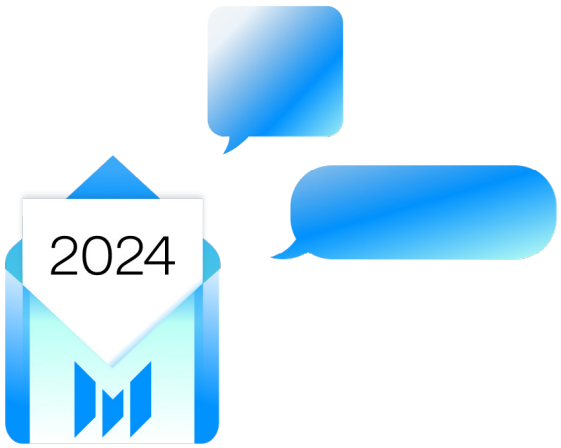
Messari

CRYPTO THESES 2024

KEY TRENDS, PEOPLE, COMPANIES AND PROJECTS TO WATCH ACROSS THE CRYPTO LANDSCAPE, WITH PREDICTIONS FOR 2024.



WELCOME

Friends:

The carnage of the past twelve months in crypto has been brutal for all of us. We've grinded through bankruptcies, lawsuits, layoffs, turnover, and a general malaise that comes with a bad hangover after a big party.

It's been surreal at times, too.

In some respects, the industry was blown back to 2013 following its first credit crisis (survivors include decade-long operators like Coinbase, Kraken, and Circle). But we have never been operating further out on the cutting edge of tech than we are today. There's lots of secure block space and scaled transaction processing, composable identity and DeFi applications, stablecoin proliferation, etc.; and Wall Street's embrace is imminent, whether Jamie Dimon likes it or not.

I didn't think Sam Bankman-Fried would be in jail by the time I wrote the 2024 Theses. But his swift comeuppance and lengthy prison sentence marked an important turning point for us all. If last year's report was "It's So Over," this year's report is "We're So Back."

We're back to bitcoin dominance. Back to building parallel financial systems "just in case" national currencies inflate, or we lose access to banking or credit. Back to peer-to-peer applications and permissionless inventions vs. cultish centralized services. Back to a focus on an uncensorable internet in an era where free speech and open communications are far from guaranteed. (Elon bought us some time, but there are growing threats.)

That's why I remain perma-bullish on this technology and this community.

There is reason for hope and optimism. A big part of succeeding in crypto is simply surviving from cycle to cycle. If you're reading this, you're one of the survivors, and I wrote this for you.

The usual disclaimers apply: this report is not investment advice, mistakes are likely in a compendium this long and rapidly written, and (this year, especially) you are prohibited from canceling me for (accurate material) political analysis that may be unpopular.

This is a free report that we're making available early to subscribers. We're still emerging from a bear market, so if you get value out of the Theses every year, I hope you'll support our team: subscribe to Pro or Enterprise, test our API, and consider Protocol Services for your community.

Don't make me put Barbara on this. Please support the builders at Messari.

Happy holidays!

-Ryan Selkis (aka TBI)

0.1 Perspective

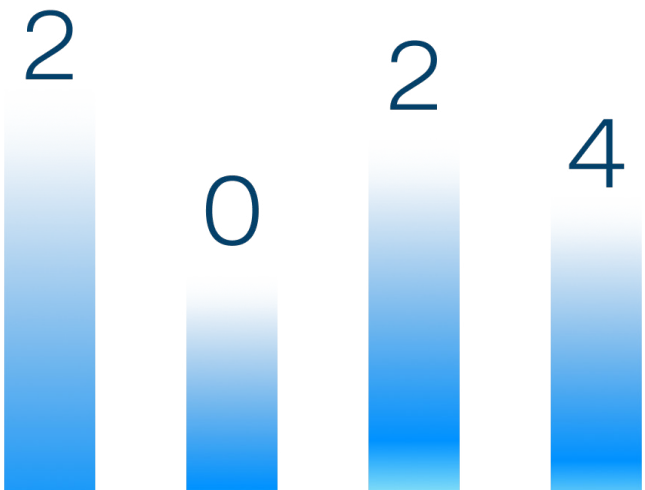
This was the industry five years ago. When in doubt, zoom out.

Asset		Price (Live)	Mcap Today	Mcap 12/15/2018	Mcap % Chg → 12/19/18	Sector
1	Bitcoin BTC	$42,408.88	$821B	$55.98B	+1,183.05%	Cryptocurrency
2	XRP XRP	$0.624	$33.24B	$11.74B	+132.08%	Payments
3	Ethereum ETH	$2,255.05	$267B	$8.56B	+2,474.72%	Smart Contract Platform
4	Tether USDT	$0.999	$90.82B	$1.85B	+4,764.99%	Stablecoins
5	Stellar XLM	$0.125	$3.46B	$1.84B	+58.10%	Payments
6	EOS EOS	$0.782	$839M	$1.64B	-64.81%	Smart Contract Platform
7	Bitcoin Cash BCH	$230.66	$4.45B	$1.40B	+143.82%	Payments
8	Litecoin LTC	$72.45	$5.25B	$1.38B	+192.50%	Cryptocurrency
9	Bitcoin SV BSV	$49.94	$949M	$1.22B	-35.56%	Cryptocurrency
10	TRON TRX	$0.103	$8.98B	$841M	+810.97%	Smart Contract Platform
11	Cardano ADA	$0.620	$21.22B	$731M	+2,273.45%	Smart Contract Platform
12	Monero XMR	$172.12	$3.09B	$646M	+299.64%	Cryptocurrency
13	BNB BNB	$246.90	$37.14B	$588M	+5,000.06%	Smart Contract Platform

(Source: Messari Screener)

Crypto remains inevitable.

