my favourite Uber facts is that they have a real-time bidding system in Lebanon because of the region's currency fluctuation. It is the only region you can haggle with a driver in the app.)

In 2009, for Uber to work, you needed three separate networks to function:

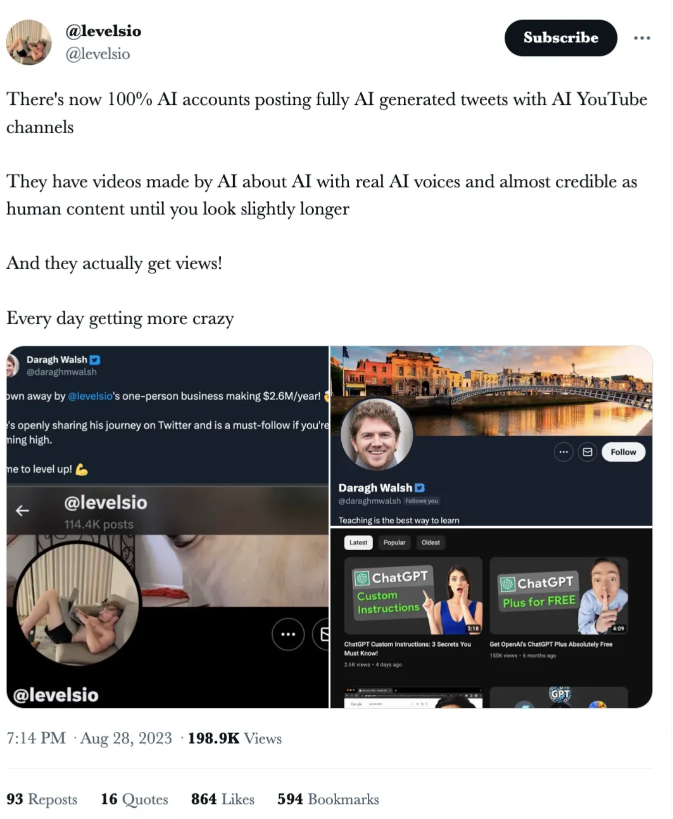
1. The GPS, which has been in development since the 1980s
2. Payment rails, which have been in development since the 1950s
3. Mobile networks, which have been coming of age since the 1990s

These had to merge into a mobile device that benefited from five decades of Moore's law. We take these things for granted, but technology evolves only with decades of work blending. The smart entrepreneur can tap into multiple trends blending. (*I would give Travis a premium for his ability to navigate taxi unions globally, but that is out of the scope of this article*).

Blockchain's next killer application will not emerge because users want to speculate. It will be embraced out of necessity, just like stablecoins and DeFi were. The internet's current landscape is evolving, and there are two things the technology does exceptionally well – verifying data and verifying identity.

At its core, a transaction is just two things: the identity of the individuals involved *(say Alice and Bob)* and the amount transferred between them (*say $50*). The blockchains we consider with such high regard (*be they Bitcoin, Solana or Ethereum*), at their core, do the same function. They act as ledgers.

They store data about individuals engaged in a transaction. And we have perfected that process. Tools like Nansen or Arkham are visual layers for identifying the individuals or patterns that emerge from this data. We are doing a long-form piece on identity and data in the coming weeks, so I'll avoid going into detail on it, but here is why I think the next phase of adoption would blend with emergent technologies like AI.



@levelsio
@levelsio

Subscribe

There's now 100% AI accounts posting fully AI generated tweets with AI YouTube channels

They have videos made by AI about AI with real AI voices and almost credible as human content until you look slightly longer

And they actually get views!

Every day getting more crazy

7:14 PM · Aug 28, 2023 · **198.9K** Views

93 Reposts **16** Quotes **864** Likes **594** Bookmarks

This tweet from Levelsio is a good indication of how human cognition is slowly reaching its limits with an abundance of AI-generated content.

The web is undergoing a transformative phase. Generative AI will soon create more content than humans can consume. It is within the realm of possibility that we see machine-generated content taking over human content in the next few years. Human moderation can barely keep up with human content to begin with. Meta has tens of thousands of underpaid employees to help moderate content on their platform. What happens when machines create more content than humans can moderate or consume?

The web will slowly become fragmented, and we will need tools to verify the source and accuracy of information. We consume content from social networks that face a trust deficit today. Twitter integrating a 'community notes' feature proves that we are currently crowd-sourcing the truth because there are no mechanisms to verify accuracy at scale. I believe blockchains could meaningfully move the needle there.

There could be a point when blockchain native identity enables social networks to verify the legitimacy of the content source. For instance, it is not far-fetched to believe that you could open your phone, conduct a FaceID verification, and sign a piece of content on a social network. In such an instance, the social network won't have access to the iris scan of the user (*like in Worldcoin's model*), but it would have verified the human-ness of the source of the content.

For the technically inclined: The model above is somewhat already in practice. Wallets use a mix of face-id with iCloud storage for private key management. Extending the same to Web3 social networks is within the realm of possibility. I am not suggesting this is a solution or a desirable outcome.

Why does this matter? In the age of endless content, we will need better tools to verify where we get our content from. Anybody can purchase the blue tick on X. Earlier this year, billions of dollars of stock value was wiped off medicine manufacturer Eli Lilly's market capitalisation when a user tweeted that their insulin would be given off for free.

That may have been a one-off case, but here's the underlying point: Nobody will be an influencer when even machines can turn into influencers. People would trend towards pieces of content that are produced verifiably by humans. And the internet does not have the infrastructure to do that at scale in a composable fashion. Surely, X and Meta have the budgets needed to do AML/KYC on their hundreds of millions of users. But how would a bootstrapped social network conduct identity checks at scale?

For context, it costs between $4 to $20 to do AML/KYC on an individual using third-party applications. Realistically, a developer would have to spend up to $500k to do AML/KYC on a small user base of just 100k users. It is a good problem, but it is still a barrier to entry that founders would rather not deal with.

Ben Evans recently alluded to this challenge with his piece on intellectual property. He argues that as generative AI comes of age, there will be a new class of copyright infringements. Instead of stealing one piece of content from a publisher, you would teach a generative AI model all the content they publish and create new articles. Who owns the IP rights in such cases?

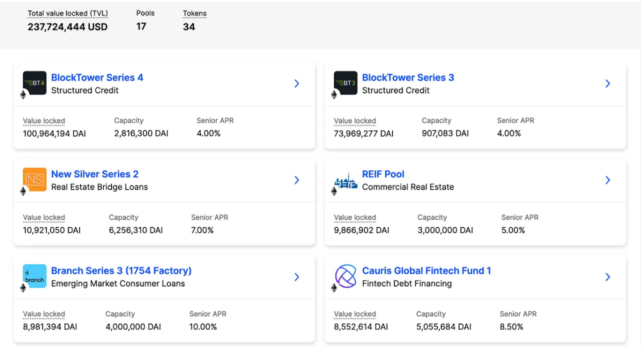
We are not at a stage where data markets can produce returns for individual users. But there's a credible case to lay for the following:

1. Using blockchains to verify the identity of who is posting content
2. Using the same layer to verify the identity of individuals reusing content

What does that look like? Mirror offers some clues. If you click on a user's profile in their product, you'll be able to notice what they have posted in the past. This profile by Livepeer, for instance, even mentions their ENS handle. Applications can use these primitives to accurately verify the provenance of content, much like DeFi applications can verify the source and validity of a token.

I mention this as a use case because it solves a necessity. The internet has already created an environment with more information than what can be consumed. This means the flow of attention would eventually be towards accurate, real, human-generated content.

The tools to verify whether content is human or real don't exist today. Generative AI is creating problem subsets that can be solved by crypto. It just happens that the influencers on your Twitter feed are not discussing it.



Total value locked (TVL)	Pools	Tokens
237,724,444 USD	17	34

BlockTower Series 4
Structured Credit

Value locked	Capacity	Senior APR
100,964,194 DAI	2,816,300 DAI	4.00%

BlockTower Series 3
Structured Credit

Value locked	Capacity	Senior APR
73,969,277 DAI	907,083 DAI	4.00%

New Silver Series 2
Real Estate Bridge Loans

Value locked	Capacity	Senior APR
10,921,050 DAI	6,256,310 DAI	7.00%

REIF Pool
Commercial Real Estate

Value locked	Capacity	Senior APR
9,866,902 DAI	3,000,000 DAI	5.00%

Branch Series 3 (1754 Factory)
Emerging Market Consumer Loans

Value locked	Capacity	Senior APR
8,981,394 DAI	4,000,000 DAI	10.00%

Cauris Global Fintech Fund 1
Fintech Debt Financing

Value locked	Capacity	Senior APR
8,552,614 DAI	5,055,684 DAI	8.50%

Centrifuge's real-time RWA dashboard is an instance of on-chain behaviour and off-chain reputation coming together.

You may think this is far-fetched. But the blurring of lines between the "real world" and what happens on-chain is already happening. RWA (real-world asset) lending uses off-chain reputation as a metric to enable on-chain transactions. You effectively use blockchains as just infrastructure to bring radical transparency into how a debt position is doing and how the capital flows occur. But the business itself happens off-chain. This is similar to how Uber used a different network (the internet) to facilitate offline behaviour (hailing cabs).

It may sound strange to think of these use cases today. It was weird to think of using a mobile device to hail a cab in 2009, using a 256kbps internet connection to bank in 1998, or believing screens and keyboards would upend education. **The arc of technology grows exponentially when it taps into human needs.** The product may look broken and unusual initially. But that is also where the opportunity subset usually exists for early-stage investors.

Blockchain-native applications have not scaled to hundreds of millions of users because the product category has no regulatory tailwinds yet. The case for scale is the following:

1. Regulatory landscapes would evolve rapidly
2. Technology (like AI) would create threats that blockchains can solve
3. Users would need tools with higher trust and verifiability.

Much like mobile networks and the internet, scale would be a function of technological improvements and use cases improving. To look at FriendTech or Unibot and suggest the industry is headed nowhere is like believing aviation is dead because of the Hindenburg disaster.

The Case for Patient Optimism

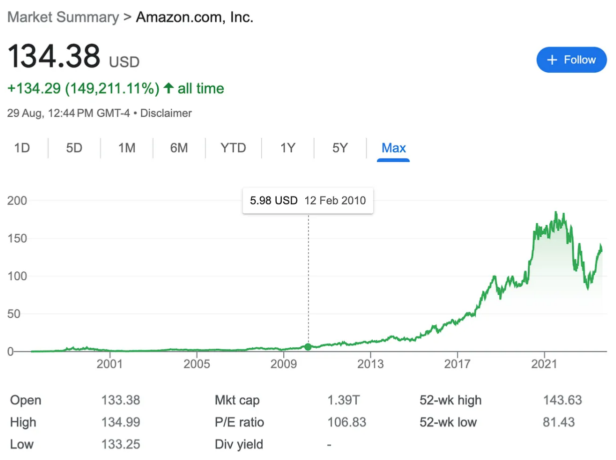
During the late 1800s, London was faced with a strange problem. A booming population meant that the city saw an increase in horse-drawn carriages. Some 50,000 horses were transporting people around London, and it was expected that they would soon produce enough dung between them to affect the health of everyone in the region.

Now, you could have lived in that age and believed things were only getting worse – much like some of us within crypto think today. Fortunately, motor vehicles took off within a few decades, and the city didn't drown in dung. Technology saved the day.

Sidenote: There are some reports that the great horse manure crisis was fake news produced by vehicle manufacturers. If the Times had used a blockchain in 1894, we could easily verify the accuracy of the news.

Present-day internet is very similar to London or New York in 1894. Generative AI will fill our feeds and mind-spaces with content we likely don't need. Blockchains are the equivalent of motor cars for this modern problem. But this piece is not about AI. It is about optimism. The reason why one should maintain relative optimism in these environments is quite simple.

Humans process experiences in linear terms. Technology evolves in exponential terms.



Market Summary > Amazon.com, Inc.

134.38 USD

+134.29 (149,211.11%) ↑ all time

29 Aug, 12:44 PM GMT-4 • Disclaimer

Open	133.38	Mkt cap	1.39T	52-wk high	143.63
High	134.99	P/E ratio	106.83	52-wk low	81.43
Low	133.25	Div yield	-		

Few things illustrate this trend, as well as Amazon's stock. You could have dismissed the internet as a fad in the early 2000s after the dot-com bubble crashed. Nobody would have thought you were an idiot for a decade – until 2010, when Amazon's stock was right around where it traded in 1999. But you would have ignored that a billion users came online in 2005. You might not have noticed that AWS was now powering Facebook, DropBox and Netflix. You would have even missed this incredible TED talk by Jeff Bezos comparing the internet to electricity.

And in the process, you would have missed out on owning a piece of Amazon as it scaled over the coming decade.

Now, I am nitpicking a stock with the use of hindsight. I was not around in the early 2000s to use these 'insights'. **My point is that it pays off exponentially more to be an optimist than a cynic when it comes to frontier technologies.** The markets discount growth in the short run and overvalue possibilities in the long run. This is why inefficient markets exist. The only way to get around it is to be a cynical optimist.

Why cynical? Because markets are also machines that transfer money from the impatient to the patient. Rushing to own a piece of every business could burn your hands, as many VC investors (including myself) learned in the past cycle. The only way to filter is through patient observation and understanding the possibilities a product can enable before the market prices it.

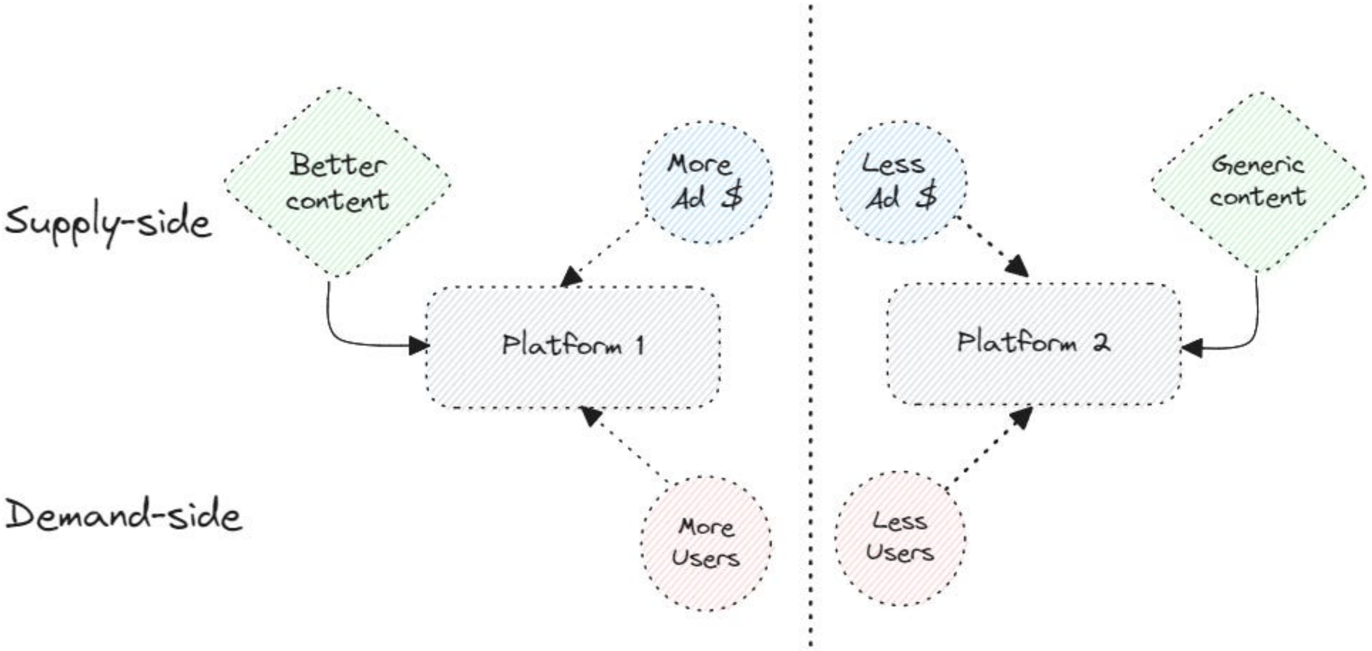
Blockchains are currently in their 'discount' phase, which partly makes them the opportunity of a lifetime in disguise.

Off to be in the arena for Bitcoin ETF,
Joel John

Siddharth
decentralised.co

The Advertisers Are Coming

For your wallets and eyeballs



Hello!

About 80% of all venture dollars went into advertisements in 1998. A year later, ventures in the '*dotcom*' sector spent more than $1 billion on ads during the fourth quarter – roughly equivalent to the combined spending of McDonald's and Burger King. In the same year, firms spent 94 cents on every dollar of revenue they made. With hindsight, it is safe to say that these expenditures were not sane. But that influx of money was crucial for the evolution of the web as we know it today. How?

Over 200 companies doubled their share prices during the dot-com bubble on listing day. The investors buying these shares came to know about firms through traditional advertisements. Consumer awareness around the internet rose substantially only because the possibility of speculatory gains (*from listing)* met a willingness to spend on ad dollars.

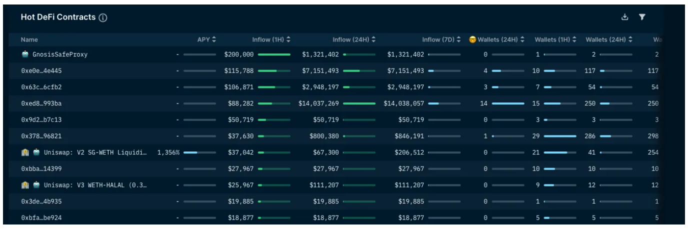
Most of that ad money eventually found its way into firms like Google and Yahoo, giving them a much-needed runway to develop the modern advertisement ecosystem.

Web3 had a close variation of this. Crypto.com and FTX purchasing stadium naming rights or Coinbase running a Super Bowl ad are examples of how an emergent technology tries using ads to purchase consumer mindshare. But while these initiatives did bring in consumer attention, the product suites within Web3 failed to retain them. Part of the reason was that we did not have mechanisms to identify, target and keep these users since their on-chain behaviour has not evolved yet.

We are entering some tricky territory here. As an industry, we have been opposed to collecting user data. But the more retail we go, the more pertinent it would become to understand the personas of users engaging with a product. Why? Because Web3 needs to transition from a transactional economy to one that can accrue attention if it has to house a billion users.

Ecosystems evolve when users can stick around without spending money. The internet exploded when users could listen to music, stalk their friends and stream movies. Web3, with primitives like Mirror, XMTP and Lens Protocol, is transitioning to a similar phase where consumer applications can scale without requiring users to make costly transactions.

But to onboard and retain user attention, the industry needs better mechanisms to surface and distribute relevant content.



Hot DeFi Contracts

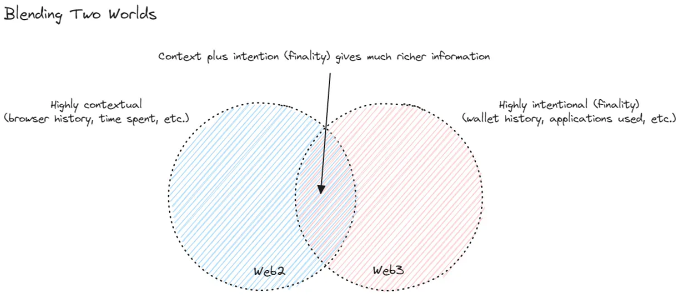
Name	APY	Inflow (1H)	Inflow (24H)	Inflow (7D)	Wallets (24H)	Wallets (1H)	Wallets (24H)	Wa
GnosisSafeProxy	-	$200,000	$1,321,402	$1,321,402	0	1	2	2
0xe0e…4e445	-	$115,788	$7,151,493	$7,151,493	4	10	117	117
0x63c…6cfb2	-	$106,871	$2,948,197	$2,948,197	3	7	54	54
0xed8…993ba	-	$88,282	$14,037,269	$14,038,057	14	15	250	250
0x9d2…b7c13	-	$50,719	$50,719	$50,719	0	3	3	3
0x378…96821	-	$37,630	$800,380	$846,191	1	29	286	298
Uniswap: V2 SG-WETH Liquidi…	1,356%	$37,042	$67,300	$206,512	0	21	41	254
0xbba…14399	-	$27,967	$27,967	$27,967	0	10	10	10
Uniswap: V3 WETH-HALAL (0.3…	-	$25,967	$111,207	$111,207	0	9	12	12
0x3de…4b935	-	$19,885	$19,885	$19,885	0	1	1	1
0xbfa…be924	-	$18,877	$18,877	$18,877	0	5	5	5

Nansen's hot-contracts are the closest our industry has to an on-chain content feed.

As of today, content on Mirror is curated and displayed by the team at Mirror. You can use tools like Nansen to filter and surface interesting on-chain interactions, but no algorithms do these independently. Evolving advertisements as a primitive, in a Web3-native way, would be crucial if we expect the ecosystem to scale beyond the users betting on Rollbit today.

On the internet, the core primitive used to identify a user is their IP address. With blockchain-native applications, the identifier is their wallet. Platforms on the internet build context around age, spending ability and preferences through the use of cookies. In Web2, much of this data is siloed, so a new developer cannot expect to have access to that information.

By contrast, with wallet addresses, most developers do not have access to context. That is, they cannot know the preferences of a user. But everyone knows the finality of a consumer's decisions through their on-chain footprint. Visually, the two worlds look like the one shown below.


Blending Two Worlds
Context plus intention (finality) gives much richer information
Highly contextual (browser history, time spent, etc.)
Highly intentional (finality) (wallet history, applications used, etc.)
Web2
Web3

We need both worlds to blend for the ecosystem to mature and scale. Very few products are in a position to enable this transition. But before we get to them, it is worth observing how products target users today.

Parsing Transactional Behavior

The most primitive form of user identification and onboarding is checking a user's historical behaviour. Products like Degenscore allow teams to restrict access to wallets that have been early to other projects or moved large amounts of money on-chain. It helps teams reduce the number of low-value addresses interacting with a product. For instance, when Gearbox launched in the beginning of the last year, early users had to meet a specific score before accessing the product.

Such filters allow teams to vet out users who may not engage in large volumes while improving service for large depositors. A different way this plays out is with transaction volumes. Apps in DeFi often offer free trading or bridging costs if the transaction volume is above a certain threshold. Taking on these costs is justified for them as customer acquisition cost (CAC) is usually relatively high for their sectors.

Tools like Guild's Balancy Playground enable marketing teams to combine requirements of holding a certain number of tokens or NFTs to export wallet addresses that can be whitelisted for a product. The problem with the current model of identifying users is that products or content do not surface depending on a user's behaviour.

The on-chain ecosystem is isolated in terms of how apps or products are discovered. This is why a considerable part of dApp marketing involves paying accounts with large follower bases on X (formerly Twitter) to announce the release of a product.

A product that can evolve in this avenue is a notification system that studies on-chain patterns and surfaces alternatives. It could involve things like:

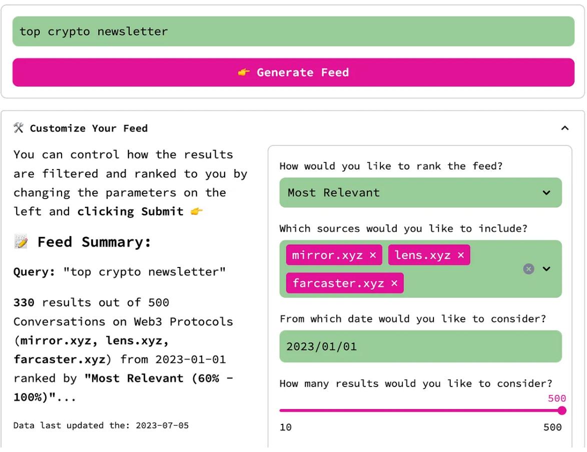
- Observing a user is depositing tokens into Aave for a 4% yield but could get better terms elsewhere,
- Flagging that a user paid 5% slippage on a Uniswap transaction and could likely have saved money using 1inch instead,
- Or even tracking and notifying users of a new NFT drop by their favourite creators.

In such a model, the data used is entirely on-chain. Products that facilitate these notifications would need to understand a user's persona solely from their on-chain behaviour and surface alternatives that are better targeted. Wallet providers like MetaMask and Phantom are well-positioned to enable such transitions.

The tools in the market today, like Cielo Finance, parse through on-chain data and notify users when a third party does a transaction. The ability to feed a system one's transactional history and get insights regarding alternative products does not exist today.

An alternative approach here, is studying on-chain behaviour to sell off-chain financial products. It's far-fetched, we know, but consider this: If you want to sell a financial product to someone, you must know the person's risk appetite. You can try selling a fixed-income product to a crypto degen, but it will likely not work. However, combining off-chain knowledge with on-chain addresses gives advertisers a more complete picture of the consumer.

If the wallet owner owns blue-chip NFTs and has spent several ETH on gas (not sensitive to gas prices), they may be interested in portfolio management services. Conversely, a user who doesn't complete a transaction when gas prices are high is likely seeking value-for-money goods. As the lines between FinTech and DeFi blur, products that can understand a user’s on-chain activities to upsell off-chain financial goods would be well positioned.



top crypto newsletter

👉 Generate Feed

🛠 **Customize Your Feed**

You can control how the results are filtered and ranked to you by changing the parameters on the left and **clicking Submit** 👉

📝 **Feed Summary:**

Query: "top crypto newsletter"

330 results out of 500 Conversations on Web3 Protocols (**mirror.xyz, lens.xyz, farcaster.xyz**) from 2023-01-01 ranked by **"Most Relevant (60% - 100%)"**...

Data last updated the: 2023-07-05

How would you like to rank the feed?

Most Relevant

Which sources would you like to include?

mirror.xyz × lens.xyz × farcaster.xyz ×

From which date would you like to consider?

2023/01/01

How many results would you like to consider?

500

10 500

Part of what makes MBD interesting is the fact that it lets you customise how and where the data that goes into your content stream is sourced from.

One place we witness this is with MBD.xyz. The product is more oriented towards content than it is to financial data. You can access their app right now and execute custom queries running across Mirror and Farcaster today. Think of it as a search engine for on-chain content. Although it is an early-stage primitive, it shows how content search engines evolve.

Someday, it is unlikely that users will go to Mirror, OpenSea, Farcaster or any number of new, decentralised content protocols. Instead, SDKs offered by MBD will bring content directly to a user's wallet. The user could mint, collect, trade or transfer on-chain primitives (like NFTs) directly from the wallet.

Why am I discussing discovery? Because unless you can map out what users are doing in Web3 today, you will be unable to surface more relevant projects for them. One place we are seeing what a Web3 native ad network would look like is with products like Brave Browser, Layer3 and Rabbithole.

Putting Users in Charge

In some sense, Brave has inverted the relationship between users and advertisers. They first started by blocking all ads. Then they began showing ads to users based on their opt-ins and rewarding them directly for doing so. A key differentiator between the ads users see on the browser, and the ones they see on Google is that Brave claims these ads are privacy-preserving and matched on the user's device.

The personal data never leaves the device. Brave crossed 50 million monthly users in 2021 (*Google Chrome had 70 million MAUs in 2010*).

For ad campaigns, it boasts an 8% click-through rate on its ads compared to the average of 2%. This means that when users choose to view ads, they follow through. The 6% gap may seem insignificant, but a purchase probability that is 4 times higher means about 4 times the revenue for every ad dollar spent.

With a lower user base, a high clickthrough rate may not mean much, but at the very least, ads are more effective when they are highly targeted and users are interested.

Applications like Layer3 and Rabbithole are onboarding platforms where developers and dApps are on the supply side, and users are on the demand side. Marketing teams for Web3-native applications use some of their CAC budgets to acquire users by giving them rewards in hopes that they will become permanent users.

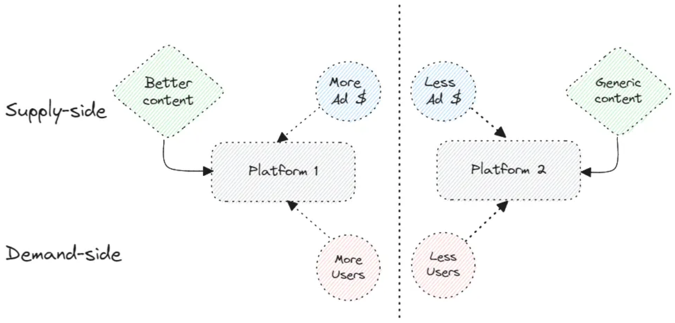
But the question for marketers is – whether the ideal user for a product somebody who is also motivated by platform rewards?

The answer is debatable, but here is what these platforms do today. They aggregate a large enough user base for Web3-native applications to have a good top-of-the-funnel.

Only a tiny percentage of their users may be interested in a product, but that does not matter when they have a million users combined between them. For scale, Metamask, with its six years of dominance as a wallet, has only two million users trying their swap product today. Quest platforms commoditise similar reach levels for any marketer with money to spend.

The difference between Brave and platforms like Layer3 or Rabbithole is that for users, ads are an auxiliary activity when they use Brave so that they can stumble upon something new.

But Layer3 and Rabbithole are for users who have already decided to use Web3 products. These users could also be mercenaries just hunting for airdrops and rewards and may never become regular users.



The quality of content on a platform dictates how much eyeballs it attracts. Which in turn, drives ad dollars. For platforms, the challenge is to scale to a point where it can offer sufficient distribution to entice creators towards making content on them.

One way Web2 platforms scaled and managed to retain users is through empowering creators on their platforms. Bill Bishop of Sinocism was one of Substack's earliest creators. Lady Gaga was one of Twitter's earliest power users. Platforms and social networks act as matching engines between creators and users. Their supply side comprises content creators, and the demand side has users. Better content attracts more users, which in turn attracts more advertisement revenue.

What has typically been the way to attract creators? Making them growth partners is the most obvious one. If the platform grows, creators get a piece of the growth. But applications like LinkedIn and Instagram didn't stop at that. They created multiple auxiliary apps that help creators create new content so that their overheads are minimised, and they can focus more on new ideas.

In Web3 native content platforms, we do not have creators producing and distributing content as the consumers (eyeballs) wanting the content do not exist yet. One way platforms (like Mirror) could break through this chicken-and-egg problem is by incentivising creators through tokens or ownership directly.

Without good content, platforms are forced to incentivise users to stick around, which has often looked like fighting a losing battle. In Web3, we are paying people to watch ads. Isn't this similar to paying people to play games when it was already established that people pay to play good games?

During the early days of the web, it was evident that advertisements would be a core part of the new digital economy. Nobody knew how to value internet companies then, but one metric used was 'mind share'.

Even the number of times ads could be displayed on the Microsoft Windows boot-up screen were considered for valuation multiples. Two decades later, fortunately, Microsoft charges for a license and does not show ads on their bootup screens. Amazon is perfecting that heinous act with their Echo devices.

We are at a similar juncture with Web3. Nobody quite knows where ads could pop up. We have barely even indexed user behaviour to a point where it can be segmented and studied for retention. But here's what is likely to happen. In the age of on-chain content, everyone could query content from others, like MBD or Family Wallet does today. In such an instance, the only way a platform could create a large enough network effect of users interacting with a product is through

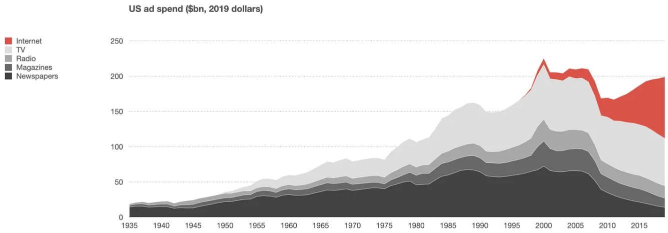
1. Onboarding creators through incentives (as mentioned above) or
2. Using data from users to combine intent and context to deliver superior experiences.

Products like Zerion and OpenSea today have millions of users interacting with their products. They are well-positioned to see what a user did on-chain and the number of times a user may have hovered around a new NFT or looked at a token's chart. They have both intent and context.

Such applications that have reached scale are in an advantageous position to begin advertising Web3 native products to users who opt-in. Given the composability of DeFi and NFTs, users will conduct transactions directly through their interfaces, and these platforms will register a fee for enabling them. But these are all hypotheticals. Any attempt to monetise attention in the industry may fail, given the industry's focus on privacy.

Two forces will be at play: teams' desire to grow at scale and market incentives for hyperscale. To scale, teams would need better mechanisms to target and retain users. Much like in the late 1990s, we will see money flow towards advertisement products again. It may seem far-fetched now, but it does not seem unlikely, given the emergence of consumer-facing applications in Web3.

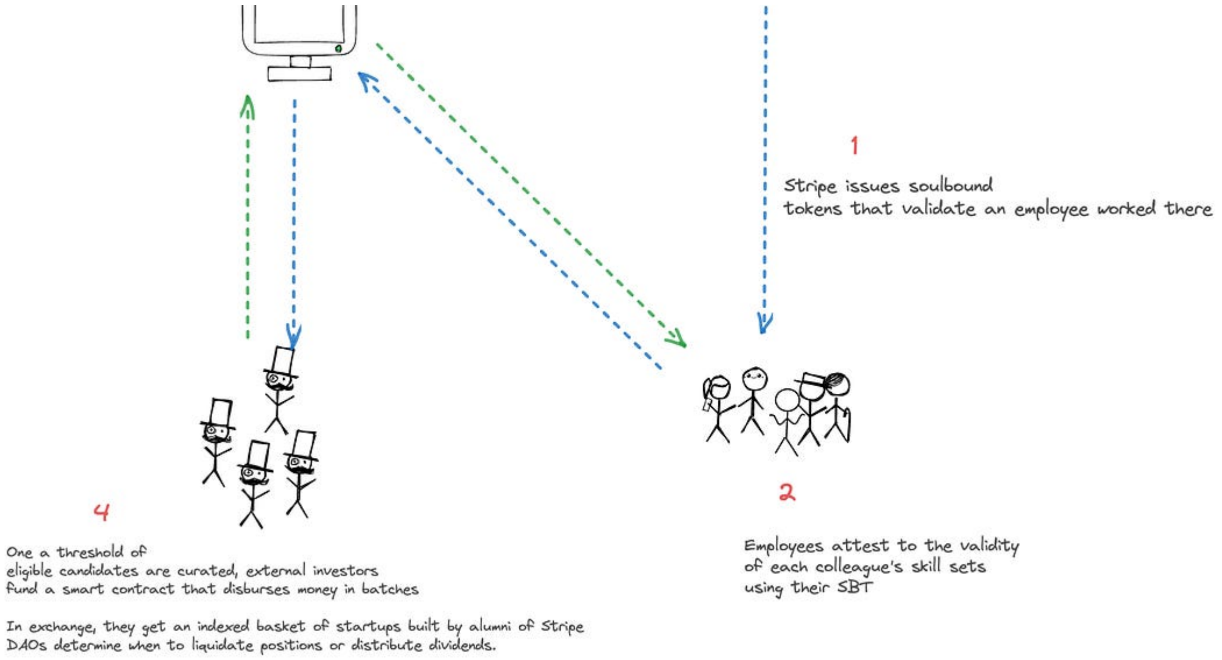
I'll leave you with this chart by Ben Evans comparing print and digital ads to understand how quickly the tides change when a new medium emerges. On-chain data is rich, contextual and accessible. There are likely billions to be made through parsing it and enabling brands to better reach users.



Joel John
decentralised.co

Soul Bound Tokens

Permanence in a world of Sybils


1
Stripe issues soulbound tokens that validate an employee worked there
2
Employees attest to the validity of each colleague's skill sets using their SBT
4
One a threshold of eligible candidates are curated, external investors fund a smart contract that disburses money in batches
In exchange, they get an indexed basket of startups built by alumni of Stripe DAOs determine when to liquidate positions or distribute dividends.

Hey there,

In 1996, Pierre Omidiyar had a strange problem. His platform (*eBay*) allowed buyers and sellers from all walks of life to meet one another and trade at the click of a button. It mostly worked, except occasionally, people did prank sales or, worse, outright fraud. How do you stop a network of people conducting trade with one another from cheating? eBay's founder set up a forum where people could leave reviews about the seller, resulting in the web's earliest identity networks.

Until then, not delivering a good or overcharging for something had little to no consequence. Twenty years later, the cost of losing one's reputation is one of the most potent detractors preventing brands and sellers on the web from engaging in fraud. The internet's transition from an unknown cluster of IP addresses to one with layers of identity has fascinated us. Siddharth spent the past few months studying identification mechanisms in Web3.

We will take it live on Thursday, but for today, I wanted to lay a precursor for the article. In our Friday issue, we explored how advertisement networks could emerge on-chain. But for an ad network to work, you need effective identifiers. I suggested that wallet addresses are the primary identifiers of a person in the blockchain ecosystem. There's only one problem with that assumption – as noted in our piece on airdrops, a person can spin up hundreds of millions of wallets in one day.

Unless you can meaningfully identify and target users, you have a problem. You may presume you have a large user base when you have a band of airdrop farmers. This is a structural problem with the crypto ecosystem today, much like it was with the internet in 1996. Vitalik Buterin proposed an alternative model in his paper on Soulbound Tokens.

Can’t Sell Your Soul

Tokens and NFTs can be transferred at will – enabling a free market for these assets. In comparison, Soulbound Tokens (SBT) cannot be transferred from one wallet to another. This means that once a user acquires an SBT, the only way to sell it to a third party is by handing over the wallet's private keys, referred to as a Soul in the model. Issuers like universities, employers or product teams could issue soul-bound tokens to eligible wallets. Other individuals holding similar SBTs could attest to a wallet's reputation.

This is similar to your university's issuing a certificate. Instead of the certificates being physical and open to being forged, an SBT system enables third parties (like employers) to verify claims of identity being made. Much like simply checking a token's smart contract address to verify if you are interacting with the right asset – a person could verify the smart contract address of institutions to which a person claims affiliation.

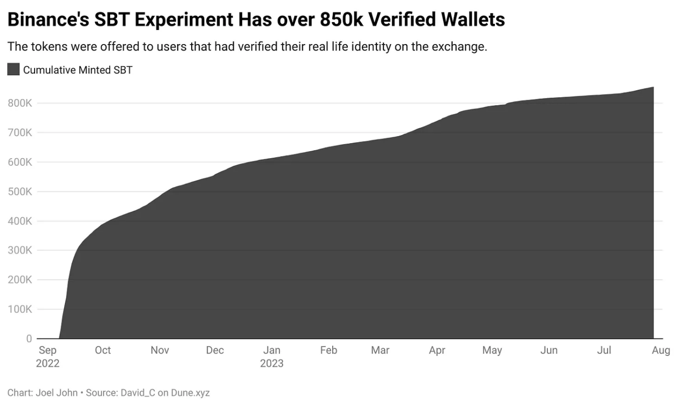
Why does this matter? Think of a platform like LinkedIn. Your identity is the summation of all the organisations you can draw affiliations with. The problem? Nobody quite knows how to validate these affiliations. The entities issuing the affiliations don't have a choice as to who can claim what on the platform.

For instance, I could claim I designed the SR-71 (*a beautiful machine*) with the Skunk Works team, and the organisation could do nothing to stop me. SBTs offer a mechanism for multiple issuers to directly establish relationships with a single entity. The entity could be a person or an institution.

What would this look like in practice? Binance offers some clues. They issued a series of BABT (Binance Account Bound Tokens) to create a network of verified accounts. Users who had done AML/KYC on the exchange could mint BABTs to their wallet addresses through the exchange. Over 855k wallets have minted account-bound tokens through Binance as of this writing. Why would users bother with tying on-chain wallets to their identities?

As with most things in crypto, it boils down to incentives. Users with verified accounts were given additional staking rewards and free in-game items.

For products, enabling additional perks for BABT holders is not an expense. They are receiving access to a network of verified users with exchange accounts. The incentives drive enough attention to have these users (potentially) trade their native tokens. At the very least, they'd know they are not being Sybil attacked by a single person spinning up wallets. The data on BABT shows some other intriguing features of how users on-chain behave when they have their 'real' identities linked to a wallet.



Binance's SBT Experiment Has over 850k Verified Wallets

The tokens were offered to users that had verified their real life identity on the exchange.

Chart: Joel John • Source: David_C on Dune.xyz

Had to go with the cumulative chart because adoption had largely flatlined in the last few months.

For instance, close to 11% of all BABT holders have 'revoked' their tokens at some point. These are wallets that lost access to their tokens. If that happens, Binance offers a mechanism for users to re-issue their tokens to a new wallet. It is quite evident that expecting users to tie all their identity-linked data to a single wallet is a terrible idea if you do not design mechanisms to retrieve the wallet.

Additionally, two-thirds of all wallets that issued a BABT token after validating their details used a new wallet. Users are paranoid about their on-chain privacy even when willing to give their details to a provider like Binance.

The whole exercise is quite interesting. If you have the numbers for what percentage of a dApp's userbase are verified, real users, you can more or less assess the 'human'-ness of a dApp. Historically, the argument with most dApps has been that bots primarily run them. According to data from @David_C on Dune, 5.5% of the total user base on Metamask interacting with Binance Smart Chain had a verified BABT account. Galxe – a platform that allows users to find new products and do quests to receive rewards – had over 13.5% of their users verifying their humanness.

Scaling Your Soul

What is the point of all this? Earlier today, Visa announced its collaboration with Solana on stablecoins. This comes a few weeks after their work on account abstraction. A new generation of fintech apps will use blockchain infrastructure to enable global-scale finance.

In such an instance, users will be 'verified' – like they do today with on-ramps before they can access the complete suite of products a fintech app offers. Metamask announced a feature that allows users to sell to their banks directly. Such use cases would require increasing amounts of gathering information on users.

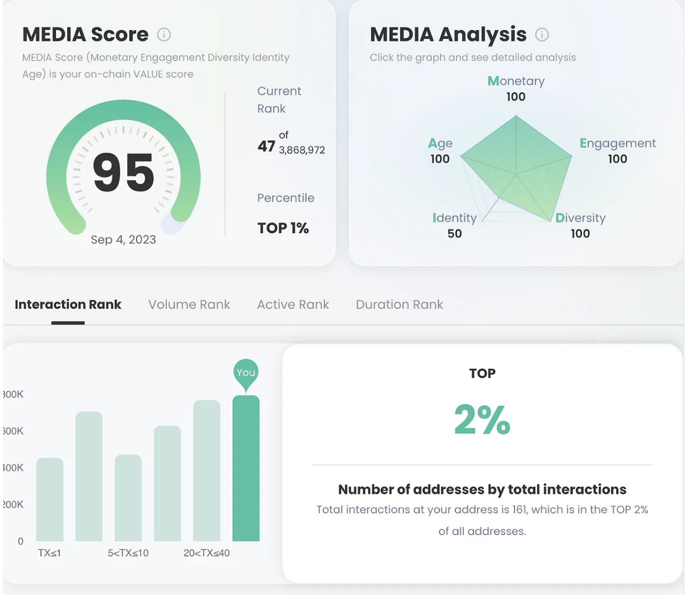
An SBT lets platforms know that users have done their AML/KYC at a third-party platform like Synaps.

A user could give their real-life documents (*like their passport*) to a service provider (l*ike Binance or Synapse*) to have a token minted that ties their real-life identity to their wallet. The service provider may not have to pass on the personal identification documents to a fintech app until the law requires it.

However, they could curate and enable a small subset of users to trade, purchase or transfer with one another. The fintech platform will only have to check if the user holds an SBT issued by the identity verification service instead of capturing the user's personal details. You replace an API call with a blockchain query in such an instance.

This curated subset of users could be buyers of instruments that have historically been kept on the periphery. Applications like income-sharing agreements, DAOs that offer dividends, or purchases of real-world assets could be enabled once user identification is activated on products.

It may seem far-fetched, but products like Gitcoin Passport enable users to tie their real-life identity to a wallet address. They do not pass your identification to an app but instead, give a score that factors in the amount of identification you provide the platform. The score could involve attributes like connecting your Twitter, Google and Facebook profiles to your wallet address on Trusta Labs to run proprietary algorithms that verify the probability of your wallet being fake.


MEDIA Score (Monetary Engagement Diversity Identity Age) is your on-chain VALUE score

Click the graph and see detailed analysis

Number of addresses by total interactions

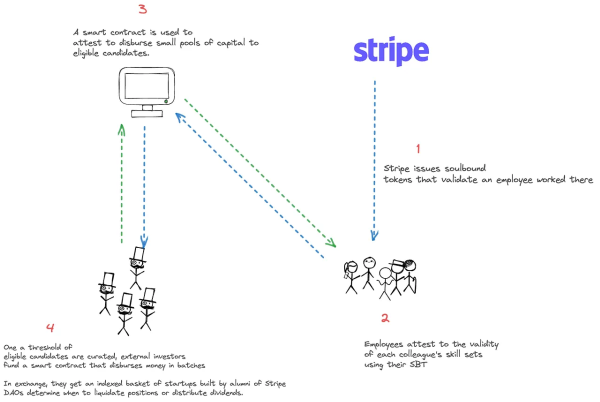
Total interactions at your address is 161, which is in the TOP 2% of all addresses.

Trusta's product allows you to plug in a wallet address and compute a score for it in less than a minute.

In other words, the mechanisms for users to verify their activity on-chain really exist here and now. SBTs could be crucial in enabling the next generation of fintech applications as they drastically reduce the barrier for AML/KYC. Assuming that platforms emerge that take on the liability of validating a user's identity, developers would soon be able to create use cases that do not involve complex on-chain gambling. Instead, things like remittance and reputation-based lending could emerge.

One of the use cases Vitalik's original paper points towards is using an on-chain reputation for venture capital. He argues that on-chain credentials could soon make it possible to offer lower, preferential interest rates depending on a person's background and probability of repayment. I believe the primitive would be used for alumni-based investment pools. This might sound a bit erratic – but hear me out.

(Or read the graphic below in the order of numbers mentioned. The blue lines indicate the flow of data, the green lines indicate the flow of capital.)


3
A smart contract is used to attest to disburse small pools of capital to eligible candidates.
stripe
1
Stripe issues soulbound tokens that validate an employee worked there
2
Employees attest to the validity of each colleague's skill sets using their SBT
4
One a threshold of eligible candidates are curated, external investors fund a smart contract that disburses money in batches
In exchange, they get an indexed basket of startups built by alumni of Stripe DAOs determine when to liquidate positions or distribute dividends.

At its core, venture capital is about building a pool of money to fund talent that ticks off specific requirements. It has become common to bet on the alumni of firms like Stripe, Spotify and Paypal. A simple use case for a DAO and SBTs would be to set up a pool of money – in a smart contract, have users verify their wallets using SBTs, have a network of colleagues attest to their capabilities and receive a line of credit.

In such a model, you are betting on a single parameter – the user's work background. Surely, this already happens today. Close colleagues already dominate friends and family rounds in the market. In a DAO model, third-party capital allocators interested in co-investing could join along with much lower friction levels. Co-investing at the speed of transferring stablecoins.

Naturally, it is foolish to do this setup for a single organisation. Such models are effective only at scale. You would need former employees of multiple prominent startups to create a marketplace for such a model. The DAO's responsibility would be to curate employees and match them with an increasing pool of capital.

(*FWIW, this would require the same kind of checks as AngelList SPV. The critical difference is in the speed and transparency of such a system's capital and data flow.*)

This could also play out in a different area – income share agreements. Present-day DeFi applications must go to great lengths to enable any RWA. However, employees could unlock 'liquidity' for their salaries (or ESOPs) by having employers issue them SBTs. An SBT could represent 20% of their income for six months in such an instance.

A third-party lender could verify the SBT's ownership in a person's wallet and offer undercollateralised loans. This already happens today with pay-day loans. The difference is that an SBT-based model allows multiple lenders to compete on the lowest interest rate a person must pay without requiring the employee to apply at multiple places.

The emergence of identity-related primitives in the industry represents a shift for all of crypto. They strengthen the interactions between the traditional world of finance and on-chain capital. Along the way, they also make security and privacy trade-offs. For instance, SBTs could target users working at specific organisations.

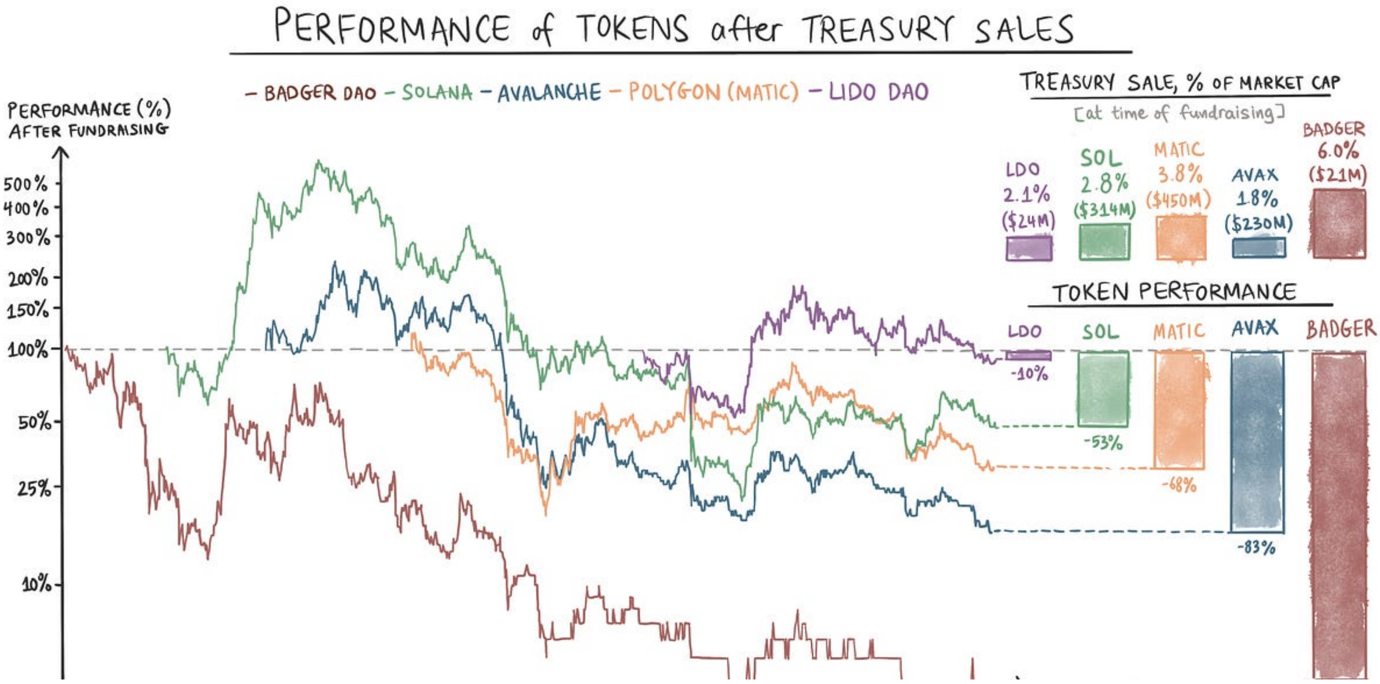
The industry often jokes about how the Bored Ape Yacht Club (BAYC) NFT owners must be relatively unsophisticated, considering how often they get phished. Inversely, they are subject to more attacks as their wealth on-chain is more evident.

The world of identity has privacy-preserving mechanisms that this piece has yet to explore. I'll be in your inbox on Thursday (or late Friday morning, given how deadlines work) with the long form on it.

Saurabh
decentralised.co

Bearproof Treasuries

Surviving 90% Drawdowns



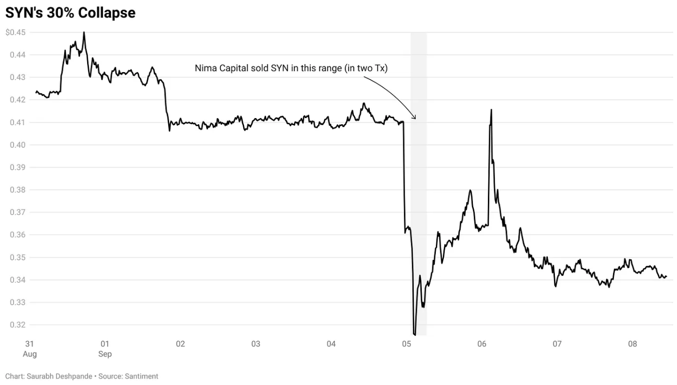
1. *We will be at Token2049 next week.*
   Drop in an e-mail response to this newsletter if you'd like to meet.

2. *There will be no paid pieces next week (Tuesday and Friday).*
   The long form will arrive mid-week.

3. *Use this link to share the article with friends for free.*
   Back to the article now..

Nima Capital received a SYN token grant from Synapse for agreeing to provide $40 million in bridge liquidity for 12 months starting in March 2023. On September 5, the SYN token suffered a ~25% drop after its partner Nima Capital breached the agreement by removing liquidity and selling its grant.

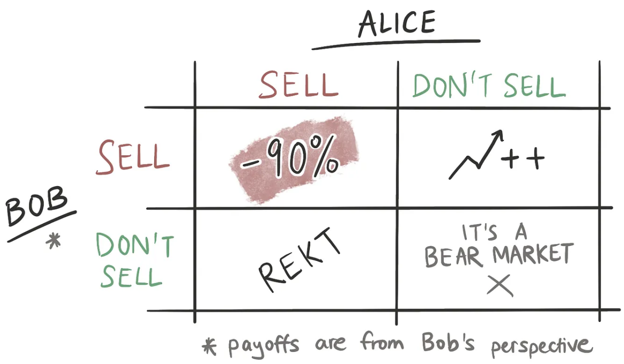
We don't know whether Nima Capital suffered a hack or consciously walked away from the agreement, but it got us thinking about the challenges of maintaining token treasuries. This piece explores why treasury diversification becomes critical and what projects can do to survive harsh crypto winters like the one we are in right now.



The price of the token went momentarily below $0.2 when Nima Capital offloaded their holdings into a thin book.

When the going gets tough, selling seems to be the only option. During the good times, you use Nansen to understand who else has bought the token to buy before it is too late. Similarly, during the bad times, you check Nansen to see who is offloading tokens and to get out before the liquidity dries up. Selling seems like the equilibrium for you in this game-theoretic situation.

A matrix for the game theoretical outcomes would look like the visual below.



		ALICE	
		SELL	DON'T SELL
BOB*	SELL	-90%	↗++
	DON'T SELL	REKT	IT'S A BEAR MARKET ✕

* payoffs are from Bob's perspective

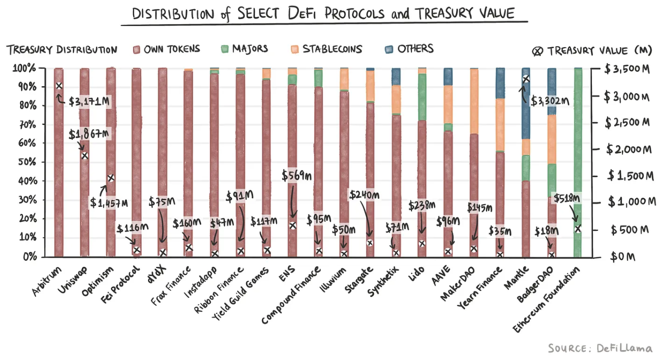
Tokens tend to lose over 90% of their value in due time, much like SPACs of the years past. Investors don't want to hold on to their inventory of tokens if they do not have high conviction on the asset. If you don't sell before or when others sell, you'll end up '*bag holding*' and hoping for a market recovery.

Of course, timing the top is almost always impossible. The next best thing is to sell around the top because prices start dropping due to a lack of buyers. Every incremental sale causes a more significant drop in the price. Strategically, it is better to sell early than late if a downtrend becomes obvious.

The fear of losing capital drives investors to sell while the opportunity still exists. (*Fiduciary duty is what the cool kids seem to be calling it.*)

Investors can diversify and rebalance portfolios to ensure low drawdowns. However, most Web3 protocols cannot do this, and their treasuries are vulnerable to the token's price performance. The following chart shows treasuries and their breakdowns for some DeFi protocols. Arbitrum and Mantle stand out – they have around the same in respective treasuries, but their distributions differ.

Mantle has only ~40% in its token, whereas Arbitrum's treasury comprises entirely of ARB. As with most things in life - token treasuries, are a spectrum.



Graph by Fongki

Protocols have operational expenses in both bull and bear markets. These expenses are usually incurred in fiat currencies. Ideally, the treasury value should not swing wildly as the token price finds its fair value. Holding the entirety of the treasury in a native asset (like UNI) exposes the team's morale to swinging prices.

Something you don’t exactly want to do. This is why compensation in the traditional world is a mix of dollars (fiat) and equity-based. Teams have been trying to work around this problem for quite some time in crypto. We studied several approaches that have emerged in the market over the years and their after-effects.

Treasury token sales

Selling a part of the token’s treasury is similar to a follow-on round in the equity world. Teams sell a portion of the tokens they hold to willing buyers at prices they are willing to buy. Since these sales happen at a higher valuation from launch, they sell only a smaller portion of their holdings. For investors, the upside is that they have a functional token with active listings when purchasing tokens.

The “*premium*” is for the liquidity profile of the asset. Generally, these sales solve two problems for a token. They -

1. Convert part of the protocol's treasury to stable assets

2. Use the VC or fund's network for things outside the core team's competence

Keeping part of the treasury in stable assets matters because expenses always remain stable. (*There's inflation, but it's not as volatile as token prices.*) For example, say a protocol has a treasury of $100 million with a yearly burn of $3 million. If the token price drops by 95%, the treasury will now be worth only $5 million. (*5% of $100 million*)

Their runway just went from 33 years to less than two years. If 15–20% of the treasury is converted to stable assets during a bull market, the team can ensure a five- to six-year runway, regardless of market conditions.

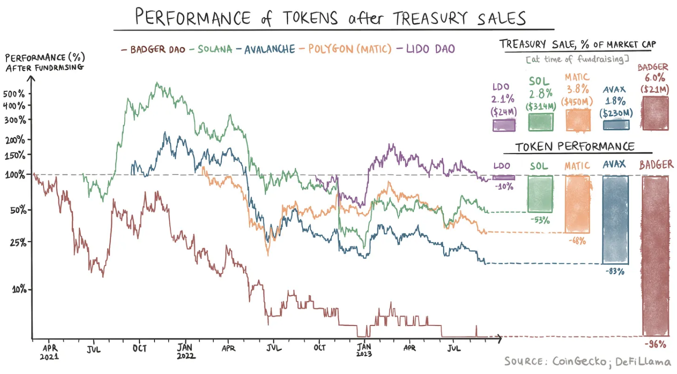
Selling tokens in the open market is almost always a bad idea. Others can frontrun you and cause panic in the markets. Also, the liquidity is usually low for large treasuries to diversify meaningfully.

According to CoinGecko, the -2% depth for Uniswap (UNI) across the top five venues is less than $5 million, and the same is less than $1 million per CoinMarketCap. Even if we consider the higher estimate ($5 million), Uniswap can only diversify 0.2% of its treasury without impacting the price by more than 2%.

The team at Uniswap would not go and dump it directly on an exchange. Service providers like OTC desks and prime brokers facilitate such transactions. But without a healthy ecosystem of growth-round investors (*like Tiger Global or Coatue from last year*), that order flow would eventually find its way to an exchange where it adds to sell pressure.

The following chart shows some projects that raised funds from investors and whether it has helped them. BadgerDAO raised $21 million in March 2021 from investors. This amount was 6% of the market capitalisation then. The token has lost 96% of its value since its raise.

Currently, the treasury has ~$4.6 million (*~26% of the total treasury*) worth of stablecoins. On-chain analysis shows that one of the investors received $1.25 million in BADGER tokens, and they moved all tokens to an OTC desk (*presumably to sell*). The investor's address did not hold any BADGER tokens at the time of writing.



Graph by Fongki

The obvious caveat for the data above is that the market has had a draw-down over the last few years. Tokens may have seen a dip in price regardless of their treasury sales. We are not trying to show that investors sell their tokens here. The point is that treasury diversification sales do not guarantee that investors will hold on to their tokens. When projects sell tokens to investors, there is no guarantee that investors will hold them for eternity.

There are examples where investors sold within months (Badger) and held on for longer (Lido). As market conditions change, they can sell tokens as they see fit, as long as they do so outside the lock-up periods. Although these types of sales do not insulate token price from the same fate as the broader market, because the treasuries of teams making such sales now comprise stable assets, they help protocols power through the bear markets.

Raising money from investors is easier said than done. When the protocol is out in the open, it has a live community that usually discusses and debates when it is time to raise new funds using treasury tokens. In the age of "decentralised governance", selling a token's treasury for fundraising requires convincing community members.

Sushi is an example of how governance can get messy. In July 2021, a proposal for a strategic raise was put forward by 0xMaki. After a lot of back and forth, the proposal was withdrawn. The plan was to sell $60 million worth of SUSHI tokens (*25% of the developer treasury was initially to be allocated to community members*).

The token's market price was ~$8, whereas the proposed selling price to investors was ~$6, a 25% discount. The discount came as a package deal with a lockup for which the investors could not sell their SUSHI tokens. As of September 7, 2023, the price of the SUSHI token is ~$0.6.

Had the community passed the proposal, it would have saved ~25% of the treasury from a 93.5% drawdown.

Selling tokens doesn't always mean investors or funds are the counterparty. One can make a case for different DeFi protocols swapping each other's tokens to diversify treasuries. This approach has limitations because almost all DeFi tokens are highly correlated. Swapping one for another is unlikely to protect any protocol treasury from severe drawdowns.

Using Derivatives

Financial markets have already figured out clever ways to hedge things. Oil and gas companies, airlines, agricultural product manufacturers, and many other manufacturing industries rely on commodities as inputs to their production units. They often engage in hedging using futures and options.

Hypothetically, the same can be done for treasury tokens. The most straightforward strategy is to sell out-of-the-money (OTM) calls and puts. This way, the treasury sells high and buys low. Of course, one can combine futures and multiple dated options to try to achieve the ideal delta for the portfolio, as the aim is not to make money from trading operations but to ensure that the protocol always has sustainable capital and price drops don't force shutting shop.

An OTM derivative is a bet that the token's price will not fluctuate wildly within a short period. A call option sold at an all-time high (ATH) of the token's price (*like in the chart below*) should generally be acceptable, as any loss is covered by the appreciation of the token's treasury. The challenge is with the signalling of such an operation. It could create complexities regarding information asymmetry between a team selling options for its token and buyers of such an asset.

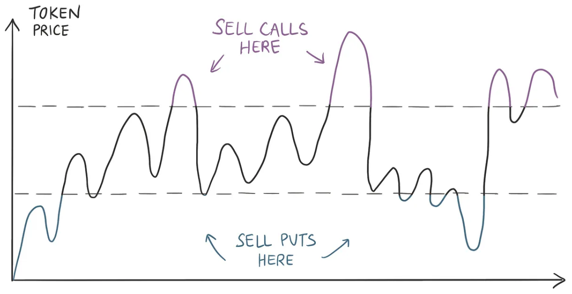


Image by Fongki

Would you buy call or put options from Apple if they sold it to you? Would that be ethical? We don't know, but here's what we do know: Despite derivatives being an elegant solution, the state of options markets in Web3 leaves much to be desired. The lack of liquidity except for ETH and BTC means that this solution is perhaps far out in the future. Market makers have tried to engage with protocols to devise derivative strategies to maintain treasuries. Still, the efforts have not yielded any results as far as we could see.

It also doesn't help that several prominent market makers in crypto have stepped back from active presence in the industry.

Joel's note: I strongly suggest following long-time supporters of this blog - Laura and Samneet to stay updated on all things options

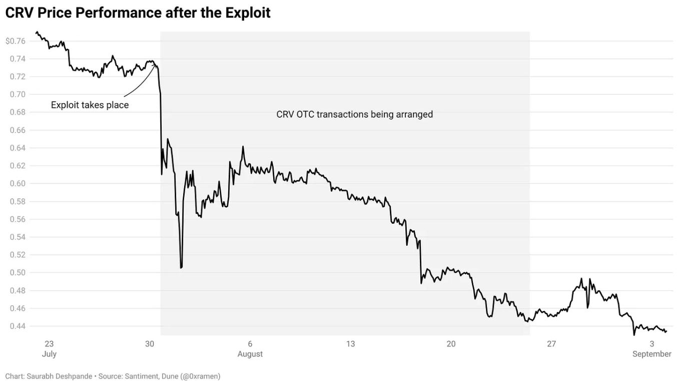
Use debt financing

Companies often use debt as a tool to finance their ongoing operations. For founders and companies, borrowing against their tokens is often a more tax-efficient option than selling tokens/shares. Using any form of leverage or debt is not without disadvantages.

When tokens lose value (*in crypto, tokens often lose 90% of their value*), there's always a risk of margin calls and their cascading effects. One instance of a token's founder using debt has been quite public recently. While not a case of "*treasury diversification*," it is a good study of what happens when tokens are used for debt.

Recently, Curve was hacked for ~$50 million. Curve's CEO, Michael Egorov, had borrowed against ~427.5 million CRV (*~49% of the total market capitalisation*). After the exploit, the token price started to drop, and there was a risk of contagion emanating from Micheal's forced CRV liquidations. Protocols like Frax increase interest rates exponentially when the utilisation factor reaches 100%. Frax's model doubles the interest rate every 12 hours at 100% utilisation (*which was hit as the price dropped*).

Micheal had to sell his tokens to investors and market makers through OTC desks. As of August 25, $64.2 million worth (160.6 million CRV) OTC deals have been arranged.



CRV Price Performance after the Exploit

Chart: Saurabh Deshpande • Source: Santiment, Dune (@0xramen)

Unlike stocks in the equity market, tokens are highly volatile. Despite the current low volatility environment, Bitcoin's volatility (*30D annualised*) is around 40%, and the same for the S&P 500 is ~14%. Altcoins like Curve's tokens are typically more volatile than Bitcoin. It is not far-fetched to say that crypto markets are not mature enough to pledge tokens to raise debt in a personal capacity or for the project without jeopardising events like Curve.

Long story short: using tokens as collateral will not help in meaningfully diversifying the treasury without risks, but they can issue convertible notes where, after certain events trigger, the debt converts into tokens. The general risk with such an approach is that market participants are incentivised to pursue it once a *liquidation price* becomes evident.

Use of range tokens

Range tokens, introduced by the UMA protocol, borrow from options and convertible notes. They are called range tokens because the buyer is protected within a range. They are exposed to the downside and upside on either side of the range.

A seller (*like a token's treasury*) optimises to avoid suffering when prices drop. There's no free lunch in markets. If they are to stop this suffering (*which means someone is willing to bear the cost*), they must also let go of the upside (*the counterparty benefits here*). In a nutshell, this is how range tokens work:

- There's a cap to the number of tokens the DAO will give away on expiry. The investor is also guaranteed a minimum number of tokens. There will be a predetermined expiry date at the time of issuance.
- Say the DAO defines its range as $20 to $40. For a $100 loan, the investor receives a minimum of 5 and a maximum of 2.5 tokens.
- If the price on expiry is below $20, the investor gets 5 tokens (per $100 invested) and 2.5 tokens for any price above $40. The number of tokens in between is 100/(price on expiry).

This is what the payoff would look like for the investor:

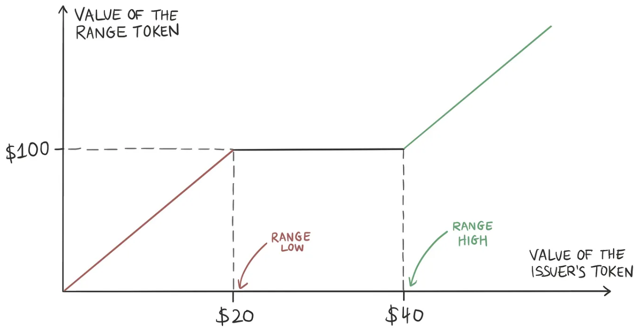


Image by Fongki

Range tokens are similar to selling call and put options (as in the previous chart). They are simple versions of selling options since complications around the time decay of options pricing are not involved. Despite being a more straightforward instrument, range tokens' adoption to diversify treasuries remains low.

Issue new tokens

We have discussed four mechanisms to raise money. None of which have scaled. Maybe it's worth looking at what happens in the traditional world at this point.

In public markets, companies can raise more money via equity even after their IPOs in two broad categories of ways – non-dilutive and dilutive. When a company wants to raise money without issuing new shares (*non-dilutive*), typically, companies can issue their treasury stock (*the company's stock in its treasury*) to the public. This increases the outstanding stock on the open market, but the total number of shares remains the same, bringing in capital for the company.

Companies can also raise money via a follow-on public offering (FPO). In this case, the number of outstanding shares and the total number of shares increase. It is a dilutive process as the denominator increases. Companies need to justify how the raised capital will increase the value for investors despite reducing their share in the company.

Most of the crypto protocols are not at a 'revenue-generating' stage. Therefore, issuing new tokens to raise more money will likely be met with much scepticism.

When a protocol diversifies its treasury, someone else is willing to take a piece of the treasury. Why would anyone do that? Because they think that owning this token will be profitable for them.

Though it seems obvious, the best way to help your diversification is to ensure the protocol has some revenue or the possibility of earning revenue.

Projects like Lido and Blur fit the bill. If Blur goes out to sell its treasury tokens, it will probably be able to do so on favourable terms because even though it no longer makes money, it will likely make money in the future. Lido already has a cash flow as it charges fees on rewards earned by stakers. This is why investors held on to the tokens they bought in Lido's treasury diversification token sale last year.

Part of the challenge with diversifying treasuries is that, too often, the tokens have not vested for founders or investors. So, at any point, doing complex financial strategies with assets that are not yet liquid becomes difficult. When they become transferable (through vesting), the markets rapidly price in any strategic sale, yield farming strategy or loan conducted by the time. It is simultaneously a bug and a feature.

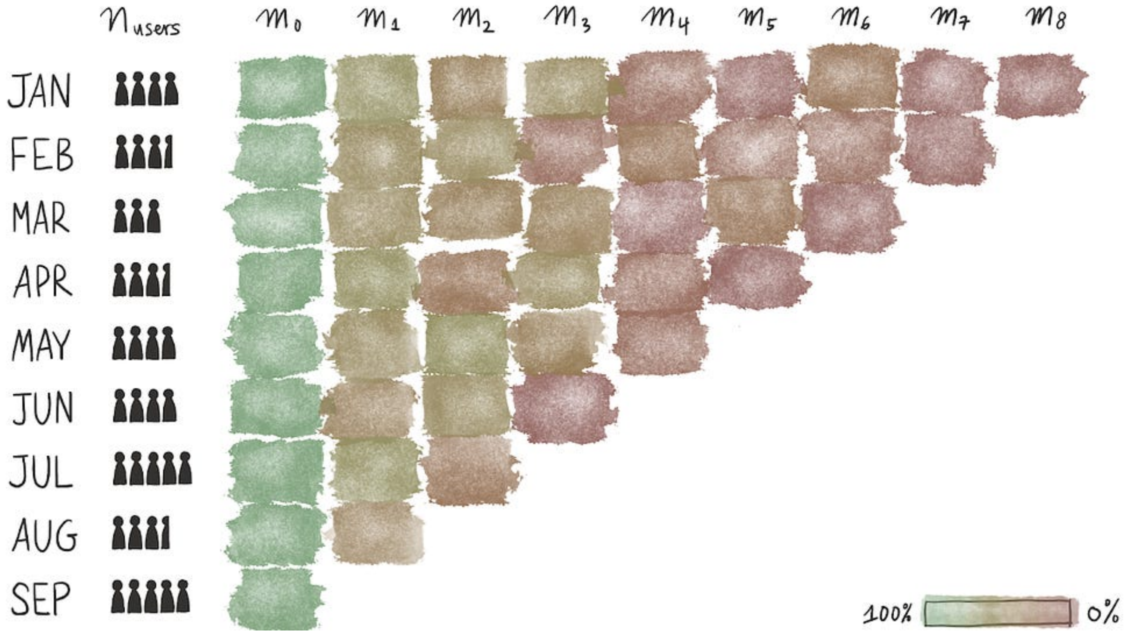
For token projects with liquid treasuries, the learning is quite simple. Diversification helps when valuations are in your favour. They may leave money on the table by selling the tokens at less-than-peak valuations, but they also extend their runway long enough to survive market cycles.

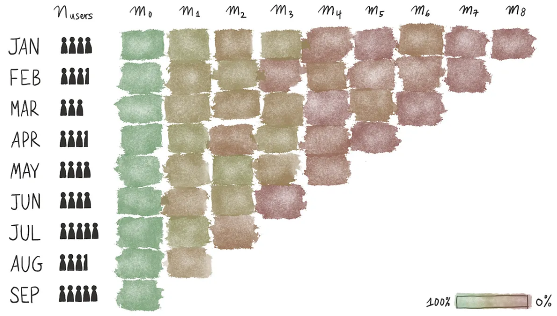
Currently, there is no magical solution for treasury diversification (*if you have one, please let us know*). But here’s what’s becoming evident. The market has just two kinds of projects at this point. The ones that can survive a steep draw-down and not be bothered due to existing runway. (*Uniswap fits that description well. Their treasury went from $20 billion to $1.5 billion.*) And the ones that may have to consider selling their tokens at steep discounts to ensure they can continue operating.

Joel John
decentralised.co

Retention in Web3

Sticky Users and Tricky Valuations





Hello!

We are back after a rather fun and productive week in Singapore. I wrote a breakdown of the general sentiment from the event on X (*formerly known as Twitter*).

A huge challenge with valuing protocols is understanding what counts as a user. Is a person interacting with a venture's Telegram channel a user? Does somebody liking a founder's tweets count as one? It is hard to say because we loosely use "*community*" in crypto. As tokens are a powerful instrument to align incentives, we often confuse a token holder with a user.

Late last week, TokenTerminal released a data set that studied the retention metrics of over 150 projects. I have been looking at the numbers to understand trends and patterns that may help readers of this blog. Today's issue breaks down a few benchmarks for retention when thinking about products in the digital asset industry.

In case you are wondering - this piece is not sponsored by them. We have been long-time subscribers of their product.

The Basics

Doing a cohort analysis of a product helps with two things. It explains the portion of users a product retains over time. In traditional applications, '*churn*' describes users who drop off from a product after having shown an initial interest in it. For this newsletter, churn would describe the readers who unsubscribe from it.

The longer you retain your initial user base, the more it adds to your active users. The product is growing as long as more new users come to a product than those who churn. (*In other words, as long as more users sign up for the newsletter than those who unsubscribe, we are in good shape.)*

Why does this matter in crypto?

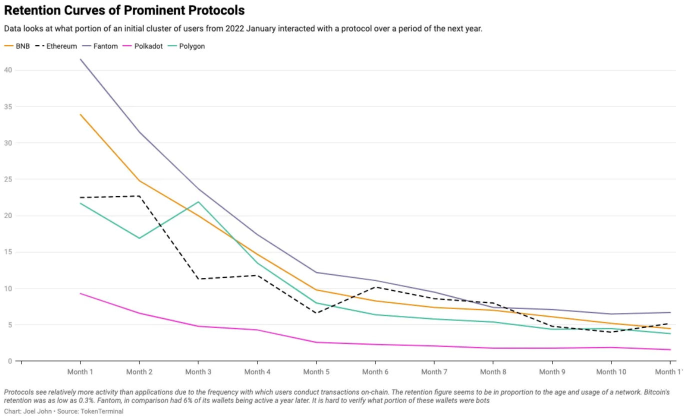
1. Firstly, user bases in crypto are not as sticky as their Web2 counterparts. The ease with which capital can move contributes to users switching between products often. Since blockchains enable faster rails for the movement of money and speculation is a core use-case, we see money flowing towards applications that offer lower fees or better yield.

2. Our estimates of the user base of a product are pretty flawed. There is an understanding that user bases grow due to large airdrops, but what portion is retained? Is an airdrop justified if a small portion of a large user base is retained? It could be. But there isn't a precise study of the numbers around them.

In this context, a *user* is an entity (*person or bot*) paying product fees. For protocols, this would be a transaction that generates fees. For dApps, a user interacts with its smart contracts and pays fees. This distinction matters, as most retention data often looks at token-holders. A user of Aave (*the lending product*) is different from a token holder of Aave (*the token*).

To come up with a baseline of what retention in the industry looks like, I began by observing how protocols retained users through 2022. In the sample set below, I considered the months starting from January 2022, when on-chain activity was at its (*relative)* peak.

The markets were still at relative highs, DeFi products were being rolled out frequently, and everybody was rushing to accumulate all the ugly JPEGs (*NFTs*). The numbers below show how a batch of active users in January 2022 behaved over time.



Retention Curves of Prominent Protocols

Data looks at what portion of an initial cluster of users from 2022 January interacted with a protocol over a period of the next year.

Protocols see relatively more activity than applications due to the frequency with which users conduct transactions on-chain. The retention figure seems to be in proportion to the age and usage of a network. Bitcoin's retention was as low as 0.3%. Fantom, in comparison had 6% of its wallets being active a year later. It is hard to verify what portion of these wallets were bots

Chart: Joel John • Source: TokenTerminal

The small dotted line represents Ethereum. In January 2022, the active number of wallets on the network was close to 2.7 million. A month later, 22% of Ethereum's initial user base remained active. A year later, it was closer to 5%. In comparison, Fantom had over 40% at the end of the first month. The variation is partly because users were likely hunting for airdrops on Fantom's DeFi ecosystem.

For a sense of scale, consider that of a cohort of close to 12 million active users in Jan 2022, only 35,000 wallets were still active on Bitcoin a year later. This may be due to power users in Bitcoin routinely switching out wallets. Ethereum’s 5% retention rate at the end of 11 months is a statistic we can benchmark other applications against.

Obvious caveat here. We will be comparing protocols against applications in this next section. Given how TokenTerminal has defined a user here, there will always be more users on protocols than on applications. You use the internet every day.

In comparison, the probability of you logging into your bank’s application is not as high. So, we are expected to see several applications with lower retention rates than Ethereum.

Comparing Applications

The first metric I wanted to check was Uniswap’s retention rates because it is one of the few applications most of us use frequently. It had over 143k users in January of 2022. The retention rate for the product was around 4.3%. When it was launched, the application had close to 7300 users, of which some 30% remained active a year later. The earliest users of an emergent product category tend to remain sticky long after it scales. Keep in mind these were also users who had received airdrops in proportion to their early usage of the product.

Saurabh pointed out that users may have no reason to stick around once they receive their incentives through tokens or low fees. To test this thesis, we checked the usage of two prominent aggregators - Metamask Swap and Paraswap. The former benefitted from the distribution of the most prominent wallets in DeFi. The latter had a live token.

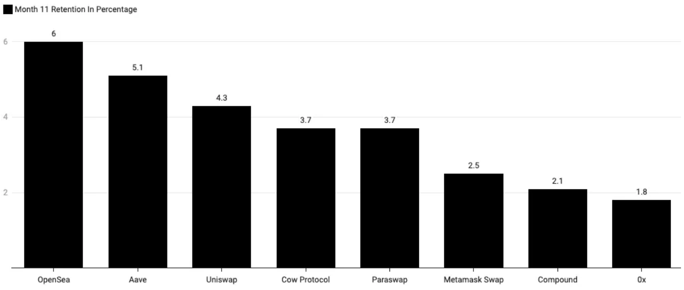
Metamask had over a million monthly active users at peak. But their retention was low at 2.5%. One reason could be that many users were making fake wallet transactions, hoping for an airdrop. Paraswap, in comparison, had a retention rate of 3.7% for a cohort from the same time. But their data had a larger story.

In October of 2021, the product saw 307k users. Of which only 0.3% were active a year later. This was partly because their airdrop was around the corner, and users were making multiple wallets to benefit from it. As the product stabilised, its user base began hovering around 50k users with a retention rate of 5%.

Only 1 in 300 users from their airdrop campaign in 2021 was active a year on.

Uniswap and Paraswap had wildly different outcomes from their airdrops. The former was launched during a bear market when most DeFi users were not using products in hopes of a token. Paraswap’s product launched at the peak of a DeFi bull run.

The difference in outcomes is a function of where the market was at the time of the product’s launch and not necessarily a function of the respective team’s product strategy.



OpenSea Retains 1 in 16 Users After a Year

Data observes what portion of a user cohort from January 2022 was still active after a 11-month timeframe on the same application

Chart: Joel John • Source: TokenTerminal

One more observation in this cohort of applications was that Aave retained twice as many users as Compound. Their expansion to new L2s and support for more tokens may have been the reason. Even when products have similar offerings and a token to go with them, the breadth of offerings determines whether a user sticks. It explains why exchanges (*like Binance*) race to add assets and product types that are trending and in demand. Retention is dependent on giving users options.

OpenSea was the outlier among the data set, seeing ~258k users in its cohort for January 2022. Roughly 6% of that user base was active a year ago. Part of the reason why consumer applications like OpenSea see incredibly high retention is that they offer users more than just "trading".

A web3 native user interacts with an NFT marketplace for one or the other reason quite often. Networks like Polygon and Solana, make it possible to use OpenSea while spending as little as $0.1

Quest products (*like Layer3 or Rabbithole*) use NFTs to incentivise and retain users. So naturally, these consumer-facing applications see higher retention over time than their financial application counterparts, as users have a reason to return and use these products even during periods of low volatility.

For instance, Lens had considerably higher retention over 11 months, albeit their initial userbases were relatively small. For a cohort of 17,000 users starting in May of 2022, 43% of Lens's users were active after a year. This may well be due to hopes of receiving an airdrop. But it appears those users are sticky and active for now.

Consumer-facing applications in Web3 appear to have lower churn than their DeFi counterparts. This is natural. When users don't see a possibility of making money from volatility, they do not rush to use trading-related applications. One way retention figures for DeFi applications could improve is by offering products that do not require speculation. Applications like BasedApp from Singapore are an instance of that.

Retaining Airdrop Hunters

The general criticism of airdrops is that they tend to attract only freeloaders. Airdrop recipients rarely return to the product within a matter of months. To understand how different user bases respond to airdrops, I compared the retention of two products around the same time (September 2022). One had what can be considered a naked airdrop. In these cases, users are given tokens that could be sold immediately.

The other had a points-based system and gave users tokens after almost eight months of use. The points-based system retained 10% of its users at the end of 11 months. In comparison, the one that gave tokens directly to users with no incentive for holding saw only 0.5% of its user base still active on the product at the end of 11 months.

In other words, an airdrop structured over months with additional rewards for users who hold on to their tokens could do more for a product than simply offering tokens.

Points Based Systems for Airdrops Retain Users Longer

Data below explores what portion of two different product's userbase was active over a period of 11 months. Naked airdrop product had a live token on month 1. The points based project launched a token around Month 7

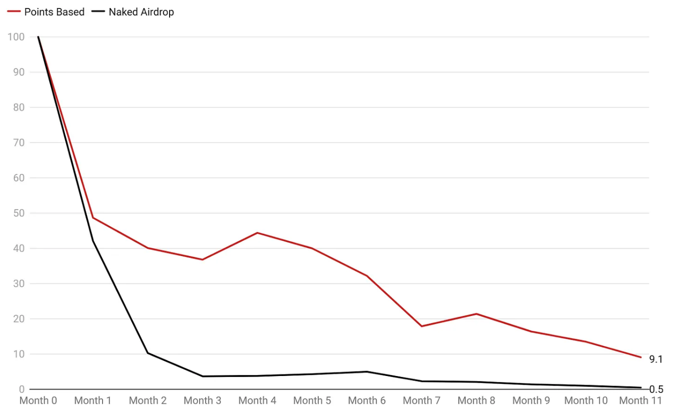


Chart: Joel John • Source: TokenTerminal

The comparison is not entirely fair. As with naked airdrop, users were given their tokens upfront and had no reason to stick around. The points-based system did not explicitly incentivise holding a token either. The only key difference was that users were incentivised to continue staying active on the product in the points-based system. A points-based system could turn out rather ugly if users sell tokens and then use the capital back on the product again to farm more airdrop tokens.

All of this is not hard science. My analysis has multiple flaws. For instance, users may swap out their wallets from time to time for the sake of privacy. Or a user may be active in a product's community but not be active on-chain. Even worse, users may be spinning up multiple wallets for specific product categories, making it seem like they have a large user base. This may be the case with consumer social applications without an airdrop (like Lens).

But what is interesting for me is that this data is now available. Instead of suggesting a product has 'X' thousand users, we can track what portion of those users stick around after a few months. The days of measuring the '*revenue generated per user*' (RPU) for crypto applications are not too far off.

Having more sensible benchmarks for valuing the quality of a user base would help capital allocators deploy money more efficiently. More importantly, it would help founders understand their product's actual value. These measures are crucial for a more rational market that builds towards sticky users that generate revenue.

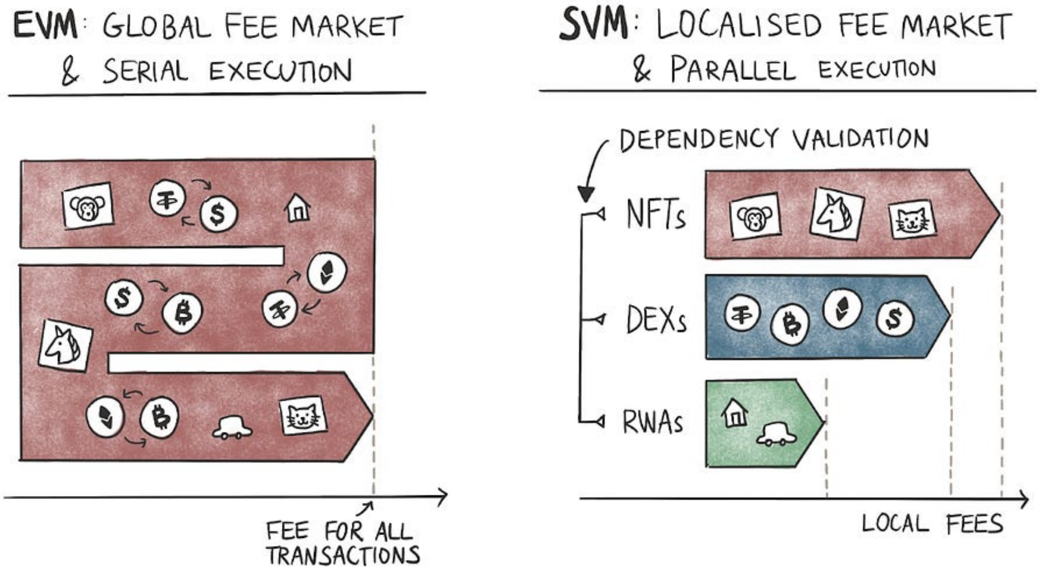
As with most things, these numbers are a spectrum. And their interpretations can vary depending on who's looking at them. I'd love to hear from you if you have alternative theories of churn or insights from Web2 products that have seen scale.

See you later in the week,
Joel

Saurabh
decentralised.co

The Modular Experiment

When chains play multiplayer games


EVM: GLOBAL FEE MARKET & SERIAL EXECUTION
FEE FOR ALL TRANSACTIONS
SVM: LOCALISED FEE MARKET & PARALLEL EXECUTION
DEPENDENCY VALIDATION
NFTs
DEXs
RWAs
LOCAL FEES

Hello,

Two interesting stories have developed in the market over the last few days. Nouns DAO was forked, and Eclipse announced the Solana Virtual Machine (SVM)–based Layer 2 that settles on Ethereum. This piece breaks down the latter and tries to understand why it matters.

Technologies seldom evolve linearly. Exponential improvements occur when elements from different lines of technology are combined. Take Google Maps, for example. It uses individual building blocks like satellite imagery, street view, aerial photography, indoor mapping, and location data to create a product used by billions. Similarly, combining computing, photography, and audio, the smartphone has become the most important device for adults worldwide.

Eclipse is interesting because it uses four pieces of infrastructure from different ecosystems to stitch together one scaling solution:

1. Ethereum for settlement
2. SVM for execution
3. Cosmos' Celestia for data availability

4. RISC Zero for ZK proof of fraud (*beyond the scope of this piece*)

Using Ethereum as the settlement layer is not new, so we won't waste time and space there. This post will highlight the key differences between the Ethereum Virtual Machine (EVM) and SVM in the following section. It is not surprising that someone would leverage Celesitia when trying to select the best from different ecosystems, although Ethereum is the go-to data availability layer today.

Why? After EIP 4844 or proto-danksharding, around 0.375 MB of blobspace (*per block*) will be allocated for all rollups. Whereas Celestia starts with 2 MB and scales to 8 MB in due course (*proposals range from 1 MB to 8 MB*). That is between 5 to 21 times larger than Ethereum.

Understanding EVM and SVM

Developers building new solutions don't choose EVM-based chains for their scalability. They choose them for their network effects. I know the term 'network effects' is often used loosely in crypto.

What I mean by network effects is borrowing two things from an established chain:

1. Development-related: Developer experience, retention and the ease with which dApps can be ported from one chain to another.
2. User experience-related: How easy it is for users to start using the new chain, in terms of existing wallets and other infra.

EVM chains sacrifice performance for network effects. But Eclipse intends to put itself in a unique position to avoid making this tradeoff by using SVM for execution. Solana has one of the highest developer bases (*which addresses the development aspect of network effects*). MetaMask recently unveiled Snaps, allowing users to interact with non-EVM chains (*this addresses the UX aspect of network effects*). But the question remains: Why SVM over EVM?

The aim is to highlight the high-level differences between the EVM and the SVM. For those like me who don't have a technical background, let's establish what VMs are. (*For those with technical chops, skip to the next paragraph*).

Think of a game like cricket or football (*soccer for Americans*). Whether you play the game in India, Australia, or America, the game's rules remain the same. Referees make sure that games are played by the rules. VMs are like referees; they can run on any computer in the world (*as long as they meet software and hardware requirements*), and they ensure that if the computer intends to participate in the network, it plays by the rules set forth by the network.

When a user submits a transaction, the VM is responsible for processing the transaction and changing the state of the chain *(updating the ledger*) based on the transaction. So, when we say that XYZ chain is EVM-compatible, it means it understands and plays by Ethereum's rules. A natural question is why this matters.

It does because applications already built on Ethereum can move to that chain without too much trouble when a chain is EVM compatible. Instead of having to develop Uniswap from scratch, with a few changes, the existing Uniswap codebase can be moved to the new chain.

Now, let's look at the differences between EVM and SVM. The two things that are significantly different between the two are:

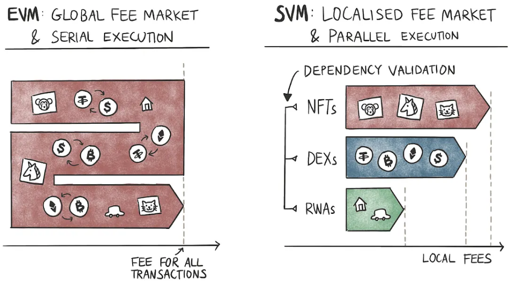
1. The ability of parallel processing (SVM) instead of serial execution (EVM)
2. Localised fee markets (SVM) instead of global fee markets (EVM)

Let's unpack. Firstly, understand that Solana uses the hardware of your computer's multiple cores. A core is the smallest processing unit of the processor that can perform tasks independently of the other cores. This is how modern computers multitask.

The EVM, conversely, does not rely on hardware to keep the validator hardware requirement low. To support parallel processing, the SVM requires transactions to tell the VM which accounts will be used to read and write (*i.e., which ledger areas will be affected due to the transaction*).

Based on this information, the SVM understands which transactions are not interdependent. That is, which does not affect the state of the same account. For example, if Sid has two transactions, one sending 1000 USDC to me and another swapping 1000 USDC for SOL, these two transactions depend on each other. Unless the SVM knows that his account has more than 2000 USDC, it cannot allow both transactions to execute simultaneously.

On the other hand, if Sid is sending 1000 USDC to me and using SOL to buy a MadLads NFT, then the two transactions do not affect a common account and can be processed parallelly.


EVM: GLOBAL FEE MARKET & SERIAL EXECUTION
FEE FOR ALL TRANSACTIONS
SVM: LOCALISED FEE MARKET & PARALLEL EXECUTION
DEPENDENCY VALIDATION
NFTs
DEXs
RWAs
LOCAL FEES

The EVM has global fee markets, whereas the SVM has localised fee markets. Think of it this way. We recently travelled to Singapore last week – in the EVM world, as the demand is high due to Token 2049 and the F1 race, hotels worldwide get expensive. But in the SVM-based world, prices for only the hotels in Singapore (*in areas around the event*) increase. Thankfully, geographical separation dictates pricing in the physical world during such hot events.

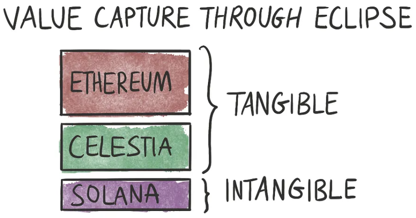
The pricing declines the farther you go from the venue, ceteris paribus. But in the blockchain world, how do we ensure that when the demand for one dApp goes up, the cost of using other dApps doesn't increase? We break down the demand to identify hotspots and limit the blockspace allocated to those hotspots.

So, just like the EVM has a block limit of how much gas can be spent per block, the SVM has a hard cap on compute units (*or the CU tracks the resources and time required to process a transaction*). To avoid fee spikes due to single events, besides the overall CU limit, the SVM also limits CUs consumed where a single account is involved to ~25% of the total limit.

So, for example, if there's a highly anticipated NFT drop and users are constantly hitting the mint button, these transactions can only occupy 25% of the block, and the priority fees users are willing to pay to mint the NFT does not affect a user intending to stake SOL using Jito.

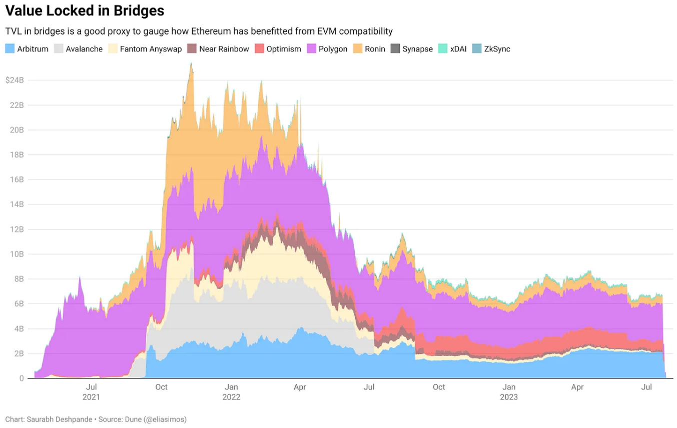
Interestingly, Visa recently announced support for using Solana as the settlement layer. The reasoning was similar to Eclipse's parallel processing and local fee markets.