TABLE OF CONTENTS



messari.io

CHAPTER 1

TOP 10 INVESTMENT TRENDS FOR 2024

1.0 Investment Trends

Last December, I retired the term “Web3” on behalf of everyone in crypto.

It was a bullshitty, PR-speak moniker that ruined every interesting thing we were trying to build. NFT pfp collections were Web3, “DeFi 2.0” was Web3, Sam Bankman-Fried was Web3. I wanted more crypto: personal wallets, transaction privacy, infrastructure advancements, DeFi, DePIN, and DeSoc primitives that didn’t rely entirely on ponzinomic schemes. Things like that.

This year did not disappoint.

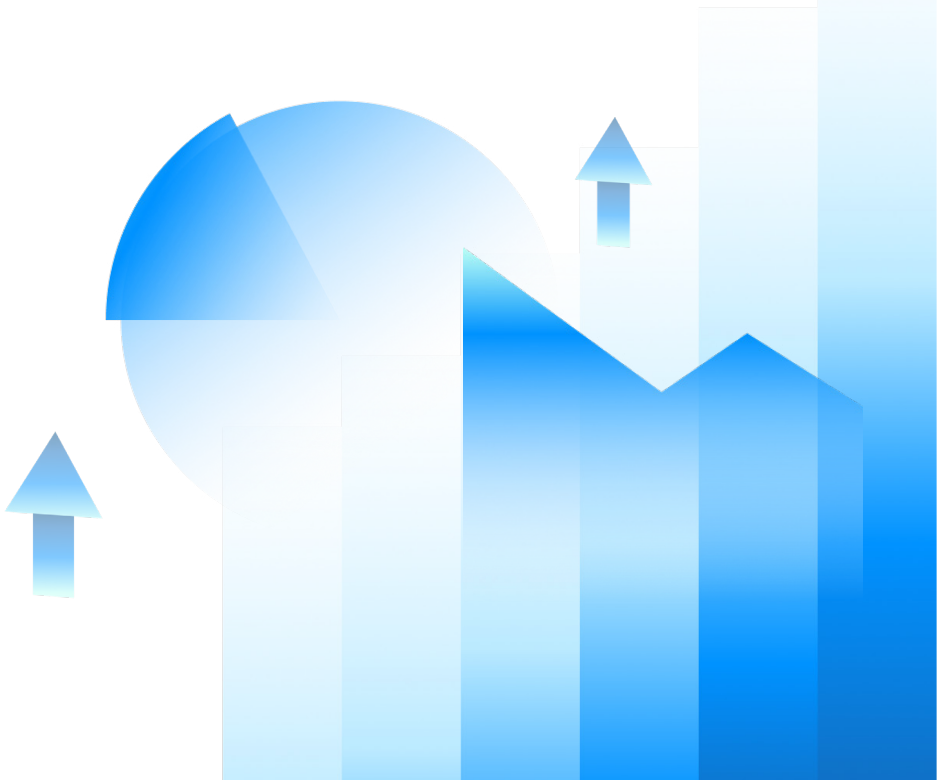
Since murdering the term Web3 in cold blood, crypto’s market cap has nearly doubled. Our biggest fraudsters are either in jail or heading there soon. Great products with slick designs got shipped. And I’m even more excited about crypto’s prospects in 2024.

In short, the state of crypto is strong.

I recognize there are some newcomers reading this treatise, so I’ll remind you that this is a 201-level course, not *Baby’s First Bitcoin*. I encourage you to play catch-up if you can: Matt Levine’s masterful crypto explainer / takeover of *Businessweek*. This list of beginners’ resources. The excellent “Foundations of Blockchains” course for the technical. Otherwise, I assume prior knowledge, and if I’m curt, it’s because time is a factor.

This opening “investment trends” section is for those of you who want to get away with telling your friends you read this whole report. I don’t feel the need to start with a victory lap on my first three sections from last year’s report (“crypto is still inevitable”), but we have nice tailwinds across a variety of market segments, and evidence to support the recent much-needed bullishness after a dark winter.

We’ll start with the bull case for bitcoin in 2024.



1.1 BTC & Digital Gold

"Where are we now? January 2015. December 2018. i.e. Sell-a-kidney-to-buy-more territory."
-My thoughts on Bitcoin in December 2022. You're welcome.

While it's difficult to predict in the short-term where bitcoin will trade, its attractiveness over longer time scales is almost indisputable at this point.