Who Captures Value?



Like many layer 2s, Eclipse uses ETH for gas. So, the value capture for ETH, the asset is clear – as the usage of Eclipse increases, the demand for ETH grows. Celestia is also a clear winner since it gets paid for its blockspace used for data availability. What is unclear is how Solana benefits from this. A good way to answer this question is by examining how Ethereum benefits from EVM.

Although there is no direct way to quantify how the EVM network effect has impacted Ethereum, using the bridge TVL is a decent approximation. At some point, this capital has touched the Ethereum blockchain and likely paid fees denominated in ETH. Something similar can be anticipated as the SVM chains' base grows larger. The following chart shows the total value locked across different bridges.


Value Locked in Bridges

TVL in bridges is a good proxy to gauge how Ethereum has benefitted from EVM compatibility

Chart: Saurabh Deshpande • Source: Dune (@eliasimos)

Solana's TVL was over $11 billion during the FTX collapse. Since FTX and Alameda were the major (and some of the largest) participants in Solana's ecosystems, their demise created a vacuum in the Solana ecosystem. As the overall value fled from the entire crypto ecosystem, thanks to the bear market, higher interest rates, etc., the

Solana ecosystem was among those experiencing the greatest impact, with TVL down by over 90%. Repairing this damage would certainly be easier if Solana didn't have to do it alone. Something like Eclipse or Neon EVM, which allows leveraging the existing EVM ecosystem, is helpful to bring capital onto Solana again.

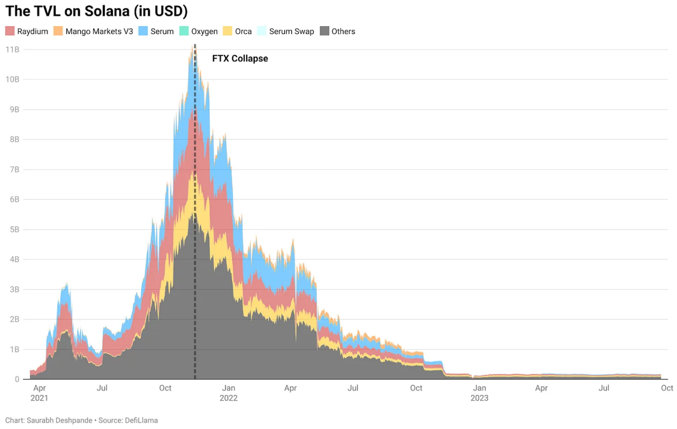
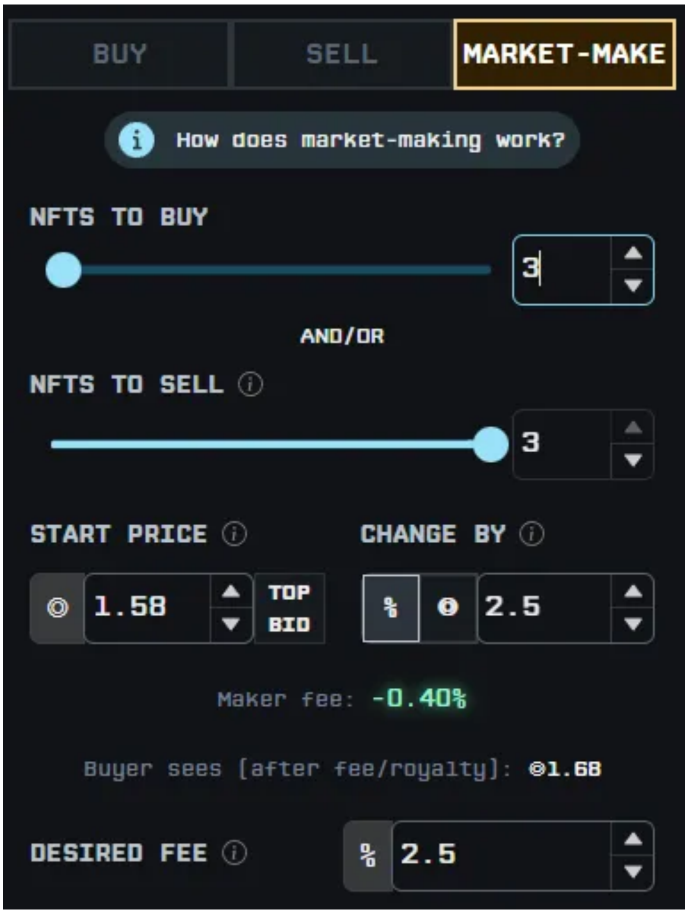

The TVL on Solana (in USD)

Chart: Saurabh Deshpande • Source: DefiLlama

It is also critical to think about how Eclipse itself accrues value. Not using its token for gas is good for UX but bad for its value accrual. At this point, its value accrual will likely be similar to its peers like Arbitrum and Optimism.

What Does Eclipse Enable?

Certain things have not been possible on Ethereum so far. Consider Tensor's market-making functions for NFT marketplaces for instance. Market-making orders allow users to keep buying and selling NFTs as the price changes by X%. You cannot do this on Blur or OpenSea. Interestingly, such order types can be used in DEXs built on Eclipse.



NFTS TO BUY 3

NFTS TO SELL 3

START PRICE ◎ 1.58

CHANGE BY % ◎ 2.5

Maker fee: -0.40%

Buyer sees [after fee/royalty]: ◎1.68

DESIRED FEE % 2.5

Source – Tensor.trade

DYDX used StarkWare's proprietary scaling engine, StarkEx, to launch an order book-based decentralised trading platform. Another example is Pyth Network. With Solana's scale and Ethereum's settlement, it would be possible to disseminate information on a desired scale. Such applications will be possible with the likes of Eclipse. But most of this is incremental innovation; it is not zero to one since these applications already exist.

One may argue that we have not seen large-scale applications like social media on-chain because the infrastructure was absent. We recently saw with Friend.tech that fees on Base started to jump as the application use grew. And at some point, if FT grows to be large, it will probably be unusable for many. But there is a larger question: Will those apps be built if the infrastructure exists? It isn't easy to answer.

We don't know whether the lack of infrastructure or some other motivation is why the absence of consumer-level products in crypto. Besides, if Eclipse manages to pull off a consumer-grade application, how long will it take for Arbitrum or Optimism to copy its features? The likes of Monad are also working on parallel processing and EVM compatibility.

Whatever it is, building applications on Eclipse is new and will take time. It won't be a copypasta like most of the EVM chains. Zk rollups claim they will bring orders of magnitude of scalability over their optimistic counterparts. Here and now has always mattered more than better and later in crypto. The only strong reason favouring something like Eclipse against all rollups is that it does not fragment liquidity. Even though rollups are composable, liquidity on Optimism is not on Arbitrum. So if something else brings significant scale to Ethereum, having the most liquidity there makes more sense.

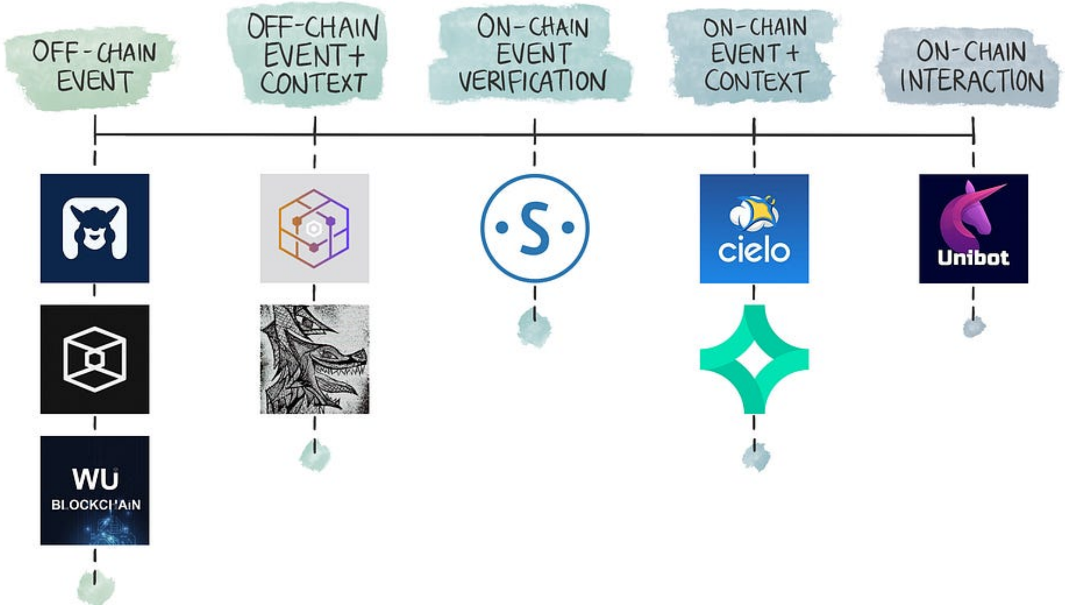
We don't know what lies in the future for applications built on Eclipse, but combining the best parts of different ecosystems is undoubtedly a fresh idea. Instead of pitting degens against each other, it tries to increase the size of the pie for everyone for a change.

Off to a vacation,
Saurabh

Joel John
decentralised.co

Using Telegram for Distribution

Build where the users are.



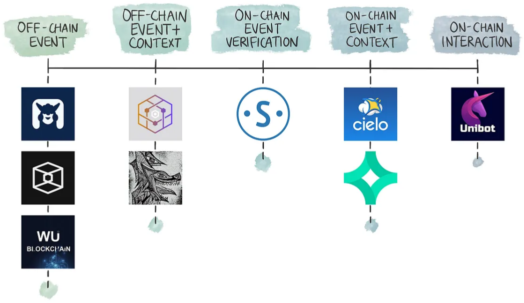
Hey there,

I spent the morning today looking at the ecosystem of tokens built around Telegram trading bots. Cumulatively, they account for $147 million in market capitalisation. The largest amongst them, Unibot, has a capitalisation of $54 million as I write this. The tokens linked with these products have undergone boom and bust cycles.

Unibot, the largest among them, is down 75% since mid-August. A more recent entrant named BANANA is still undergoing price discovery. This piece will not bore you with the specifics of the activity on these Telegram-based apps. I highly recommend referring to this Dune dashboard to track activity.

Instead, I will summarise what they do and why market participants run towards them today. We'll then explore what kind of applications could be built on them.

The Present



On one end of the spectrum, you have content feeds. On the other, you have user-generated transactions that are powered through on-chain data streams.

Telegram's current bot landscape (*in relation to crypto*) is a spectrum. On one end, you have the usual bots that bring in news about Web3 events from platforms like Twitter (*now X*) or RSS feeds. They are not crypto-native products but use Telegram for distribution. Wu Blockchain, DeFiLLama and The Block, each have Telegram news channels that relay updates.

Tools that use on-chain events and give context alongside them are usually handled by smaller startups or creators For instance, Jobstash has a feed of new jobs listed by Web3 native platforms. Officer CIA has a feed with a curated subsection of security related articles.

The next layer of products are wrappers on AI tools like ChatGPT. This mix of products allows users to train a bot (*on an external website*) and introduce it to a Telegram community or use Telegram as an interface to communicate with a bot. PaalAI, for instance, allows you to ask questions like 'W*hat is today's* top-performing *coin?*'

Similarly, NoiseGPT and ChainGPT allow users to produce deepfakes using Telegram as an interface. While elements of crypto can be pretty active in these products, many of them are not 'Telegram applications' but interfaces. (*I'll explain the difference between the two shortly.*)

Tools like Collab.Land and Guild.xyz are verification tools for token- or NFT-gating communities on Telegram. Here's how they function: a user goes to these products, links their wallet, and signs a message (*from their wallet*) to prove they own the wallet. The product then checks if the wallet being linked has the necessary number of tokens or NFTs to permit access for a user. In such a product, the "*on-chain"* function is verifying asset-ownership.

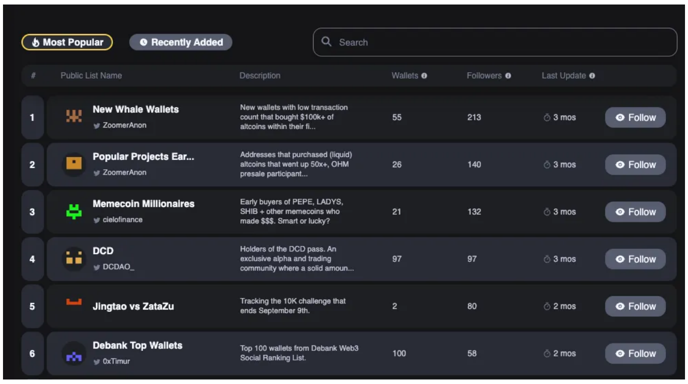
The next group of apps on the spectrum have been around since at least 2019. Santiment, for instance, tracks on-chain events and notifies users. Similarly, Nansen tracks the movement of assets from funds and informs users through the app. While Santiment uses raw data (*X wallet moved Y tokens to exchanges*), Nansen gives additional context (*the owner's name of wallet X*) when notifying users.

These are not Telegram applications either. They notify users of the movement of assets through Telegram as a medium.

The tokens that have been all the rage on Twitter in the past few months are full-fledged applications. The difference between an application and an interface (*in my definition*) is that an application can function fully on Telegram and leave an on-chain imprint without requiring external wrappers (*like ChatGPT*).

Both Unibot and Banana Gun permit users to set up new wallets, track the launch of new meme tokens and allocate a portion of their wallet balances towards buying these assets without signing transactions each time.

These applications are unique because they create verifiable imprints on-chain. Products like LootBot take this one step further by offering a SaaS-like option for users to farm airdrops on-chain. I could not test the product personally, but according to their Telegram handle, they have enabled some $4.5 million worth of transactions on-chain for users looking to game airdrops.



#	Public List Name	Description	Wallets	Followers	Last Update	
1	New Whale Wallets ZoomerAnon	New wallets with low transaction count that bought $100k+ of altcoins within their fi...	55	213	3 mos	Follow
2	Popular Projects Ear... ZoomerAnon	Addresses that purchased (liquid) altcoins that went up 50x+, OHM presale participant...	26	140	3 mos	Follow
3	Memecoin Millionaires cielofinance	Early buyers of PEPE, LADYS, SHIB + other memecoins who made $$$. Smart or lucky?	21	132	3 mos	Follow
4	DCD DCDAO_	Holders of the DCD pass. An exclusive alpha and trading community where a solid amoun...	97	97	3 mos	Follow
5	Jingtao vs ZataZu	Tracking the 10K challenge that ends September 9th.	2	80	2 mos	Follow
6	Debank Top Wallets 0xTimur	Top 100 wallets from Debank Web3 Social Ranking List.	100	58	2 mos	Follow

Cielo's curation of wallet subsets that could be tracked via Telegram.

One of the businesses that have been making waves is being built by a community member at Decentralised.co. Cielo has Telegram native wallet trackers that can track thematic wallet lists or tokens. The interface (*on the website*) allows users to select a pre-curated list of wallets such as the top 50 earners on FriendTech or wallets that have made millions trading meme-coins in the past.

Users get a notification anytime a user from these wallet subsets makes a transaction. Part of what makes Cielo interesting for me is the number of chains and early-stage types they are quick to support.

For instance, quite recently, they were one of the earliest to allow users to track FriendTech key's trades, historical P/L and user behavior through Telegram. There is a complex engine parsing data in the background. But the medium of interaction (*chats on Telegram*) fuels the product's growth.

According to the founder (*Matt Aaron)* , using Telegram as a medium for distribution has unlocked niches they previously didn't know about. For instance, a subset of their users have been using Cielo to track NFT loans on Blur. (*Presumably to buy liquidated NFTs at a discount*). These users receive a notification via Telegram each time a loan is made or NFTs get close to liquidation.

The team behind Cielo began noticing how multiple Telegram apps can be combined to create easier user flows. For instance, forwarding a message from Cielo to Maestro (*a trading bot*) automatically imports the smart contract addresses of the tokens involved. This allows users to place orders at a fraction of the time it usually takes to do the same on Metamask and Uniswap.

Matt told me (*while simultaneously tending to his 1-year-old*) that timing becomes of the essence when it comes to Telegram-based applications. Being able to roll out event-specific updates within meaningful periods helps with growth. For context, during the BALD token hype, Cielo sent some 2.5 million notifications on Base (*the chain)* alone in 48 hours. They track over 20 different blockchains. That is scale, facilitated by Telegram. They have over 44,000 users as of writing this.

All of these are interesting, but what is the opportunity set? To explore that, one should understand what Telegram enables today.

The Assets

At its crux, Telegram is a distribution medium. If you treat it like a social network (*like Facebook in 2008*), it will become easier to understand why applications have been growing virally. What it enables is surpassing the app store's restrictions to create chat-based interfaces that function off a wallet generated in the product.

Naturally, security trade-offs exist, as the user often does not entirely control the wallet. But for smaller transactions that do not require a cold storage wallet, Telegram enables interacting with a product without switching applications.

In this regard, it is similar to WeChat, except that its APIs and policies are sufficiently open to allow developers to create applications on top of it. Telegram has a wallet feature natively enabled on it. It allows users to hold assets like Bitcoin and several stablecoins.

The purpose of this integration is the possible monetisation of large chats like LobsterDAO. For instance, the community on Telegram has 23,000 active members. It is reasonable to think 10% of that community would convert to paying $20 a month, which should be $40k+ in revenue for the person running it.

As a platform, Telegram is inching closer towards integrating crypto natively into its product. This allows developers to target crypto-native users directly in the chat application. But what if a person does not already hold crypto? Telegram has a solution for that, too.

They just rolled out P2P markets and credit card purchases of crypto in the product. So, an application can launch and collect payments (*in stablecoins*) from credit card users worldwide in a few clicks. You could not historically do this on other social networks like Twitter (*now X*), WeChat or Meta if you were a crypto application.

We have a distribution medium, on-ramps and a native wallet. We also have multiple communities with tens of thousands of people. This is similar to when Zynga relied on Facebook for its growth in the late 2000s.

I often wonder if Zynga grew due to Facebook or if Facebook grew due to Zynga. One way to think of it is like this: As Facebook expanded beyond the English-speaking world, many users in emerging markets did not have experience with the mannerisms that came with interacting online.

Games like Farmville made the internet more usable at a time when much of the emerging world was slowly coming online. You no longer had to write a 500-word punchy status update for Facebook to be relevant to you as a user. Even the user who wanted to play Farmville (*like me in 8th grade*) had something to do for our daily dose of dopamine. Why does this matter?

Chat-based applications on Telegram could make crypto more relatable over the next few years. Not everybody wants to be the owner of a limited-edition monkey face. The market where participants put tokens in smart contracts and get a yield on it saturates rapidly in a bear market.

We expand the user base only when social applications that allow retail participants to engage without layers of complexity involved. For instance, AR seeped into the public psyche with PokemonGO in 2016. More recently, PlayStation's VR headset and Apple's Vision Pro have brought virtual reality to the masses. Technologies scale when they become accessible to individuals. Telegram, as an interface, could catalyse this for crypto.

But why do I say so? We must look at what Telegram could enable and the mix of applications that could be built on it to understand.

The Possibilities

Long before FriendTech became all the rage on Twitter (*now X*), the Collab.Land bot allowed token and NFT holders to enter gated chats and communicate. At its core, a person's FriendTech key has the same value proposition as an NFT (*for entering a permitted chat*). It gives access to a creator (*or brand*) with whom you can chat. The difference is that FriendTech released a stand-alone app with keys on a bonded curve. Where

NFTs had flat prices, bonded curves surged substantially in value.

FriendTech also tapped into Twitter users' social graphs from Twitter to enable discovery and used a points-based system to incentivise users to buy keys. But all of this could have also been replicated on Telegram. Nothing stops Telegram (*or a third-party developer*) from releasing a FriendTech clone that allows all of the user's contacts to discover, speculate and interact through the chat application.

The core barrier here is that people already talk to one another on Telegram without holding keys. If I suddenly decide I will only respond to Siddharth if he owns a key of mine on Telegram, this would lead to some unpleasant interactions. Especially given that Siddharth (*like everyone else on the chat app*) is habituated. to getting responses from me on Telegram without holding a speculatory key.

The opportunity subset is for large community owners looking to monetise. Telegram has multiple communities with tens of thousands of users, yet no monetisation model. If these communities decided to monetise with a key-like system (*as on FriendTech*), creators could monetise at a massive scale with minimal friction. If a royalty model like the one on FriendTech is enabled on Telegram, it could create sufficient revenue to enable a DAO, which could be responsible for curating and scaling a community.

FriendTech on Telegram in itself is not massively interesting. What excites me is the interface between a mobile application and on-chain activity becoming far simpler. For instance, a bot could generate an NFT by simply uploading a photo. Similarly, a user's location data could be captured from their Telegram interface. Imagine going to a concert, opening Telegram, uploading your location to prove your presence and getting a NFT minted directly to your wallet.

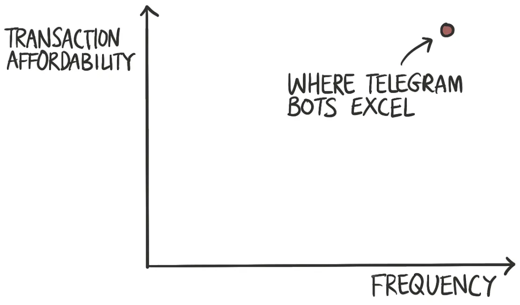
Each of these, on their own, is not groundbreaking technology. But they make the possibility of blurring lines between on-chain and on-device far easier.

For instance, an NFT could be issued whenever someone verifies they visited a cafe. Then, the number of NFTs a person owns could unlock discounts or be traded for dollar amounts in a free market built directly on Telegram. Much like how eBay "normalised" auctions on the internet, Telegram as an interface could normalise conducting on-chain actions without ever going through MetaMask.

One way this could play out is by tracking a third-party user's on-chain transactions (like a fund's) and copy-trading the same through a chat-based interface. In such a model, a bot would track on-chain events, notify a user, and ask if they'd like to replicate the same.

A user could then change variables (*the amount, gas costs, etc.*) and initiate the transaction through the bot. (*The example I mentioned above involving Cielo and Maestro bot does this function across two apps. A smart developer could bring this into a single interface and chart a small fee*).

Alternatively, products could emerge to track a user's on-chain behaviours and offer alternatives. For instance, if I had a loan on Aave and could get a lower interest rate through Compound, a Telegram-based bot could notify me of the arbitrage and initiate a transaction on my behalf. In all of these cases, Telegram is used as an interface.



At its core, Telegram applications that scale would follow a simple pattern: enabling high-frequency transactions at an extremely low cost. The immediate use case for such an application is (ironically) gambling. Telegram allows users to roll the dice or run a slot machine through chat-based interfaces today.

What truly interests me amongst these applications is the (*probability of*) training chatbots in the learning of an entire community. I keep going back to them as an example, but consider that LobsterDAO has 4 years of DeFi-power users talking to one another in their community.

It has a knowledge base of 23,000 users sharing links, stories, fears and hopes in the chat. What if an AI could summarise the knowledge of the community? In such a model, the ownership of a token or NFT could (*theoretically*) gate access to an AI that could tap into the knowledge base of a community's expertise to provide user insights.

This may seem far-fetched, but we have already seen requests to create such a bot within our community at Decentralised.co. We did not accept it because open communities do not (*generally*) own the conversations generated by their users. Collecting all the members' consent would be a daunting task in itself. But it is quite possible, that in the future, we see AI Bots trained on a community's interactions. These bots could then be paywalled and used by members who don't want to search the community's chat logs.

As an interface, Telegram facilitates an opportunity subset (*of on-ramps and interface*) among a concentrated user base that understands crypto well. The applications built on it could go viral due to the relative ease of discovery and on-boarding. Developers building social apps, on-chain games and AI-based products stand to benefit the most from building on Telegram as a distribution mechanism. Does Telegram have incentives to kill such applications if they scale? Absolutely.

History offers some precedence here. In 2010, Zynga was under threat of being shut down by Facebook if they chose not to use Facebook's Credit system. It was a payment method on Facebook that took 30% of the revenue as Apple does in its stores today. So, anytime somebody made a virtual purchase on Farmville, Facebook would make a cut of that transaction. As of 2012, nearly 19% of Facebook's revenue came from such in-game purchases.

The partnership was to end in 2015 when Zynga could break out and launch its games as a stand-alone firm on its own website without paying Facebook any royalty. Did that transition eventually happen? Not really. By 2016, the building Zynga operated out of was worth more than the firm itself. This fall from grace shows what happens when a distribution medium gets cut off.

Platforms like the App Store can command their platform fees because of the distribution they enable. Today, Telegram does not charge a royalty fee. But if they see large troves of users interacting with crypto-native products, it is not far-fetched to believe they have an incentive to enable fees. Does that make it a bad place to build apps?

Quite frankly, no. You have a product where crypto-native users spend most of their time with an integrated wallet. Building products with Telegram as a distribution mechanism is one way to keep the CAC at an absolute low when resources are scarce. Build, where the users are.

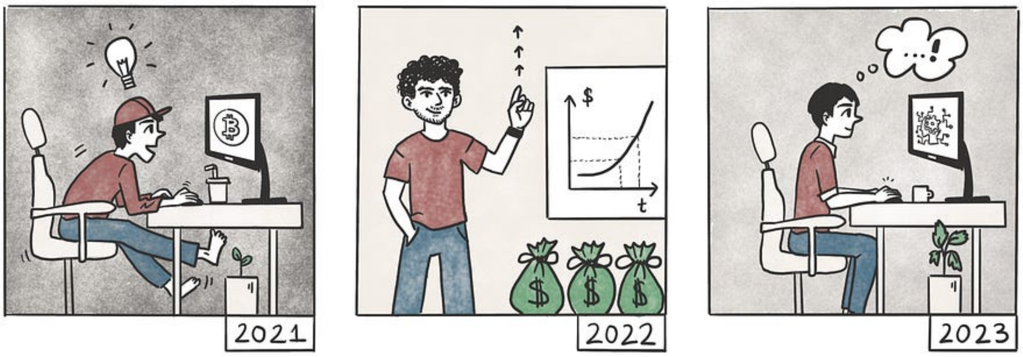
Thinking of shawarma,
Joel John

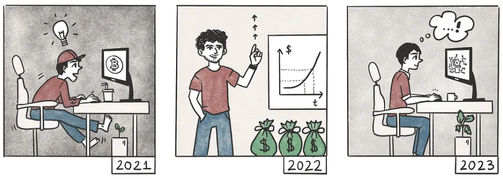
Disclosure: I am a moderator on LobsterDAO's Telegram community.

Joel John
decentralised.co

The Funding Environment

We are all just indexed bets.





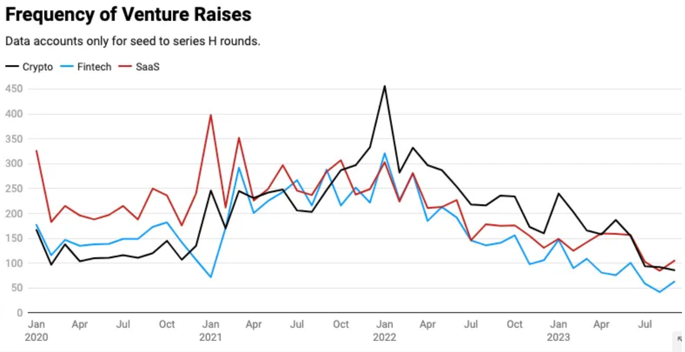
Sam, Sam!!? Sam!

Hey there,

I started writing this post to update founders about the funding environment in Web3. But then I realised it is not rocket science to conclude the environment is bad. Most founders raising in this market have been stuck for months. Venture capital funds are in the middle of raising for themselves. And consumer apathy is at the worst levels we have seen for quite a few quarters.

It is like suggesting one's limb is broken. We all know the limb is broken. Because it hurts. You don't need me to explain the extent to which it is broken, as we all feel the pinch in the market. So I decided to zoom out and understand what is happening in venture-land. In today's piece, we will study whether everybody's limbs are hurting instead of explaining how and why our limbs are broken. Maybe we could find ways to fix our limbs in the process. (*No more limb references, I promise*)

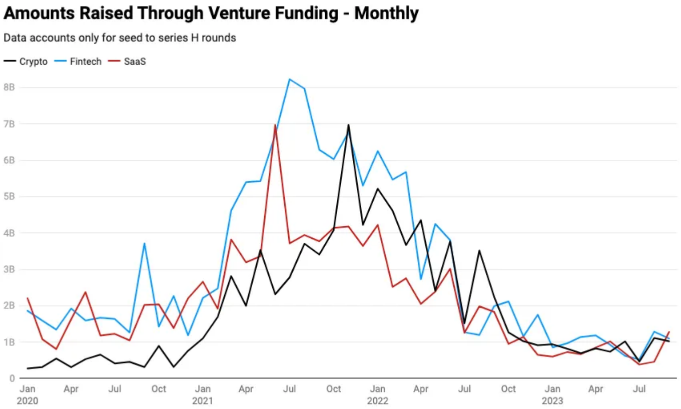
Before we begin, consider the chart below comparing the frequency of investments into SaaS, fintech and crypto-related ventures since 2020. I had to bring data from around ±25,000 investment events over the last few years to make the chart below. (*It seems like it was worth the effort*).



When we read crypto fundraising news, the general assumption is that capital inflows have reduced drastically over the year. And that is indeed true. But to suggest that without context on what is happening is ingenuine. I took fintech and SaaS verticals as comparables here due to their relative maturity compared to blockchains as a technology. But as you can see, there's a draw-down applicable across the industry, much like an increase in appetite for risk a while back.

What does this look like in terms of the amounts raised? I cleaned up the data to account for raises only from seed to Series H, as otherwise, I'd have to include IPO data. From the perspective of venture capital investment comparables, it did not make much sense to add it here.

Interestingly, SaaS and crypto as sectors peaked around the exact amounts of dollar values going towards them each month (around $7 billion). I presume SaaS and fintech rallied in late 2020 partly because of COVID-19. People spent all their time in front of screens, often hitting the buy button hard for intellectual stimuli as the world shuts down that year.



Notice how crypto trails a few months later? That is because pension funds, venture capitalists and hedge funds recognised they were deep in the money on their portfolios during the pandemic. Across asset types, the risk appetite increased substantially as portfolios turned green. It helped that interest rates were at their lowest in a while, and consumers had excess money through stimulus or savings from lockdowns. A mix of these factors made crypto rally.

More mature verticals would often have fewer investments (in frequency) but higher amounts of money going to them. But the point is, we are all indexed bets on some pension fund's appetite for risk. It is not that crypto fell off the rails. It is that the economy itself had a rude awakening, and capital allocators stopped dreaming about what they could do with NFTs and on-chain ponzinomics. (*I'll explain what this means for founders in a bit.)*

The Relevance of CAC

So where do we go from here? All great ecosystems have, at their core, a mix of good talent and patient capital. As capital in the market dries up, so does latent talent willing to continue building in the industry. Given the opportunity cost of not working on something hot (like AI), most firms will have to pay more to employees if they hope to retain them. Either in cash or equity.

It helps to have a perspective on investor motivations at this point. For some context, let's look at what raised money last week.

- IYK raised $16.8M
- SupraOracles announced a raise of $24M
- Rated raised $12.8M

The conservative, somewhat apprehensive tap of liquidity at large venture funds is slowly opening up for select ventures. What do these ventures do? IYK provides infrastructure to verify the authenticity of physical goods using NFC chips. The next time you purchase an Adidas sneaker, you could receive an on-chain reward for it by just tapping it with your phone.

SupraOracles and Rated are both infrastructure plays oriented towards data. These are firms where you can show some form of meaningful traction. Investors lean towards what is novel, new and viral in markets like the one we are in now. Why is that the case?

There's the obvious reason that most investors likely have sufficient exposure to primitives, like NFTs and DeFi, that are deep underwater, and they may not want to add to that exposure. On the other hand, novel applications see rising demand from users seeking something new. This translates to traction and, by extension, the lowest CAC a firm could have.

That last bit – CAC – determines everything at this stage in the market. During past bull markets, firms could allocate tokens to acquiring customers. Their treasuries were ever-expanding. If you were a venture that raised equity and planned a token launch, you may rarely have had to worry about where users would find you. Greed (*or market incentives*) did the marketing for you. Investors knew they would have liquidity from their investments through tokens. Founders knew they would have an ever-expanding treasury once the token became liquid.

During bear markets, consumers and investors rarely have a reason to care for products where a token is not on the horizon. Your effort to make them care could be distilled and measured as your CAC. One way to measure a protocol or dApp's appetite for consumer acquisition is through tracking their token treasuries. In a bull market, managers at these protocols are comfortable taking risky bets as the value of their treasuries rise substantially. Concerns of protocol revenues do not exist as the token becomes the product. In a bear market, this effect works in reverse.

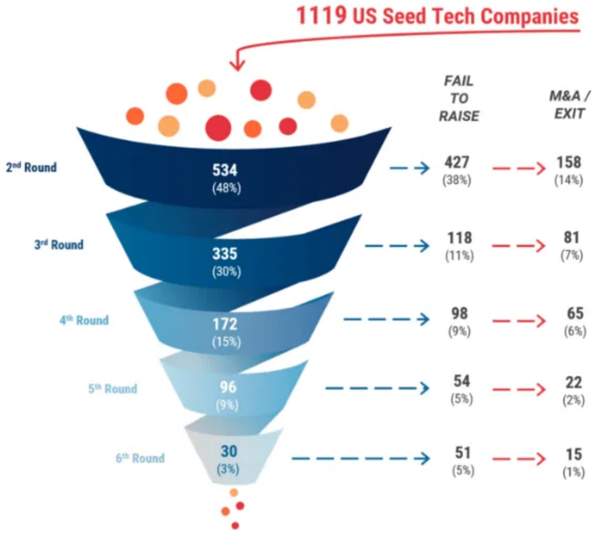
The ability (*and appetite*) to use tokens for consumer acquisition rapidly dwindles as firms recognise that selling tokens at low prices could hurt an already illiquid market for their tokens. The lack of focus on CAC or revenue is not a problem endemic to crypto ventures alone. AirBNB, Uber and WeWork are each instance of ventures that were not highly profitable for prolonged periods. The difference is that with crypto, the incentives are liquid and volatile if a token exists. It has a direct impact on CAC.

Layer3 is a quest platform with one of crypto's largest top-of-the-funnels. They help brands discover users through running quests. According to Brandon's latest tweets, they have 800k users. If I presumed the market in crypto for active users is ~2.5 times that, we are all hunting for a portion of 2 million users. That would be the total market size in the industry today if I had to think of "*how many people are active*?"

There is the caveat that these are the users doing transactions. The market for users whose mindshare is close to crypto is likely 10x [at 20 million], and for users who have used crypto at some point, it is expected to be 100x [at 200 million]

Any founder who has ever raised a penny is chasing a portion of this small user base. For B2B leads, the number is even smaller. In a bear market, as firms reduce spending, the CAC would reduce in tandem. But that is often not the case as the total number of active users also reduces faster when token prices reduce. This is where viral products (*like FriendTech*) stand out as conservative bets, even when you know activity can drop off if the airdrop is released. They have the lowest amounts in CAC.

Projects that raised money in 2021 (*or earlier*) with products at their core must find mechanisms to keep CACs low while maintaining morale as their runways dwindle. This is why we wrote about Telegram and churn over the past few weeks. CACs determine a firm's ability to survive at this market stage. Founders with traction are increasingly becoming the ones who set the price for their rounds. The ones without are often stuck in loops of adding feature sets in hopes that a superior product will attract users.



Source: CB Insights

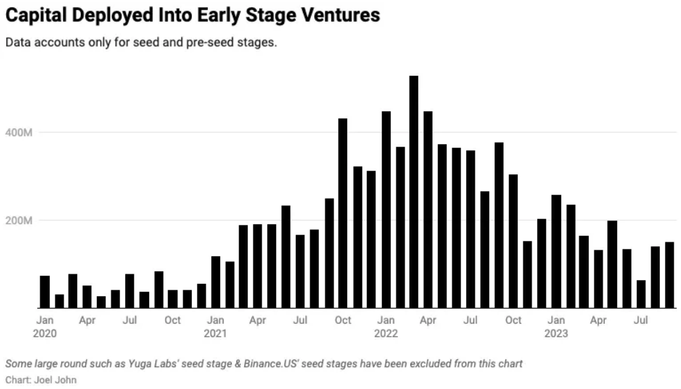
These are ugly truths. In a WAGMI world, we all would have made it, and every venture would result in an IPO. But we live in efficient markets where you have a 1% chance of becoming a unicorn. That metric was calculated in 2018. The number is likely even lower now considering how much more the competition has increased due to excess venture dollars going into startups.

This is a scary statistic that the venture world ignores, but as markets dwindle, it is worth repeating this to most founders. This is why I have been observing two things. A handful of founders have begun shutting their ventures or considering M&As. Some other founders have been job hunting while updating their investors about running out of runway.

In a bull market, you can spend time thinking of TAM.
In a bear market, your best bet for survival is to obsess about CAC.

There Is Hopium

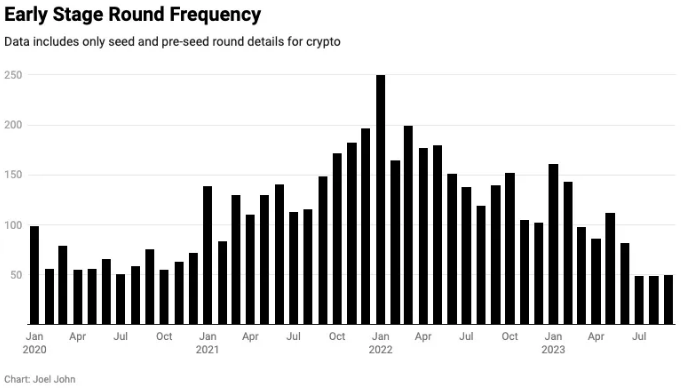
Now that I have sufficiently scared you, I can get to the bit with hopium. The data below shows the frequency and amounts that have gone into seed stages. Naturally, there's a drastic decline from the highs of January 2022. But we are more or less in a return to rationality mode rather than an absolute collapse. Most of the data around the frequency and amounts raised looks at the draw-down from the peak.


Capital Deployed Into Early Stage Ventures

Data accounts only for seed and pre-seed stages.

Some large round such as Yuga Labs' seed stage & Binance.US' seed stages have been excluded from this chart

Chart: Joel John


Early Stage Round Frequency

Data includes only seed and pre-seed round details for crypto

Chart: Joel John

But if you study the chart, it becomes apparent that we are still at 2020 activity levels for early-stage ventures. There is a decline compared to early 2022, but investor interest in Web3 has not vanished.

I mentioned CAC because in the early stages, a venture is an arbitrage on CAC. Your "valuation" is determined by the number of users you can acquire per unit dollar. We use a different mental heuristic for this in the market and ask, "*Do you have traction?*".

Naturally, not all products will have traction early on. Sometimes, founders have to raise capital to build a product in the first place. In such environments, signal value is shown through a handful of methods.

- Firstly, if it is a profoundly technical product, you're better off explaining it properly and in-depth than building a broken MVP that puts off potential backers. Blog-posts, podcasts or hanging out in large communities and signalling expertise is a lever for grabbing investor attention.

- Secondly, if it is a consumer application, you do have the possibility of bootstrapping a community of a few hundred people around the concept itself. Early communities don't scale quickly, so much of the building process would involve cold DMs and strong rejections.

- Thirdly, most startups are built on secrets. Founders who can show they have a wedge in an underexplored market can likely raise funds simply due to understanding the market. When firms are similar, founders struggle to stand out.

The more I study firms struggling with raising funds, the more I see recurring patterns of founders holing up in a cave and staying there. Building is an incredibly long, hard and tiresome task. Speaking to users and investors is draining. You run out of energy at some point. But early-stage ventures are pivot machines. Founders can pivot (*or conduct gradual iterations*) several times to find PMF. But if you don’t speak to your customers, you don’t get to do any iterations.

But the shorter your runway gets, the more pertinent it becomes that you can form meaningful signals if you aim to raise. Signal value (*of expertise or community*) can be the bridge that helps a startup hire or retain employees, when people know that a startup may have to shut shop in 12 months if they cannot raise funds.

What Next?

I pulled up that chart comparing crypto to fintech and SaaS because I wanted to show the indexed nature of the venture ecosystem. If you build a startup reliant on venture dollars, you are inadvertently part of an indexed bet run predominantly by pension funds and family offices. That is an uncomfortable truth most VCs would not admit, but it is what it is. Flows towards venture investments will return if and when an ETF is approved or when Bitcoin rallies. (*Boom, I said the obvious.*)

1. Most ventures that raised funds in the last few years do not have a follow-on. Until a clear PMF exists, firms struggle to do a Series B or C. This means the trickle-down effect of appetite for earlier-stage investing has rapidly declined among VCs. An MVP shows your ability to build. Paying customers demonstrates your ability to sell. Firms with both have an edge.

2. The markets are crowded with too many variations of the same thing. Maybe some of the brightest minds I know should spend their time on options and perpetuals. I do not have an issue with these instruments, but they seem to discount how small the market is. The caveat is that a new generation of L2s can form customer experiences on-chain that are better than their centralised counterparts. One of the ventures I saw recently doing that is Synquote.

3. With most DeFi and NFT primitives, the models being built are from 2021. And as Blur showed last year, it only takes one new entrant to change the model (around royalties) entirely. Businesses that can change the model in novel ways will generate value for themselves and their shareholders.

   This is easier said than done. The most innovation we have seen within DeFi has come from CowSwap, but their share of the AMM market is woefully low. In some sectors, even novelty does not translate to valuations rising.

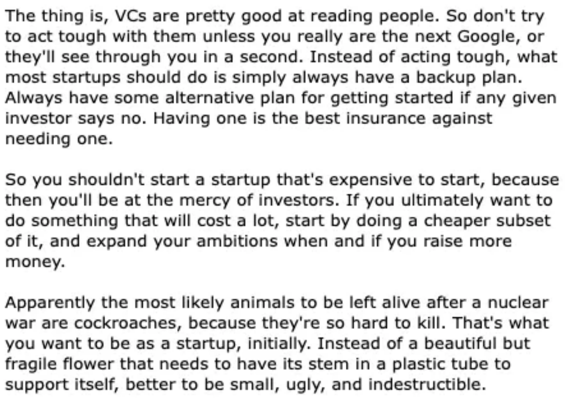
4. There is a mix of ventures that have not tokenised since 2021. They are battling the constant decay of consumer and investor attention. There will be friction internally as to when they should tokenise.

   What is better? A firm with a token doing badly, or a firm that is dead because it ran out of runway? That's the decision many founders will soon have to make. And rather sadly for them, their investors may not respond when they want to have that conversation or think it through.

5. Revenue multiples. Bull market revenue multiples were at 50–100x. So the unicorns we saw in 2022 likely have Series A levels of traction to show. Until they can build cash flow to a point where their valuations are 20–30x of multiples, many of them will struggle to do a follow-on. The good news is they have ample runway and could likely fix the problem with M&A.

This newsletter took a day extra to hit your inbox because I planned a trip with some (*friends who are*) developers to a desert near Dubai. Apart from Rust, Vim and several other things that flew above my head, they were discussing how during a bull market, the only thing they did was blow up their money on Luna or a random DeFi farm. Some saw a 75% pay cut compared to what they were paid last year. But they mentioned something that grabbed my attention. That building in a bear market is more meaningful because it is just fun to work on hard problems without the distractions of token prices.

The primitives we build in a bear market - be they intents, token-bound accounts or autonomous worlds, are intellectually stimulating for the brightest minds in our industry. People will continue to iterate and pitch them to users, regardless of whether venture dollars are flowing into the sector. As Paul Graham once famously explained in an essay, founders can be cockroaches.



The thing is, VCs are pretty good at reading people. So don't try to act tough with them unless you really are the next Google, or they'll see through you in a second. Instead of acting tough, what most startups should do is simply always have a backup plan. Always have some alternative plan for getting started if any given investor says no. Having one is the best insurance against needing one.

So you shouldn't start a startup that's expensive to start, because then you'll be at the mercy of investors. If you ultimately want to do something that will cost a lot, start by doing a cheaper subset of it, and expand your ambitions when and if you raise more money.

Apparently the most likely animals to be left alive after a nuclear war are cockroaches, because they're so hard to kill. That's what you want to be as a startup, initially. Instead of a beautiful but fragile flower that needs to have its stem in a plastic tube to support itself, better to be small, ugly, and indestructible.

From Paul Graham's blog.

The opportunity subset for VCs in this market is in finding the cockroaches. Because it takes a certain kind of conviction (*or delusion?*) to believe survival is possible after everything we've been through in the last two years. For founders, the opportunity is finding talent that finds meaning in continuing in the industry, even when mentioning blockchain at the dining table is awkward. Those still with crypto or Web3 in their dating profiles are likely golden hires around this market phase.

Talent that seeks opportunities based on what is trending is now building wrappers on AI and raising money for it. Even venture funds within crypto are rebranding themselves to capitalise on that opportunity. This means that there is very little competition within the industry when it comes to newer primitives that are coming of age. That lack of competition is the bull case for continuing to build even when crypto looks like a non-consensus bet.

Day and night. Bull and bear. Hot and cold. The world works in contrasts that are needed to balance one another. There is no way I can meaningfully argue it is a great time to build in Web3 without accepting the challenges that come with it. But as they often say, most things worth having in life come hard.

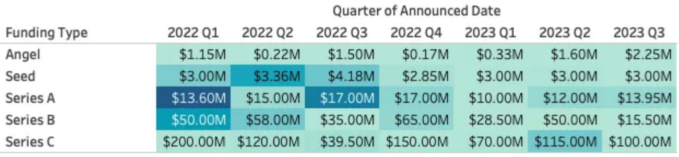
Off to eat dessert at Al Fanar,
Joel

Data Dump

The easy thing to do while writing this article would have been to dump the data around the frequency of raises and average amounts raised and call it a day. But I figured it would be intellectually lazy and useless to somebody building a startup in this space.

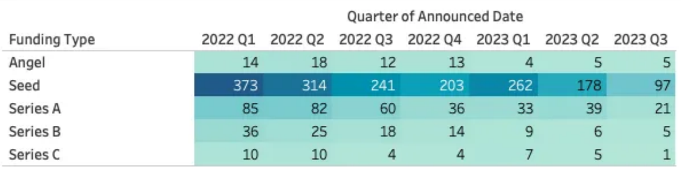
That said, doing a piece on venture funding would be unfair without the average raise amounts shared. So here's the data for those that need it. E-mail me if you need a more detailed breakdown if you are a founder.