We don't know whether the Fed will raise rates further or slam the brakes, reverse course, and begin quantitative easing in earnest. We don't know whether we will face a recession fueled by commercial real estate or if we will successfully manage a "soft landing" for the economy after the surreal, post-COVID period of monetary and fiscal whiplash. We don't know whether stocks will drop or chop, or if bitcoin will prove to be correlated to tech stocks or gold.

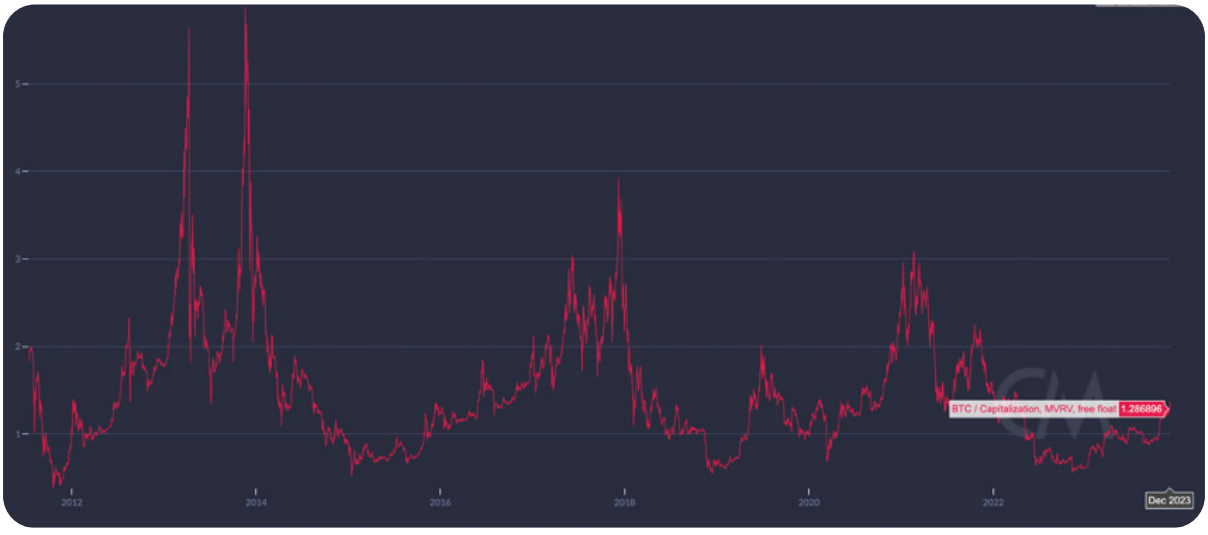
On the other hand, the long-term thesis for bitcoin is straightforward. Everything is going digital. Governments are overly indebted and profligate, and they will continue to print money until they fail outright. There are only 21 million bitcoins that will ever become available to investors. And the strongest meme in the markets has its quadrennial marketing event coming up, via the 2024 bitcoin halving.

Sometimes you have to just keep things simple!

To stay consistent year-over-year, let's revisit the sell-a-kidney MVRV graph I wrote about last year. Recall that this compares the current market value (MV) of bitcoin (price * total supply = MV) to the *realized* market value (RV) (the sumproduct of price * unit supply *at the time each unit last moved onchain* = RV).

A ratio under 1 is golden. A ratio over 3 has always marked a cycle top.

Is bitcoin still a good "buy" after a 150% rally this year? Kinda.



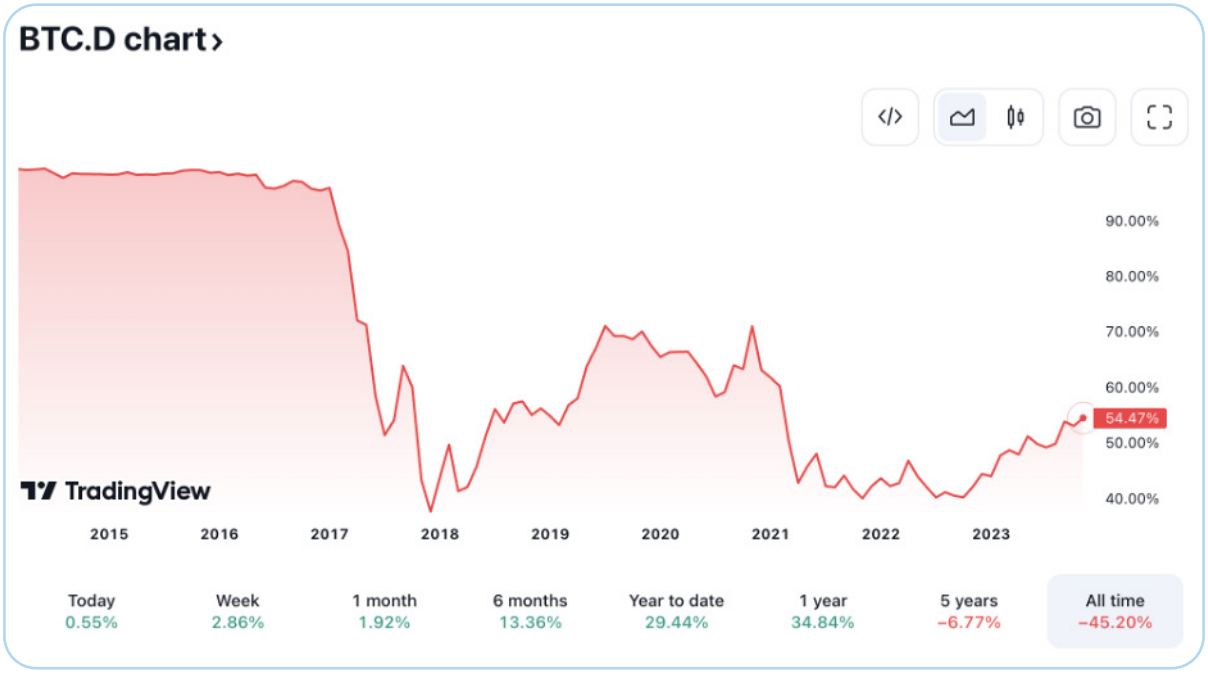
(Source: Coin Metrics)

Maybe we're not in deep value territory any longer, but investors certainly aren't taking a leap of faith in buying bitcoin at a 1.3 MVRV given some of the institutional tailwinds now at our backs (ETF approval, FASB accounting changes, new sovereign buyers, etc. See Chapter 4.1).

Keep in mind that as more bitcoin inevitably gets locked up in ETF products, the MVRV ratio will get pulled artificially higher, too, as new buyers won't show up as frequently onchain versus on the NYSE and Nasdaq tape. An MVRV slightly over 1 is right below the historical median.

You know what's even more enticing, assuming you're excited about crypto as an asset *class*?

Bitcoin tends to lead recoveries. We've recently seen multi-year highs for bitcoin dominance, but still nothing close to the high-water mark we attained at the beginning of the 2017 and 2021 bull runs. Bitcoin dominance shrank from 87% to 37% in 2017. It reclaimed 70% during its consolidation phase and run-up to $40,000 in 2021 before dropping to 38% at the height of the bubble. We just tapped 54%. There's still room to consolidate.



(Source: Trading View)

It's difficult to see catalysts for another crypto boom that *do not* begin with a sustained face-melting bitcoin rally, to be honest.

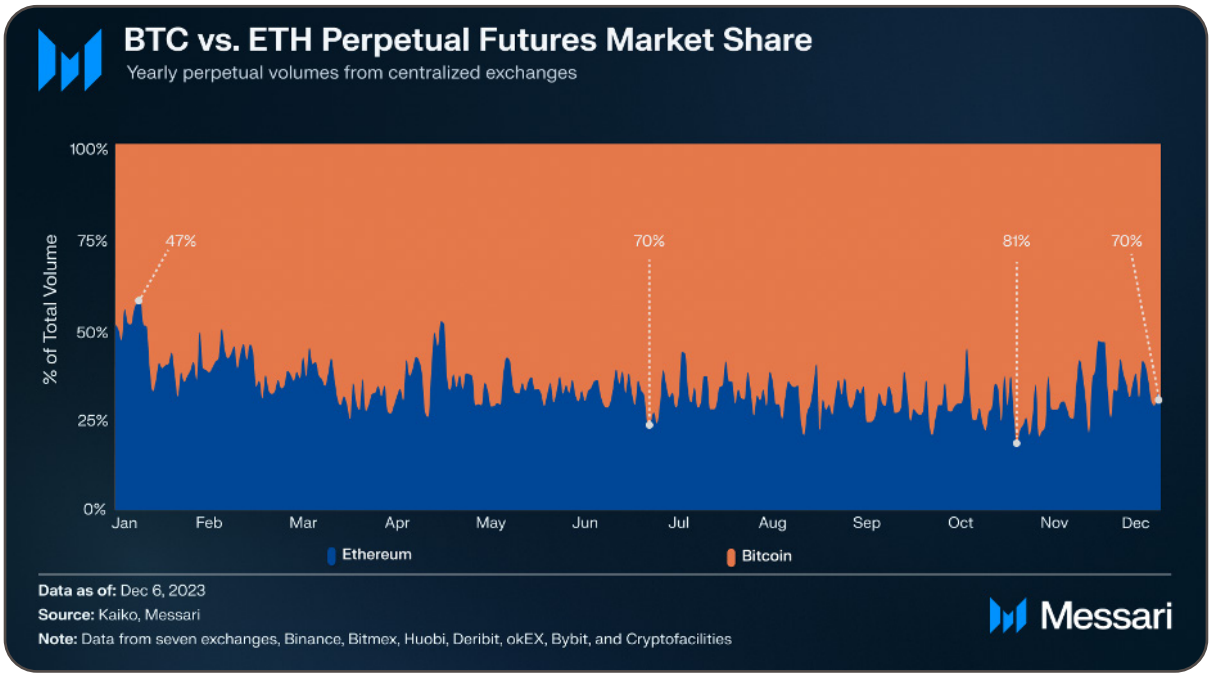
DeFi has ongoing regulatory headwinds that will crimp growth in the short term. NFT activity is mostly dead. Other up-and-coming sectors (stablecoins, gaming, decentralized social and infrastructure, etc.) are more likely to tick up slowly and steadily, not sharply and suddenly.