Median Amounts Raised



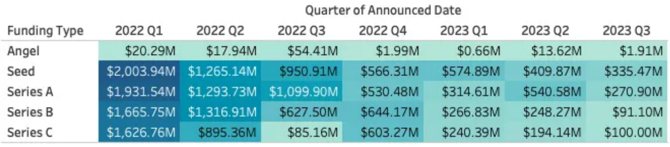
	Quarter of Announced Date						
Funding Type	2022 Q1	2022 Q2	2022 Q3	2022 Q4	2023 Q1	2023 Q2	2023 Q3
Angel	$1.15M	$0.22M	$1.50M	$0.17M	$0.33M	$1.60M	$2.25M
Seed	$3.00M	$3.36M	$4.18M	$2.85M	$3.00M	$3.00M	$3.00M
Series A	$13.60M	$15.00M	$17.00M	$17.00M	$10.00M	$12.00M	$13.95M
Series B	$50.00M	$58.00M	$35.00M	$65.00M	$28.50M	$50.00M	$15.50M
Series C	$200.00M	$120.00M	$39.50M	$150.00M	$70.00M	$115.00M	$100.00M

Round Frequencies



	Quarter of Announced Date						
Funding Type	2022 Q1	2022 Q2	2022 Q3	2022 Q4	2023 Q1	2023 Q2	2023 Q3
Angel	14	18	12	13	4	5	5
Seed	373	314	241	203	262	178	97
Series A	85	82	60	36	33	39	21
Series B	36	25	18	14	9	6	5
Series C	10	10	4	4	7	5	1

Total Amounts Raised



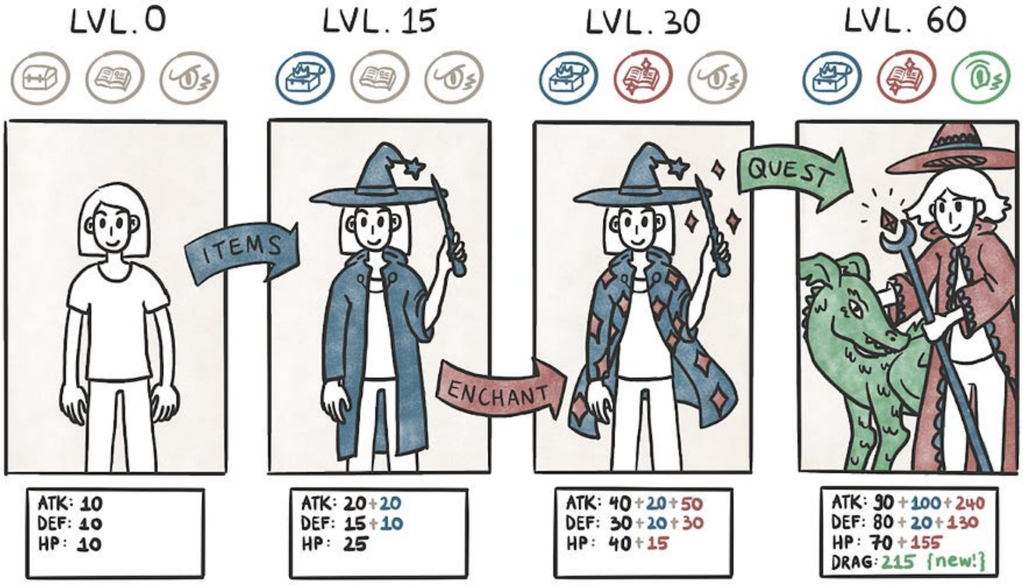
	Quarter of Announced Date						
Funding Type	2022 Q1	2022 Q2	2022 Q3	2022 Q4	2023 Q1	2023 Q2	2023 Q3
Angel	$20.29M	$17.94M	$54.41M	$1.99M	$0.66M	$13.62M	$1.91M
Seed	$2,003.94M	$1,265.14M	$950.91M	$566.31M	$574.89M	$409.87M	$335.47M
Series A	$1,931.54M	$1,293.73M	$1,099.90M	$530.48M	$314.61M	$540.58M	$270.90M
Series B	$1,665.75M	$1,316.91M	$627.50M	$644.17M	$266.83M	$248.27M	$91.10M
Series C	$1,626.76M	$895.36M	$85.16M	$603.27M	$240.39M	$194.14M	$100.00M

We'll update this data on VCData.site in a v2 due for launch soon.

Joel John
decentralised.co

Token Bound Accounts

When NFTs become wallets



Hello!

We had the pleasure of meeting Gabby from YGG during our trip to Singapore a few weeks back. One of the many things we discussed was the evolution of Tokenbound Accounts (TBA) and why they are interesting. I did not allude much to it in our piece on identity because I figured it deserved a stand-alone piece of its own, much like we did with soulbound tokens (SBT).

Some basics in case you are hearing about it for the first time: ERC-6551 is a token standard that allows an NFT to act as a wallet. This means an NFT can own assets like stablecoins, open positions in DeFi products or other NFTs. An ERC-721 asset (NFT) is a stand-alone, isolated asset that cannot necessarily be upgraded or hold assets like a wallet does.

Note: I will use TBA for token-bound accounts and SBT for soulbound tokens for ease of reading throughout this piece. We need to find words that are easier to say..

When you buy an NFT, you buy a single asset, which may give you access to third-party services such as an event or product perks. Bored Ape Yacht Club (BAYC) NFT owners had access to a restricted

Discord chat and rights to mint a handful of tokens released by Yuga Labs.

An SBT is a non-transferable asset sent to an individual's wallet, attesting to their credentials. Below, I provide a quick recap on both contexts before we dive into TBAs.

In the context of identity, these assets are currently used in two ways.

- NFTs are used to attest ownership by simply checking wallet balances. Using NFTs to prove identity would mean a person was either wealthy enough to acquire it (*with capital*) or skilled enough to mint it early on when the NFT was released.
- An SBT, on the other hand, cannot usually be acquired by capital alone. By nature, they are nontransferable1, so users have to put in effort and time to acquire them.

But what if you had a mechanism to combine SBTs, simple assets (*like stablecoins*) and NFTs into a single standard and gave it the ability to transact? That is ERC-6551. In this model, you convert an NFT into a wallet. A user's action can add layers of assets to the NFT. These layers can be metadata that is hosted on centralised servers or assets that are held on-chain. A user with the TBA can move single assets (*like stablecoins*) or transfer the TBA along with all of the assets held by it.

The term “metadata” above could be a bit confusing without context. Generally, an NFT itself does not hold any data of its own. It points to a third-party hosting service. What I mean by “*hosted on centralised servers*” is that an NFT’s capabilities could evolve based on what a developer wishes to be within a game. A server could check which assets are held in a wallet and customise the user’s experience accordingly.

For instance, it could unlock a certain level or enable access to a region in a metaverse. The experience itself (*within a game*) could evolve from time to time so long as a user owns a particular NFT. In such a model, the NFT is less about ownership of a static asset and more about the unique experiences it enables within a game.

Wait, what? Why does this matter? BAYC offers some clues.

In-Game Loyalty

In March of 2022, the price of BAYC NFTs dropped over 30% in the days that followed the airdrop for APE tokens. That is because a simple mechanism exists to price the value of an NFT like BAYC before an airdrop.

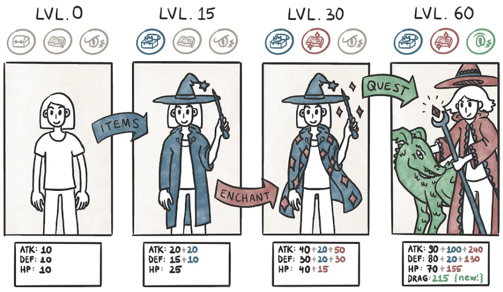
Think of it like this: The price at which a BAYC used to trade in the days before the token’s release was the implied value of an anticipated airdrop combined with the latent value a market gives for the underlying NFT itself.

Once the airdrop was claimable, markets rapidly repriced to reflect what the NFT was worth on its own. This behaviour is partly because NFTs have historically been static assets with limited use cases. Users are not incentivised to hold on to them if they don’t see an economic case behind them.

ERC-6551s offer a mechanism to drive value and loyalty to the NFTs a user owns. Currently, most NFTs are priced based on their rarity. When limited-edition collections are dropped as NFTs, users sift through them to find scarce attributes and price them higher. ERC-6551s allow users to build NFTs with differentiations that go beyond what an artist created when releasing an NFT.

To understand this analogy, we need to go into gaming. Remember when Play to Earn was all the rage and Axie Infinity's NFTs were trending? Part of the challenge was that very little differentiated one NFT from another. There were attributes to the NFTs that made some rarer than others, and you could combine them for specific advantages within a game.

But for the vast majority, a user's progress within a game had no impact on the NFTs they already owned. ERC-6551s and SBTs allow an alternative.



Each upgrade would be an NFT that is acquirable by the user, but a game would not recognise it unless the user has sufficient XP.

The image above tracks the evolution of a game character throughout a game.

- We presume all users start with a tokenbound account. The NFT is a wallet.
- Users spend time in the game to receive XP (*experience points*) that are given out as SBTs. A user cannot trade the XP itself. There is no liquid market for XP in the above hypothetical example. If users had to transfer their XP, they would have to transfer the NFT. The equivalent of this on the web today is selling your RuneScape account.
- On reaching certain levels of XP, a user can mint additional NFTs that go into the user's wallet. A game could interpret these NFTs as upgrades to the character. For instance, owning a wand or a hat could give an edge in terms of the attack or defence capabilities of the character.
- Remember that these NFTs representing upgrades could be transferred to an external wallet by the TBA. Unless a user has the necessary XP, it could be discounted by the game's server when upgrading the character.
- As the game evolves and players receive more XP, they could unlock additional NFTs representing upgrades. These NFTs could be minted directly from the game (for free) or traded in a free market.

What does this solve for? Structurally, it reduces the amount of speculation with a game's assets. Since the reward is XP and cannot be transferred or traded as quickly as tokens, it should create a base of loyal users more interested in the game than the asset rewards they receive.

Additionally, it keeps users retained longer, as selling their assets is the only way to cash in. There's the alternative of selling stand-alone NFTs that translate to upgrades within the game. But the market for those assets would be small as only users with sufficient XP would trade their assets with one another to combine NFTs and unlock specific abilities within a game. (*The reason is a game would not recognise a TBA that does not have the necessary XP simply owning NFT upgrades. The XP would be a mandatory check on the server side*).

TBAs are interesting for guilds because they allow stand-alone characters (or gamers) to form decentralised autonomous organisations (DAOs). In the current guild model, there are very few mechanisms to vet the actual capabilities of a gamer. If TBAs were used, members forming a guild (or a DAO) to coordinate and play games together could vet the XP, past transactions and assets owned by a gamer. It makes coordination between gamers easier when coordinating and taking on hard levels within a game or competing.

I found this image on Pinterest, but Red Dead Redemption 2 is easily one of the most beautiful games.

In games like RDR2, every upgrade to a character's dressing is purchased with cold hard dollars. The belt, gun, hat, necklace and earrings could each be an SBT in a hypothetical world where Rockstar games embrace NFTs. A player could use the same TBA in GTA 5 to have a completely different set of perks, given that the server-side interpretation of a TBA could vary from game to game.

Why would Rockstar Games - the publishing studio behind both games, do this? Part of the reasoning is that it allows third-party developers to create value for their userbase by creating unique experiences for players with a TBA from Red Dead Redemption. A simpler reasoning is that such a model where a gamer can receive perks on multiple games for purchases in any one could create more brand loyalty and user retention.

The challenge is that such a model would not work in games where everybody starts from scratch. Would it be great to build a Red Dead Redemption or GTA 5 character with such upgrades? Definitely. But a model like the one above would fall apart in a game like DOTA where every player starts at the same level.

It is important to note that token-bound accounts are a new design philosophy. If we are to look at it from the lens of 2019 NFT trades, they may not make much sense. In the past, NFTs were optimised to switch hands frequently because it meant the developer received royalties on each trade. In 2022, Blur disrupted that model entirely by reducing royalties paid by traders.

All these sound interesting on paper, but one has reasons to wonder: Where has such a standard seen any traction?

Co-creating Influencers

Naturally, not everyone plays games or needs to upgrade an in-game character constantly. There is a larger game we all engage in: social networks. They are uniquely suited for such a token standard, as we tend to 'own' our social profiles for long periods. Web3 native social products like Mirror or Lens allow users to collect posts by their favourite creators.

They also allow multiple clients to surface content to users. Lens's latest update (v2) allows the creation of token-bound accounts in their protocol. It means that an NFT (*like a crypto-kitty or a BAYC character)* could have its own Lens account, which – in turn – owns its list of assets. Why is this relevant at all?

I believe it gives a new infrastructure for how we think of intellectual property rights and asset ownership in Web3.

For instance, a creator who has built a brand around a non-existent, AI-based character could sell it to a third party willing to pay for it. This happens in the Web2 world already. Pages with millions of followers on Twitter or Instagram are sold quite often. The only difference is that with a token-bound account, this process would be as simple as transferring an NFT to a third party. The recipient would, in turn, have access to the follower base and assets owned by the NFT in question.

Image Source: The Cut

Does it seem far-fetched? Yes. There aren’t enough users on Web3 native social networks to warrant such a use case. But technological trends elsewhere point to the need for this. Consider the case of Lil Miquela. In 2018, she was one of the Time’s most influential people online. She has collaborated with brands like Calvin Klein and Prada. That's justified when you consider she has over 2.7 million followers on Instagram. The kicker is she's AI-generated.

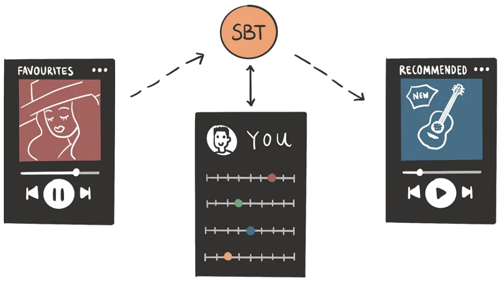
As generative AI makes it easier for creators to develop virtual influencers, the desire to collaborate, co-own and trade digital brands will become increasingly relevant. Web3 native primitives allow multiple individuals to own the art or data sets that go into training such a model. They could even stream the payments (from brands or audience bases) to multiple contributing wallets.

It may seem impossible because brands take years to build and form trust. The Lindy effect of a brand (*like Gucci*) may not be replicated soon. On the flip side, though, a community-owned influencer that engages in co-creation may be able to scale an audience base far faster than traditional influencers or brands. As the tooling around DAOs, AI, and on-chain IP come together, we will see brands disrupted like influencers disrupted traditional media.

How does any of this relate to the token standard I just mentioned? If Miquela were an NFT and had SBTs for each brand interaction or on-chain proof of her collaborations, the NFT would be worth way more than the generic ones we have in the market today. If we are to see thousands of virtual influencers online in the future, wouldn't it make sense that they should be tradable? That would be far-fetched but within possibilities, considering we already trade human keys on FriendTech.

A future where multiple creators fine-tune a virtual influencer to scale and sell to a third-party buyer seems dystopian. Perhaps we should step back and look at what is possible here and now. A different approach to scaling ERC-6551 as a standard would be to look at a user's Web2 data to identify patterns that may make the person valuable.

For instance, although multiple products (*like Audius*) exist to help connect emerging artists with an audience base, none have meaningfully scaled. This is because the on-chain social graphs of Web3 native music product users are not built by observing a user's ability to identify and endorse an emerging artist.



One way to solve this problem would be to scan a user's Spotify playlist history and issue SBTs in proportion to how early they identified with an emerging artist. Weightage could be given based on how early and frequently users listened to an emergent artist who has since blown up. Asset Money seems to be taking a similar approach with their product launch.

If NFTs that are token-bound accounts are issued to such users, and reward badges (*like the ones you receive on Audible or Apple Watch*) are given as SBTs, you could – in theory – create a curated, on-chain graph of music enthusiasts who are incredibly adept at embracing and endorsing new musicians.

A major artist like Taylor Swift may have no reason to use such a product. But somebody up and coming could better target the most active listeners using tools like this. Naturally, artists are not data scientists developing SBTs from your Spotify data—a third-party platform would have to do this for them.

Platforms like these would tap into Web2 native data to create on-chain graphs of user bases with specific characteristics. These users could then be incentivised with discounted tickets, exclusive merch and so on to help build an audience base. One of my favourite instances of an artist building loyalty is J. Cole doing concerts for $1 during the early days of his career.

Such products open up highly profitable niches that do not exist on the internet today.

Long-Term Games

ERC-6551 is a standard and an early stage one at that. Developers and creators decide what's built on top of it. The standard is intriguing because it focuses on building reputation and credentials instead of acquiring and selling an asset. Using it for games, music, or creator brands would be more about gradually developing value around its NFT core than public speculation.

A simple way to consider this is through the lens of venture capital. When a venture capitalist (VC) invests in a firm, he has, in essence, a SBT of sorts. An investor's track record measures conviction and skill in detecting early-stage ventures. The VC's access to better deal flow at lower valuations increases depending on how many successful bets they make. This process is how reputation is built in the off-chain world. It takes time, but reputation aids in compounding value in the long run and unlocks new levels much like in a game.

At its core, ERC-6551 enables this long-term reputation-building for digital assets. The digital asset can be a media brand, a user's behavioural patterns or an in-game character. Gradually adding characteristics to an asset can be crucial in building consumer retention and loyalty in Web3. Is it as rewarding as seeing a token pump? Absolutely not. But not everybody wants to flip assets and deal with volatility. TBAs are one of many tools that empower users who want to hold an asset and build a reputation around it.

One of the things I did not explore sufficiently in this piece is the role the token standard would have in finance. For instance, bills of lading are increasingly going digital, and there is a strong case for using ERC 6551 there. But we'll dig into that another time.

Joel John
decentralised.co

Revisiting The Metaverse

Feels Meh, could get worse.

Hello!

Today's article is part one of a two-part series examining the past and the future of Metaverse projects. In this issue, I explain why metaverse projects in Web3 have struggled to retain value. In the next, we will be looking at the approaches an emerging game from South-East Asia is taking to solve for user retention and monetisation.

In 2021, mentions of metaverse in corporate earnings calls reached a new height, with 170 firms mentioning it over 500 times at its peak. A report released a year later by Gartner showed that 64% of enterprise clients believed that the metaverse was mostly hype.

Over the past few days, I have pondered whether the metaverse is dead. Part of the reason is that I have been reading Neil Postman's Technopoly. The book argues that the tools we use shape human culture as much as we shape the tools we use.

In 1440, when Gutenberg released the printing press, he could not have known that his invention would fuel the Protestant Reformation in 1517. The monks who developed the clock might not have realised they were laying the foundations for a time-based capitalist economy.

The metaverse – like the radio, internet, television and books – is a medium. It is a tool that is so new that we barely know the impact it can have on human culture. We had a hype cycle in the recent past because human attention was funnelled into new digital mediums during the pandemic. Games, social networks and even Zoom were in the limelight during the pandemic days. And as a portion of that attention went towards on-chain assets, we presumed it would continue to be a hot sector.

Before I tread any further, I should lay some basic definitions of the terms I will use throughout this piece. The metaverse, in the context of Web3 native apps, has historically referred to platforms like the Sandbox or Decentraland. These virtual worlds allow you to own assets represented as NFTs and build immersive worlds around them. The core use case of a blockchain in these platforms was to track asset ownership or enable payments.

But the metaverse is nothing new. If seen as a graphical interface through which humans interact, metaverses have existed since the early 2000s. For instance, MIT wrote about how Second Life enabled a parallel economy for gamers as early as 2007.

Much of the discourse around the metaverse today is dominated by two firms:

1. Meta, which owns some 47% of the market share for VR devices and
2. Roblox, a platform that made $680 million in revenue last year alone.

For this piece, we will first dive into the state of the metaverse in Web3 and then zoom out and look at what has happened with the narrative over the past few years.

What Went Wrong

In 2022, metaverse real estate was so hot that JP Morgan had purchased a plot for itself on Decentraland. As of this writing, there are ~30 unique land traders for the three leading metaverses daily. Volume has dwindled from $17 million to a mere $50,000 today. For a sense of scale, in 2022, a single person paid nine times that amount for a single plot of land next to Snoop Dogg's plot.

Today, the combined market capitalisation of real estate assets is a little over $250 million. Even when measured in ETH terms, lands on Decentraland and the Sandbox have dropped 90%. According to data from BinaryBuddha on Dune, the average volume of metaverse assets is down over 98%.

Some things must be made clear before we continue. Given that price and volume are a function of the market's state, I don't want my mentioning the metrics to be an interpretation of what I think of the team—my commentary on what went wrong critiques the sector itself, not the individuals or teams behind it.

With that out of the way, what went wrong? Much like DeFi, NFTs (*and metaverse assets*) were heavily dependent on the flow of liquidity from existing assets like Bitcoin to risk-on assets like NFTs. Given that the supply of NFTs (*like Bored Apes*) or land was low, assets with capped supplies saw a substantial uptick in their value for short periods. But they could not retain that value for long because nobody built sticky experiences within these virtual worlds.

One parallel to draw here is that of a city. Properties in a city are expensive if one of two things happen:

1. Local legislation makes owning property there profitable for tax, immigration or commerce-related reasons.

2. There is a massive influx of individuals to the city, so an increasing number of people want to avail a scarce asset.

The digital land boom went bust because we never optimised for masses coming to our virtual worlds. Between setting up wallets, acquiring tokens and trying not to get hacked or scammed, individuals spending time on metaverse properties dwindled rapidly. The few remaining were traders looking to make a quick buck by being early to the asset class. As the price (and interest) of the properties they held in these virtual worlds declined, so did the speculators' interest in them.

The broader 'miss' we had in the last three years is the obsession with the idea that Web3 is all about ownership. In our pursuit of decentralising governance (*whatever that was*) and ownership, we forgot that gamers strive for something simple: fun.

We never had a large enough userbase of Web3 native gamers, which was challenging due to the friction associated with crypto native rails. Would you rather download a game on XBOX and get into gaming or go through the hassle of sending your passport to a strange exchange in your country?

These challenges are now solved through on-ramps like TransFi that aggregate regional payment methods. In such a model, a gamer could come through any regional payrails and access instant payouts from a game using crypto. Naturally, such a model would only take off in emerging markets where payment rails are not strong enough, and the premium for buying crypto is as high as 10% compared to local currency.

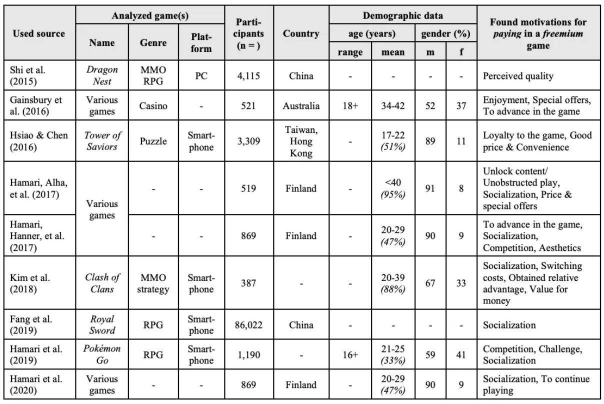
Motives and Retention

Fun could not be prioritised because these virtual world products had short development cycles and relatively small budgets. For context, the large AAA titles we consider to be '*successes*' needed between $80 to $250 million to launch. The metaverse as we know it was built by firms that had raised seed rounds in 2019 and were building along through the worst phases of the market.

Profit motives were the only immediate incentives most traders (and users) had in these apps at the time. They gave up fun for the sake of 'money'. However, if you study the academic literature on the motives of gamers, particularly regarding what makes free-to-play gamers convert to paying gamers, you see why the model broke.

In the early 2010s, the economics of gaming changed drastically. The rise of affordable Android devices meant that increasing numbers of people were open to gaming but were unwilling to pay for it upfront. How do you monetise such a crowd? You onboard them with no upfront payment and sell them items via micro-transactions. In 2020, a paper studied the motivations behind why gamers pay in such applications by summarising the results from 17 different research papers.

The table below indicates their findings. There is a recurring theme you'd find. Socialising, enjoyment and competition are the crux of what made those games desirable for users.



Used source	Analyzed game(s)			Parti-cipants (n =)	Country	Demographic data				Found motivations for *paying* in a *freemium* game
	Name	Genre	Plat-form			age (years)		gender (%)		
						range	mean	m	f	
Shi et al. (2015)	*Dragon Nest*	MMO RPG	PC	4,115	China	-	-	-	-	Perceived quality
Gainsbury et al. (2016)	Various games	Casino	-	521	Australia	18+	34-42	52	37	Enjoyment, Special offers, To advance in the game
Hsiao & Chen (2016)	*Tower of Saviors*	Puzzle	Smart-phone	3,309	Taiwan, Hong Kong	-	17-22 *(51%)*	89	11	Loyalty to the game, Good price & Convenience
Hamari, Alha, et al. (2017)	Various games	-	-	519	Finland	-	<40 *(95%)*	91	8	Unlock content/ Unobstructed play, Socialization, Price & special offers
Hamari, Hanner, et al. (2017)		-	-	869	Finland	-	20-29 *(47%)*	90	9	To advance in the game, Socialization, Competition, Aesthetics
Kim et al. (2018)	*Clash of Clans*	MMO strategy	Smart-phone	387	-	-	20-39 *(88%)*	67	33	Socialization, Switching costs, Obtained relative advantage, Value for money
Fang et al. (2019)	*Royal Sword*	RPG	Smart-phone	86,022	China	-	-	-	-	Socialization
Hamari et al. (2019)	*Pokémon Go*	RPG	Smart-phone	1,190	-	16+	21-25 *(33%)*	59	41	Competition, Challenge, Socialization
Hamari et al. (2020)	Various games	-	-	869	Finland	-	20-29 *(47%)*	90	9	Socialization, To continue playing

Table 2. Overview of analyzed studies to derive *freemium* game players' motivations for *paying*, and provided demographic data (ordered chronologically by publication year, and alphabetically)

Source Link

We were kicking the can down the road: "*There were no users, so the platform died.*" It's a relatively simple argument to make. So, I studied how long it takes to convert gamers to paying users. A different study examined the probability of a user converting to a paid user on freemium games. The data below considers the likelihood of a user becoming a paid user depending on their level in the game, number of days played and cumulative playtime. The data sets are for two games - Age of Ishtaria and Grand Sphere. As you can see, in the free-to-play world, it takes hundreds of hours and weeks of player retention for a gamer to convert to a paying user.

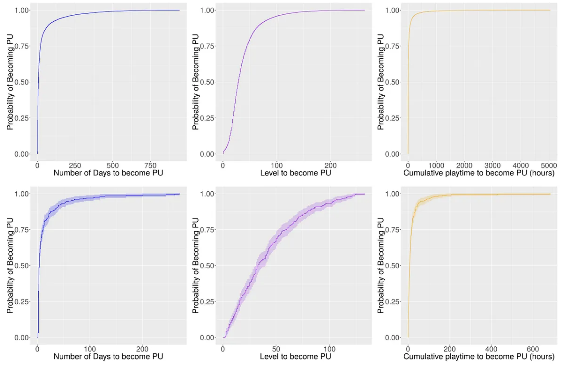


Figure 3: Cumulative incidence functions, showing the probability of becoming a PU as a function of the number of days since registration (left), game level (center) and cumulative playtime (right), for PUs only, in the games AoI (top) and GS (bottom). The shaded area represents the 95% confidence interval.

Source Link

This combination of an extremely low entry barrier and sticky user behaviour powered the free-to-play economies of the past. At least some of my readers will think this is an apples-to-oranges comparison. The metaverse, as we know it, is not about onboarding users. It is about enforceable scarcity and verifiable ownership. But our obsession with enforcing scarcity alone cannot sustain the markets. Consumers need and demand more.

My point is that the metaverse, as folks in Web3 consider it, didn't take off for several reasons. We thought that artificial scarcity and speculation would be permanent trends. It turns out they aren't. We believed trader personas would stick around in a bear market. It turns out they don't. As their portfolios of altcoins sank, their risk appetite declined. They had no reason to continue spending their time in our versions of virtual worlds.

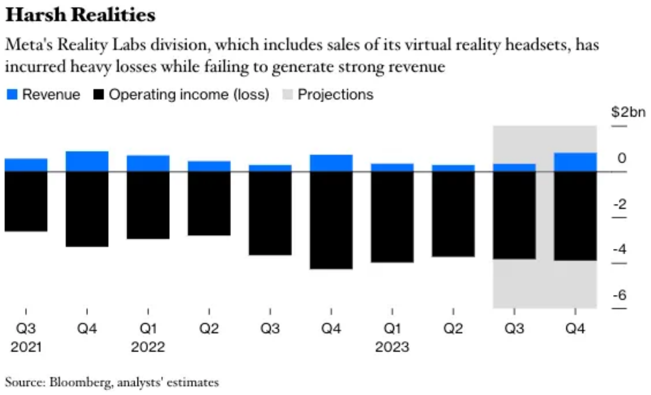
We thought that obsessing about expanding the user base did not matter as metaverse games have higher revenue per user. However, a considerable part of the motivation for gamers is socialising and relative rank. High-priced NFTs help with signalling (*and establishing rank*), but in the context of games, it is the equivalent of pay-to-win.

Gaming markets are increasingly specialised in that marketplaces, game design, payment rails and a game's management are increasingly separated and compartmentalized. When Web3 native metaverses took off, we expected firms that were at Series A levels to be able to tackle all of the above simultaneously. Founders had to scramble to solve issues ranging from collapsing in-game economies to developing fiat on-ramps to expand their user bases.

I believe it is nearly foolish to think that the metaverse in Web3 will take off in 18 months. Rockstar Games had decades of game-building experience before GTA 5 took off. To expect Web3-native firms to be able to establish a sector and retain users in the span of a single market cycle is akin to filling a car with jet fuel and hoping it will land on the moon.

Zooming Out

It is not only the Web3 version of the metaverse that struggled to find PMF. All forms of it have experienced an uphill battle. Meta has lost more than $21 billion in investing in the metaverse as a concept. Much of it went to hardware research, but until recently, the avatars in their Quest devices barely had legs. Even today, the hardware costs $500 and is beyond what is affordable for much of the world. Enterprise interest in the metaverse has waned rapidly as AI becomes the hot new thing.



Harsh Realities

Meta's Reality Labs division, which includes sales of its virtual reality headsets, has incurred heavy losses while failing to generate strong revenue

Source: Bloomberg, analysts' estimates

Data source: Link

While researching this piece, I wondered what venture investors were thinking when they presumed users would flock to virtual worlds at scale. Why did researchers (including myself) think we had crossed the chasm with the metaverse? Which person, in their right mind, would think commerce, love and education would happen through graphical interfaces? We were all excited about a new medium. And there is likely a part of us thinking that, much like the internet, this new medium would make the world more equitable and accessible as we would no longer see people for their real-life identities but just as virtual avatars.

Whenever a new medium comes around, it takes decades before it changes society. The printing press was invented in the 1440s, but it took until the Protestant Reformation of 1517 for it to enter wider usage. It took a few more centuries before the general peasantry could read. So not only did you need a hardware upgrade (the press), but you also had to wait till humanity synced with this new firmware release (the skill of reading).

Similarly, television took the world by storm in the 1950s. But it was not until the 2010s that short-form video content became mass-produced by everyone. The medium existed for decades but disrupted the world through TikTok and cat videos decades later.

For this new medium (t*he metaverse*) to take off, we will need an increase in network bandwidth, a decline in hardware costs and a shift in cultures. Apple's Vision Pro is a step in that direction. Meta, in collaboration with Rayban, recently launched a headset resembling the Google Glass from the mid-2010s. It uses AI to overlay graphics onto your glasses so that you can interact with the world world through Meta's hardware. However, we don't yet know whether consumers will embrace such devices.

Meta's virtual world, Horizon World, had over 900 users a few weeks back. This is a trillion-dollar firm that has spent billions of dollars on hardware and is struggling to retain over 1,000 users. The product has barely managed $10k in transaction volume. In 2022, Mark Zuckerberg's goal for the virtual world was to have more than 500k MAUs. They are at *checks notes* 0.18% of the way there. Despite Meta's tremendous distribution across WhatsApp, Facebook and Instagram, they have struggled to onboard users.

It's safe to say that Web3 teams won't have much luck in comparison. Meta has a history of acquiring assets or spending heavily on experiments for outsized returns. They spent over $19 billion on WhatsApp and another billion on Instagram. Both of which have yielded outsized returns.

The metaverse is an evolving oncept, and it is easy to obsess about how little (*or how much*) has been done with it. One of the things a developer friend (named Suzu), who has been on the internet since the 1990s, mentioned while discussing this piece is that developers working on the metaverse in crypto are trying to make a Biriyani Lasagna. These are beautiful, useful things when kept separate. But in force-fitting them with one another in ways that don't blend well, we create worse-off products for users.

Founders and investors often ignore the beauty of communities (*like Second Life, GTA 5 or Red Dead Redemption*) - and argue that a Web3 native metaverse could replace all of them. One way to fix this would be to mandate that Metaverse experts spend real time in the worlds they are designing.

If you think of the current forms of the metaverse – like Roblox, Fortnite or Apple's VR devices – we already have functional worlds where people spend billions of hours. They don't spend all that time and money wondering if they own these worlds. They spend their time there because they have fun.

We need to take a few steps back and consider what it would take to bring a million users into a metaverse. All commerce requires human attention. We obsessed too much with ownership and governance while conveniently forgetting what it would take to accumulate and hold on to human attention in a world where TikTok, Roblox, and ChatGPT compete for attention.

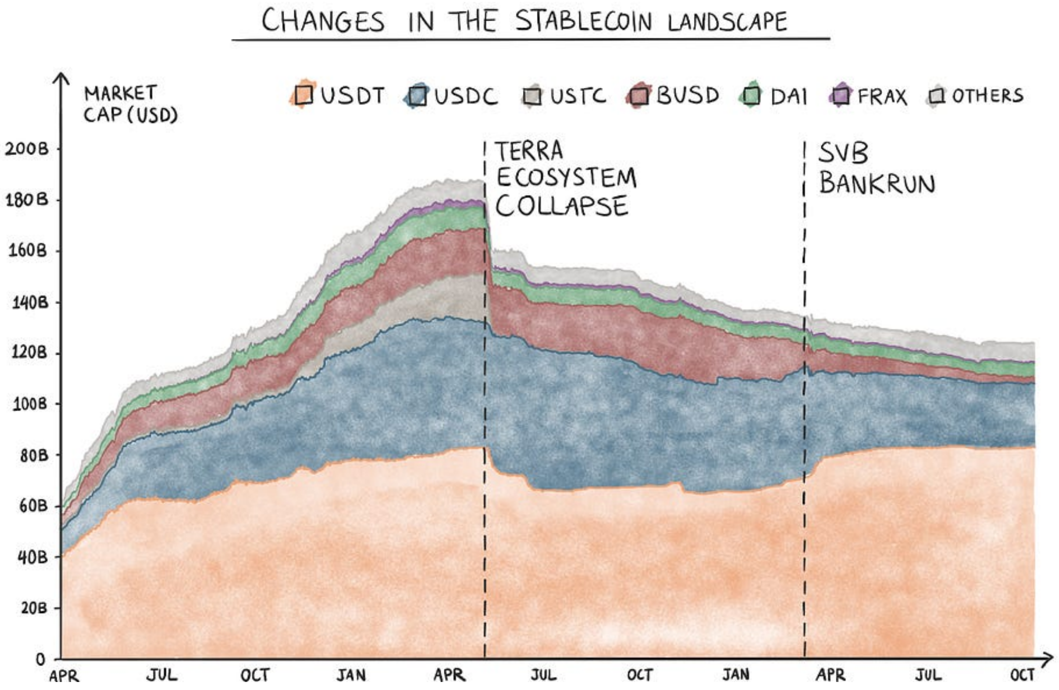
Next week, we'll study how a game from India is trying to solve challenges in acquiring and retaining users in the Metaverse.

Off to work on the week's long-form article,
Joel John

Joel John
decentralised.co

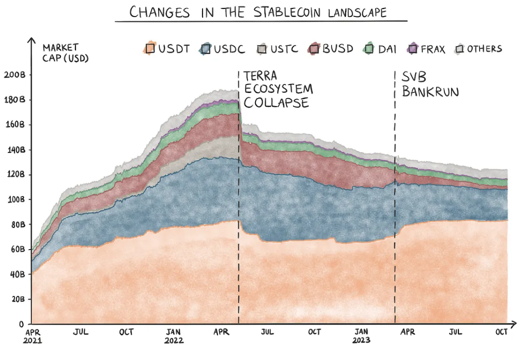
Keeping it Stable

Maintaining value as a stablecoin



Hey there,

Stablecoins are one of the few parts of crypto that have seen meaningful PMF. Despite the bear market, stablecoins maintain a market capitalisation of over $123 billion. Several types of stablecoins make up the market, from USD pegged to the ones pegged to other currencies like EUR or commodities like gold. The success of USDT, USDC, and DAI has led to the proliferation of several different projects launching their stablecoins with many (*not so creative*) designs.

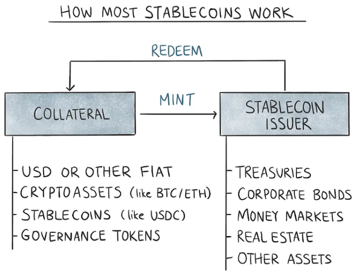


DATA: DEFILLAMA CHART: SAURABH DESHPANDE DESIGN: FONGKI

Stablecoins maintain their desired pegs through various mechanisms. Most do so by holding underlying assets at least worth their respective market capitalisations. The stablecoin issuer takes collateral from minters. They typically use the collateral to earn yield via short-term instruments. The health of the business depends on how the issuer balances redemption demand and earning yield since the capital is locked when earning yield.

It is tempting to think that involvement on the issuer's part can be a source of inefficiencies, which pushed the industry to explore algorithmic stablecoins. If you have a central party (*like Tether*) taking deposits (*in dollars*) and issuing an on-chain representation of it, you add to the fees. So much for 'decentralisation'. You have a risk of simply imitating central banks on the blockchain. Except this time, they are private corporations.

Algorithmic stablecoins have been intellectually intriguing due to the possibility of replacing these centralised parties altogether.



The Devil Is In The Details

Algorithmic stablecoins were all the rage until Terra crashed last year and $40 billion of value evaporated. In simple terms, such stablecoins were typically backed by make-believe assets with no apparent reason for their value. I get that the value of all assets is subjective. But I think subjectivity of value is a spectrum.

Value depends on the number of people who believe an asset (*like equity or altcoins*) is worth a given number of actual dollars and their willingness to trade for it. This number depends on several factors, such as who creates the asset, how it is created, how and where it is used, and the volatility of the asset's price.

The value of the USD is less subjective than an algorithmic stablecoin backed by a governance token. When the belief in the asset that backs a stablecoin gets shaken, it loses value, and the stablecoin loses its peg. What happened to the Terra ecosystem is a case in point. Since then, projects have been getting creative about structuring their stablecoin's collateral.

As yields in decentralised finance (DeFi) dropped while interest rates surged, protocols like MakerDAO adapted to incorporate real-world assets (RWAs) into the mix. As of October 12, 2023, the RWA component contributes ~67% to the revenues and ~60% of the collateral for DAI.

MakerDAO's success with RWAs was a proof of concept for many upcoming projects. They built models around RWAs such as US Treasuries, real estate, corporate debt, etc. This aligns with the theme we covered a couple of months ago, where we observed that the boundaries between traditional finance and crypto/Web3 are blurring. While combining features from both worlds, the design choices likely borrow bad practices from both.

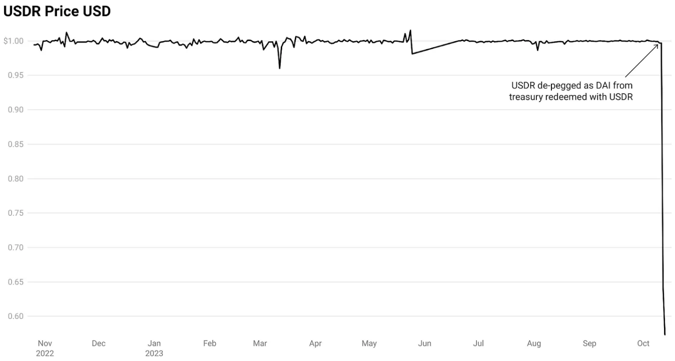
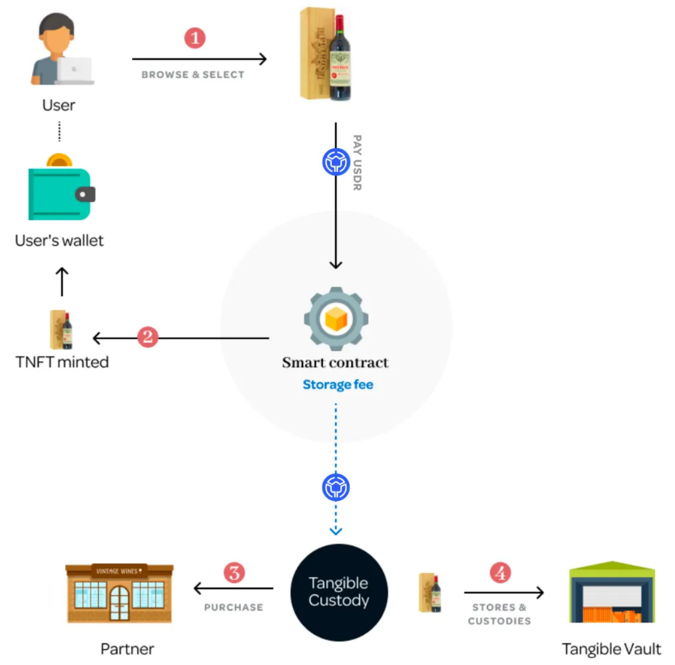


Chart: Saurabh Deshpande • Source: CoinGecko

Tangible used a 'Terra-esque' design due to which, under certain circumstances, the stablecoin could become partially backed. This resulted in its stablecoin losing its peg to trade around $0.5. This piece explores what happened with Tangible's stablecoin and its effect on the RWA space.

Tangible's Design

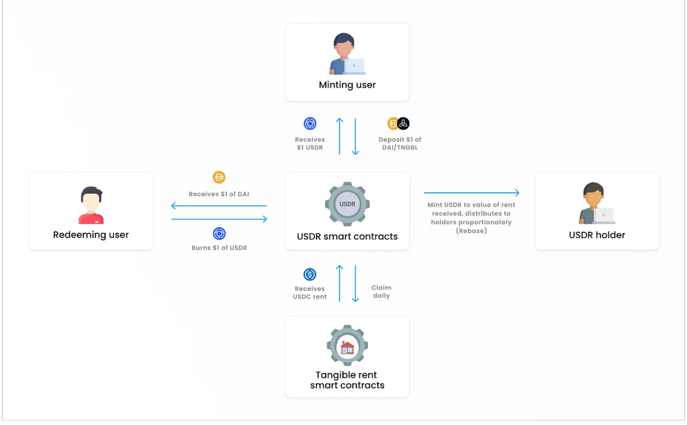
Tangible uses real estate as a core asset to build its protocol. It describes itself as an ecosystem of tokenised RWAs. It uses its native real estate-backed stablecoin, Real USD, or USDR, to let users access tokenised and fractionalised RWAs through its marketplace. When users buy tokenised assets on the platform, they get what are called TNFTs. These assets could be redeemed for actual products later.



Source – Tangible

How does real estate come into the picture? Tokenised properties that can be easily rented out are used as partial backing for USDR, along with DAI, insurance funds, and Tangible's governance token – TNGBL. It is designed so that the USDR that can be minted with TNGBL never exceeds 10% of the USDR minus the USDR redeemed.

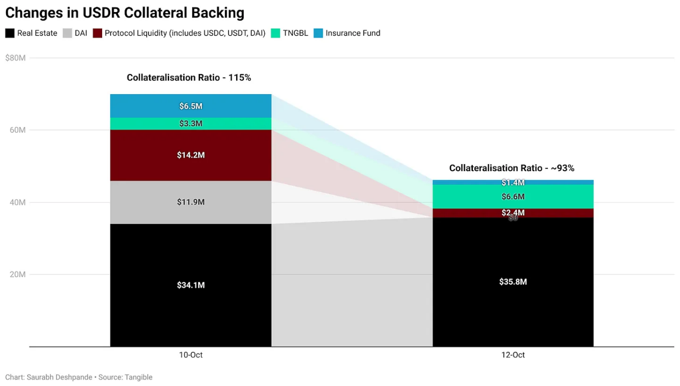
Tangible buys properties that can be easily rented out, which Blackstone does on a massive scale. The rent from the properties is the yield. The image below shows how the protocol works. This article is excellent if you want to learn how it works.



Source – Tangible

Between 10 and 12 October, all the DAI in the treasury, close to $12 million, was redeemed for USDR, resulting in USDR depegging by 47%. The collateral ratio dropped from ~115% to ~93%. This is where the problem starts. The collateral mix is vital for maintaining the perceived value of the stablecoin. We have seen what happens when this mix skews towards another asset (without any material cash flows attached to it) of the stablecoin issuer.

UST took three days to wipe out $40 billion worth of perceived value, so it's critical that assets with network effects back stablecoins. Luckily for Tangible, not all hope is lost because most of it is backed by real estate. It brings us to the next problem with this design – the stablecoin was a liquid asset backed by an illiquid asset. Let me explain..



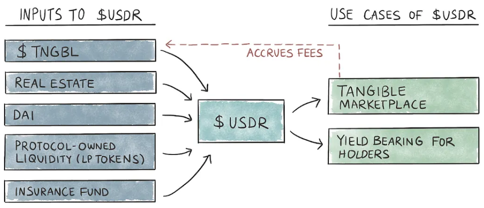
Changes in USDR Collateral Backing

Chart: Saurabh Deshpande • Source: Tangible

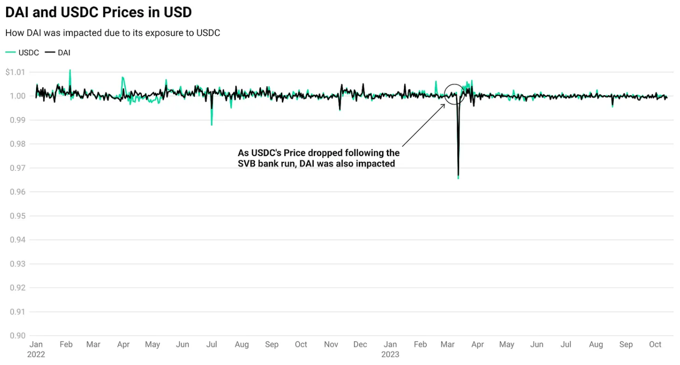
Right now, USDR is backed by $6.6 million worth of TNGBL. Learnings from LUNA dictate that we must mark TNGBL and insurance funds down to 0 to assess how bad the situation is. This leaves us with $35.8 million of real estate and $2.4 million of other stablecoins from protocol-owned liquidity backing 45.5 million USDR – an ~84% collateralisation ratio.

(Joel's Note: That means $38.2 million worth of assets are backing $45.5 million in liabilities on the protocol).

But the problem is whether we can consider the real estate worth $35.8 million. If Tangible has to sell these assets, will it be able to sell for the entire value? If yes, how long will it take? This uncertainty is why, despite having provisions, the market is valuing USDR at 53% of its peg instead of 84%. Distressed assets usually sell at a discount. By limiting the stablecoin's exposure to TNGBL, the team has only ensured that USDR doesn't go to zero. But the design doesn't help in keeping the peg to $1.