The big money managers agree, too. Binance had some excellent research recently that showed "bitcoin" sentiment crushing "crypto" sentiment among asset allocators over the

summer (though perhaps that sentiment is shifting with ETHBTC's underperformance). With momentum like this, my bet is that bitcoin dominance retakes 60% in an ETF-driven rally (leading the way up) OR severe macro stress (consolidating the way down).

Even if I'm wrong, and we've already seen this cycle's high-water mark for bitcoin dominance, I find it extremely unlikely that bitcoin prices decline nominally AND relatively. The highest EV play in the early stages of a crypto bull run has always been to bet on the king, and this cycle has been (and will continue to be) no different.

I will reiterate what I said last year: I find Ethereum's "ultrasound money" thesis to be wholly unconvincing. If such a meme had legs, then the liquidity scoreboard wouldn't look like this, even after an ETH futures ETF was approved:



We probably won't see another 100x for bitcoin, but the asset could easily outperform other established asset classes once again in 2024. Eventual parity with gold would yield a price per BTC of over $600,000. And remember: gold has many of the same macro tailwinds, so that price isn't necessarily a ceiling.

If monetary crises get bad enough, no price will be too high: 1 BTC will be worth 1 BTC.

[Required Reading: BTC Q3 Quarterly Report]

1.2 ETH & The World Computer(s)

Ethereum's successful "Merge" (Sep. 2022) and its completion of the "Shapella" upgrade (Apr. 2023) were some of the most technically impressive software upgrades of all time. The Merge also ushered in a new era for ETH as a net deflationary digital asset.

I love Ethereum and everything it has spawned. Messari itself doesn't exist without the cryptoasset ecosystem that Lord Vitalik built. But the long-term *investment* case for ETH looks more like Visa or JPMorgan than Google or Microsoft, or a commodity like gold or oil.

ETH is straddled. BTC outperforms ETH as digital money thanks to institutional allocators' interest in the digital gold "pure play" while broad availability of Ethereum substitutes (L0s, L1s, L2s) will likely lead to those substitutes' outperformance as they sop up onchain volumes relative to the Ethereum main chain. I don't see a scenario where ETH outperforms bitcoin AND its up-and-coming, higher-beta peers.

That said, I would not bet against ETH, *nominally* speaking.

It's survived multiple technical challenges and market cycles. It's (arguably) got better supply dynamics than bitcoin does today. I agree that any ETH bridged to other rollups is likely gone forever and "not coming back to hit the bid."

If anything, being bearish on ETH relative to the field is not an indictment of *Ethereum*, but rather a clear-eyed realization that ETH as an asset has been *incredibly dominant* so far, and has set the bar impossibly high to maintain over a 60% market share in its network token peer group. When I think of Ethereum vs. Solana, I think of Visa vs. Mastercard, not Google vs. Bing in terms of relative strength.

Even if I give ETH maxis a fair shake, I must again point to the scoreboard and note that ETH is less of a bargain than BTC.

(Source: Coin Metrics)

I'll be talking more about the tech later on, but I know you aren't sitting around the fireplace salivating for my take on proto-danksharding. You want the 70 IQ bull/bear recommendation, and betting on ETH is right in the middle of the bell curve. I'll argue about this with the *Bankless* guys sometime soon, I'm sure.

(Note: While I hate hedging, this strong opinion has weakened since I first drafted this section. With BTC now up ~150% and SOL up more than 6x year-to-date, we're overdue for some mean reversion for ETH, which has been a stablecoin for too many months and lagged considerably.)

[Required Reading: ETH Q3 Quarterly Report]

1.3 The (Liquid) Field

BTC, ETH, and U.S. dollar-backed stablecoins represent 75% of the $1.6 trillion in total crypto market cap today. That won't always be the case.

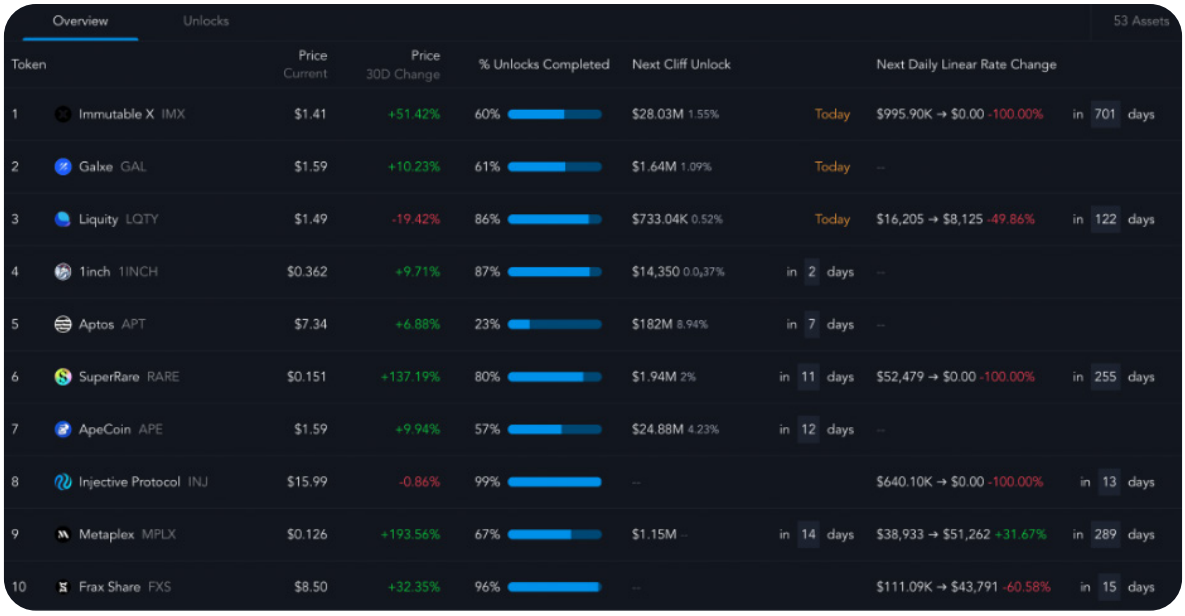
I founded a company on the thesis that the other 25% of the crypto pie would grow 100x over the next decade and that investors would need sophisticated diligence tools to parse thousands of crypto assets, not just two. A 100x for "the field" from today's market size would put the liquid crypto capital markets just north of the private capital markets ($20-25 trillion) and about 30% and 35% of the size of the global debt and equity capital markets, respectively.

What's more: if you believe (as I do) that blockchains are accounting innovations at their cores, then all assets will eventually be "crypto" assets that trade on public blockchains versus legacy clearing and settlement systems, whether they are "utility tokens" or "security tokens." Over time, the Venn diagram of crypto versus TradFi looks more like a circle.

There are pros to just sticking with a market cap weighted index of BTC and ETH, though.

For one thing, it's been a winning hand historically, and you (definitionally) captured 75% of the market's upside over the past ten years if you simply went to the 2014 North American Bitcoin conference in Miami and bought whatever Vitalik was selling (the Ethereum ICO and bitcoin). Those blue-chip assets are now crypto's best "hard" investments, in that you don't run the risk of getting crushed by supply dilution over the course of time either. Many other top projects have gargantuan treasuries that get sold off by insiders over time. Their "market caps" could go up while their token prices stay flat or decline.

(This is one reason we launched our token unlocks dashboard this quarter. We want people to understand where sell-side pressure could come from, as I find it unlikely that we'll return to the "bullish unlocks" madness of 2021.)



Overview | Unlocks | 53 Assets

	Token	Price Current	Price 30D Change	% Unlocks Completed	Next Cliff Unlock		Next Daily Linear Rate Change	
1	Immutable X IMX	$1.41	+51.42%	60%	$28.03M 1.55%	Today	$995.90K → $0.00 -100.00%	in 701 days
2	Galxe GAL	$1.59	+10.23%	61%	$1.64M 1.09%	Today	--	
3	Liquity LQTY	$1.49	-19.42%	86%	$733.04K 0.52%	Today	$16,205 → $8,125 -49.86%	in 122 days
4	1inch 1INCH	$0.362	+9.71%	87%	$14,350 0.0,37%	in 2 days	--	
5	Aptos APT	$7.34	+6.88%	23%	$182M 8.94%	in 7 days	--	
6	SuperRare RARE	$0.151	+137.19%	80%	$1.94M 2%	in 11 days	$52,479 → $0.00 -100.00%	in 255 days
7	ApeCoin APE	$1.59	+9.94%	57%	$24.88M 4.23%	in 12 days	--	
8	Injective Protocol INJ	$15.99	-0.86%	99%	--		$640.10K → $0.00 -100.00%	in 13 days
9	Metaplex MPLX	$0.126	+193.56%	67%	$1.15M --	in 14 days	$38,933 → $51,262 +31.67%	in 289 days
10	Frax Share FXS	$8.50	+32.35%	96%	--		$111.09K → $43,791 -60.58%	in 15 days