In March 2023, Silicon Valley Bank (SVB) experienced a bank run and could not honour withdrawals. At the time, Circle held ~$3.3 billion in SVB. This write-off caused USDC to briefly depeg. But this was a time of contagion. It didn't stop at the USDC depeg. Leading up to this event, MakerDAO had increased its collateral exposure to stablecoins, largely USDC. Intraday, USDC went down to ~$0.93. And since USDC was one of the collaterals for DAI, the latter also dipped to around $0.9.

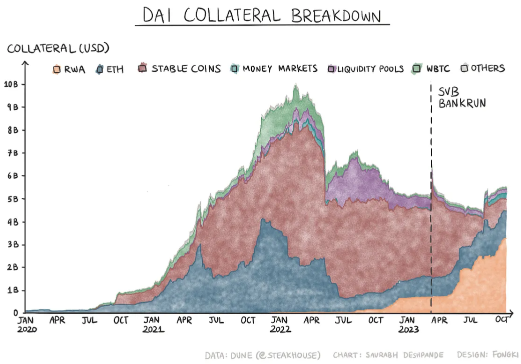


DAI and USDC Prices in USD

How DAI was impacted due to its exposure to USDC

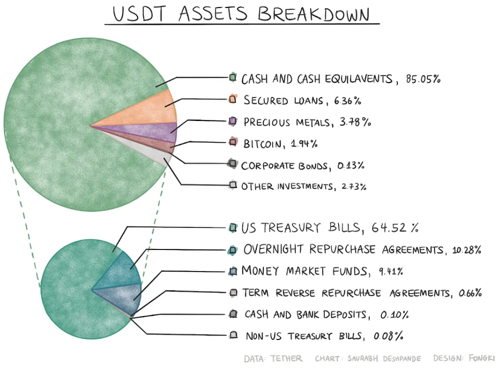
Chart: Saurabh Deshpande • Source: CoinGecko

MakerDAO realised that extending support to collateral assets increased risk exposure and left DAI vulnerable to de-pegging. The SVB incident ushered in a significant change to the collateral mix of DAI. The exposure to stablecoins was significantly reduced in favour of RWAs after the SVB bank run.

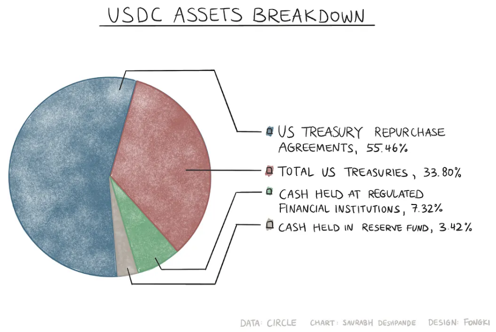

DAI COLLATERAL BREAKDOWN

DATA: DUNE (@STEAKHOUSE) CHART: SAURABH DESHPANDE DESIGN: FONGKI

It's worth exploring how Circle and Tether- the two largest stablecoin issuers, manage their assets. Both have allocated an overwhelming percentage of their assets to short-term US Treasuries, one of the most liquid assets. Indeed, the current high-interest rate environment is also why they choose US Treasuries. But this helps create a perception of safety in the mix of assets.


USDT ASSETS BREAKDOWN

DATA: TETHER CHART: SAURABH DESHPANDE DESIGN: FONGKI


USDC ASSETS BREAKDOWN

DATA: CIRCLE CHART: SAURABH DESHPANDE DESIGN: FONGKI

The RWA Connection

Growing a stablecoin that is even partially backed by your own asset is similar to countries trying to maintain pegs of their currencies at a much smaller scale. Stablecoin projects have a fraction of the resources that a country has. Despite disproportionately high resources, currency pegs have a mixed history. Evidence shows that sometimes pegs work, with examples like the Hong Kong Dollar's peg to the US Dollar and the Singapore Dollar's peg to a basket of currencies. But history is filled with instances where pegs proved expensive to manage or were simply not worth it.

Governments use levers to maintain currency pegs, such as spending their foreign exchange reserves, employing strict capital controls, and making frequent interest rate interventions. History is rife with examples of governments preempting unpegging their currencies (Switzerland did this in 2015) or abolishing currency pegs due to a crisis (the Asian currency crisis in the late 1990s forced Thailand to let go of the peg).

One of the primary reasons countries went off the gold standard is that it limits the ability of governments to respond to crises. Whether government intervention is good is not the point here. Not having a country's currency (and, in turn, value) tethered to other assets allows governments to manipulate the supply depending on prevailing economic situations. Despite so much freedom, it is debatable whether governments get it right.

Asset-backed stablecoins, by default, have constraints on how the issuers can respond to crises. A more straightforward design for a real-estate-backed stablecoin like USDR is to eliminate the governance token as collateral. Keep the collateral composed of highly liquid crypto assets and RWAs. There's a reason why DAI cannot be minted with MKR.

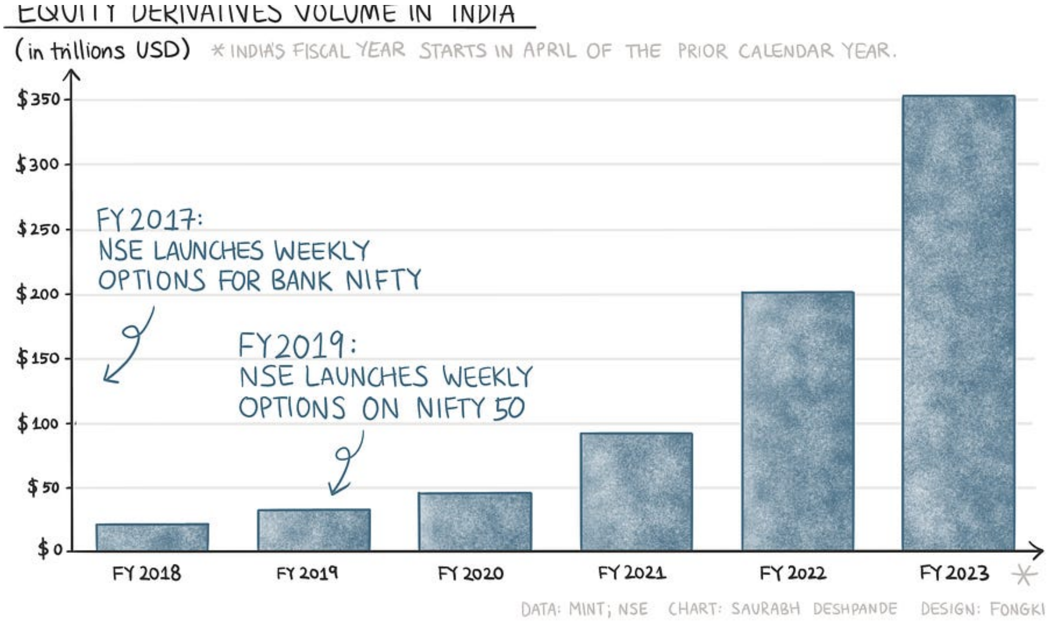
A drawback of not using your governance token as collateral is that you don't have enough 'use cases' for the governance token, as governance as the only use case may not fetch enough premium. This limits the team’s ability to bootstrap and spend on user acquisition.

Using tokenised RWAs to help generate yield on-chain is critical if we want to blur on-chain and real-world boundaries. But the means to achieving this determine the sustainability of projects. What happened with USDR will serve as a lesson for Tangible and other teams; hopefully, we will see better designs in the future.

Saurabh
decentralised.co

It is All Derivative

What's holding the industry back



Hello!

'I bought the call options', said one of the characters in the movie *Dumb Money*, which narrates a David versus Goliath tale set in the financial markets. It is about how an army of Reddit users took sophisticated investors head-on. Consequently, one of the larger hedge funds, Melvin Capital, had to shut shop after losing billions of dollars.

I have been constantly thinking about crypto derivatives since last Friday. Maybe we could all rally together and hunt down hedge funds like the GameStop crowd did last year.

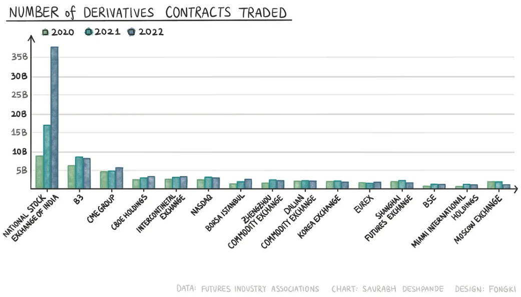
Currently, the market landscape for derivatives feels lethargic. While thinking through how the landscape is likely to change, I started to think about how financial primitives in crypto are nothing but replications of TradFi primitives with different infrastructures. Generally, it is safe to assume that crypto financial primitives will follow the same course as TradFi.

Following what happened in traditional derivatives markets like India in the last decade will explain what we can expect in crypto. Why do I say India?

Because in the last decade, India's derivatives market has evolved substantially, and I had a front-row view of it in Mumbai - India's financial capital.

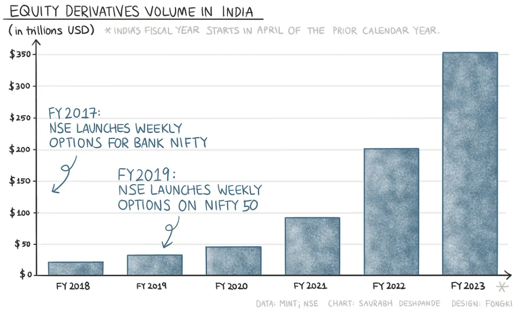
Emerging A Market

India's National Stock Exchange (NSE) is the leading market regarding the number of contracts traded (*this is not the notional value*). Equity derivatives volume has picked up in India in the last few years.


NUMBER of DERIVATIVES CONTRACTS TRADED

DATA: FUTURES INDUSTRY ASSOCIATIONS CHART: SAURABH DESHPANDE DESIGN: FONGKI

According to the Economic Times, India's derivatives market volume is ~400 times the underlying cash or spot market. Usually, this number is five to ten times the underlying cash market. Derivatives volume constitutes 99.6% of the overall volume in India, compared to ~70% in the US. Options dominate the derivatives volume with a 99% share.


EQUITY DERIVATIVES VOLUME IN INDIA

(in trillions USD) * INDIA'S FISCAL YEAR STARTS IN APRIL OF THE PRIOR CALENDAR YEAR.

FY 2017: NSE LAUNCHES WEEKLY OPTIONS FOR BANK NIFTY

FY2019: NSE LAUNCHES WEEKLY OPTIONS ON NIFTY 50

DATA: MINT; NSE CHART: SAURABH DESHPANDE DESIGN: FONGKI

This is the notional traded value, not the value of settled contracts.

But why did this change happen in the first place? Maybe we could replicate some of it with products in DeFi.

Better Instruments

For a long time, India only had derivatives products with monthly expiry. One of India's exchanges, the NSE, started offering short-dated options in FY 2017 with weekly options for Bank NIFTY; it launched weekly options for the NIFTY 50 Index in FY 2019. As of FY 2023, weekly options account for 95% of the trades.

Improved Access

Opening a dematerialised (demat) account was tedious before the internet and mobile penetration. With the FinTech revolution in India, opening a demat account within minutes became the norm. This has been facilitated by access to financial markets via apps like Zerodha, coupled with increased internet access. As a side note, the average cost of 1GB of data in India is $0.16 compared to $6 in the US.

Zerodha was launched in 2010 with significant discounts on brokerage charges. By 2013, it was among the very few tech platforms with a user-friendly UX. By 2017, Zerodha had already launched an education platform (Varsity), a trading API (Kite.Trade), and a mutual fund investing platform (Coin). Zerodha's strategy, in general, forced all major brokers to launch tech platforms that were more user-friendly.

Following Zerodha's success, investment platforms like Groww, Dezerv, and Wint hit the market, trying to address the different needs of investors. This development contributes towards increasing the number of people participating in the markets. It was not a single app that improved the market.

The Growth Economy

India has a demographic advantage among the major economies. The dependency ratio of India (~48%), the percentage of dependents compared to the workforce, is among the lowest in major economies.

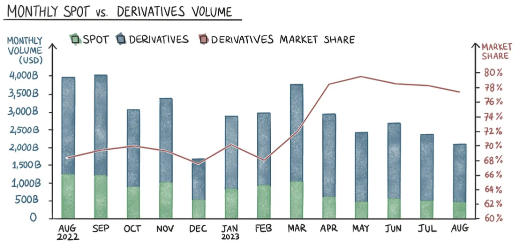
With the FinTech revolution and a huge workforce, India is often compared to China in the 1980s, with almost a consensus view that it will be among the fastest-growing major economies in the world in the near future, meaning India is likely to remain among the preferred investment geographies.

Despite the growth, the Indian market has significant room to grow. Paytm's red herring prospectus states that as of 2020, only ~3% of the Indian population participated in the stock market vs 55% in the US. Although this number has grown over the last few years, it remains significantly low compared to developed markets like the US. India has a per capita GDP of ~$2400, compared to ~$77k in the US.

How It Relates To Crypto

What has this got to do with crypto? One may hypothesise that an average crypto user lies somewhere along the spectrum of emerging markets like India and developed markets like the US. Some drivers for the growth of India's derivatives market can apply to crypto markets. **While the share of derivatives volume (as a percentage of total spot + derivatives volume) in India is 99%, it is around 78% for crypto**.

But unlike India's derivatives volume mix, which is heavily skewed towards options, futures are more popular among crypto traders for reasons we describe later in the piece.



DATA & CHART: CCDATA DESIGN: FONGKI

Options vs Futures

In traditional markets, the maximum available leverage depends on the nature of the underlying asset. It is essentially a function of the volatility of the underlying asset. For example, available leverage in the currencies market is typically much higher than in equities because currencies are much less volatile than equities. Typically, the initial margin for stock futures is 3–12% of a contract's notional value.

This means the available leverage is capped at 33X. However, options inherently offer more leverage since the buyer knows exactly how much they stand to lose. When the options premia (*the amount you pay to buy an option*) are low, the leverage factor in options can be more than 100X. This is why options end up dominating the notional volume in many markets like India.

The story is different in crypto. Perpetual futures were a hit product with the launch of BitMex (probably because 100X leverage was easily available). It is likely that since leverage is so abundantly available in futures, a more straightforward product than options, options never took off.

CeFi vs DeFi

There's a significant gap when you look at CeFi offerings and compare them to DeFi futures. Binance invariably conducts $20 billion in daily volume on its futures product, whereas the volume on the leading futures DEX, DYDX, hovers around $600 million, just ~3% of Binance. The problem is that the state of DeFi options is even worse (as shown in the following section).

Many of us are now mobile first. Over half of web browser traffic comes from mobile devices. It also explains why applications like Zerodha in India or Robinhood in the US have a huge user base. Trading options and futures from these applications is easy; you can do it from a beautiful UI on your phone. However, you can't trade crypto derivatives as easily. Yes, I know Deribit has a cool app, but most DeFi is still designed for desktops first.

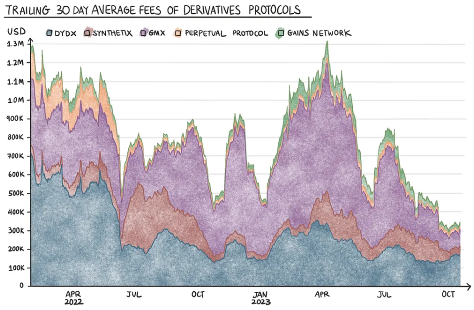
With centralised venues, this has never been a problem. Binance and Coinbase have prioritised both platforms — mobile and desktop. However, the regulatory dynamics forced them to limit where users can use their products.

Coinbase recently launched futures trading for non-US residents. Mainstream applications like Coinbase offering derivatives products will likely move the needle going forward. The issue is not that futures and options have been unpopular among crypto users. Centralised venues like Binance and Deribit lead categories in futures and options, respectively. The issue is with DeFi derivatives.

Where We Are At

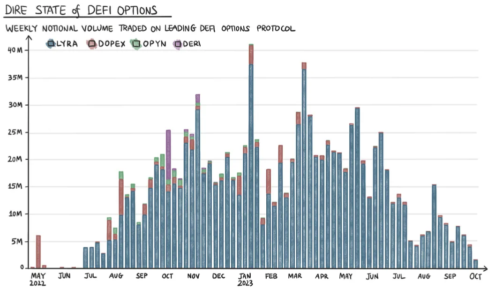
DYDX has been the leading futures DEX. Unlike many other DEXs, it is based on order books and matches orders off-chain. This is one of the reasons why when you trade on DYDX, it barely feels like a DEX. It also offers similar spreads (the difference between the highest bid and lowest ask) to Binance on leading pairs like BTCUSD and ETHUSD.

The chart below compares fees on the leading futures DEXs. I've compared fees here because it is a good indicator of how much users are willing to pay to use the products. One can also look at volume as an indicator. Notice the periods when fees across exchanges expand. Typically, these are periods of increased volatility. The recent local peaks in fees came in July and April 2023, when the prices of crypto assets increased from their lows, sparking interest among traders.


TRAILING 30 DAY AVERAGE FEES OF DERIVATIVES PROTOCOLS

DATA: TOKEN TERMINAL CHART: SAURABH DESHPANDE DESIGN: FONGKI

DeFi options are significantly underdeveloped compared to DeFi futures and CeFi options due to a severe lack of liquidity and high volatility. These factors essentially mean that even though buyers would want to get options exposure to smaller assets as protection or speculation, sellers find it difficult to write options.


DIRE STATE of DEFI OPTIONS

WEEKLY NOTIONAL VOLUME TRADED ON LEADING DEFI OPTIONS PROTOCOL

DATA: DUNE (@AHKEK) CHART: SAURABH DESHPANDE DESIGN: FONGKI

The combined weekly notional volume on the four leading DeFi options trading platforms is around $5 million. In contrast, on October 20, Deribit supported a volume of $820 million for BTC and $400 million for ETH, a combined notional volume of over $1.2 billion. Although a $1.2 billion notional volume isn't much, DeFi options stand nowhere close to their centralised competitors.

The reason is the lack of liquidity in decentralised venues which occurs due to the horrendous capital efficiency and bad user experience in general. Let me explain what I mean by that....

Say you want to sell ETH calls on Deribit for a $1800 strike price, and the position requires an initial margin of 1 ETH. Now, if you want to buy calls for some other strike price (or expiry) or go long on ETH, Deribit doesn't require you to put more collateral as long as the position sizes are commensurate. The logic is simple: since you are opening positions in opposite directions, gains and losses will offset each other to an extent.

And as long as they are not heavily skewed in one direction, you should not be mandated to put up more collateral. But for the same scenario, DeFi options require separate collateral. In addition to this, options protocols do not recognise collateral from futures. **For all the composability claims of DeFi, derivatives in the sector have not been composable. The problem is futures and options are treated as separate buckets, and the margin used for them is isolated.**

Currently, it may seem like there's little hope for on-chain options. But there may be ways in which they can be made more functional, i.e., more capital efficient. If there were a liquidity layer in DeFi that allows protocols to recognise collaterals and positions from each other, then DeFi derivatives could function as a cohesive unit to provide a CeFi-like experience to power traders. But this also means that the risks of these protocols are no longer localised. A vulnerability in one protocol may affect other protocols.

If you ask traders why they don't trade futures or options via their self-custodial wallets, typically, they will tell you lack of liquidity and subpar UX are some of the leading reasons. Liquidity comes with users, but projects that make their design suitable for users will likely attract liquidity.

I was interested to see which projects are addressing these core issues. Recent developments in Synthetix aim to address these issues.

On Synthetix v3

Synthetix has been one of the oldest DeFi products. But its design had a significant flaw. It used to let users stake SNX, Synthetix's governance token, to mint its stablecoin Synthetic USD (sUSD). sUSD would then be used to trade futures and mint synthetic assets. The collateralisation ratio was 8X; that is, if you wanted to mint $100 worth of sUSD, you had to lock $800 worth of SNX.

This pooled SNX acted as counterparty or liquidity for trades facilitated by Synthetix, the exchange. So, if traders won, stakers lost, and vice versa. Although the overcollateralisation helped keep sUSD around $1, the design was highly inefficient. And since only SNX was allowed as collateral, there was a cap on how liquid it could be.

Recently, Synthetix shipped an upgrade that allows other assets to be used as collateral, essentially moving towards becoming a permissionless liquidity layer for DeFi.

This is where DeFi composability starts to materialise, where all kinds of markets like spot, futures, options, insurance and other exotic products can tap into a liquidity pool instead of trying to bootstrap it separately. But creating infrastructure is not enough. The experience has to be at par with the CEXs.

DeFi builders should not assume that users are willing to bear with subpar experience because they get to use non-custodial products. The idea should be that users choose DeFi because the experience is as good as the centralised alternatives. To that end, the upcoming Infinex exchange is leveraging the Synthetix ecosystem to create a CeFi-like DEX.

Another factor besides capital efficiency contributing to lower liquidity is that DeFi needs fiat onramps. It is either stablecoins like USDT or USDC, with centralised entities, or ones like DAI that are overcollateralised – which is capitally inefficient from the get-go.

Arthur Hayes proposed a solution: creating a stablecoin, Naka USD, which is $1 of Bitcoin + Short 1 Bitcoin per USD in Inverse Perpetual Swap. I won't get into the design specifics, but it would need custodians and a DAO to act in good faith. Along these lines, BitMex has already launched Quanto Perpetual contracts that allow users to trade futures without stablecoins. Although this seems fine on paper, it has two issues:

1. It's difficult to support the permissionless development of protocols using this design.
2. A lot of good actors need to come together to bring this to fruition – and remain good.

We need solutions that do not rely on centralised parties playing "*good*". Last year, the industry placed its hopes on Terra and FTX. We have learned some harsh lessons from that. When you consider that MakerDAO's DAI, has stuck around longer than some of these centralised alternatives, it becomes easier to understand why we need more decentralised primitives to scale DeFi.

Although the state of DeFi derivatives is not encouraging based on the numbers we have today, reflection on the previous cycle gives me hope. Back in 2018, there were no scaling solutions. Rollups are live now. Lower fees and account abstraction primitives will add towards creating a seamless, CeFi-like experience. Products like DYDX prove that DeFi products can feel like their centralised counterparts.

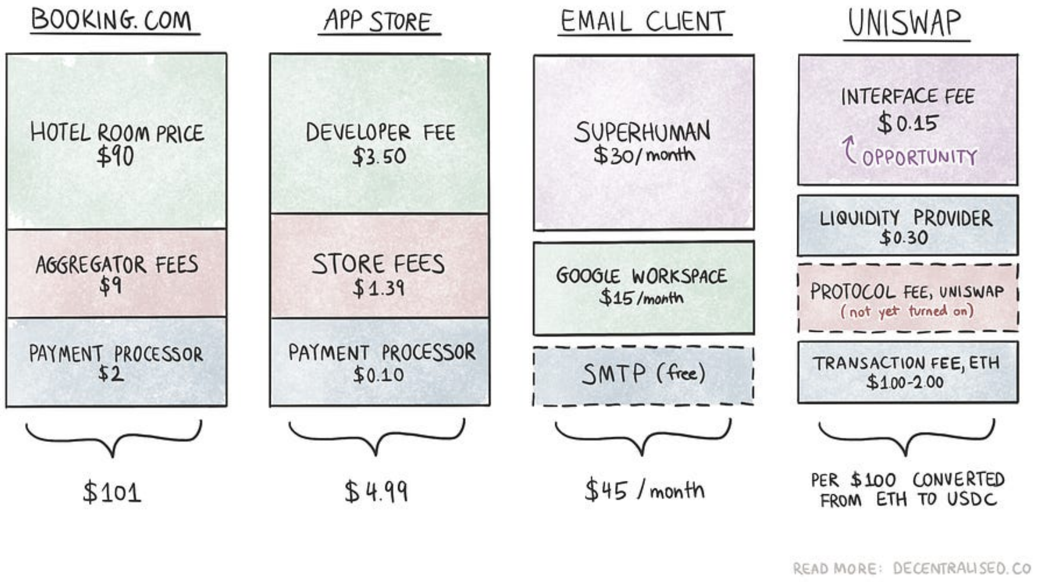
It doesn't take too long for things to change in our industry.

Signing off,
Saurabh

Joel John
decentralised.co

The Interface Dilemma

Finding the fee switch



Hey There,

Last week, Uniswap announced a fee for individuals using the product directly through their website. It is being referred to as an "*interface fee*". At 0.15%, it is a small sum to be paid by anyone using the product until you realise that Uniswap does not own the inventory of assets on its exchange. They have little marginal cost for enabling each new transaction on the product. I thought it would be worth exploring as it marks a time when business models in the industry are evolving rapidly.

Before we dive into the unit economics of interfaces, it helps to revisit what I mentioned in my piece on aggregation in Web3. The nature of smart contracts allows protocol developers to source third-party liquidity by incentivising users with either tokens or platform fees. When you allow your money to stay at a bank, part of the promise is to receive a return on that idle capital.

But banks cannot print money out of thin air themselves. *(You could argue central banks can, but the commercial banks can't.*) They are required to find sources of yield that generate dollars. There are marginal costs incurred in generating yield. On the other hand, DeFi platforms see exponential revenue growth without costs surging.

Banks need to hire personnel as they scale from managing $1 billion in deposits to $10 billion in deposits. GMX or Uniswap does not see a similar cost growth as smart contracts facilitate most platform transactions. You don't need human labour in proportion to the transaction volumes.

Incentives for Liquidity

Token incentives are a powerful mechanism to drive liquidity. Aave and Compound tokens were given to bootstrap a market for lending ETH and receiving a fixed yield. Similarly, Uniswap tokens incentivised people to put ETH and USDC into a pair on a smart contract. Unlike banks, protocols in crypto can mint assets to incentivise user behaviour. Blur took this to an extreme when it came to NFTs.

Their model incentivised users to put bids and asks closest to the spot price of an NFT. So, if you were a liquidity provider on Blur and an NFT was trading at $100, you would receive more points for providing liquidity at $99 instead of $90, which may have been a better price to acquire the NFT. Blur's model worked so long as the token incentives justified the losses incurred in providing liquidity for large NFT collection holders. There is a distinction to be made here between liquidity and efficiency.

1. An efficient market reflects the collective information market participants hold about an asset in the least amount of time. In this sense, a CeFi platform (like Binance) can be more efficient than a DEX (like Uniswap), as there's a minor lag depending on the blockchain where an exchange happens.

2. On the other hand, a liquid market is one where large position sizes can be purchased or sold at prices close to the spot price. Blur brought liquidity to an illiquid market and, by extension, arguably made it more efficient.

Take, for instance, this example of a trader who sold $9 million worth of Bored Apes in a single transaction. By allowing large holders to enter and exit an NFT ecosystem, the platform allowed NFTs to behave closer to tokens (in terms of price) than a more illiquid asset (like real estate). Why does this matter? The platform does not take the 'risks' on traded assets.

The risk is instead handled by users who hope to gain through the platform's tokens. As a token declines in price, the incentive for providing liquidity wanes rapidly.

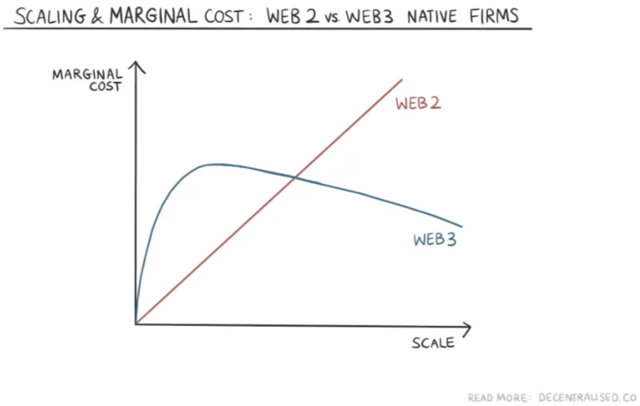
Marginal Costs

Why does this matter? To understand, we must look towards Web2 aggregators like Uber or Spotify. When Uber launches in a new city, there are marginal costs in managing drivers. Surely, the firm does not often own the fleet or have marginal costs in hiring drivers. But there's labour involved in managing the fleet. Your operational expenses for fleets rise in proportion to the number of drivers you have.

Similarly, on iTunes or Spotify, the core commodity (music) has a fixed cost that rises in proportion to the size of your library. These costs increase proportionately to how extensive your library is, which depends on the number of labels and artists you sign.

The demand side for both these platforms does not add to marginal costs for them. Uber and Spotify can scale to hundreds of riders a day so long as they can manage their relationships with drivers or record labels. But the supply side has a fixed cost, which scales in proportion to how many offerings you have.

iTunes can lose out to Spotify if they don't have support for music in local languages in markets like India. Uber will quickly see users flocking to traditional forms of transport if they cannot provide drivers in meaningfully short wait times.



READ MORE: DECENTRALISED.CO

Web3 native products are unique because the teams behind platforms do not bear the marginal cost of liquidity. Initially, you take the cost through your native token given to users in an airdrop. Uniswap gave tokens. Aave gave tokens. These tokens, through their price and relative value in governance, incentivise users to continue being engaged in a product. But what happens if a platform's fees do not accrue to token holders? What incentive do users have to continue providing liquidity?

Projects like Aave and Uniswap are unique in that they could circumvent a critical level of liquidity to find PMF before interest in acquiring tokens waned. An AMM like Uniswap will always have users providing liquidity as long as

1. Token holders want a non-CEX avenue to trade, and
2. There is interest in receiving a passive yield on the asset.

Similarly, a platform like Aave will always have users providing liquidity if people want to put their idle crypto assets to work. The sustained rise (*and eventual collapse*) of DeFi in the quarters that followed Uniswap and Aave's launch helped them turn into products that saw enough volume to justify users putting their idle assets to work there.

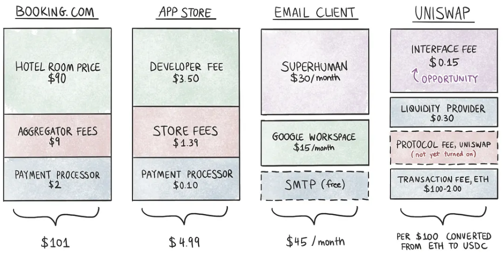
Why does any of this matter? As token rewards wane, teams behind products like Uniswap must find new mechanisms to monetise themselves. Sure, there's the option of selling tokens, but it means giving up governance rights if you are truly decentralised, as you claimed when you issued the token.

Uniswap avoids switching on a protocol fee as it could mean liquidity and users flock towards zero-fee platforms. It also opens up their token to being interpreted as a security. OpenSea saw a meaningful threat from Blur when they launched a zero-fee model for NFTs.

At the crux of the interface dilemma is a simple question.

How do you monetise as a protocol when you don't own the core commodity your users flock towards you for?

Firms like Uniswap Labs (*the entity that owns and develops the website at Uniswap*) could generate revenue if they switched on the protocol fees. But they don't 'own' the protocol. The token holders do. You could argue that they could pass a proposal to switch the fees between the team and investors' tokens – but that would drive users towards their competitors.



READ MORE: DECENTRALISED.CO

Interface monetisation is not a new concept. We have seen variations of it in the past.

So, in the interest of optics and relative market positioning, they go for what is now dubbed interface fees. Users who go to Uniswap from their native website will be paying 0.15% in fees each time they make a trade. Protocols are not new to the internet. SMTP has facilitated the transfer of emails for years. However, there are value-added services that private firms have built on this new protocol.

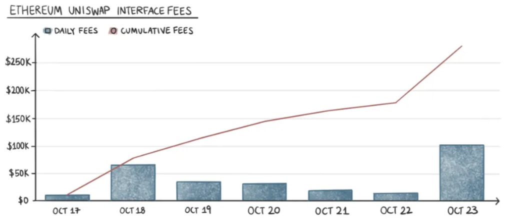
You can get a custom email hosted by Google for $15 monthly. An app like Superhuman can help you manage inbound emails for $30 a month. These are interfaces built on top of a free protocol (SMTP).

Wouldn't this obliterate Uniswap's volume? Well, not really. According to data from @tt_tyler on Dune Analytics, about 4.2% of all trades occurring on Uniswap pay some form of fee today. In terms of volume, about 3.6% pays fees. Keep in mind, not all pairs on Uniswap pay fees. For scale, consider that Uniswap Labs made $35k in fees on some $655 million of volume on the protocol over the past day.

(*Note: The wording above may be confusing. For clarity, of that $655 million, only $23 million went through Uniswap's interface. A 0.15% fee on that, translates to $35k. The rest of the volume on Uniswap comes through bots, external apps (like wallets) and aggregators.*)

Those look like terrible metrics, but consider that users may continue using Uniswap because of

1. The idea that they are using the right exchange and are less likely to lose money to a hack
2. The acquired habit of going to a domain they are used to visiting every time they wish to exchange



DATA & CHART: THE BLOCK DESIGN: FONGKI READ MORE: DECENTRALISED.CO

For now, that 0.15% is a small premium for users to pay to know they are interacting with the right product. Cumulatively, Uniswap Labs has made over $250k over the last few weeks through putting a fee for their interface. It is similar to using Amazon over an unknown e-commerce brand or preferring Starbucks over a local coffee shop when you travel. People like the familiar, even when it comes at a slight premium. But what about protocol fees? Can they be switched on? There is quite a bit of nuance to that question.

Monetising Interfaces

At its core, the fees on Uniswap are reflective of a larger problem faced by token-based projects in the industry. When the marginal cost of servicing is next to zero, can you profit off stakeholders without rewarding them, too? Let me explain.

At its crux, Uniswap (as a product) is a group of intangible assets. The fact that they can scale with minor updates to their codebase is a bug and a feature. If they are perceived to be profiting off a public commodity (user liquidity) without passing on rewards, it could hurt how token holders perceive the firm. The token's price could collapse overnight, as users will have no reason to keep holding onto them.

Conversely, a DAO that continuously sells its governance token to incentivise developers and manage its operational expenses is signalling that it is willing to give up protocol control in exchange for an extended runway. This disconnect between governance rights and incentives is why interface fees will be trendy among protocols that have scaled meaningfully, like Uniswap.

Enabling interface fees is not just about Uniswap, though. It is about creating a healthy mix of front-ends through which users can interact with a protocol. A good instance of this is MetaMask, which struggled to monetise meaningfully until it began charging 0.875% on swaps through its product.

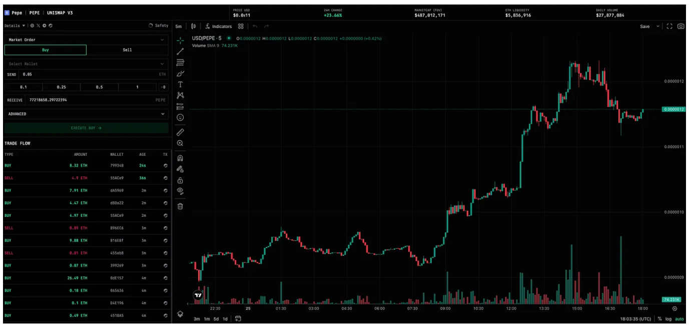
Through charging a market-up on each conversion, the wallet opened up a way to generate revenue for itself. In the future, we'll see a separation of protocol and application. The protocol itself may not charge any fee (unlike Uniswap), but the application could build meaningful cash flow by taking a small chunk of a large transaction volume.

Developers will profit off tapping into a protocol's liquidity without necessarily holding all the smart contract risks themselves. This sounds a lot like aggregators, but there is a core difference. A user going to an aggregator is usually looking for the best price. A developer building an interface will likely interact with one of two user types.

1. A niche-specific user, such as those with gaming-oriented wallets that emerged during the Web3 gaming boom
2. A user that is being onboarded through a more straightforward, non-degen-oriented app

A developer could charge higher fees in both cases, as the user is often not price-sensitive. Instead of Uniswap's 0.15%, a product could charge 0.5% if the interface is meaningfully better. The increase in clients would mean better user experiences for everybody.

What does that look like? The interface below from Thunder by Eversify offers some clues. It pulls in blockchain data to show the price feed. Uniswap owns the liquidity pool, so the developers have minimal smart contract risks on their platform. And it allows tracking buy or sell orders in a simple-to-use interface.



Pepe | PEPE | UNISWAP V3

PRICE USD $\$0.0_{5}11$ | 24H CHANGE +23.66% | MARKETCAP (FDV) $487,012,171 | ETH LIQUIDITY $5,836,916 | DAILY VOLUME $27,877,084

Market Order

Buy | Sell

Select Wallet

SEND 0.05 ETH

0.1 | 0.25 | 0.5 | 1

RECEIVE 77218658.29722394 PEPE

ADVANCED

EXECUTE BUY →

TRADE FLOW

TYPE	AMOUNT	WALLET	AGE	TX
BUY	8.32 ETH	79934B	24s	
SELL	4.9 ETH	55ACe9	36s	
BUY	7.91 ETH	dA5969	2m	
BUY	4.47 ETH	d80a22	2m	
BUY	4.97 ETH	55ACe9	2m	
SELL	0.89 ETH	896EC6	3m	
BUY	9.88 ETH	816E8f	3m	
SELL	0.01 ETH	455eb8	3m	
BUY	0.07 ETH	399269	3m	
BUY	26.49 ETH	0dE157	4m	
BUY	0.18 ETH	065636	4m	
BUY	0.1 ETH	D4E196	4m	
BUY	0.49 ETH	4518A5	4m	

Interfaces like the one above show a time when developers are incentivised to create custom front ends for existing liquidity pools. It removes the need for launching a token or requiring people to park money in your smart contracts. Interface fees drastically reduce the entry barrier for smaller teams to launch DeFi front-ends and generate cash flow. But how will an interface build a moat? Why would users go to one wallet over the other? Network effects could be one way.

Of Network Effects

Think of Apple Pay. For those not in the know, it uses NFCs to enable transactions at your favourite cafe or restaurant. People switch over to Apple Pay because it is embedded well with a mobile device (the iPhone) they carry around all the time. You can use cards stored on Apple Pay for your in-app purchases (on the device), app subscriptions, and payments at local outlets. The number of places you can pay with Apple Pay makes it a compelling pitch.

Wallets in Web3 do not have such network effects today. For interfaces to charge more than what Uniswap does, effort needs to go into curating multiple applications into a single interface. Avocado by Instadapp is one instance of a venture pursuing such an opportunity. Backpack wallet also allows users to trade, stake and collect on-chain primitives directly from their interface.

In my view, interface fees will likely be how many wallets focusing on Web3 social users will monetise themselves when content becomes composable and user-owned. Unlike Facebook or X (formerly Twitter), Web3 social networks won't have sufficient user data to show ads. One way they could monetise is by charging a small fee on each user interaction, as Uniswap aims to do with their interface fees. This is a whole different rabbit hole, so we will explore that further in another piece.

Interface fees are not rocket science. They are also not a paradigm-changing innovation either. But a large protocol like Uniswap enabling them signals a point in time where protocols are beginning to take their business models more seriously. Much like how Blur disrupted the royalty model for NFTs, even whilst OpenSea could hold too much of the user-interface fees, signals that it is okay for a developer to charge for simply building a curated front-end.

This possibility of a developer having a revenue source to bank on whilst not taking on the risks of developing a protocol from scratch is fundamentally exciting.

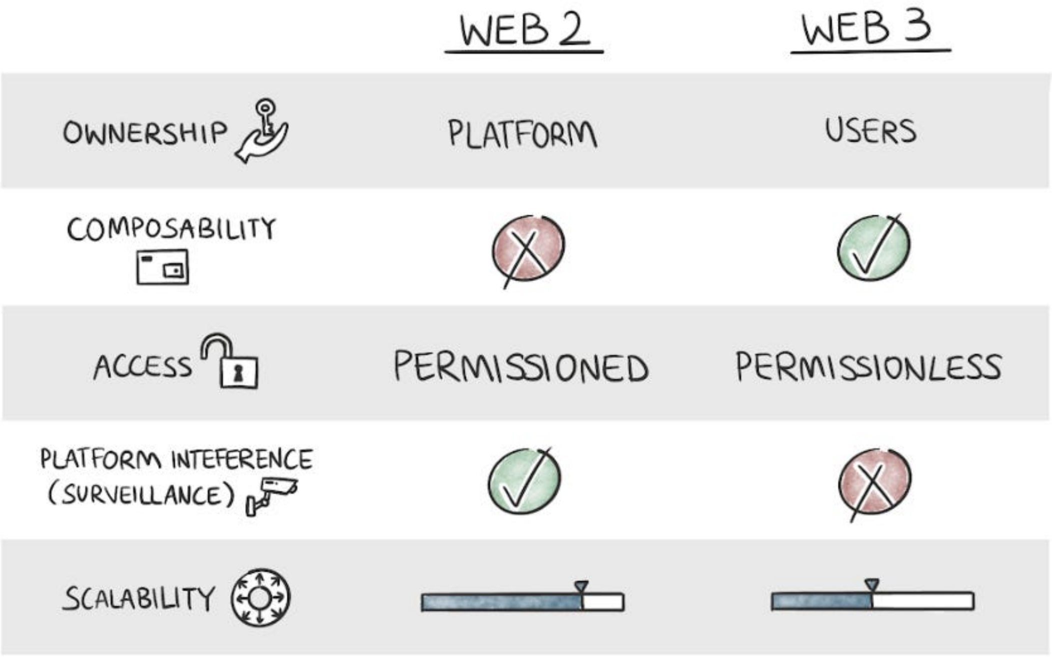
Is it a 0 to 1 innovation? Not at all. It is an incremental change that enables more developers to monetise earlier whilst building consumer-facing products. To me, that is exciting.

Currently reading Creativity Inc,
Joel John

Saurabh
decentralised.co

Zero to One

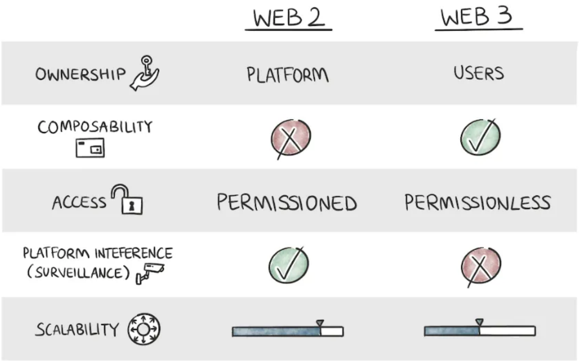
Scaling Web3 Social Networks



	WEB 2	WEB 3
OWNERSHIP	PLATFORM	USERS
COMPOSABILITY	✗	✓
ACCESS	PERMISSIONED	PERMISSIONLESS
PLATFORM INTEFERENCE (SURVEILLANCE)	✓	✗
SCALABILITY	▰▰▰▰▱	▰▰▱▱▱

Hey there,

We have been discussing Web3 social networks internally. A few applications are beginning to see traction. In today's piece, we won't go into the specifics of why it matters. We covered the key differences and a thesis for a new internet in the past here. What I want to focus on today is how Web3 native social networks can go from zero to one.



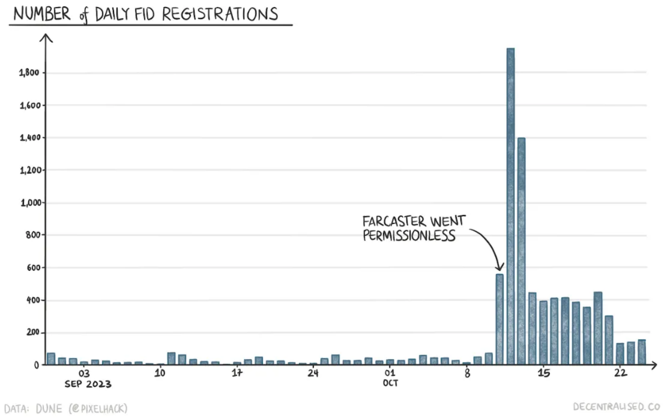
	WEB 2	WEB 3
OWNERSHIP	PLATFORM	USERS
COMPOSABILITY	✗	✓
ACCESS	PERMISSIONED	PERMISSIONLESS
PLATFORM INTEFERENCE (SURVEILLANCE)	✓	✗
SCALABILITY	▰▰▰▰▱	▰▰▱▱▱

A quick recap of the design differences between Web2 and Web3 native social networks

On October 11, Farcaster opened the platform to everyone. Developers could use the platform to build applications, and users could sign up without anyone's approval. I wanted to try out what an application built on Farcaster would feel like. I downloaded Warpcast, a microblogging application like X (*formerly Twitter*).

The first thing is it asks you for an upfront $1 per month payment, which is used for gas. My first reaction was that this step creates friction for an average user. After all, how many paid users does X have? ~640,000 out of 330 million active users is ~0.2%. But the fee is 1/8th of X and can be considered a feature, as it helps fight bots and keep things real. The good thing about this payment is you don't need crypto. You can pay in your local currency through the app store.

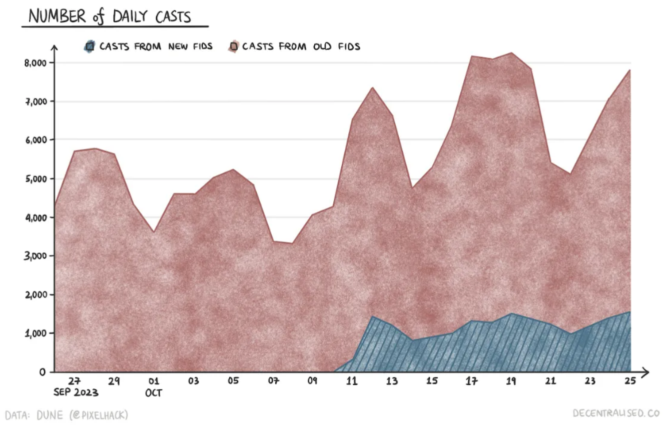
Once you get past the fee barrier, the experience is similar to Web2 counterparts (more on this later). I wanted to see how the metrics changed after Farcaster went permissionless, so I looked at the number of ID registrations and casts.



DATA: DUNE (@PIXELHACK)

DECENTRALISED.CO

The number of users registering on Farcaster shot up after October 11, and they contributed to ~20% of the new casts (posts) on the network. Farcaster has ~191k IDs registered compared to ~125k profiles on Lens. Note that Lens is not yet permissionless, although they are soon to be releasing a new version which will be. You can see how opening access to the app has impacted daily casts on the protocol in the chart below.



DATA: DUNE (@PIXELHACK)

DECENTRALISED.CO

A few questions stood out to me while using the app:

- Why do users keep going back to X?
- Why did Threads fail to retain users in the initial weeks?
- Why would anyone move from X to Warpcast? Or What can Web3 social networks do to onboard more users?

The following is a breakdown of how I believe social networks in Web3 will first imitate and then redesign incentive mechanisms on the Web.

Replicating Incentives

X's moats are network effects and incentives for creators. Network effects are straightforward. I go to X every day because the content is interesting to me. The content is interesting because the people I want to hear from are active there. The people I want to hear from are there because their incentives are aligned.

Two kinds of incentives exist for creators:

1. Direct, where X recently started sharing revenues with creators. In September, X paid out $20 million to its creator community.

2. Indirectly, as a creator, your audience is on X. When you try to move to a different application, it's unlikely that all your audience will move there unless there's a strong reason. It is because creators to audiences is a many-to-many relationship, not one-to-many. That is, you are not the only creator for your audience. So, your move doesn't guarantee that your audience will move.

When Meta launched Threads, users were excited about it for one weekend. After a few days of headlines around the demise of X (then Twitter), eventually, the migration tapered off. According to Similar Web, after its launch, the DAUs plummeted from ~49 million on July 7 to 10 million on August 7. A new application fights for users' attention with the incumbents.

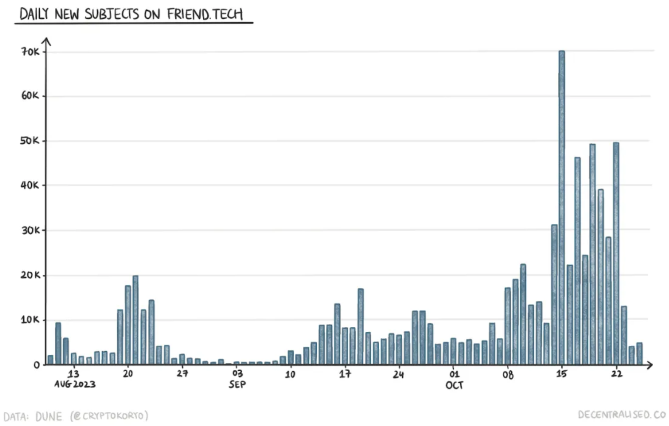
It offers novelty as a hook for users. As Chris Dixon once said, come for the tool, stay for the network. Threads could not bring out one character or feature over X (*and Instagram*) that resonated with users and, as a result, failed to take over X in terms of the number of users.

Threads wasn't the only competition for X. Mastodon, a decentralised social network built in 2016, started gaining traction in 2022 when Elon Musk bought Twitter. But the Mastodon UX wasn't intuitive. The growth spurt had been a flash in the pan. When a user joins the network, they have to join a server, which is an interest-based community. Managing and growing a user's social graph on the server is cumbersome.

> “
>
> When something feels like work without incentives, it is unlikely to attract a critical mass. The cost of switching from Twitter to Mastodon was too high for little gain.

Besides UX, Mastodon had an incentive problem. Servers usually have volunteer moderators who struggle to scale server capabilities due to the growth spurt. The non-profit nature of Mastodon meant that moderators had to ask for user donations. Although users foot the maintenance bill, server maintenance and moderation require time and energy, resources that are difficult to obtain for free.

Although user growth on Farcaster and other Web3 social ecosystems has been sluggish, Friend.tech (FT) offers clues for user onboarding. In over three months, FT has gained more than 800K unique subjects (users). Granted, the category differs from what platforms like Warpcast and Lenster try to achieve, but the drivers of success overlap.



DATA: DUNE (@CRYPTOKORYO)

DECENTRALISED.CO

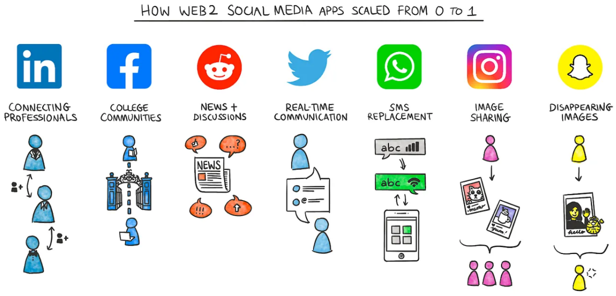
Users are flocking to FT, hoping for an airdrop. But airdrops are anticipated for almost every protocol and application. So, airdrops cannot be the only reason FT is so far ahead of others. Another obvious answer is they have the backing of leading VCs like Paradigm. But VC backing can only take you so far. In my view, there are two reasons for FT's success.

1. **Using existing Web2 social graphs.**
   FT used X for onboarding users. It is safe to say that out of all the Web2 social media applications, X has the most active participation from crypto natives. Using X to let users borrow their social graph has immensely helped FT to reduce user onboarding friction. It allows FT to piggyback on X's network effects.

2. **Gamification.**
   Call it speculation/gamification/incentivisation, FT hooked users. When there's money involved, attention typically follows. What percentage of FT users are actually there to be connected to people they follow is up for debate, but it's clear that FT has managed to grab and retain attention so far. Users may go to FT to trade shares of influencers but keep using it to chat with them occasionally.

Returning to the third question of what Warpcast can do to attract more users, there are a few learnings from the hits and misses discussed above.

All About The Hooks



Every successful social media application has had its unique feature or character that helped with the cold start problem – no users, so no good content; no good content, so no users. It can be considered a "*cyclical loop of boring*", as anybody who has spent time on emergent Web3 social apps would have seen.

With the benefit of hindsight, most social networks tapped into user behaviour that was emergent but not captured at scale yet. X, for instance, was initially a text-based social network. You could send texts (*through a mobile network*) to have them show on a feed, which is why the platform originally had a 140-character limit.

As a medium, it allowed more users to share relevant news in shorter spurts than traditional media. Reddit, on the other hand, was a reinvention of Google in a loose sense. Where Google indexed pages by rank (hence the term PageRank), networks like Reddit and Hacker News used human curation (upvotes) as a measure of how user submissions should be ranked. This transfer of the filtering mechanism from Google's algorithm to human upvotes was powerful at a time when content was just exploding on the internet.

Similarly, WhatsApp launched when many still communicated through text messages or the BlackBerry Messenger. Using the internet for text messaging through a mobile interface was not as common then. For a consumer to switch over, the value proposition was simple: You save on how much you would pay for texts.

Every social network scales with a value proposition that feeds into a certain user behaviour. To a certain degree, Friend.tech managed to replicate this model for success. The team enabled vanity (*like Instagram*) by giving value to a person's share and allowing users to trade it. They combined a person's need for validation with an industry's desire to speculate.

> “
>
> In our view, the next generation of social networks (in Web3) will need to have a strong hook that taps into an existing human behaviour or emergent user need.

When I was using Warpcast, most of it looked like an X clone. But the bar on the left side is cleaner and has channels. These channels are pre-curated communities of sorts. Users can tweak channels as per their interests. Instead of ‘onboarding creators’, if Warpcast can help create niche channels unique to the platform, the likelihood of some users getting hooked increases.

Once an initial base of loyal users is created, scaling becomes easier. Wield and Farquest, similar to Rabitthole and Layer3, can make the discovery easier for users.

Users typically use applications when people they know also use the same application. It is difficult to judge which Web3 social application will be the one with critical mass. Aggregators can encourage users to be application-independent. Firefly and Yup are creating a platform interface that allows users to interact with their social graphs across platforms like X, Threads, Farcaster, Lens, Bluesky, etc.

The internet experimented with RSS (*Really Simple Syndication*) feeds as a means of distribution. RSS feeds allow content to be distributed without users going to individual websites. If a user has an RSS reader installed, the reader checks all the feeds the user has subscribed to and automatically brings updates to the user. Although it is efficient, it is limited to text.

RSS feeds are less user-friendly than applications like Facebook. They are also decentralised, so a platform or company has little control over the content broadcast via its sites. So, the adoption of RSS feeds has been limited. New aggregation models are significantly more user-friendly compared to RSS feeds. They are more collaborative.

Allowing users to sign up with X or Facebook helps with two things: the friction of switching is reduced, and it helps with network effects. FT is an example of how using existing network effects can help. While FT leverages X, Song.Tech is using Spotify to bootstrap its user base. We will likely see multiple social apps trying to replicate these models in the coming months.

The reason why these apps make use of existing social graphs and borrow elements of UX that already exist is to obfuscate the complexity of the new tech stack. When paradigms change in technology, we take elements from the previous era to make the transition easier for the user.

Redesigning Incentives

We have been internally debating whether Web3 is about ownership or changing incentives. Most users do not care about custodying their assets or identities. It is a burden they would instead outsource. What they care about are incentive mechanisms that directly impact them. Web3 design principles offer a way for users to simultaneously own their identity/data and change the incentives on social networks.

For instance, social networks have historically leaned towards aggressive bickering because it is a good way to keep users hooked longer. The headlines in our newspapers have become more negative in the past few decades because fear keeps us returning and buying more of the newspapers. The incentives for media in the last century have been to evoke emotions that can be bad for the consumer.

Quite recently, a documentary on Juul dropped on Netflix. For quite a while, people looked towards it as an alternative to cigarettes. Then, the regulator clarified that it can release considerably higher amounts of nicotine into the human body. Social networks today have a similar impact on the human mind. And the regulators might be sleeping at the wheel.

We need them for the sake of our democracies and free speech. The world is better off with more people voicing their opinions in the great town square that is the internet. But if the incentive mechanisms are designed to leave users feeling worse off, we must consider how to fix them.

Blockchains being payment rails means Web3 social networks can reward users globally without needing platforms to tap into user data or run advertisements. A social network that focuses solely on allowing users to be compensated (in stablecoins) for the content they post has value.

It is not here yet, but it will emerge sooner or later as individuals realise that many social networks leave them worse off mentally. Much like the food we consume, the ideas we entertain and source through social networks have a bearing on our minds. For us, the question is — does changing the incentive mechanisms for social networks pave the way for a better internet? Do Web3 social products have a shot at doing that?

It is a big vision to build towards. But a worthy one that goes beyond speculating on tokens.

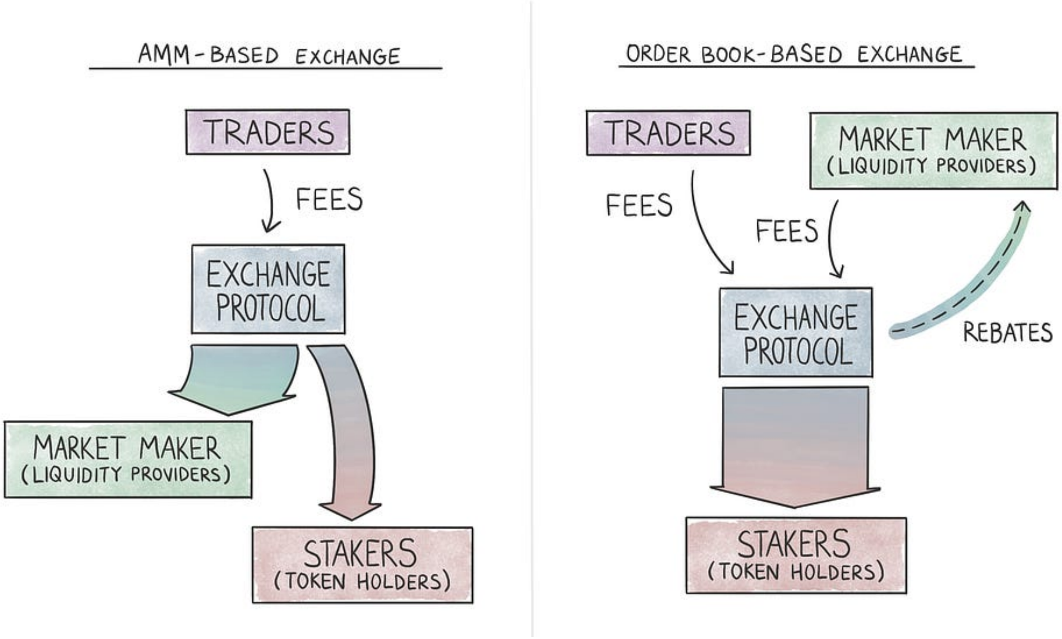
Signing out,
Saurabh

Acknowledgment: Conversations with Jakub and Mitch helped me crystallise ideas for this piece. I'm grateful to both for spending time with me on calls to discuss all things Web3 Social

Saurabh
decentralised.co

On dYdX

When apps become chains.



Hello!

A small note before we begin. Nothing written in this piece is financial advice. I am just nerding out some elementary napkin calculations and commenting on what I think. I would appreciate inputs on the model used if you are a fellow finance enthusiast.

My interest in finance keeps me looking for news from DeFi projects. On October 24, dYdX announced that their appchain was live. In the following days, dYdX proposed enhanced utility of the DYDX token.

What changes with the launch of the chain? The token (DYDX) gets three utilities instead of one:

1. Governance – DYDX is already the dYdX application's governance token. It now expands to be the governance token for the chain too.

2. Gas token – All the gas fees paid on the new chain will be in the DYDX token.

3. Security – As a POS-based chain, DYDX will be staked to secure the chain. As a result, stakers will get staking yield. The upside here compared to other staking is that even the fees accrued by the dYdX application (in USDC) will be distributed to stakers (and validators).

It is meaningful because, in the last 30 days, the dYdX exchange has generated over $6 million in fees. The figure is at $65 million YTD. The fees will be distributed to token holders. But how does this differ from an exchange like Uniswap?

Unlike most DEXs, dYdX is an order-book-based exchange. It matches order books off-chain, whereas most DEXs are automated-market-maker-based (AMM-based). A critical feature of providing liquidity to AMM pools is that the liquidity provider (LP) invariably ends up holding more inventory of the token that devalues compared to the other token in the pool.

Let me explain.

- AMMs are typically based on the A*B = constant model, meaning the product of values (price times quantity) of the two tokens in a pool remains constant.

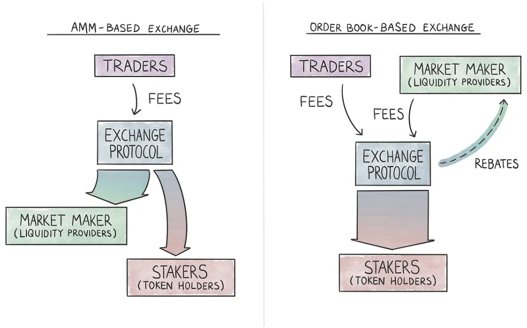
- Say an LP adds $100 worth of tokens X and Y in a pool with a total liquidity of $1000 (after the LP adds), a 10% share of the pool. Assume the price of X is $1, and Y is $5, and the LP added 50 X and 10 Y. The pool has 500 X and 100 Y.

  Product of values of X and Y = ($1 * 500) * ($5 * 100) = 250000.
  Each Y is worth 5 Xs.

- After a few trades, assume the pool now has 1000 X and 50Y tokens. The prices are now $0.5 and $10, respectively, i.e., each Y is now worth 10 Xs. Notice the product is still ($0.5 * 1000) * ($10*50) = 250000. But the LP now has 100 X tokens *(10% of 1000)* and 5 Y tokens *(10% of 50)* with a total value of $100 instead of 50 X and 10 Y tokens (value = $125). So, the LP has lost $25 by adding liquidity to the pool.

In traditional markets, where exchanges are based on order books and derivatives markets are mature, market makers have much more flexibility around hedging. In the AMM design, hedging is constrained. As a result, providing liquidity on AMM-based exchanges is more difficult (*and, thus, risky*) compared to orderbook-based exchanges.

Naturally, AMM-based projects must offer more incentives to LPs. Without liquidity, there are no traders. And there are no fees or revenue without traders. So, exchanges end up sharing a significant chunk of fees with LPs.

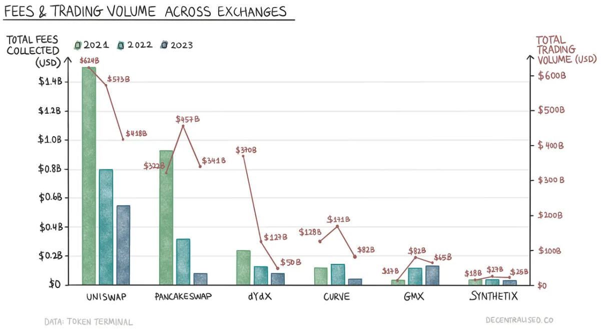


On the other hand, since MMs on order books have more freedom to hedge their inventory, they don't need as many incentives from the exchange. Their incentive lies in earning the spread between the bid and ask prices. For similar reasons, we saw Hubble Exchange move from AMM-based to orderbook-based designs. Often, exchanges compensate market makers via rebates to incentivise deeper liquidity.

Don't get me wrong: I'm not saying that the order books are better than AMMs in an absolute sense. Orderbooks require active participation and an off-chain component. AMMs are fully on-chain (so they are more transparent) and are perhaps a better choice for LPs who aren't as active as traditional market makers.

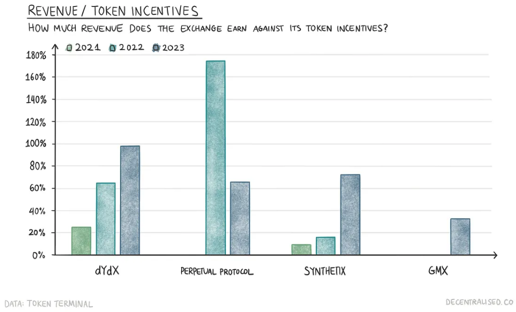
Benchmarking Peers

The easiest way to see how DEX peers have evolved over the years is to see how much trading volume they supported and the fees they earned. Notice how spot exchanges (like Uniswap and Pancakeswap) dominated. Read this piece if you want to read more about DeFi derivatives.



The order book design allows dYdX to share all the fees with token holders and validators. This is why $75 million annual fees earned by dYdX differ from those earned by an AMM exchange. While dYdX earns fee revenue, it also spends DYDX tokens as incentives, as almost all applications do. And how does that impact applications?

The chart below compares how much token incentives exchanges have given out compared to the revenue they earned: that is, revenue generated for every $1 spent on incentives.



Every exchange needs to incentivise liquidity in some manner. Some do it with token incentives, and others do it via sharing fees with LPs.

In the chart above, ~180% for Perpetual Protocol in 2022 suggests that for every $1 they spent on incentives, token holders received $1.8 in revenues. After the recent overhaul of Synthetix, more volume started flowing through it, and it started earning more fees. As a result, for every $1 on incentives, revenue increased from ~$0.2 in 2022 to $0.8 in 2023.

GMX has a low ratio because most of its fees are shared with LPs instead of token holders. So, for GMX to give value to its token holders, either the fees need to increase a lot, or the proportion of fees shared with token holders needs to grow.

Valuing dYdX

Before delving into the valuation details, I must emphasise that all valuation models are inherently flawed. Some are more flawed than others, and this one is probably more flawed. However, I resort to this exercise because it helps me think through different projects and compare the ones belonging to the same sector using the same metrics.

The first step was to choose which models apply to a DEX like dYdX. Usually, the model depends on how granular the data is. For equities, one of the most famous valuation models is the discounted cash flow model, popularly known as the DCF model. The crux of the model is as follows:

1. It gets into the specifics of every line item on the revenue and expenses side by trying to project their growth a few years later. In the end, it assumes a terminal growth rate and calculates the values for line items using the sum of an infinite arithmetic progression series.

2. It then goes into the free cash flow at the end of each year and for the terminal year.

3. It brings the calculations back to today by using the time value of money, usually known as discounting. This is the present value of the company based on its future cash flows.

Every line item you project into the future invites inaccuracies and questions about your growth numbers. The more broken down revenue and expense streams into several line items, the better the model. How you read between the lines of annual reports and the quarterly/yearly guidance the company provides determines the model's accuracy.

Price targets stemming from these models (or from any model) should be taken with a grain of salt because the exercise is more art than science, in my view. If you are interested, check out this video from Aswath Damodaran (one of my go-to valuation resources) to understand how complex it can get.

Using DCF for any of the projects in Web3 is difficult because we don't have data sources that are granular enough. I imagine we can indulge in these models a few years/months out based on the work data sources like Token Terminal are doing.

Anyway, the lack of revenue and expense line items to expand on meant I had to resort to a much simpler approach of using multiples. Since I'm valuing the DYDX token, I want to understand what the token holder gets for staking the token. So, I looked at the **price-to-revenue multiple (P/R)** at the end of 2024 using data from Token Terminal. The P/R ratio suggests how the market prices the exchange for every dollar of revenue going to token holders.

1. I annualised the numbers for 2023 and assumed different growth rates for the trading volume to arrive at the 2024 value. For example, the 60% change in the 2024E column assumes that the trading volume growth on dYdX is 60%.

2. The fees/volume number assumes the overall fees as a percentage of the volume. This is how I arrived at the fees for 2024.

3. dYdX intends to pass on all fees to stakers or validators. So, this becomes the revenue in question.

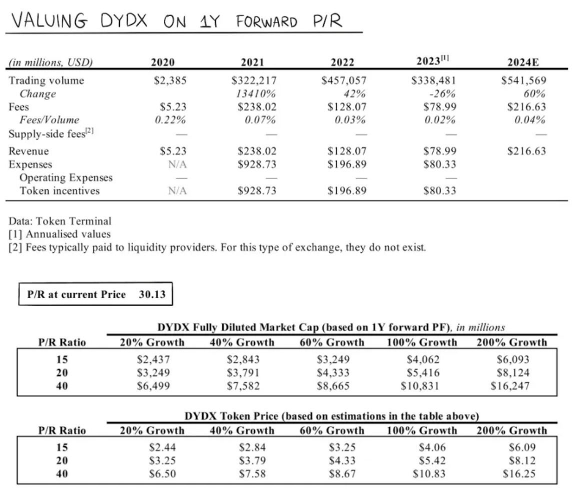
4. The second table shows different growth scenarios in point 1 – ranging from 20% to 200%. Naturally, the higher the growth, the higher the value.

5. In 2023, the price (the fully diluted market capitalisation) to the revenue multiple is 30.13. This number suggests how much premium the market places on revenue earned by dYdX. The second table shows the value based on three multiples – 15, 20, and 40. These are arbitrary numbers surrounding the current multiple.

6. The third table calculates the price per token by dividing the respective values in Table 2 by the total number of tokens.

7. I perform a similar exercise for GMX to understand how GMX fares against dYdX. Note that GMX fees get split into two parts –

LPs (since GMX is based on AMM) and token holders. For a like-to-like comparison, I only consider the component routed to GMX token holders.



VALUING DYDX ON 1Y FORWARD P/R

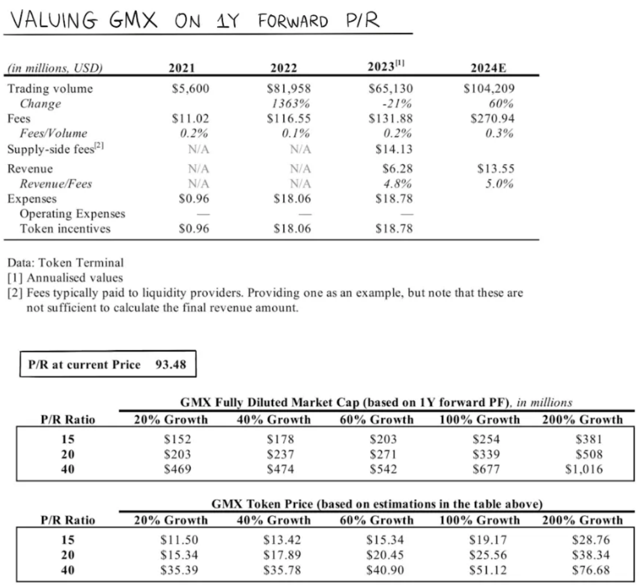
(in millions, USD)	2020	2021	2022	2023[1]	2024E
Trading volume	$2,385	$322,217	$457,057	$338,481	$541,569
Change		*13410%*	*42%*	*-26%*	*60%*
Fees	$5.23	$238.02	$128.07	$78.99	$216.63
Fees/Volume	*0.22%*	*0.07%*	*0.03%*	*0.02%*	*0.04%*
Supply-side fees[2]	—	—	—	—	—
Revenue	$5.23	$238.02	$128.07	$78.99	$216.63
Expenses	N/A	$928.73	$196.89	$80.33	
Operating Expenses	—	—	—	—	
Token incentives	N/A	$928.73	$196.89	$80.33	

Data: Token Terminal
[1] Annualised values
[2] Fees typically paid to liquidity providers. For this type of exchange, they do not exist.

P/R at current Price 30.13

	DYDX Fully Diluted Market Cap (based on 1Y forward PF), *in millions*				
P/R Ratio	**20% Growth**	**40% Growth**	**60% Growth**	**100% Growth**	**200% Growth**
15	$2,437	$2,843	$3,249	$4,062	$6,093
20	$3,249	$3,791	$4,333	$5,416	$8,124
40	$6,499	$7,582	$8,665	$10,831	$16,247

	DYDX Token Price (based on estimations in the table above)				
P/R Ratio	**20% Growth**	**40% Growth**	**60% Growth**	**100% Growth**	**200% Growth**
15	$2.44	$2.84	$3.25	$4.06	$6.09
20	$3.25	$3.79	$4.33	$5.42	$8.12
40	$6.50	$7.58	$8.67	$10.83	$16.25



VALUING GMX ON 1Y FORWARD P/R

(in millions, USD)	2021	2022	2023[1]	2024E
Trading volume	$5,600	$81,958	$65,130	$104,209
Change		*1363%*	*-21%*	*60%*
Fees	$11.02	$116.55	$131.88	$270.94
Fees/Volume	*0.2%*	*0.1%*	*0.2%*	*0.3%*
Supply-side fees[2]	N/A	N/A	$14.13	
Revenue	N/A	N/A	$6.28	$13.55
Revenue/Fees	N/A	N/A	*4.8%*	*5.0%*
Expenses	$0.96	$18.06	$18.78	
Operating Expenses	—	—	—	
Token incentives	$0.96	$18.06	$18.78	

Data: Token Terminal
[1] Annualised values
[2] Fees typically paid to liquidity providers. Providing one as an example, but note that these are not sufficient to calculate the final revenue amount.

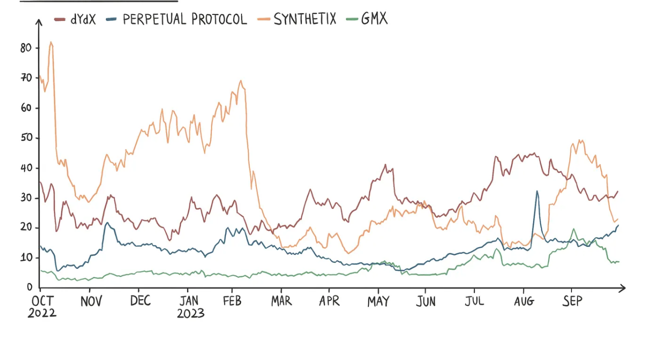
P/R at current Price 93.48

	GMX Fully Diluted Market Cap (based on 1Y forward PF), *in millions*				
P/R Ratio	**20% Growth**	**40% Growth**	**60% Growth**	**100% Growth**	**200% Growth**
15	$152	$178	$203	$254	$381
20	$203	$237	$271	$339	$508
40	$469	$474	$542	$677	$1,016

	GMX Token Price (based on estimations in the table above)				
P/R Ratio	**20% Growth**	**40% Growth**	**60% Growth**	**100% Growth**	**200% Growth**
15	$11.50	$13.42	$15.34	$19.17	$28.76
20	$15.34	$17.89	$20.45	$25.56	$38.34
40	$35.39	$35.78	$40.90	$51.12	$76.68

Another way to compare futures DEXs is to look at how much users are paying in fees to these platforms (either to LPs or to token holders) with respect to their fully diluted market capitalisation. Currently, DYDX has the highest PF ratio among the four leading futures DEXs. This means DYDX is more expensive than other DEXs. In other words, the market is attaching more value to the fees dYdX earns compared to its peers.

PRICE TO FEE RATIO



DATA: TOKEN TERMINAL

DECENTRALISED.CO

How does this compare to centralised finance (CeFi) exchanges? Coinbase has a revenue (*a good proxy for DEX fees*) of $2.58 billion with a market cap of $17.46 billion and a price-sales (*P/S, analogous to the P/R or P/F ratio mentioned above*) ratio of 6.76. A more established exchange, Nasdaq has a market cap of $24 billion against $4 billion in revenue, a P/S of 4.

As companies and industries mature, growth tends to taper off and become steady. Usually, the premium attached to revenue multiples arises from the fact that there's room to grow. As DeFi and crypto are still early in their life cycles compared to more traditional companies, they naturally command a higher multiple in anticipation of growth.

Why is dYdX commanding a premium? There are a few reasons in my mind.

- dYdX is the only perpetual futures DEX with order books. This means the exchange can afford the luxury of sharing all the revenue with token holders. In comparison, AMM-based DEXs have to share fees with the LPs. Token holders get a share of the fees at best.

- Similar to Uniswap for spot trades, dYdX is an established brand for futures trading. The brand is an intangible asset that holds value.

- The market is likely speculating on what is next for dYdX. I take a stab at this in the next section.

The Future

Recently, the Chicago Mercantile Exchange (CME) almost caught up to Binance regarding open interest (OI) on the Bitcoin futures. This is a good gauge of institutional interest. With the imminent Bitcoin ETF, this interest will likely grow. If 2021 is any guide, DEXs will be beneficiaries of the spillover into DeFi.

When dYdX launched a chain, they mentioned they were primarily focused on DeFi derivatives. With this new chain, dYdX is uniquely positioned to create a Deribit-like experience. dYdX already has perps based on order books. Assume they build options alongside perps with portfolio margin enabled for both perps and options. We will be looking at a DeFi-native alternative to Deribit. One that is more transparent and where no customers can be given special treatment, thus not allowing unknown counterparty, liquidity, and insolvency risks to creep into the system. Remember Alameda? We could avoid that disaster from happening yet again.

Aevo (*Ribbon Finance*) already has options and perps based on the off-chain order book. The product is similar to Deribit but lacks liquidity. Compared to dYdX's 24H volume of $869 million and $309 million OI (*open-interest*), Aevo only has $5.7 million daily volume and $4.7 million OI. dYdX is already ~100X bigger.

Given Aevo's capital efficiency (*as it allows users to trade futures and options through the same capital*), it may not need 100X OI to support 100X volume. At the moment, Aevo is a superior product but lacks liquidity. dYdX's leading position depends on whether it can launch a suite of products to evolve into a derivatives ecosystem before Aevo manages to attract 100X liquidity.

Both dYdX and Aevo are independent app chains, allowing them to get more creative with how the token fits into their offerings. While dYdX is a Cosmos-based chain, Aevo is an Ethereum rollup. Both are in the early stages of developing their respective ecosystems.

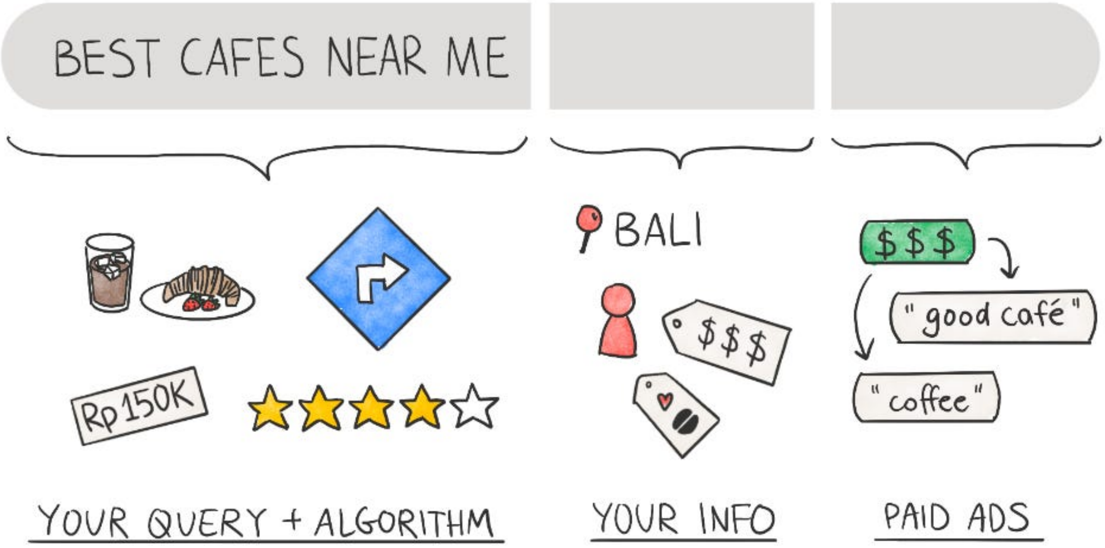
If they are successful, are other successful applications like Uniswap also considering launching their chains? If yes, will it be as an L2 on Ethereum (like Aevo) or a completely independent chain? How does the bridging ecosystem evolve to enable a smooth flow of capital and information among these independent appchains?

These are just a few questions I've been thinking about since dYdX's announcement, and I will write about them when I have answers.

Joel John
decentralised.co

Matching Engines

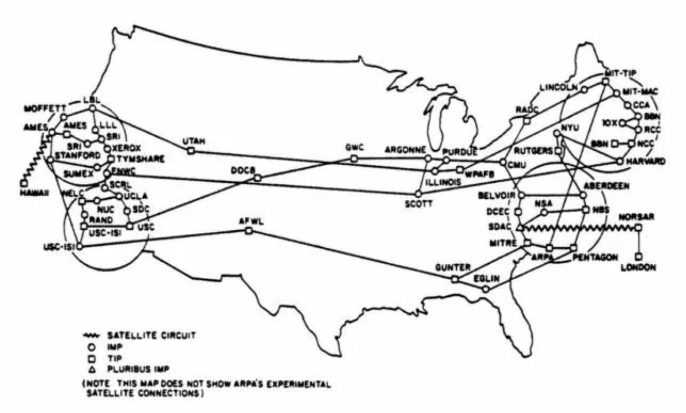
Context as leverage



Hello,

The concept of a matching engine fascinates me. It is the part of an exchange that determines how orders are matched when a user places an order. The speed and quality of a matching engine determine how often people trade on the exchange it powers. If an engine lags, inefficiencies will creep into the market. For instance, traders running bots may be unable to place orders fast enough, or there may not be enough liquidity for large orders.

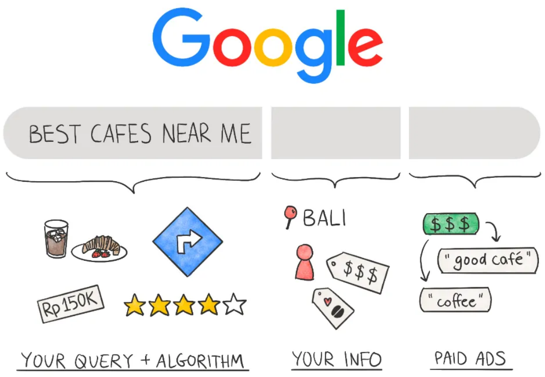
I like the concept because matching engines process data from the buy and sell side millions of times daily. And in doing so, they generate a portion of the trade volume in revenue for the exchange. Scaling matching engines enables orders from all kinds of traders to come through and settle without hiccups. Think of them as traffic lights for modern-day financial transactions. Platforms on the web can be imagined as matching engines.



A visualisation of Arpanet as a graph. Source

The internet is a graph that maps out content and services. In the 1980s, this graph consisted of a handful of universities and defence research personnel, as shown in the visual above from Arpanet. As the number of participants on this graph scaled, we needed mechanisms to recommend and match queries with the right participant.

Search engines like Google are 'matching engines' that match a user's intent with relevant information on this graph. There is tremendous value in becoming a matching engine that recommends the right content, and that value is reflected in Alphabet's market capitalisation.



Nightjar cafe is likely the best cafe near me.

You search Google for '*best cafes near me*', which becomes the equivalent of a market order on an exchange. You are querying for information, much like a seller is putting an intent to sell an asset. Google then looks through its database of information and surfaces cafes relevant to you. To rank the information it surfaces into a list, Google would consider your location, transaction history, reviews from locals and advertisement dollars from sponsors.

Like an exchange, the buy side of this order consists of firms that have paid to be on the list and have earned their spots there.

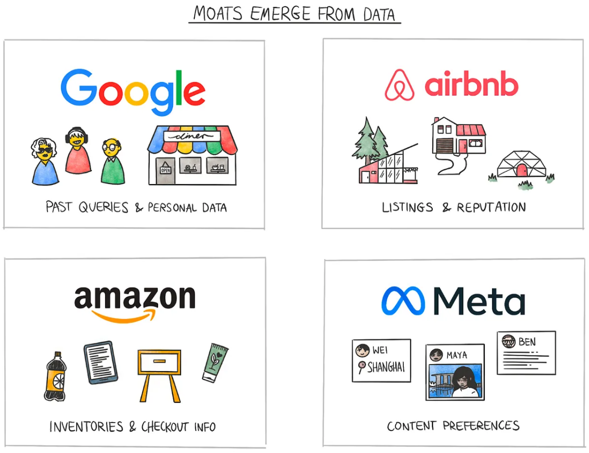
Given enough labour and computing power resources, large recommendation engines could be developed if the users have the intent. On social networks like X, formerly Twitter, matching engines (for advertisements) have never taken off at scale because the users' intent is not to make purchases. It is to consume content. Erstwhile twitter optimised to distribute good content that could retain users for longer.

Platforms like TikTok became popular because of how sticky they could make a content feed with the very small amount of information a user passes on to the platform. Google has an incentive to balance how finely they match your query. Too many advertisements, and users would not trust them any more than they trust Craigslist today.

Contextualising content that is specific to you whilst balancing commercial interests is Google's fine art. In some sense, they have become a matching engine where liquidity consists of human attention and indexed content from the internet.

Humour me for a bit longer. Much of the internet today functions like matching engines. Amazon matches consumers with product inventories. Instagram matches creators with an audience base.

X matches users with regrets about going online. Tinder or Bumble matches users with potential partners, experiences or regrets. Surely, there are operational aspects to these businesses. But at their core, they match supply and demand, like a matching engine at an exchange.



Moats for these matching engines come from the proprietary data they own. For instance, Uber has the largest database of drivers in some cities. Airbnb has a closed database of properties: the reviews they receive and historical data of how many properties open up in each city at different seasons. The data is the secret sauce based on which businesses can monetise themselves in myriad ways. It is an asset developed through the scale these businesses have reached and the longevity with which they function.

I will resist the urge to go into large language models (LLMs) and AI for now, but my point is that **the closed-off data sets these platforms have is their moat**. Every once in a while, aggregators or platforms interact with one another. For instance, you can book an Uber from Google Maps in some regions.

So, interoperability of assets – be they drivers, products or inventories of houses – exists today. **But they are owned by the businesses that maintain the inventory and can be shut off at will.** The moats of these businesses exist in closed graphs that are privately owned. Quite recently, Reddit was mired in controversy for restricting API access to third-party applications that showed content from the platform.

Open Graphs

Smart contracts enable decentralised matching engines on the open graphs that blockchains are. Unlike data on centralised servers, blockchain data is accessible to anyone. Uniswap is a matching engine for assets to convert from one to another. Aave is a matching engine that holds an asset in exchange for giving another as a loan.

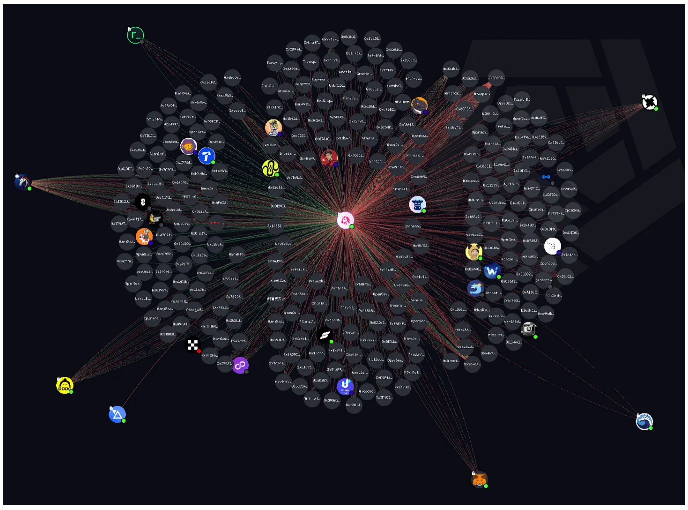
These matching engines work without human intervention or external data because their logic is pretty simple. Aave checks if a loan amount is collateralised for the right amount. Uniswap's smart contract sends tokens to a pool and withdraws assets based on the AMM formula used.

These engines provide rich public data that providers like Nansen index. At scale, you can take data from matching engines like Aave and Uniswap to provide historical context. Labels on Nansen are assets developed using data from public matching engines. How do they work? You study a user's behaviour over time to track their historical P/L. Wallets that were early to an NFT and held a token through a bear market or early to new smart contracts are considered 'smart money'.

Historically, the demand side for such context came from traders who wanted to study other traders' activities. Knowing a large fund is selling a token or using a smart contract provides a tactical advantage when managing millions of dollars online. So service providers have considered DeFi the core market for building context and data sets. I have written at length about this in *The Data Wars.*

The incentives to retain and continue using a wallet have been relatively low. For instance, you use the same Uber account for years because your reputation determines the quality and pace of service you receive. A low rating could mean worse drivers for you. On Airbnb, hosts check your past bookings to see if they'd want to open their house to you.

Even in games like GTA 5, being a bad player that goes around killing other players in a server (*called griefing*) gets you put in a server with other griefers. Your reputation holds value in the digital world, even when pseudonymous.



The image above from Arkham Intelligence is a representation of the open-graphs blockchain data enables. It shows the number of swaps from associated apps like Metamask, DODO, Paraswap and 0x protocol. Developers can identify, target and study transactional behaviour of anonymous wallets interacting with Uniswap

The incentive structures for blockchain applications have historically skewed towards anonymity for the average user. When spinning a new identity is as easy as clicking a button and there are no incentives to retain a wallet, we end up with many wallet addresses with scattered context. This is the crux of what limits Web3-native apps to grow beyond the crypto market. Applications in the industry face challenges in two unique ways.

1. Anybody can query a user's historical behaviour with a product by querying blockchain data. No competitive advantage comes from privately storing information the way Meta or Alphabet does today.

2. Products generally lack context that goes beyond on-chain data about their users. Tools like ArcX are beginning to capture user information from browsers, but we are restricted in the nature of applications that can be built, as user information is often not captured.

Don't get me wrong. There are some relatively novel solutions. For instance, Passport by Gitcoin allows a user to tie their real-life identity to a wallet. So, you could hypothetically have an AML-KYC'ed user on a perpetual exchange that uses a smart contract to match orders. Or you can use Worldcoin for a network of ~3 million users who have proved they are humans. In other words, the primitives we need to have a network of users with verified identities exist here and now today.

But you don't have much when you look at the supply side of applications that can cater to such users. Users have no incentive to verify their identity and be onboarding themselves.

To summarise :

1. Blockchain applications have historically been open graphs of economic interactions.

2. Smart contracts enable applications to become decentralised matching engines.

3. Users are not incentivised to add context to their economic activity on-chain.

4. Applications are restricted in what they can offer users due to the lack of context they have on users. This lack of context translates to an absence of moats among products built with open-source code especially if their communities have rallied around a token.

Due to this, the nature of the applications we build is optimised for low trust. Need a loan? Yep, you will need excess collateral for that. How about an asset swap? Sure, you need to be able to provide the exact amount for it. Wish to collect an item on a social network? Cool. Send in enough gas fees to mint the NFT and send it to your wallet.

The emergence of context at the periphery – through providers like Passport or Gitcoin – will soon enable a new generation of matching engines. And unlike DeFi or NFTs (which are huge on their own), this new generation of applications will potentially become what I consider 'Internet-scale'. There will be a time when the use cases enabled by blockchain applications become relevant for the entirety of the web.

What would that look like, and how do we reach it?

Internet Scale

I was studying how transactional systems scale and saw a recurring pattern. Almost all of them initially focused on a dense network before they grew exponentially. Consider Visa, for instance. In the early years, they sent out some 60,000 unsolicited credit cards to a population of 250,000 in California.

By having ~25% of the population own credit cards in a region, they could convince some ~20,000 merchants to begin accepting Visa for payments. Keep in mind the geographical density of the consumers is what drove the merchants to adopt Visa. If the users were distributed worldwide, it would be like crypto today: too small a market for a merchant to care about.

When Stripe began making online payments easier, it started relying on Y Combinator's network of startups to go from 0 to 1. This was despite being in touch with both Elon Musk and Peter Thiel as investors. Y Combinator helped the startup find its initial group of users.

You had a variation of this with Web2 native social networks, too. Facebook launched with a geographic focus on students from Harvard. Y Combinator was critical for Hacker News' growth in the early days. Alexis Ohanian from Reddit admitted to creating fake profiles on Reddit during its early days to signal activity on the platform. Without a user base, focusing on specific niches and mimicking activity becomes crucial to attract and retain users.

Web3 user accounts are public by default, and payment information is easily available to everyone. **Moats in the industry would come from social networks that can build additional layers of context on top of the transactional data**. What would that look like? Much like how Visa and Stripe had to focus on geographical density, Web3 social networks would have to look at niche-based density to scale.

These use cases must appeal to a large user base without making an incumbent feel deeply entrenched. Think, for instance, of Google Maps—a large use case with no strong incumbents. *(Yes, GPS existed, but mobile-based mapping was not free).*

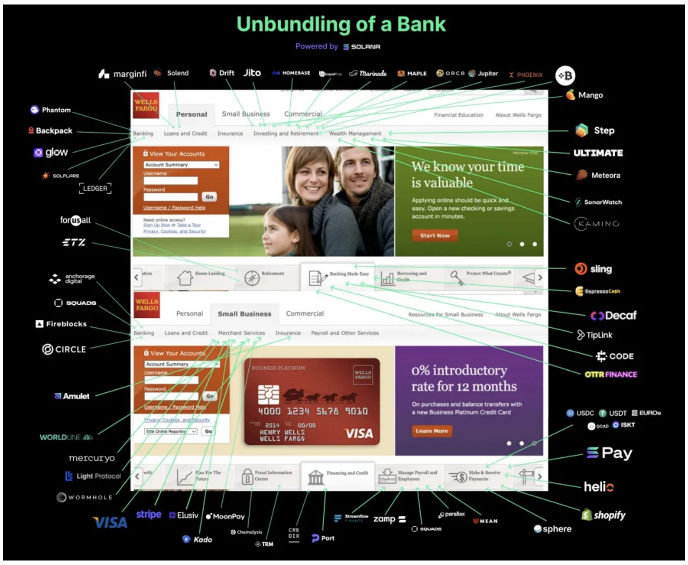
When you think of Web3 payment networks in comparison, most products struggle to differentiate themselves due to two factors:

1. The core payment experience on Ethereum or Solana is excellent on its own. Transacting

through a centralised provider often feels worse off than just using a wallet for a stablecoin transfer.

2. Startups struggle to differentiate themselves if payments (or transactional products) are the only USP. This is partly why there is a sea of dead DAO tooling startups.

One instance of a business I noticed in the wild providing ‘value’ beyond payment settlements is Request Finance. It is a simple invoicing product that allows users to collect invoice payments in stablecoins. I find it interesting because the product also has a repository of vendors on top of publicly available payment data (*from wallet addresses*).



Building context on users will be crucial to unbundling a bank using Web3 primitives. The image above from Yash Agarwal, is a good depiction of how Web3 alternatives are slowly serving the functions of a bank.

In such a case, blockchain data (of payments) with private context (on vendors and their relationships) built through providing a service (its invoicing product) helps the business develop a layer of context that is differentiated and unique to it. Whilst I’m not sure if the team plans on expanding to a marketplace, it is well within the possibility that they could build a repository of the best service providers, advertisers and DAOs using customer data they have access to.