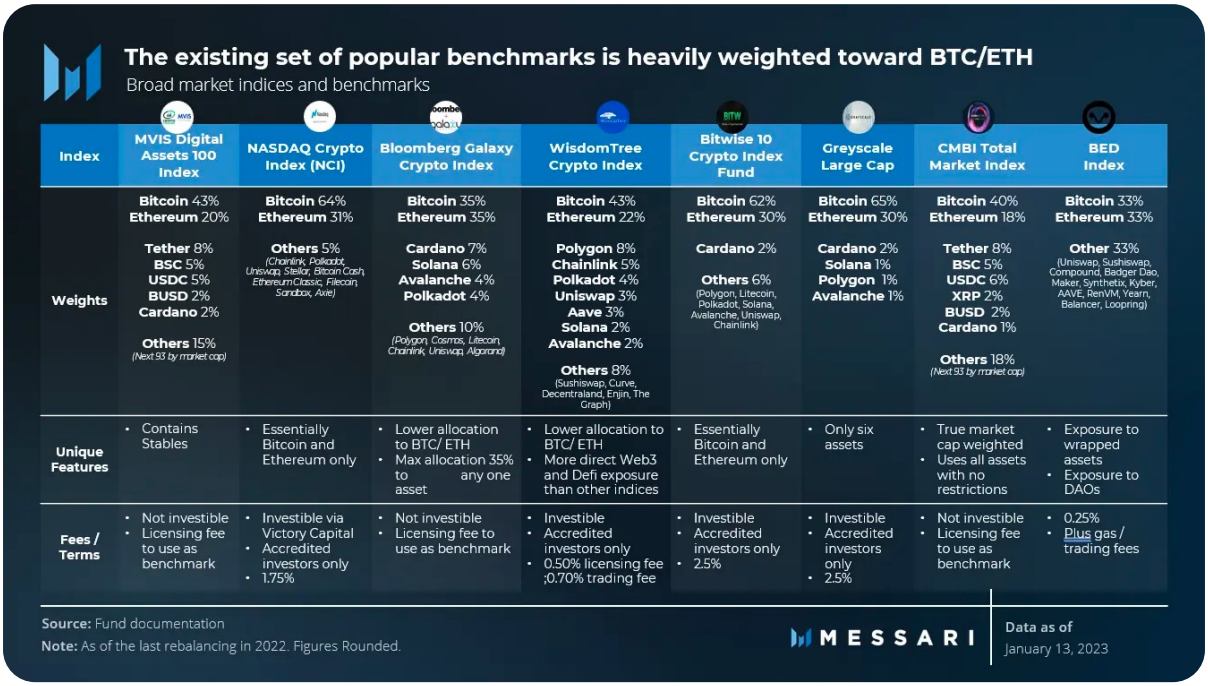
(Source: Messari)

Obviously not investment advice, but as a student of history, I know that:

A. BTC and ETH may be today's market leaders, but they are not permanently unassailable; and

B. Of the 26,000 stocks traded since 1926, just 86 stocks were responsible for half of the appreciation in the U.S. markets.

Very few stock market leaders from the '20s are still around today, and crypto will be no different. So what is a passive index enjoyoooor like me supposed to do?



Index	MVIS Digital Assets 100 Index	NASDAQ Crypto Index (NCI)	Bloomberg Galaxy Crypto Index	WisdomTree Crypto Index	Bitwise 10 Crypto Index Fund	Greyscale Large Cap	CMBI Total Market Index	BED Index
Weights	**Bitcoin** 43% **Ethereum** 20% **Tether** 8% **BSC** 5% **USDC** 5% **BUSD** 2% **Cardano** 2% **Others** 15% (Next 93 by market cap)	**Bitcoin** 64% **Ethereum** 31% **Others** 5% (Chainlink, Polkadot, Uniswap, Stellar, Bitcoin Cash, Ethereum Classic, Filecoin, Sandbox, Axie)	**Bitcoin** 35% **Ethereum** 35% **Cardano** 7% **Solana** 6% **Avalanche** 4% **Polkadot** 4% **Others** 10% (Polygon, Cosmos, Litecoin, Chainlink, Uniswap, Algorand)	**Bitcoin** 43% **Ethereum** 22% **Polygon** 8% **Chainlink** 5% **Polkadot** 4% **Uniswap** 3% **Aave** 3% **Solana** 2% **Avalanche** 2% **Others** 8% (Sushiswap, Curve, Decentraland, Enjin, The Graph)	**Bitcoin** 62% **Ethereum** 30% **Cardano** 2% **Others** 6% (Polygon, Litecoin, Polkadot, Solana, Avalanche, Uniswap, Chainlink)	**Bitcoin** 65% **Ethereum** 30% **Cardano** 2% **Solana** 1% **Polygon** 1% **Avalanche** 1%	**Bitcoin** 40% **Ethereum** 18% **Tether** 8% **BSC** 5% **USDC** 6% **XRP** 2% **BUSD** 2% **Cardano** 1% **Others** 18% (Next 93 by market cap)	**Bitcoin** 33% **Ethereum** 33% **Other** 33% (Uniswap, Sushiswap, Compound, Badger Dao, Maker, Synthetix, Kyber, AAVE, RenVM, Yearn, Balancer, Loopring)
Unique Features	• Contains Stables	• Essentially Bitcoin and Ethereum only	• Lower allocation to BTC/ ETH • Max allocation 35% to any one asset	• Lower allocation to BTC/ ETH • More direct Web3 and Defi exposure than other indices	• Essentially Bitcoin and Ethereum only	• Only six assets	• True market cap weighted • Uses all assets with no restrictions	• Exposure to wrapped assets • Exposure to DAOs
Fees / Terms	• Not investible • Licensing fee to use as benchmark	• Investible via Victory Capital • Accredited investors only • 1.75%	• Not investible • Licensing fee to use as benchmark	• Investible • Accredited investors only • 0.50% licensing fee ;0.70% trading fee	• Investible • Accredited investors only • 2.5%	• Investible • Accredited investors only • 2.5%	• Not investible • Licensing fee to use as benchmark	• 0.25% • Plus gas / trading fees