In fact, they could even expand to offering lines of credit to platform users as they can see the frequency and amounts with which people are paid.

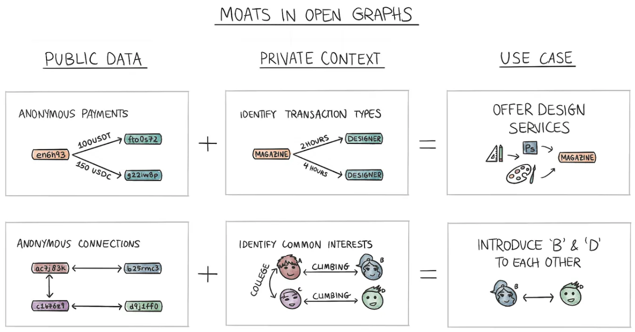
Combining user data from a blockchain and internal data sets from a service will likely enable the next generation of blockchain-native apps to scale. And much like we have with Web2, they will become matching engines at scale. In the example above, I presume that Request could expand into a marketplace model with a fintech component. However, most businesses are not there yet. The TAM of vendors and service providers in crypto is relatively miniscule.

Context Machines

Large businesses on the internet inevitably transit to enabling transactions on their products. Facebook, for instance, went from being a social network to having its own marketplace. In 2021, storefronts by the platform enabled 250 million users to transact with over a million shops. Apple went from being a hardware manufacturer to issuing its credit cards. This occurs because having context on user's financial behaviour makes it far easier to monetise the data you already hold on them.

As Saurabh wrote in our piece titled 'Zero to One', Web3 social networks might struggle to attract a critical mass of users because the incentives don’t exist for a normal user on the internet to port over. However, we have primitives that allow the identity of individuals to be verified far easily than on a Web2 platform.

For instance, a business that has context in the form of AML/KYC and financial history (from traditional sources like a bank) on a user, could offer undercollateralised loans to an individual. Today, when you use an app like Wally (*a personal favorite*), you give your spending habits to an app. What if it could be used to offer you credit from a protocol like Aave at better rates?



Collecting user data directly and mapping it to anonymous interactions on-chain can build better applications. I began working on this piece, wondering what it would take to make a better Web3 version of Tinder. I realised the use of open social graphs to enable dating goes back to 2013 when Hinge launched.

Dating apps are incentivised to retain users for the longest period because their revenue depends on it. Match.com would not be making $750 million every quarter if their userbase lived happily ever after with a few swipes.

But if we were to use Web3 primitives, one way to build a better dating app would be to

1. Capture user information in-app and through off-chain sources (such as Spotify, Instagram, Reddit and X)
2. Mapping social graphs to find friends of friends with shared interests and matching users with one another.

It sounds easy, but nobody is building it yet. The closest we have is a prediction market on Manifold. Speculating on whether a couple will stay together or not is, frankly, the most crypto-native outcome that could occur. Perhaps love - like many other human things, is not a problem for technology to fix. So, back to finance we go.

Combining on-chain transaction history and collecting off-chain data from users. If you use a Mercury bank account, you'll be offered invoice-based financing options to meet short-term credit requirements. The way the bank can offer you this is by keeping track of your revenue and matching you to external pools of capital. The bank itself has only one core asset: it's data on you. The service it provides is its ability to match you with a source of credit that can use that data.

As yields in DeFi dry up, platforms will emerge that tap into user data from off-chain sources and collaborate with on-chain liquidity pools to offer a higher yield. The difference between these tools and past versions of 'undercollateralised' lending would be the verification of user identity and the consequences of loan defaults.

This may seem far-fetched, but consider that both Maple Finance and Goldfinch service this function for SMEs today. They have privately held context through the data they collect from the users. They tap into a publicly available pool of money to underwrite and execute their loans.

A different place private context is built is in interfaces, such as websites or wallets. If you know a large number of users spend time on a certain kind of content or digital good, you can propagate it further to retain users. A new generation of content-related algorithm products, like MBD and Pond, are beginning to develop SDKs that make it easier to aggregate and create feeds of on-chain content.

But what if you could track user behaviour for how long they spend on certain content? Mirror's team already curates stories on their landing page. This is one instance of a platform that can track how long users spend on each story to curate content.

In both instances, I presume that a public good – be it liquidity or content – can be better indexed and offered to niche users if you have private context as a product. But what incentives do businesses have to engage in such a model? It boils down to profit margins. Unlike Aave, a business lending to SMEs or individuals could demand a higher amount in yield.

A content aggregation platform that has scaled could (*ironically*) advertise products relevant for users. Unlike social networks of the past, a content aggregation platform relying on Web3 social graphs *(such as the ones on Lens or Farcaster*) would not have to maintain user databases or content. Their cost is in curating relevant content and capturing enough user data to be able to continue surfacing good content.

But how does such a system scale? App-chains offer clues. Last week, we wrote about dYdX. If you have an ecosystem of verified users (as on Worldcoin) or ones that bridged to your chain specifically to trade derivatives, you have drastically reduced CAC for newer DeFi projects looking to target users. Similarly, chains like Base, BNB and Kraken's yet-to-be-launched L2 have a disproportionate amount of context on users as they already have data from their exchanges on each wallet.

It is kind of similar to the concept of agglomeration in economics. In bringing together large troves of users with similar interests, you unlock disproportionate amounts of economic activities compared to generic L2s, whose only edge is the speed at which they can enable a transaction.

This may seem far-fetched, but this version already exists within gaming today. Guilds like YGG are creating rich graphs consisting of users' history on-chain. Game developers are incentivised to build for these users as they have rich, contextual data on their history. They could whitelist a handful of users who were early adopters of similar games and onboard them with incentives.

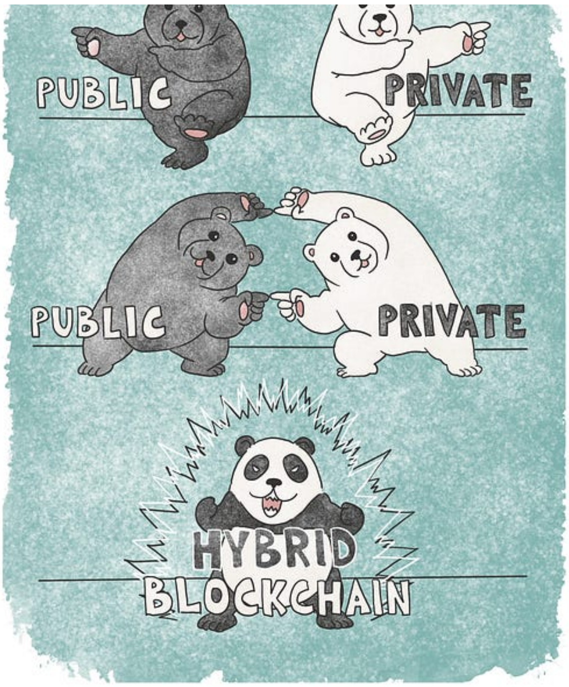
If you study the usage of Uniswap or Aave, it becomes pretty clear that Pareto laws apply to web3 native products, too. Building context on users is one more way businesses would accelerate the pace at which these laws emerge in our industry. So, are we repeating Web2 all over again? Not really. If settlements, social graphs and the content itself are on-chain, users cannot be deplatformed as quickly as they can be on Twitter or on a bank today.

In other words, the user can control their assets even when businesses build moats. The emergence of multiple clients - be it for seeking a loan or consuming content, would mean a user will have more alternatives than we do in a version of the internet where platform monopolies control our fates. For me, that is fundamentally exciting about the direction the internet is heading in.

Joel John
decentralised.co

Beyond Consortiums

When interoperability comes to private chains.



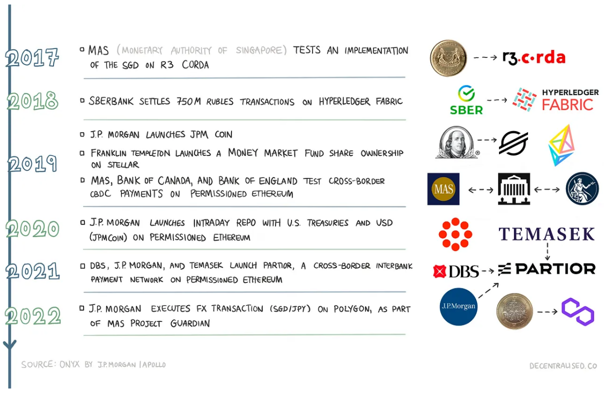
Hey there,

TL:DR: Today, we break down one of J.P. Morgan's research publications on interoperability between enterprise blockchains. I explain why it matters, then zoom out and ponder why enterprise solutions have historically struggled to disrupt anything.

Around 2017, during my initial years as an analyst, I kept a tracker for enterprise adoption of blockchains. The naïveté of youth and the exuberance around distributed ledgers made me believe that large corporations would soon embrace blockchains. Safe to say, that did not happen to the extent of my prediction.

With every market cycle, teams at enterprises with interesting titles like '*Innovation Management*' or '*Future Initiatives*' develop blockchain use cases. When the cycle wanes, they shift to other things, like AI or chatbots. I gradually realised that large organisations' incentive models generally do not allow management to embrace emerging technologies.

If the past few years prove anything, enterprise blockchain solutions struggle to scale. The timeline below is a handy list of enterprise initiatives that have emerged as Proof of Concept (*PoCs*) over the years. And yet, if you ask around how many people have used these, you may not know anybody. The land of enterprise blockchains, is filled with initiatives that eventually wind down.



- MAS (MONETARY AUTHORITY OF SINGAPORE) TESTS AN IMPLEMENTATION OF THE SGD ON R3 CORDA
- SBERBANK SETTLES 750M RUBLES TRANSACTIONS ON HYPERLEDGER FABRIC
- J.P. MORGAN LAUNCHES JPM COIN
- FRANKLIN TEMPLETON LAUNCHES A MONEY MARKET FUND SHARE OWNERSHIP ON STELLAR
- MAS, BANK OF CANADA, AND BANK OF ENGLAND TEST CROSS-BORDER CBDC PAYMENTS ON PERMISSIONED ETHEREUM
- J.P. MORGAN LAUNCHES INTRADAY REPO WITH U.S. TREASURIES AND USD (JPMCOIN) ON PERMISSIONED ETHEREUM
- DBS, J.P. MORGAN, AND TEMASEK LAUNCH PARTIOR, A CROSS-BORDER INTERBANK PAYMENT NETWORK ON PERMISSIONED ETHEREUM
- J.P. MORGAN EXECUTES FX TRANSACTION (SGD/JPY) ON POLYGON, AS PART OF MAS PROJECT GUARDIAN

SOURCE: ONYX BY J.P. MORGAN | APOLLO

DECENTRALISED.CO

For instance, IBM's food-tracking solution launched in partnership with Walmart only tracks leafy greens and bell peppers. Maersk's supply chain product was shut after several pilots. Even spending $150 million+ on blockchain initiatives doesn't help sometimes. In 2016, ASX (*Australia Stock Exchange*) began an initiative to clear trades and issue dividends using a blockchain.

Theoretically, it made sense. In reality, senior executives failed to bring the product to market after repeated attempts and eventually scrapped the project altogether after apologising in 2022.

A recent paper by JP Morgan's Onyx initiative caught my attention. Partly, instead of observing standalone use cases such as supply-chain management or debt issuance, it prioritises connecting different kinds of blockchains. So an enterprise (*say McDonald's*) might have BurgerChain, and a different one (*like KFC*) could have FriedChickenChain – and the two would have mechanisms to interact with one another.

This interested me because it addresses a core problem with all enterprise blockchain initiatives. Instead of replacing silos (*databases*) with new silos (*private, permissioned chains*), JP Morgan is trying to connect silos. Think of it as blockchain bridges for enterprises.

Today's newsletter examines how the company is building these bridges and what it could mean for the industry going forward.

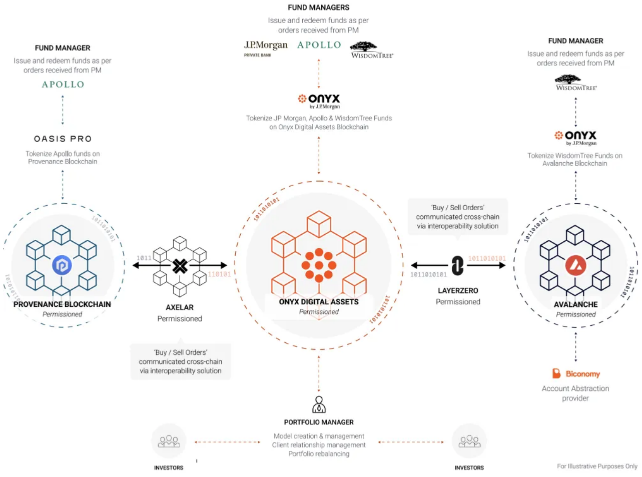
The PoC

The paper starts with a simple problem. Trillions of dollars in value are held in what is considered 'alt' investments. An alt investment portfolio could include a mix of collectables, real estate holdings, and private equity allocations. Unlike listed equities, alts struggle from a lack of liquidity and regulations, often leading to the mispricing of assets that go towards them.

A person might want to sell highly desired artwork at a distress price. Or there might be a person on a different continent willing to pay more for debt given to artists of a certain genre.

These alt assets often struggle with a lack of liquidity. The PoC made by JP Morgan had two aims:

1. To facilitate global reconciliation and settlement of ledgers for illiquid investments
2. To improve liquidity for said investments globally and across financial institutions



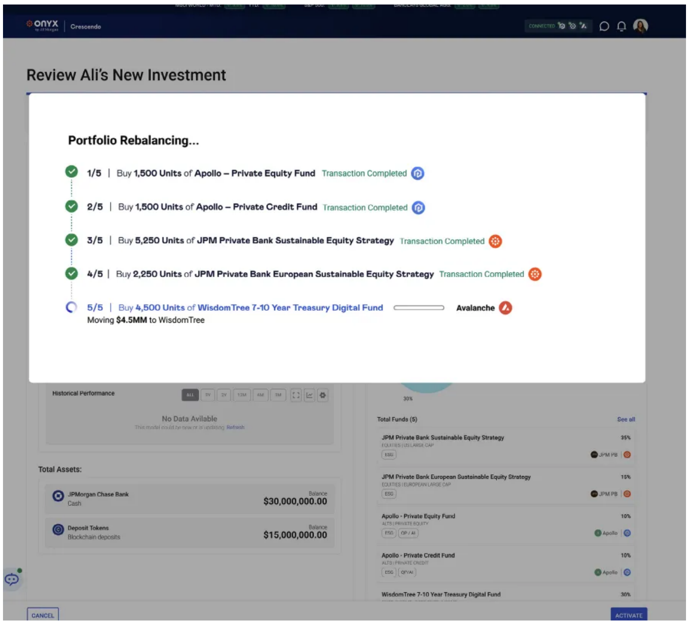
FUND MANAGERS
Issue and redeem funds as per orders received from PM
J.P.Morgan PRIVATE BANK
APOLLO
WISDOMTREE
FUND MANAGER
Issue and redeem funds as per orders received from PM
APOLLO
OASIS PRO
Tokenize Apollo funds on Provenance Blockchain
ONYX by J.P.Morgan
Tokenize JP Morgan, Apollo & WisdomTree Funds on Onyx Digital Assets Blockchain
FUND MANAGER
Issue and redeem funds as per orders received from PM
WISDOMTREE
ONYX by J.P.Morgan
Tokenize WisdomTree Funds on Avalanche Blockchain
PROVENANCE BLOCKCHAIN
Permissioned
AXELAR
Permissioned
'Buy / Sell Orders' communicated cross-chain via interoperability solution
ONYX DIGITAL ASSETS
Permissioned
'Buy / Sell Orders' communicated cross-chain via interoperability solution
LAYERZERO
Permissioned
AVALANCHE
Permissioned
Biconomy
Account Abstraction provider
PORTFOLIO MANAGER
Model creation & management
Client relationship management
Portfolio rebalancing
INVESTORS
INVESTORS
For Illustrative Purposes Only

Source

When you build a portfolio on-chain with crypto, your best bet for distribution is an extensive integration or token rewards. Yearn was an excellent outlet during DeFi summer. An alternative is an exchange partnering up with you. However, exchanges have no reason to distribute financial products to users as its business model is (*generally*) predicated on users' completion of multiple trades daily.

JP Morgan's PoC assumes individual portfolio managers (PMs) would distribute it to clients. These PMs would suggest assets (*to clients*), balance portfolios, and source liquidity for their portfolios using the product. JP Morgan calls the front end of the product Crescendo. It is a simple interface that allows PMs to allocate money attached to assets that may be held on separate chains across different financial organisations.

All of this feels like standard stuff. I can buy a mix of mutual funds from my bank account today. But what happens in the back end is what holds promise. Much like what occurs with traditional wealth management products, PMs suggest a mix of assets for a portfolio. These portfolios are issued as smart contracts on Onyx Digital Assets.



Review Ali's New Investment

Portfolio Rebalancing...

1/5 | Buy 1,500 Units of Apollo – Private Equity Fund Transaction Completed

2/5 | Buy 1,500 Units of Apollo – Private Credit Fund Transaction Completed

3/5 | Buy 5,250 Units of JPM Private Bank Sustainable Equity Strategy Transaction Completed

4/5 | Buy 2,250 Units of JPM Private Bank European Sustainable Equity Strategy Transaction Completed

5/5 | Buy 4,500 Units of WisdomTree 7-10 Year Treasury Digital Fund Avalanche
Moving $4.5MM to WisdomTree

No Data Avilable
This model could be new or is updating Refresh

Total Assets:

JPMorgan Chase Bank
Cash
Balance
$30,000,000.00

Deposit Tokens
Blockchain deposits
Balance
$15,000,000.00

Total Funds (5)

JPM Private Bank Sustainable Equity Strategy 35%
EQUITIES | US LARGE CAP

JPM Private Bank European Sustainable Equity Strategy 15%
EQUITIES | EUROPEAN LARGE CAP

Apollo - Private Equity Fund 10%
ALTS | PRIVATE EQUITY

Apollo - Private Credit Fund 10%
ALTS | PRIVATE CREDIT

WisdomTree 7-10 Year Treasury Digital Fund 30%

From JP Morgan's paper

Tokenised instruments representing fixed-income products, private equity or private credit are issued on Provenance Blockchain, Onyx (*by JP Morgan*) or an Avalanche chain by service providers like Oasis Pro. A token standard compliant with ERC-20 named the Onyx Digital Assets Fungible Asset Contract (ODA-FACT) is used on all of them. Axelar and LayerZero are used for sending messages for buy or sell orders, whilst Biconomy is used to abstract the complexities of managing private keys or holding gas for transfers.

The result is a simple interface that allows investors to see what their PMs are investing in. PMs in exchange, have a trail of each of their orders going through the platform. The tokenised instruments – be they debt, equity or more esoteric instruments, like art – are still managed by large wealth management services like JP Morgan. But now, you have a mechanism allowing these instruments to interoperate with services from different banking entities with a fraction of the friction.

In these instances, the wealth management services still own and manage the underlying instruments. That is, you are not buying debt from a fintech company in an emerging market or real estate from a developer; the issuers for all of those assets are still large banks like WisdomTree, JP Morgan or Apollo. This process drastically reduces the typical risk for a person holding an investment portfolio with the platform as (*I presume*) the bank would have done necessary due diligence before listing an asset as an investment opportunity.

But why does any of this even matter? I believe it illustrates a moment when the lines between DeFi and fintech are increasingly blurred. Let me explain – first, with a breakdown of why enterprise blockchain initiatives have historically failed and then with an explanation of why DeFi products fail to scale.

Why It Matters

Enterprises usually struggle to find PMF for their blockchain initiatives. It comes down to the economics of operating blockchain-native business models. There aren't enough people rushing to track their milk supply on-chain.

Surely, certain luxury items can be traced on-chain if a user wants to; however, the market for that is currently tiny because consumer perception of blockchains as a verifiable trail of a product's provenance is not established yet.

Bringing off-chain goods - be it fruits, Gucci bags or real-estate to the blockchain requires long, manual processes that don't happen easily. The tracking has to be integrated into processes in a way that is tamper-proof. Digital goods on the other hand, are relatively easier to show provenance for.

A different reason why enterprise blockchain initiatives struggle is that they interface with multiple parties in the real world, each of whom has very different incentive mechanisms. In some instances, systems would stick to relative obscurity even when it slows down the process because that benefits the stakeholders involved.

For instance, replacing the invoicing systems used at a dock could (rightfully) cause friction for a corrupt officer working there. Or a farmer may have little reason to spend his time slapping blockchain-native QR codes onto his produce if it does not mean he can charge more. The incentives break down when you take a nascent technology to multiple stakeholders.

What the PoC from Onyx has done stood out for a few reasons.

1. Firstly, they stuck to a handful of assets the banks already distributed among the wealthy clientele who interfaced with them.
2. Secondly, they created interoperability among all of them for the assets. A PM could source liquidity from bank A (*which uses Provenance Blockchain*) to service a client who uses bank B (*which uses a permissioned instance of Avalanche*).
3. Lastly, they stuck with a pretested business model. The focus of the PoC was to bring speed (*and possibly composability*) into a relatively slower fragmented process.

Now, one could argue this sounds like interoperable databases. It seems like the engineers at these organisations have managed to make a server on AWS speak to a server on Azure. But it goes beyond that, in my view.

The token standard used is ERC-20 compliant. So hypothetically – and this is a big IF – there is a pathway for these banking instruments to interface with permissionless public blockchains. I don't expect them to be accepting deposits in ETH, especially if it came from trading a random meme asset. There are compliance risks with that.

We have written about how the lines are blurring between DeFi and CeFi in the context of loans. You can extrapolate it to more nascent consumer categories, too. For instance, Zamp and Dinara are examples of B2B banks that permit remitting money to employees in both fiat and stablecoins. Mastercard has a program that allows issuing debit cards to crypto-native users.

But here's what may have gone unnoticed in that PoC

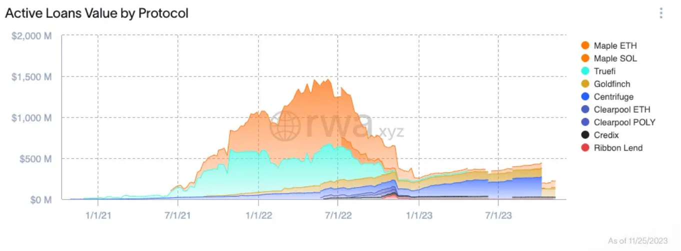
1. Enterprise blockchains could communicate with one another.
2. They could (theretically) onboard crypto-native sources of capital or issue assets that settle on-chain in a public, permissionless environment.

Blurring boundaries between private and public blockchains opens up new use cases that were not possible in the past. Before I explain, let's quickly revisit the current state of DeFi.

What It Means

You'll see a consistent, repeating issue when you consider projects in DeFi focused on real-world use cases (*or RWAs, as the cool kids call them*). The average person in crypto is not looking to make a 7% APY over the next year. Their incentive is to be risk-on and generate 30–50%.

The way it historically worked is that lending pools would offer native tokens in exchange for lending on them. Thus, for depositors on DeFi platforms, part of the yield did not come from the borrower; it came from selling tokens. But what happens when token rewards no longer exist? The appetite for lending declines rapidly.

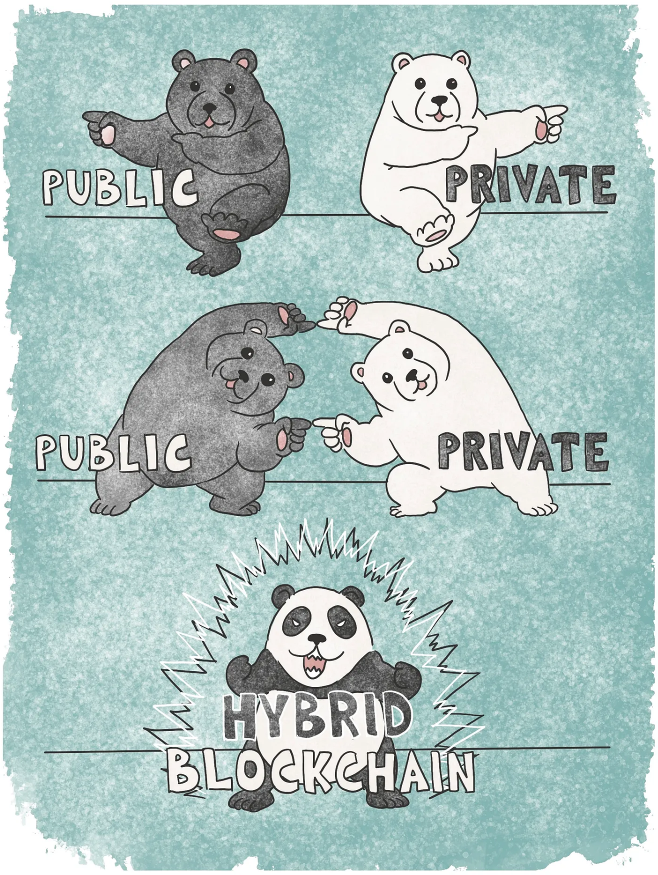


Source: RWA Dashboard

Present-day DeFi products that source capital from crypto-native users struggle to scale because token incentives can only take them so far. According to DefiLlama, some $55 billion is locked in DeFi. Of this, less than $250 million is deployed into RWA projects. We are at less than 0.5% penetration with crypto-native sources of capital for RWAs because what users want and the products offered are quite different. - Users want volatility. RWAs offer stability.

Between the countless hacks in DeFi and regulatory risks founders face while building in the space, I believe enterprise chains (like Onyx) offer an alternative that may scale faster. They combine all of the functional elements public blockchains enable, like transparency and speed, with what banks already have. For founders building financial primitives, enterprise chains could offer more scale than DeFi could in the next five years. It may feel like a far-fetched statement, but it is beginning to become apparent.

For instance, an RWA product like Centrifuge could list its loans on Onyx and benefit from the network of investors on these wealth management platforms. Or a private equity firm could tokenise portions of a publication like The Block and syndicate accredited investors. In the distant future, there could come a time when ESOPs can be tokenised, transferable and traded through brokerage accounts that settle directly in your bank account.



I could have used a Venn diagram. But what fun is an article on enterprises without a hand drawn meme in it.

It is quite likely that banks release a "safe" or "compliant" version of DeFi protocols in a permissioned environment. One example of this in the wild is that of Aave's institutional product. It connects some 30 institutions to one another in a permissioned lending pool. Another example, is that of banks tinkering with stable coins. For instance, JPM Coin (*yes, that's a thing*), recently settled over $1 billion in transaction volume daily for partners.

Can such a system rival SWIFT network? It is quite hard to suggest it would. SWIFT benefits from decades of entrenched network effects. But systems like Onyx could see meaningful transaction volume within a few years. The efficiencies of speed and cost it offers, could onboard an increasing number of businesses to such solutions.

At some point in time, banks may want to settle certain types of transactions on a public blockchain like Ethereum if immutability is a requirement. Much like we see with L2s, they may conduct large parts of the transaction on their internal, permissioned environments and have finality on a public blockchain.

None of these applications are permissionless or censorship-resistant. Banks can boot users whenever they wish. They could have faulty compliance software that flags users and seizes their assets at will. The model I suggest above has nothing to do with what Bitcoin or Ethereum was built for.

For a good number of founders, building fintech applications that scale, matters more than decentralisation. They have every reason to tinker with enterprise blockchains, especially if regulators like MAS (*Monetary Authority of Singapore*) create sandboxes for such use cases. Ultimately, founders want the best technology that fits the use case. Sometimes, it is AWS. Sometimes, it is Ethereum. Maybe, in the future, it could be an enterprise-chain run by a bank. Who knows.

Suits vs Hoodies

All of this is not to imply that enterprise variations of blockchains are a guaranteed success. There have been attempts since at least 2014. The appetite for risk, especially for enabling new financial instruments whilst taking on the scorn of the regulator for little-to-no profit margin, may not be high at banks.

But what we see with this PoC is one instance of how blockchains are evolving beyond what we are used to.

If JP Morgan can make a small portion in revenue (*say 0.01%*) for every transaction through such a system, they have every incentive to scale it. By their admission, they have enabled some $900 billion in transaction volume for tokenised US treasuries on Onyx. That would be some $90 million in additional revenue if they could charge the small fee mentioned above. Is that large enough on its own? Not really. But keep in mind that these figures scale exponentially.

According to the report, the PoC created by JP Morgan can help reduce the operational aspects of handling 100,000 clients from 3000 steps to a few clicks. They don't talk about how settlements for these instruments would look like. But I presume it could be better than the T+2 settlement times equity markets have today. That speed efficiency could translate to better capital efficiency as the assets could be reinvested.

But change takes time when large enterprises are involved. For instance, a consortium of banks is trying to replicate what Google Pay and Apple Pay do. Quite late, I would argue. In the early 2020s, much of our ecosystem was looking towards Libra (*Facebook's consortium of enterprises*) as the new blockchain standard. It died a sad death.

The number of people coordinating on how risk is taken and the politics that play out while those decisions are made makes enterprises the wrong place for great ideas. (*I may have annoyed future sponsors by saying that out loud*). So, it remains to be seen if there can be large-scale impact in terms of blockchain adoption through enterprises with all their resources and distribution.

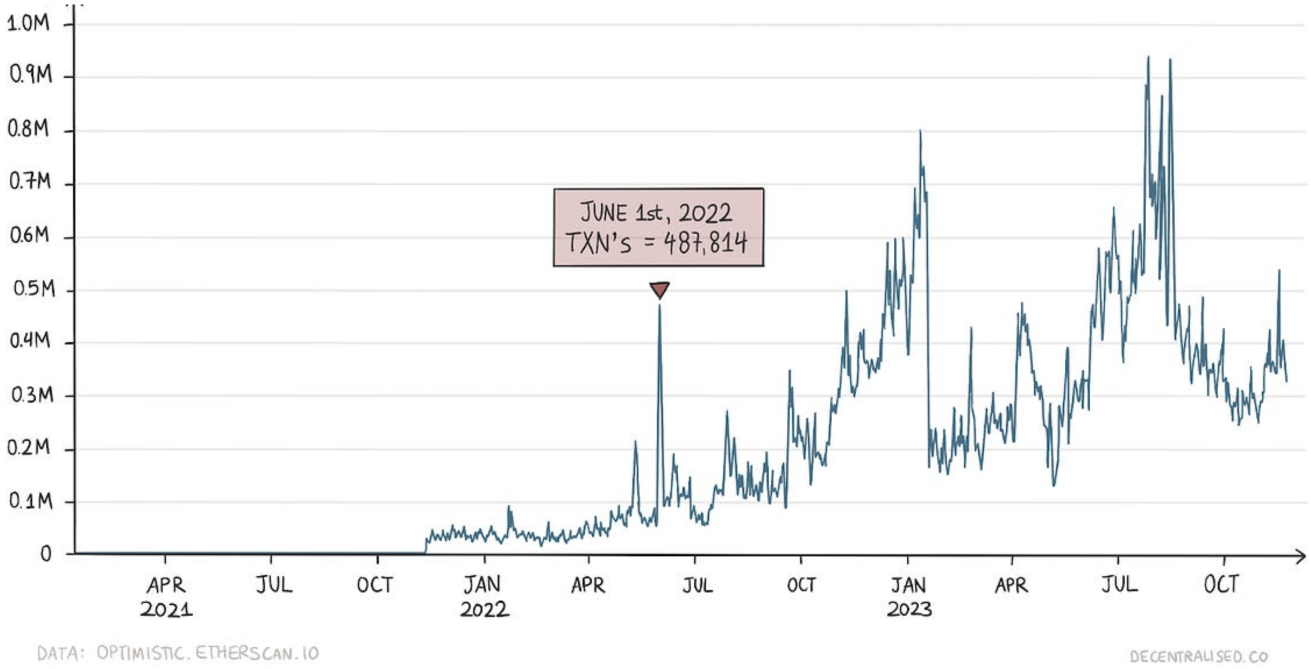
I don’t know if such blockchain standards focused on enterprise interoperability would take off, but I would argue that a class of use cases will require robust compliance in the coming years. A handful of enterprise chains are evolving to be better places to build, given the scale of the institutions developing them and the ease of staying compliant while making on them.

Founders have good reasons to explore them before writing them off if decentralisation and censorship resistance are not the core focus of their products.

Saurabh
decentralised.co

Stress Testing

How networks are optimising for growth.



Hey there,

TL:DR : Today we build further on the ideas presented in the L2 Paradox. I lay down what happens when networks are stress-tested via airdrops, how developers are optimising for uptime & the incentives for founders to build on different networks.

It is the time of monolithic chains. It is the time of modular chains. It is the time of localised fee markets. It is the time of global fee markets. You see where this is going!

The Solana ecosystem was almost written off when the FTX news broke. But it has survived and is making a strong comeback, not just with the price but with some of the fundamentals of the network too. I don't mean to say it's all hunky-dory in Solana land. It has its issues, but achieving scaling and decentralisation together is hard.

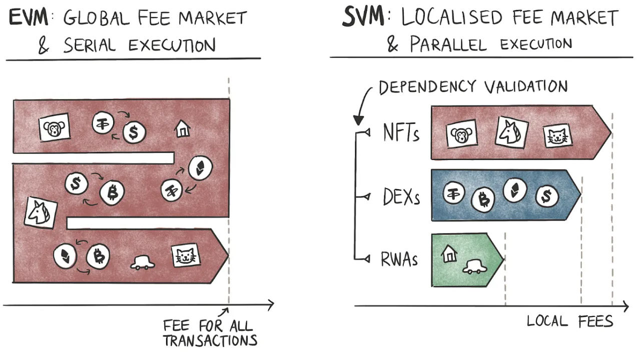
The point is that it's time to pay attention to how different approaches to scaling web3 are playing out. Solana's approach is unique in that it wants to do everything on the same layer by utilising hardware capabilities; one may also say it relies on

Moore's law. Let me explain what I mean with some data from the past few months.

Solana and EVM

Solana and Ethereum Virtual Machine (EVM) chains take drastically different approaches to achieve similar goals. Ethereum is like a storied metropolis, which aims to keep adding layers to achieve scale. Solana is like a city that can quickly expand in all directions, so building layers is unnecessary.

One of the significant differences between Solana and Ethereum is how the fee markets are designed. The EVM chains' fee markets are global, whereas the Solana fee market is local. Before jumping into what I mean by that, here's a quick recap from my modular experiment piece.

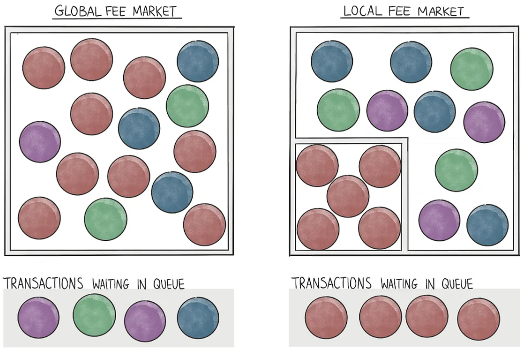

EVM: GLOBAL FEE MARKET & SERIAL EXECUTION
FEE FOR ALL TRANSACTIONS
SVM: LOCALISED FEE MARKET & PARALLEL EXECUTION
DEPENDENCY VALIDATION
NFTs
DEXs
RWAs
LOCAL FEES

Solana uses the hardware of your computer's multiple cores. EVM, conversely, does not rely on hardware to keep the validator hardware requirement low. To support parallel processing, Solana requires transactions to tell the VM which accounts will be used to read and write (*i.e. which ledger areas will be affected due to the transaction*).

Based on this information, Solana understands which transactions are not interdependent. That is, which does not affect the state of the same account. This is how Solana facilitates parallel processing at a very high level.

Just like Ethereum, Solana also charges for computation. The gas equivalent for Solana is the compute unit (CU). Each block can spend a maximum of 48 million CU. Each account or smart contract has a cost tracker that tracks how much CU it consumes. An account can consume up to 12 million CU or 25% of the total block limit for one block.

So, if there's a much-anticipated NFT drop, it can only consume 25% of the block's compute limit. The priority fees get spiked only for this particular account (*or contract*). Interactions with other accounts remain smooth during this time. On Ethereum, the fees surge for the whole network.



Stress Tests

Much-anticipated NFT mints or airdrops usually act as stress tests for chains. The more anticipated the airdrop or mint, the more the stress on the chain as an increasing number of people are rushing to claim these assets. It is worth studying how networks performed during these events to understand their readiness for web2 scale mass adoption.

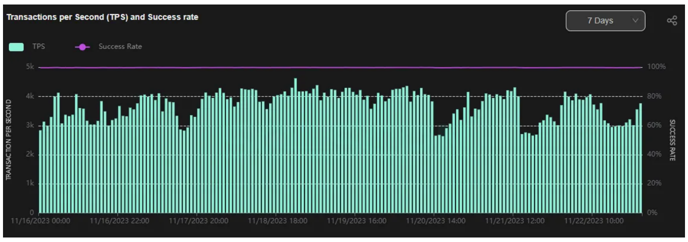
Pyth's Airdrop on Solana

Pyth Network is a first-party oracle. On November 20, it made its PYTH token claimable to over 90,000 wallets. In addition, Backpack distributed PYTH to 74,000 wallets. Being one of the anticipated airdrops on Solana, it was a good test for the network's performance.

As Pyth Network is a first-party oracle, data providers host Pyth nodes. This means that data providers and oracles are more or less the same, reducing the need for middlemen. This oracle design has benefits like reduced latency, lower cost, and higher transparency. With over 40 blockchains and 230 applications, Pyth Network has over 380 data feeds that update data more than 65 million times. PYTH is the governance token of the network.

The TPS on Solana dropped from ~4,000 to ~2,600 as users rushed to claim the airdrop (note that the drop can't be directly attributed to the airdrop since it is a common occurrence). Note that this is the overall TPS measure. Solana's transactions include voting and non-voting. Voting transactions are validators voting to reach a consensus, and non-voting transactions are normal user transactions.

Typically, non-voting transaction TPS is ~400 transactions. The average fee remained at a fraction of a cent. The total number of non-voting transactions reached 20.9 million from 18.9 million a day prior. The share of non-voting transactions jumped from 5.3% to 6.5% in the same period.



Source: Solscan

Solana Network suffered six outages in 2022 and one in February this year. One of the reasons for the outages was excessive demand (*mainly from bots*). The fact that Solana transactions are cheap to execute works against the network at times. The cheap cost encourages DDoS (*denial of service*) attacks or bots trying to mint certain NFTs.

One of the major steps to mitigate these issues is Firedancer, Solana's new client software being developed by Jump. Client software or validator client is nothing but a piece of software required to turn your computer into one of the validating nodes on the network. For the node to participate in consensus, it needs to verify transactions and blocks and be able to propose blocks (in the case of a block proposer node).

The client software allows a computer to perform these activities. As Firedancer is a third-party client, it helps Solana decentralise at the base level, besides creating redundancy and not inheriting bugs from the existing client. Firedancer is currently deployed on the test net and is expected to be deployed to the main net by the summer of 2024.

While Ethereum is notorious for pricing out users the moment demand surges, comparing Solana and L2 chains to how they respond to load is not so straightforward. One reason is that a single entity operates most L2s (*Like Arbitrum, Starknet and many others*). Managing sequencers (*block producer equivalent for L2s*) is much easier when it's only one entity. On the other hand, Solana has over 2000 vote accounts (*block producer equivalent for Solana*) situated worldwide, managed by different teams.

For the end user, what matters is whether their transactions are included in blocks. We can look at times of high demand and see whether other chains faced any issues.

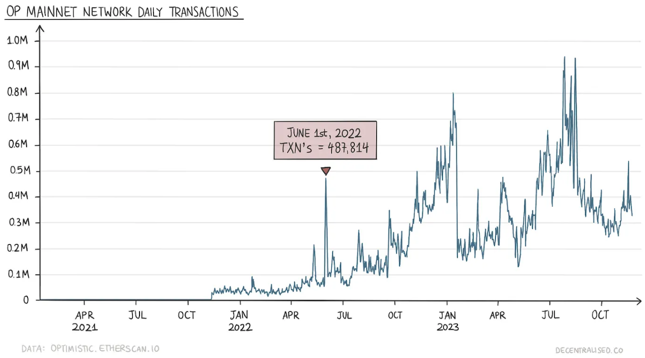
In summary, two changes promise to lend more stability to Solana – local fee markets that limit high demand spillover to other contracts and

Firedancer that doesn't inherit bugs from the Solana client.

How does any of this compare to some prominent L2s? Let's take a look at the numbers.

OP Token Drop on Optimism

When Optimism made its OP token claimable to over 250,000 addresses on June 1, 2022, the network got overwhelmed by the demand and the claim process was stopped for a few hours. If you look at the number of transactions, the jump on June 1 was ~2.3 times the previous peak. The peaks after the June 1 incident did not hamper the network's performance.



DATA: OPTIMISTIC.ETHERSCAN.IO

DECENTRALISED.CO

Optimism did not stop producing blocks, but they paused the claim process. What would have happened if pausing was not possible? And if Optimism had multiple third-party nodes to produce blocks? It would perhaps be in a similar situation as Solana, where all the validators must work on a solution off-chain (*like Solana reaching out to validators via Discord or Twitter*). This is not an Optimism-native problem. Older L2s like Polygon have had their share of issues.

Polygon PoS Reorgs

First of all, block reorganisations (*reorgs*) are nominal. Lower block times, network latency, and soft consensus are some factors causing these reorgs. What matters is the depth of reorgs. This 157-block reorg was not typical for Polygon, although it has had several briefer re-org in the past.

In general, reorg is when a block gets accepted on the network first, but then a block contradicting the said block gets accepted later at the same network height (*block number*). In this case, transactions in the re-orged block get reversed as if they never took place. Network latency and congestion can cause propagation delays. The after-effect? Different validators see different chains of blocks.

As a result, the new leader who is supposed to propose block N+1 may not be aware that block N has already been proposed because they see only N-1 blocks. So, they propose block number N, which is in contention with the earlier block. The new leader then has a choice to build on two different Ns. The reorg depth is the number of blocks getting rewritten. The lower the depth, the lower the impact on users and network participants.

On Polygon PoS, 15–20 blocks getting reorged is not damaging. This is why the 157 block reorg mentioned above is noteworthy. Before the incident in February, the network had undergone a hard fork (*where the validators must upgrade the older version*) to reduce gas fee spikes and address reorgs. The February incident occurred because increased network activity forced validator nodes to delay block production.

This resulted in backup block producers kicking in to produce blocks. As multiple block producers were proposing blocks simultaneously, reorgs increased. The team deployed additional RPC nodes to reduce the mempool burden that caused block producer delays. You can read more about the plan here.

What Does This Mean

Building L2s is like building great roads in a city that doesn't offer anything else. Such cities will likely become ghost towns like these infrastructure failures. Thriving ecosystems need applications that users want to use regularly. If a builder wants to build an application, its nature will probably dictate which chain or environment they use.

Parameters like uptime, block records, transaction costs, languages supported, availability of robust RPC endpoints, other applications, user base, etc., are critical in deciding which blockchain or L2 builders want to use.

Almost every now and then, a new layer 2 launches on Ethereum. This makes their choice difficult. Let's consider an artist like Jack Butcher, who created Visualise Value. If he wants to launch a new collection in the Ethereum ecosystem, where does he do it? FYI, he recently dropped a new collection on Ethereum, not on any L2. Some reasons can be the following:

- NFT buyers being insensitive to gas costs
- Underdeveloped NFT marketplaces on L2s in terms of liquidity
- Only ~10k NFTs, which means there is no need for the 'average' fee-conscious user to participate

Blast (*by Blur's team*) is a new L2 that provides native yield on ETH and stablecoins. This yield comes from depositing users' ETH and stablecoins into protocols like Lido and MakerDAO. Moreover, the Blur team also intends to deploy applications like NFT perps onto Blur to facilitate cheap trading of NFTs and their derivatives.

A developer looking to build similar products may choose Blast over other L2s because it offers better composability with the NFT ecosystem than other alternatives.

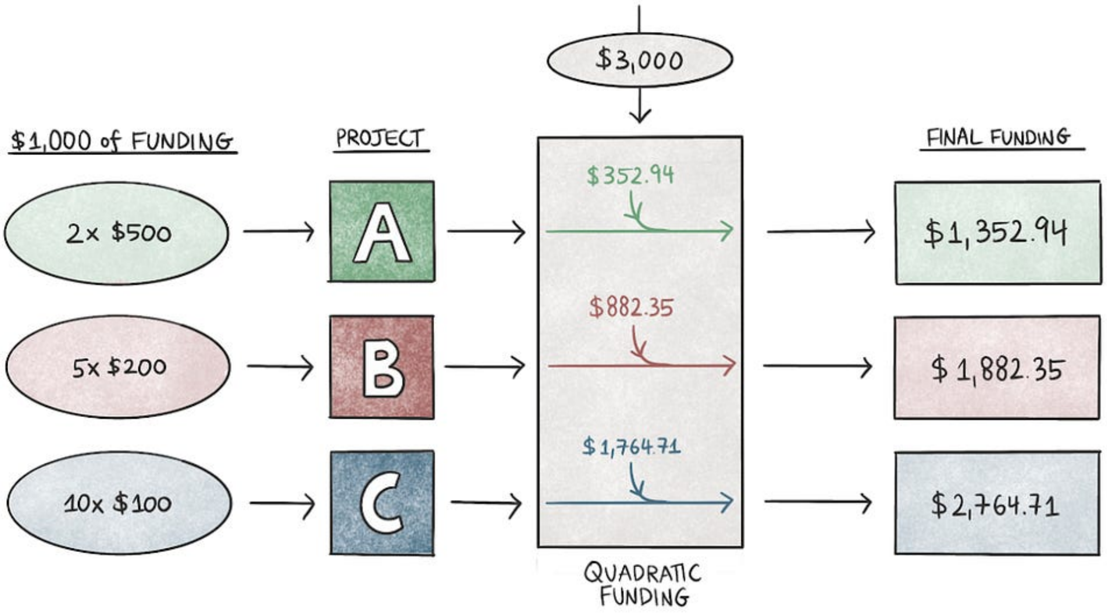
In a different scenario, a game developer who wants to launch a game where millions of NFTs need to be minted on-chain and then transferred to players will probably go for Solana, given that its compressed NFTs lower the minting costs to a fraction of costs on L2s or scaling solutions.

What about an exchange like dYdX, where traders expect performance like Binance? It gets tricky to think of Solana right away because of the outages. Can you afford to halt trading for 18 hours or more? Even TradFi doesn't wait that long for T+1 settlements. This is where Solana has scope for improvement. Hopefully, with Firedancer, stability issues will be resolved, and we will see Solana being an even better challenger to mighty Ethereum, L2s, and appchains.

Joel John
decentralised.co

Passport Please

How Gitcoin is improving the web.

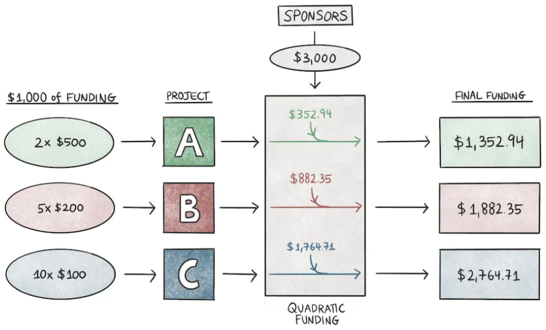


Hey there,

When we covered Soulbound tokens a few weeks back, I briefly mentioned Gitcoin Passport. It is an identity verification protocol to help users validate who they are while interacting with applications. We have since reached out to the Passport team to learn more about how it is used and why it matters. Today's piece summarises my conversations with Jeremy, the product lead for Passport.

Here's a quick reminder on Gitcoin and quadratic funding. Gitcoin enables public goods to raise funding from donors. The platform often matches pools of donations in proportion to the number of people who have contributed to a campaign. Each Gitcoin round runs for two weeks quarterly. At the end of each round, the platform verifies which public good had the most people donating and matches donations in proportion to the number of participants.

This differs from a single donor putting $1000 into a pool and having it matched in equal amounts. In such a model, products or services with more individuals donating to them are matched disproportionately.



More donors, more problems. Or something like that.

The image above gives a quantitative breakdown of what it would look like in practice. In the case of project A, the final funding was an additional 35% ($1352) compared to the additional 164% project C raised from external sponsors.

Why does this matter? A simple heuristic is that the higher the number of individuals donating to a campaign, regardless of the sums they provide, the higher the likelihood that people find it valuable. This is a democratic approach to public goods funding. Whilst there are both good and bad aspects with such a model, it is worth noting that as of Q1 this year, Gitcoin has helped raise over $50 million from 3.8 million unique donations.

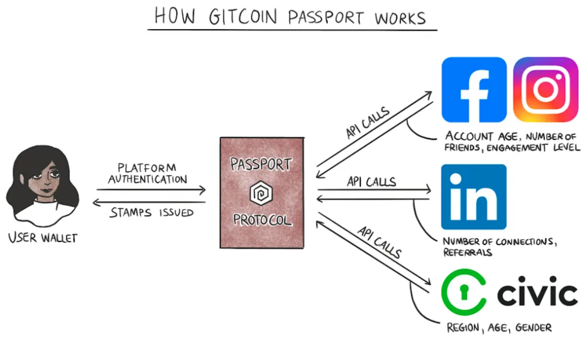
What does any of this have to do with the identity?

Given how easy it is to spin up wallets, a team listed on Gitcoin could spin up new wallets, split $1,000 into different wallets and end up with more in donations raised. They could require that wallets have a specific transaction history before they are considered for quadratic funding, but they would still be easy to Sybil.

So, the crew behind Passport decided to develop an internal solution for allocating a 'trust' score to wallets. But before I go into that, it helps to understand how Passport works.

Understanding Passport

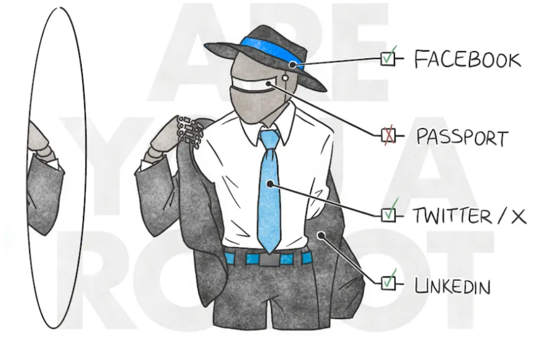
When you sign in to your Gitcoin Passport, you are greeted with 25 services that can be used to add to a score. According to Gitcoin's systems, you must have a minimum score of 20 to be considered verifiably human. Collecting individual stamps here refers to signing in with an external account (like Google) and offering API access to validate your claims. Doing so gives you a stamp, with a pre-designated score allocated in proportion to how human an activity could look.



Easy-to-Sybil accounts like Twitter or Google have a low score of 1, whereas having verifiable code that goes back considerably is weighed at 7.25. Externally validating your identity using a passport on services like Civic gets you around 6 points. Interestingly, having a single identity, such as a license or LinkedIn account, is not enough. Gitcoin requires you to add layers of information about your humanness before hitting the minimum score of 20.

Once sufficient stamps have been collected, users can also mint the stamps on-chain through a low-cost network like Optimism for about $2, but the minting is not necessary to use the protocol. Developers can also use API calls to Gitcoin to verify if a wallet has the required stamps. But minting on-chain reduces the dependency on a centralised provider. Note that a stamp expires every 90 days.

So if you issued a verification for the status of your LinkedIn account or showed that your passport had been validated on Civic, you would have to return to the product and reissue a stamp every 90 days. This procedure helps the network validate that you are who you claim to be and that a third party is not using the wallet on your behalf. It is also useful if a wallet is compromised and a user wishes to mint a verification to a different wallet.



Not me trying to claim yet another airdrop with a spare wallet.

Think of each stamp as part of your attire. You choose your clothing based on the event and nature of the place you are visiting. Gitcoin Passports serve a similar function. You put on additional stamps for increasingly sophisticated use cases. A simple community may require you to own an NFT. A more sophisticated fintech application could require that you validate your identity on Civic using a passport and tie your GitHub account to your wallet before they give you access to the product.

My point is that a fake one could be easily spun up when a user needs to validate a Twitter or Facebook account. But add layers of complexity, such as requiring a GitHub account with transaction history or passport verification, and suddenly, it becomes hard to Sybil a product for a quick buck.

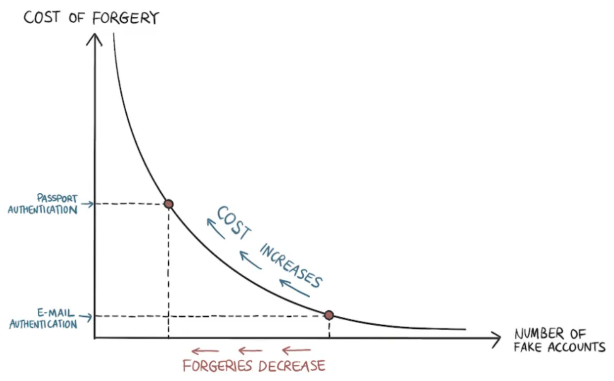
Passport is an open protocol that allows users to plug in centralised services and on-chain activity to validate whether or not they are human. Once users mint their stamps as passports, Gitcoin is not directly involved in validating each claim once the stamp is minted. An external application like Uniswap could use the stamps to open access to certain parts of their product. One challenge is that the model still relies on Gitcoin if the user does not mint the stamps on-chain. A fully decentralised version is set to be released in the coming quarters.

Why does this matter? To understand why, it helps to have context on the benefits for both users and protocols.

Matter of Incentives

Let's start on the protocol side. Whenever an airdrop occurs, on-chain activity is taken as proof of humanness. This activity offers token design experts some relief in the fact that the individuals getting the token are legitimate actors whose on-chain footprints validate that they are real people. But as I'd covered in our story on airdrops, teams looking to Sybil accounts have designed some complex operations.

The modus operandi is quite simple. You study the patterns of usage that could lead to a wallet being given an airdrop, replicate it across hundreds of wallets, claim the airdrop on the day a token is released and profit in the millions by selling it on an exchange.



The higher the incentives, the more likely that identity forgery on a protocol would occur. **The higher the cost of forgery, the lower the probability that a person would try to Sybil a network.**

Products like Worldcoin took a different approach to the matter. They had individuals scanning their eyeballs to validate that they were human. Since eyeballs are unique to the individual and hard to replicate, the network could claim they had the most 'human' network on-chain.

Here's the problem, though: Nothing stops users from setting up a booth to scan eyeballs and split the airdrop with participants. While we have no evidence of such large-scale Sybil attacks, there have been reports that the financial incentives partly drove unknowing users to the network.

Why does this matter? It matters because understanding who constitutes a 'user' in crypto has been one of the hardest challenges so far. Blockchains are payment networks, so it is natural that hundreds, if not thousands, of bots will do millions of transactions on these networks. But until a network is verifiably transitioning into being used by humans (*or, as in the case of ETH, bots are paying large fee*s), it is hard to argue that value is accruing to the network itself. **The more human a network is, the higher its relative value.**

Gitcoin Passport gives developers a simple way to verify whether a user is human and has the credentials to partake in an early-stage product. The following are a few ways this could have been used today:

1. Lens Protocol could allow early access to Twitter users with over 10,000 followers.
2. A protocol focused on on-chain data could verify and offer airdrops to individuals who have worked with one of the Big Four audit firms by checking their LinkedIn history.
3. A protocol could airdrop only to users that could verify they are humans using a passport on Civic ID.

I believe a generation of applications that could historically not vet whether a user is who they claim to be could now be built using Gitcoin Passport. There are a few distinctions to be made here. Unlike when you do AML/KYC on Binance using a third-party service provider, Gitcoin's Passport Stamps don't require you to upload a passport for every application you do – a single API call checks whether a user's stamp is valid.

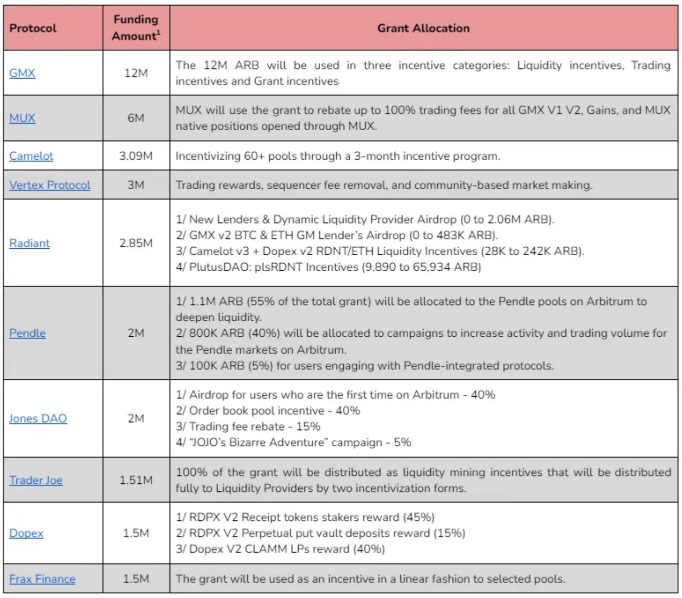
Once they have validated (and minted) a stamp, they could use it across applications in an ecosystem using the standard. Present-day identification products often struggle with the network effects of multiple applications using the same standard. Gitcoin Passport, given the savings in time and costs, could make a meaningful dent here.

Users can mint multiple stamps for the same identity proof (like a passport) in different wallets. Depending on the use case, they may want a pseudonymous identity. However, an application could discern if a person is spinning up multiple identities using hashes on the stamps.

I could have multiple wallets where I have linked my GitHub, Twitter and Linkedin, but I could not claim I am a different individual with each wallet, as the developer could see I have used the same identity proofs. It is important to note here that whilst your off-chain identity proofs (*like Passport or Github profile*) could be replicated to new wallets, a wallet's history itself cannot be replicated easily

The combination of on-chain transaction history validated through a tool like Degenscore with a primitive like Passport helps developers quickly identify human users with an on-chain history of expertise.

The most obvious use case for such a product (after quadratic funding) is for incentivised testnets and grant programmes.



Protocol	Funding Amount[1]	Grant Allocation
GMX	12M	The 12M ARB will be used in three incentive categories: Liquidity incentives, Trading incentives and Grant incentives
MUX	6M	MUX will use the grant to rebate up to 100% trading fees for all GMX V1 V2, Gains, and MUX native positions opened through MUX.
Camelot	3.09M	Incentivizing 60+ pools through a 3-month incentive program.
Vertex Protocol	3M	Trading rewards, sequencer fee removal, and community-based market making.
Radiant	2.85M	1/ New Lenders & Dynamic Liquidity Provider Airdrop (0 to 2.06M ARB). 2/ GMX v2 BTC & ETH GM Lender's Airdrop (0 to 483K ARB). 3/ Camelot v3 + Dopex v2 RDNT/ETH Liquidity Incentives (28K to 242K ARB). 4/ PlutusDAO: plsRDNT Incentives (9,890 to 65,934 ARB)
Pendle	2M	1/ 1.1M ARB (55% of the total grant) will be allocated to the Pendle pools on Arbitrum to deepen liquidity. 2/ 800K ARB (40%) will be allocated to campaigns to increase activity and trading volume for the Pendle markets on Arbitrum. 3/ 100K ARB (5%) for users engaging with Pendle-integrated protocols.
Jones DAO	2M	1/ Airdrop for users who are the first time on Arbitrum - 40% 2/ Order book pool incentive - 40% 3/ Trading fee rebate - 15% 4/ "JOJO's Bizarre Adventure" campaign - 5%
Trader Joe	1.51M	100% of the grant will be distributed as liquidity mining incentives that will be distributed fully to Liquidity Providers by two incentivization forms.
Dopex	1.5M	1/ RDPX V2 Receipt tokens stakers reward (45%) 2/ RDPX V2 Perpetual put vault deposits reward (15%) 3/ Dopex V2 CLAMM LPs reward (40%)
Frax Finance	1.5M	The grant will be used as an incentive in a linear fashion to selected pools.

Data from Launchy by Marco Manoppo

For instance, several ventures that have received tokens under Arbiturm's grant programme are redistributing the tokens to their products' users as shown in the image above. How do you ensure the people receiving tokens don't dump them immediately? How can you minimise the chances of a user running thousands of bots on a product?

A requirement could be to have a Passport score of 20 to ensure actual users receive tokens from such incentivised testnet programmes. This instance may seem far-fetched, but recently, Shapeshift used Gitcoin Passport to determine how OP tokens are passed on to some 6,000 users.

Beyond Transactions

In my previous article, I wrote that apps will eventually have to build context on users by collecting behavioural data to build moats. I also clarified that the approach felt like a repeat of what we already had with Web2 native surveillance capitalism. Gitcoin's Passport is interesting because it creates an open graph of verified product users. Why do you need verification? What role does having stamps that validate your activities elsewhere play on the web? A good start would be understanding the web's nature today.

In 2018, some ⅔ of all links posted on Twitter were by a bot. Between 43–60% of all internet traffic occurs from a bot. The web can afford this because of the decades of work that has gone into building the infrastructure that carries bits and atoms to your devices. In India, where I grew up, 2 Mbps internet was a luxury.

In Dubai, 600 Mbps internet has become the norm on 5g devices. (*You can download entire movies in under ten seconds*). Blockchains will undergo a similar trajectory. And before we realise it, an increasing number of users on applications with financial incentives in the form of token rewards will be merely bots.

Tools like Gitcoin Passport allow newer primitives – like Web3 social networks – to have a community of verifiably human members. The use-case goes even further when you think of models like guilds in gaming. Surely, smart enough individuals will learn how to programmatically engage in a game to generate rewards. In such instances, apps being able to verify if a user is human or not with a single API call or on-chain query is powerful.

A recent paper by Karthik Srinivasan from Booth School of Business explains why user verification would matter in simpler terms. He studied how online creators behave in response to getting attention for their posts across TikTok and Reddit. The researcher used generative AI to synthetically boost engagement with posts to understand how creators would behave.

He noticed that a creator receiving 50 upvotes or three comments would be twice as likely to continue posting. But scale that up to 500 upvotes or six comments, and the creator would have no visible increase in the frequency of their posts.

I found the study interesting because it is tangible evidence that

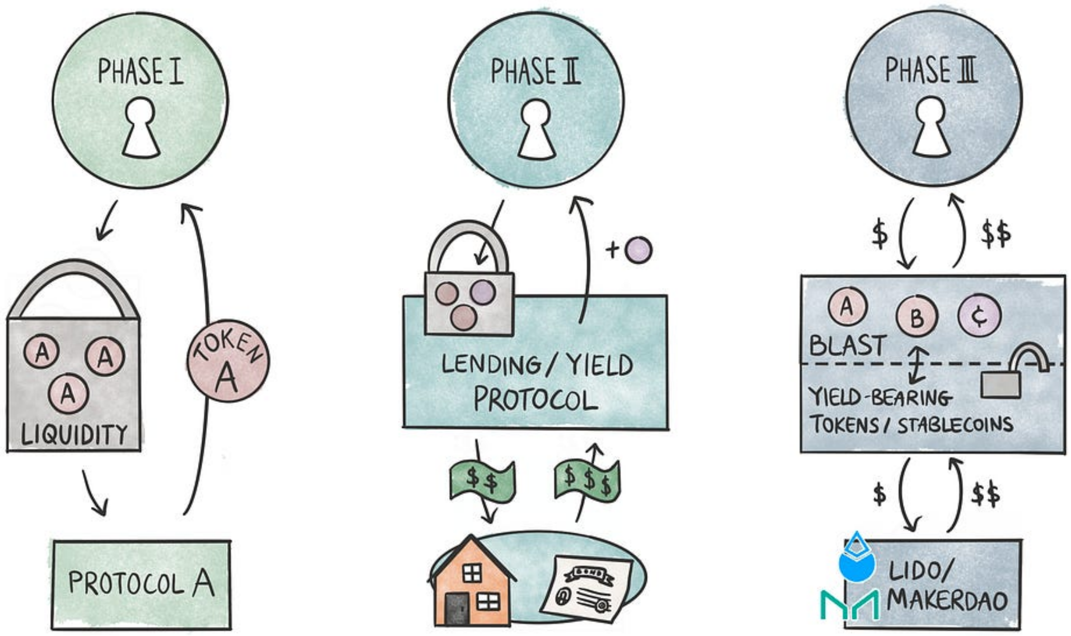
1. Generative AI can synthetically show engagement to a degree where creators don't realise it.
2. Bots can influence the behaviour of not just consumers but also creators.
3. Past a point, more attention has no impact on how frequently creators post.

Any new-age social network – Lens, Mirror, Farcaster or Mastodon – will inevitably need tools like Gitcoin Passport to ensure their users are actual humans in the age of generative AI. In my mind, it is only when we realise that we need better tools to verify who is creating the content we consume that we will eventually embrace primitives like Gitcoin Passport.

Saurabh
decentralised.co

Blast From the Past

Native yield for L2s as the new meta in crypto



Hello!

Ethereum scaling has been one of the most worked areas in crypto. A new L2 that promises to scale Ethereum is announced every few days. Blast, a new L2, was announced on November 21. It has been discussed continuously for the past few days, and you may be tired of reading about it. I hope this piece leaves you with something different.

We're diving into Blast's launch approach, the products the team plans to launch, how this impacts airdrops, the risk-free rate for the Ethereum ecosystem, and what Blast can potentially unlock.

Yield Bearing L2

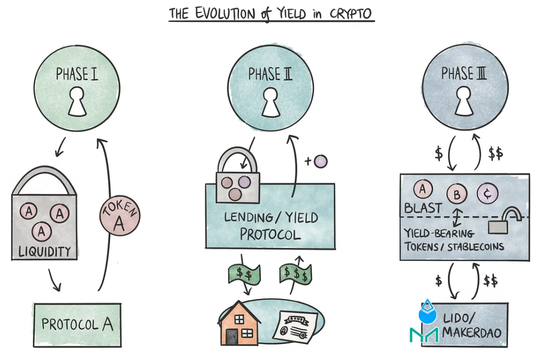
Interest or yield has been one of the core components of finance for centuries. Typically, interest rates are associated with time and risk. Risk is a spectrum. On one side (*least risky*) lie countries with stable governments and policies where doing business is easy. The other end of the spectrum (*most risky*) is penny stocks and unaudited smart contracts deployed by unknown developers. Everything else is in between.

When you lend money to governments, interest and risk are lower. The interest is higher when you lend to a small company with no track record. Every time you lend your money, you earn appropriate interest. Your interest rate depends on the risk-free rate plus the risk premium. The risk-free rate is the interest rate when the risk is assumed to be zero.

Interest rates on bonds issued by governments such as the US, Germany, and Japan are typical benchmark rates (risk-free rates). Every other interest rate in those respective countries is typically higher than the benchmark risk-free rate. This is because every other investment is considered riskier than the investment pertaining to the risk-free rate.

If one looks at how yield evolved in DeFi over time, there are probably three phases.

- The first was when Synthetix started yield farming (*yes, it was Synthetix, not Compound to do it the first time*). Other protocols soon followed. The idea was simple – provide liquidity and get rewarded in tokens. Some protocols offered unfathomable interest rates, which meant nothing because the yield was offered in their 'governance tokens', and they went to almost zero.
- The second phase was when MakerDAO transitioned into RWAs to tap into the real-world yield, and other protocols followed and offered products like bonds. In both these phases, users had to look for applications that provided yield actively. And mostly, when you were earning yield, you could not be bidding on NFTs.
- The third phase is where the yield is starting to become **native and passive.** That is, you hold tokens that start accruing interest without doing anything. And use the same tokens to bid on NFTs or do other things on-chain.



When you keep money in the bank, you earn interest (*in parts of the world where interest rates are positive*). When you keep dollars with Circle or Tether to mint USDC or USDT, Circle and Tether earn interest by investing your dollars in various instruments. But you don't earn interest for holding either. You don't earn any interest when you hold ETH in your Metamask or exchange wallet on Ethereum or any other layer - Blast aims to change that.

The yield earned by Ethereum validators for producing blocks can be considered the risk-free rate of the Ethereum ecosystem. This is because the current monetary policy is designed such that as long as Ethereum exists, validators will keep earning this interest. So, just as every investment in countries is riskier (*relatively*) than investment related to the risk-free rate, every investment (*including lending*) in the Ethereum ecosystem is riskier than staking ETH to produce blocks.

The yield on staked ETH can also be thought of as inflation (*yes, I know 1559 reduces ETH inflation and sometimes makes it deflationary*), and on-chain treasury products give users 4–5% interest. So, when users earn less interest than the validator yield on ETH and T-Bill products on stablecoins, they are technically losing money. One way to change this is to offer native yield. The protocol itself stakes ETH and stablecoins into products to let users earn yield.

Blast says that when you put your ETH on any chain, ETH should earn interest as if it were staked with validators. When you deposit ETH on Blast, it puts that ETH into applications like Lido to earn interest. The USDC deposited on Blast gets deposited into MakerDAO's on-chain T-Bill protocol.

Blast's value proposition simply is this – *you bridge 1 ETH on Blast carry-out activity for a year, and when you withdraw a year later, you will have ~1.05 ETH instead of 1 ETH. The additional ~0.05 ETH comes from native yield. With other chains, as they are currently, you'll only get your 1 ETH back.*

It turns out that 1 ETH does not remain 1 ETH in Blast. But what even is this new protocol?

Origin and Go-To-Market

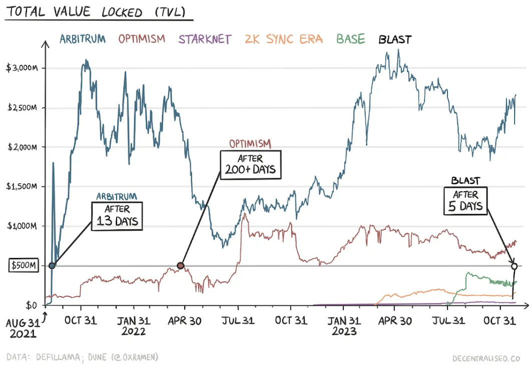
Blast is the new L2 from the team behind Blur. The chain is not live yet, meaning there are no applications or block production. However, it accepts deposits in the form of ETH and stablecoins like DAI, USDC, and USDT. These deposits are only withdrawable once the chain goes live in February 2024.

The Blur team is building an ecosystem of financial products for NFTs (*such as perps*) that encourage higher trading frequency. Secondly, the stablecoin USDB is a rebasing stablecoin that can be considered an interest-bearing stablecoin. The Ethereum L1 infrastructure is not sufficient to support these activities. The motivation for Blur to get into an L2 business is twofold:

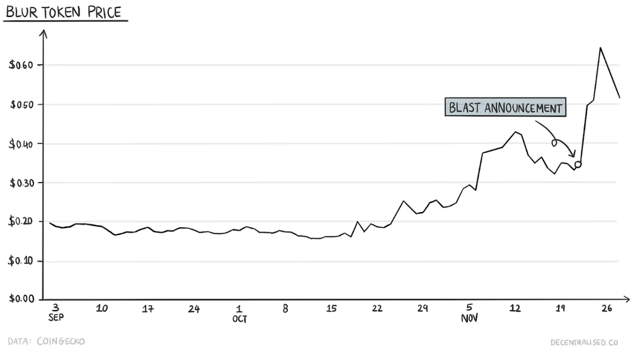
1. L1 (Ethereum) has high gas costs that limit participation and trading frequency.
2. There's no way to earn a native yield on deposits into a protocol on Ethereum.

As a result, Blast is an L2 that provides native yield on ETH and major stablecoins. Currently, it is a multisig with an upgradable contract. The Blast TVL has attracted over $600 million in about a week. As per Coin98, Blast was the fastest to reach the TVL of $500 million.

It did so in 5 days. Arbitrum managed to do the same in around 13 days. This performance was probably due to the signalling effect of the team and investors behind the project.



The Blast team already has a proven track record. Blur has dominated the NFT market with ~80% of the market share. Plus, since the funds are on-chain, tracking movement is easier. Each user who deposits assets to Blast gets points, which will later be redeemed for Blast's anticipated token. Another way to earn points is to stake the Blur token. Following the Blast news, Blur was up ~40% the next day.



The Blast website makes it clear that the airdrop is happening. In addition to points for bridging assets and holding BLUR, Blast has also resorted to referral points to invite more capital. CT (*Crypto Twitter*) is torn on whether this is a good idea. Many call the referral strategy a Ponzi because some of the points from your referrals and their referrals (*and so on*) flow to you. At the same time, others are calling it a clever approach to attract more capital. This is not the first time referrals have been used as a go-to-market (GTM) strategy.

Web2 companies such as Dropbox, Airbnb, and Uber employed referrals as critical growth engines. Dropbox attributes ~10% of its growth to the referral programme. Airbnb stated that its daily bookings tripled after launching referrals. Uber was another example where referrals drove significant growth. So, referrals have been a battle-tested growth strategy; there's nothing wrong with using them. Startups give discounts on their products and offerings to incentivise users.

In comparison, Web3 projects give tokens (*money*) to users to incentivise them to use products. The mechanism is slightly different, but the effect is more or less the same.

Blur (*the Blast team's first project*) launched with a point system for traders. It was clear that the points would later be redeemed for BLUR tokens. When Blur launched, OpenSea was the dominant player. But, a better product with aligned incentives helped Blur attract a significant volume from the incumbent leader and quickly become the largest NFT marketplace by traded volume.

Solana's leading marketplace, Tensor, offers similar reward mechanisms – points for high trading activity, staking Tensorian NFT, and referral points (*higher points for more Tensorians staked*). Much like Blur, Tensor was able to attract a significant volume from Solana's leading NFT marketplace, Magic Eden. Tensor currently has ~66% of the volume share, whereas Magic Eden controls ~26% of the total NFT trading volume.

But having a referral system alone doesn't work. **Businesses need moats to ensure that they retain customers who join through one-off incentives**. **In the case of Blast, native yield could be a moat, at least for some time.** This is because currently, there's little cost to move from, say, Optimism or Base to Blast. In fact, capital moving from one chain to another in anticipation of airdrop is quite common. **For the first time, there will be an opportunity cost to move. If you move, you won't earn native yield.**

Blur used a points system for its airdrop. As soon as the exchange launched, it was known that the token would launch at some point, and users were incentivised to earn points by trading. Blast follows the same playbook but with a pre-product one-way bridge like Ethereum's beacon chain.

In my view, the primary contention with Blast's approach is that they are taking users' money until the mainnet launch in February 2024 (*for ~3 months*) without allowing them to withdraw. But couldn't one argue that's what Ethereum's beacon chain did? The beacon chain was launched circa November 2020, but the withdrawals (*from the deposit contract*) were made available only after the Shanghai fork in April 2023.

Yes, the withdrawal address was controlled by users, but when users could withdraw was unknown. Reputation damage to Paradigm and Standard Crypto is likely more than the TVL if the funds are lost. Interestingly, Paradigm was vocal about disagreements with the Blur team on launching a bridge before applications and not allowing withdrawals for three months.

Another issue is with the rebasing of the stablecoin. As the balance of the stablecoin consistently changes, it is less composable. Why? Think of it this way. When you deposit this coin in a contract (say, a DeFi protocol), it reads the balance of the token and stores this value. But your balance changes over time, whereas the value stored in the contract doesn't.

In summary, Blast's GTM is the following:

- Offer passive yield on ETH and stablecoins without users having to do anything.
- Launch points and referrals to align incentives and drive growth.
- Share 100% of the gas revenue with developers. Other L2s keep this revenue for themselves.

The Yield Meta

L2s (blockchains in general) are fighting for users and their capital. A high number of L2s translates into fragmentation of liquidity and users across layers. In this light, competing against other L2s is challenging. With many L2s offering essentially the same things – lower fees and similar applications – how do you differentiate yourself from the rest of the pack?

Remember, you need one thing as a hook: one feature that users care about that is unique to you. You will likely attract users when you are the first mover in a new category of services or applications. Web2 companies like Facebook, Instagram, and Twitter had one unique aspect that appealed to users.

Blast's native yield offering is the hook to take it from 0 to 1. No other L2 offered native yield until now. So, if you are staking/lending ETH on Ethereum or Arbitrum at 3 or 5%, Blast is a better alternative. You have little reason to stay with the others because it offers you the primary validator yield (~4.5%) and a token airdrop.

The Blur team's decision to build Blast stems from the fact that over $100 million idle TVL in Blur pools doesn't earn interest. But Blast wasn't the first to put idle capital to use. Gnosis Chain upgraded its xDAI bridge to deploy its reserves into Spark Protocol's sDAI vault so that the capital sitting in the bridge earns interest. The proposal was made in late August and implemented in early November.

Second Order Effects

I think almost all L2s are watching what happens to Blast. If they want to attract users from Blast, it is not as easy because, suddenly, there's an opportunity cost to move the capital from one chain to another. There will probably come a point when almost every L2 employs native yield in some way.

So far, Blast says that they are only using applications such as Lido and MakerDAO to earn yield for users. However, there may come a time when Blast or other L2 developers use other avenues to offer a higher yield. Logically, these avenues will be riskier. At this point, **developers will be turning into asset allocators**, which is perhaps not the most desirable outcome. What I mean by this is that more chains will start offering "native yield" on user deposits by deploying assets into "safe" protocols like MakerDAO and Lido.

Soon enough, someone will want to differentiate themselves by offering a higher yield. Naturally, this means more risk. Developers will likely think of more ways to increase the yield or hire hedge funds to generate more yield. Although this is much like what FTX did, the only solace here is that funds are on-chain, so tracking the movement is trivial.

Cobie once wrote on his blog that *'winners' are a good catalyst for a meta. People are inspired by the success of a project and they want to look for* *things that are similar. Founders decide they can build something like that, but better! Investors want to be early for the next version of this great idea.*

Something similar should be expected here. The likes of Ronin and Aevo have already hinted at similar offerings. Once this approach is successful, offering native yield may become a hygiene factor. There are ~5.3 million ETH locked across L2s as of November 27. If we see native yield as the new meta, a significant chunk of this can get staked via different protocols such as Lido.

28.6 million ETH is staked via validators to secure Ethereum, 23.8% of the circulating supply. If all of the L2 ETH gets staked, the total staked ETH will reach ~33.9 million, or over 28% of the circulating supply. Staking protocols will likely be among the primary beneficiaries of the native yield trend.

There are a few things that excite me about the Blast launch:

- The GTM combines Ethereum's beacon chain approach and how Blur attracted its core user base.
- Does Blast maintain its first-mover advantage in the new native yield meta?
- How do established L2s such as Arbitrum and Optimism respond?
- What hooks do the new L2s provide to attract users?

These questions will be answered with time, and I can't wait to see how this unfolds and write again.

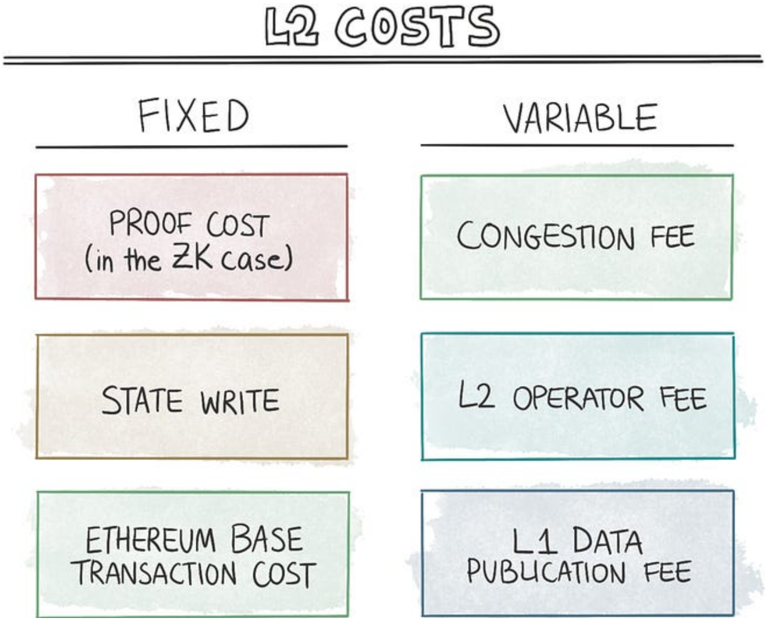
What I would like to see is Blast becoming a full-fledged NFT-fi ecosystem. In the previous cycle, we realised that the qualities offered by NFTs could be valuable. Knowing the provenance of a digital good becomes trivial with NFTs. We want to "own" the media we consume on a daily basis. There is a market for digital-first products. However, the ecosystem to support these assets doesn't exist today.

Blur already has a lending product, Blend. And the team is building an NFT perpetual futures product to be deployed on Blast. So, the Blur<>Blast offering will have spot and futures NFT trading plus lending. The lower transaction cost on Blast can be a factor that drives a higher volume of NFT trading. When you have to pay $100+ in gas fees, it doesn't make sense to trade low-value NFTs, but with fees dropping to 1/1000th, NFTs become accessible to more people and are likely to unlock new use cases.

Saurabh
decentralised.co

The L2 Paradox

A little bit of weekend economics.



Hello,

TL:DR : Roll-ups are like lanes which require resources to maintain. If there aren't enough vehicles passing through the lanes, the cost incurred by each vehicle rises substantially. The lack of traction on rollups ironically adds to the per-transaction cost on them. We explore how this affects liquidity and users in today's issue.

In 2017, during periods of peak demand, the cost of a transfer would surge to $3. Occasionally, when ICOs or NFTs clogged the network, the fees would surge to $10. The Ethereum ecosystem acknowledged the problem of high fees and pivoted to a rollup-centric roadmap. Remember that rollups reduce the computation burden on Ethereum. Because there is a limit on gas that can be consumed per Ethereum block, rollups serve to free up the gas required for computation and use it for settlement and data availability.

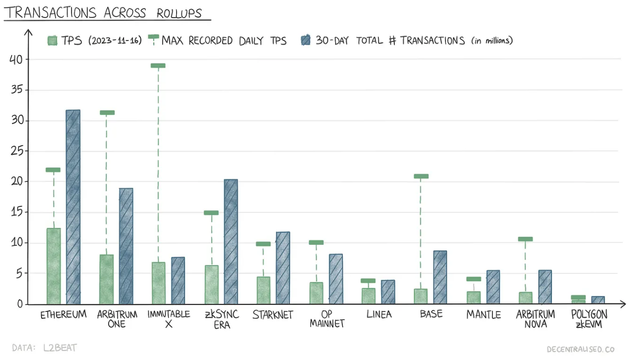
Let me explain with the example of a restaurant that has expandable space to accommodate guests during peak hours. Guests are served and catered to in a different space separate from the main building. But all their bills are settled at the cash register in the main building. The separate space is a rollup, whereas the main building is the Ethereum chain. Bills or invoices sent to the main building are analogous to rollups posting data on Ethereum. This article by Delphi is a good read that will provide more context about rollups.

Consider the act of transporting bills from the separate space to the cash register at the main building as "submitting" proofs. There's an element of cost in that an employee would have to ensure all the items were priced right in the bills and port over all of the data to the main cash register. As this "cost of submitting proof " is fixed independent of the number of bills, it declines for individual bills if there are multiple customers doing transactions. But if an employee does it for each bill, the benefit of having a separate place for billing reduces. This, is the crux of what we explore today.

Being rollup-centric allows Ethereum to be the most secure and decentralised chain for rollups. If the base layer focuses on ensuring security and decentralisation, it makes sense to outsource computation. Rollups are supposed to scale Ethereum between ~50 to ~500X. In the last few years, several rollups were launched to make Ethereum more scalable. A recent surge in fees on the Polygon POS chain makes the case for rollups.

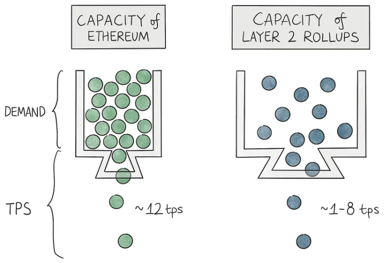
On November 16, users started minting PRC-20 tokens like Bitcoin's Ordinals. The number of transactions on the chain jumped 8X, from ~2 million to ~16 million, from the previous day. As a result, the fees also skyrocketed by about 70X.

Currently, this is what the transactions per second (TPS) for several rollups looks like: While Ethereum shows a TPS of ~12, rollups like Arbitrum and Starknet are at ~7 and ~5.



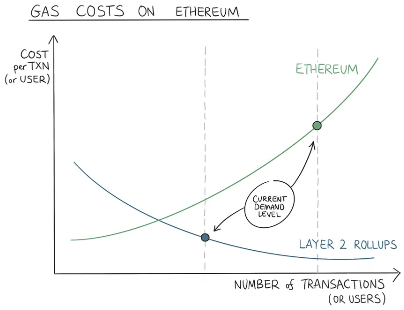
Note that this is Polygon zkEVM, not Polygon POS. To read more about zk EVMs, visit here.

Despite the potential of rollups, they haven't really lent scale to Ethereum yet. But what even is scale in the context of L2s? TPS is a good metric when the capacity is completely utilised. But as of now, the demand for L2s has yet to test their capacity, so as a metric, the TPS is a bad measure of scale. It is like suggesting a car has a mileage of 500 km. Does that matter if its fuel tank is empty? L2s without users have a lot in common with empty fuel tanks.



For zero-knowledge (ZK) rollups, the cost of posting a batch of blocks or transactions onto Ethereum remains more or less fixed in terms of gas consumption (note that the price of gas changes based on demand). Typically, posting transaction data on the mainnet constitutes ~95% of the costs associated with rollups; the remaining 5% is for computing.

Usually, these costs remain the same regardless of the number of transactions. For example, a swap on Ethereum costs 100,000 gas, and the same swap on Starknet costs ~1100 gas. But the proof costs ~5 million gas.



As the number of transactions on L2s increases, the cost per transaction decreases. With the increased number of transactions, L2s can post data on Ethereum more frequently. Ethereum produces one block in ~12 seconds, but the time taken by different L2s to post batches of transactions or blocks varies based on the type.

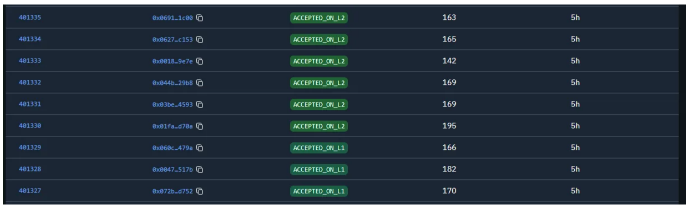
Optimistic rollups (ORUs) don't provide proof of correctness to the base layer (Ethereum), whereas Validiums or ZK rollups do. These proofs are bulky in terms of gas consumption. As ORU transactions don't submit proofs, there's no way of knowing if the rollup operated has indeed played by the rules of Ethereum (*a simple way of saying whether the state changes carried out by the ORU operator are correct).* This is why ORUs post transaction data more frequently to Ethereum.

For example, Arbitrum submits batches to Ethereum every ~5 minutes. The number of L2 blocks and transactions in these batches varies based on the overall transaction demand on Arbitrum.

On the other hand, since ZK rollups post proofs, they can afford the luxury of being less frequent. When I checked on Starknet Explorer, the last confirmed or accepted block on Layer 1 was 5 hours ago. This means that Starknet submits batches of blocks to Ethereum every few hours. Whether it is 5 hours or 1 hour doesn't matter at the moment. The gap between the two checkpoints is higher than desired. Functionally, this delay doesn't hamper users because most of the applications are aware of the L2 state. But it is about trust.

Until a transaction is finalised on L1, we are trusting the L2 operator. If we were okay with trusting entities, we did not need Web3 at all. Any activity that involves external stakeholders who don't want to trust L2 operators will have to wait for L1 confirmations.

The gap can be lowered when the cost of proof is amortised across many transactions. The low number of transactions prevents Starknet from posting proofs and state updates to Ethereum more frequently. For context, Ethereum clocked ~31 million transactions compared to Starknet's ~15 million in October, according to data from Token Terminal.



401335	0x0691…1c00	ACCEPTED_ON_L2	163	5h
401334	0x0627…c153	ACCEPTED_ON_L2	165	5h
401333	0x0018…9e7e	ACCEPTED_ON_L2	142	5h
401332	0x044b…29b8	ACCEPTED_ON_L2	169	5h
401331	0x03be…4593	ACCEPTED_ON_L2	169	5h
401330	0x01fa…d70a	ACCEPTED_ON_L2	195	5h
401329	0x060c…479a	ACCEPTED_ON_L1	166	5h
401328	0x0047…517b	ACCEPTED_ON_L1	182	5h
401327	0x072b…d752	ACCEPTED_ON_L1	170	5h

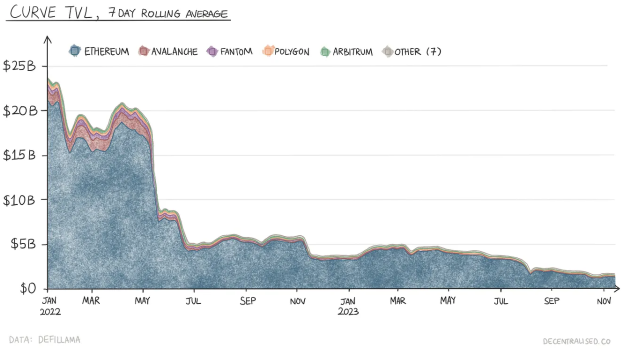
Source – Starknet Explorer

The point is that **the per-transaction cost on Ethereum increases linearly or, at times, even exponentially with the demand. And per-transaction cost on ZK rollups decreases as transactions increase.** We are currently in a phase where the transaction demand on L2s is insufficient to reap the benefits of off-chain computation.

The total number of transactions on Ethereum was ~32 million, whereas the most used L2, zk Sync Era, was ~20 million, followed by Arbitrum One at ~19 million. The number of transactions across L2s gets fragmented, not letting any one of the L2s achieve economies of scale.

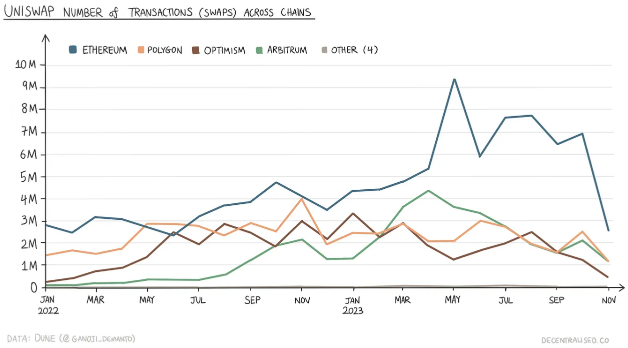
Fragmentation

Liquidity, users, and transactions, the metrics that can help an L2 to scale meaningfully, are all scattered across different L2s. I looked at Curve's liquidity distribution across chains: 93% (~$1.6 billion) of Curve's TVL is on Ethereum.


CURVE TVL, 7 DAY ROLLING AVERAGE

DATA: DEFILLAMA

Looking at the number of Uniswap transactions (swaps) across different chains paints the same picture. About 43% of the transactions take place on Ethereum, whereas ~21% take place on Arbitrum.


UNISWAP NUMBER of TRANSACTIONS (SWAPS) ACROSS CHAINS

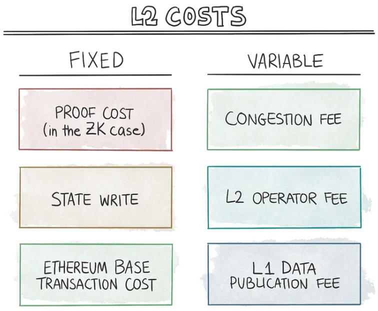
DATA: DUNE (@ GANOJI_DEMANTO)

These data points indicate a cap on the number of L2s that can thrive. Infrastructure exists to support applications and users. Currently, there are more lanes than required. A developer building on these layers must consider how the application can be deployed across a maximum number of L2 chains.

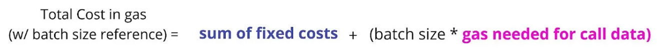
In some cases, like Starknet, developers need to place a bet on the ecosystem because the development environment is different.

Rollup economics – the more is not the merrier

Fragmentation of users and liquidity means that rollups cannot make consistent revenue. When a user executes a transaction on a rollup, they pay a fee. This fee plus the maximum extractable value (MEV) make up the value of the transaction. L2 operators earn a component of this fee. Operators provide critical infrastructure to run the rollup software. For rollups to be sustainable, they must be profitable.



Users come to rollups because they are cheap, and they can be cheap only when there is demand. A few developments are underway that could help ease gas costs. Although this is not a substitute for higher user demand, it will help lower L1 data publication costs. As this cost is passed on to users, they will pay lower fees. Lower data publishing fees also mean that the numerator of cost to post data on Ethereum is reduced, helping more frequent updates to Ethereum and very likely higher throughput gains.



Total Cost in gas (w/ batch size reference) = **sum of fixed costs** + (batch size * **gas needed for call data)**

Source – Celestia Forum

Currently, every byte of data in the call data field requires 16 units of gas (it is read-only data storage for Ethereum; this is where rollups post their data in Ethereum blocks). EIP 4844 proposes to reduce this cost to 3. This is ~5X scalability gain for rollups as the cost drops ~1/5th.

Data availability layers like Celestia, which are cheaper ways of storing data than Ethereum, will reduce the size of the data needing storage on Ethereum. Such cheap data storage can be used by a different flavour of zk rollups where the data is not posted on Ethereum but onto a chain managed by a data availability committee. These efforts will drastically reduce costs for rollups.

There can be some analysis of the number of daily transactions for different rollups to break even. But that's for another day. Signs point towards a future where we are left with a handful of rollups. A lot of projects launched L2s because they were in vogue. But, finding users to keep these L2s going will likely be a tough task. And no – token incentives are not a solution. **Tokens are equalisers, not differentiators.**

What I mean by that is launching a token won't give an L2 any competitive advantage. When the first L2 launched a token, it was almost a given that every other L2 would have to launch a token. **Rollup moats will most likely lie in their ecosystem – projects and communities, developer support, and how easy it is to port existing Ethereum applications to L2**.

I think there will be consolidation in the rollup landscape simply because there's a cap on the number of users and, in turn, transactions. I am on the lookout for how this plays out.