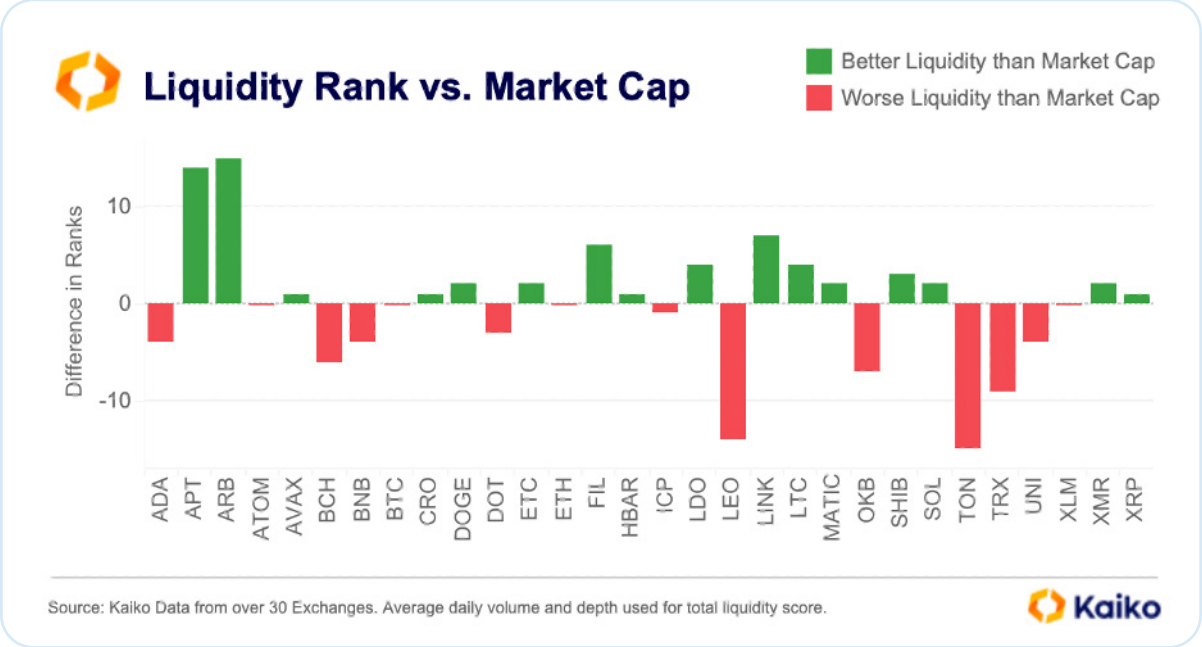
Not much to be honest. The current alternatives for crypto index products are not very

compelling, and I doubt that will change in 2024.

A low-fee, auto-rebalancing index that factored in token supply overhang and market liquidity would be a *killer* investment vehicle. But to get index exposure today, your options are to either pay too much on the AUM (200-250 bps like Grayscale's products), transaction fees (actively managed crypto funds), or the methodology (complex to get right, with significant regulatory and technical risk to execute onchain).

The only "cheap" path for investing in crypto-assets #3 through #1,000 is to bet on yourself and your own investing prowess. I'll give you one example.

A back-of-napkin index play to run at home might be to monitor this liquidity list from Kaiko and rebalance it quarterly. If you buy the assets in green (liquidity rank > market cap rank), and sell the assets in red (market cap rank > liquidity rank), you would mostly mirror my personal long/short list so far this year out of the large-cap assets (again not investment advice, people).



(Source: Kaiko)

It would be nice to build an index fund around this methodology without running the risk of being sent to Gary's gulags in the U.S. But for now, you can run these strategies manually by using tools like our asset screener to help select the critical filters and data transformations that help with portfolio balancing. (We'll see if the "Kaiko trade" still looks attractive next quarter, and maybe we'll do a follow-up report with Kaiko backtesting this strategy for our Pro subscribers.)

[Required Reading: Messari Unlocks Report, Crypto Portfolio Management]

1.4 The Resurgence of Private Crypto Markets?

I pissed off a bunch of crypto fund managers a few years ago when I wrote that their business models amounted to "losing alpha" on behalf of customers. I was right.

(I'm not gloating, so much as reassuring myself that I made the right decision in passing up the most lucrative business model in the world when I could have been on that 2-and-20 grind since 2017 without having to clear a BTC/ETH hurdle rate. GLORIOUS.)

Many crypto investors are not only underperforming the market, but dead. Some liquid investors got caught up with bad levered positions (3AC), bad counterparties (Ikigai), or both (we cover DCG in Chapter 6). You already know all that. I don't need to rehash last year's crises.

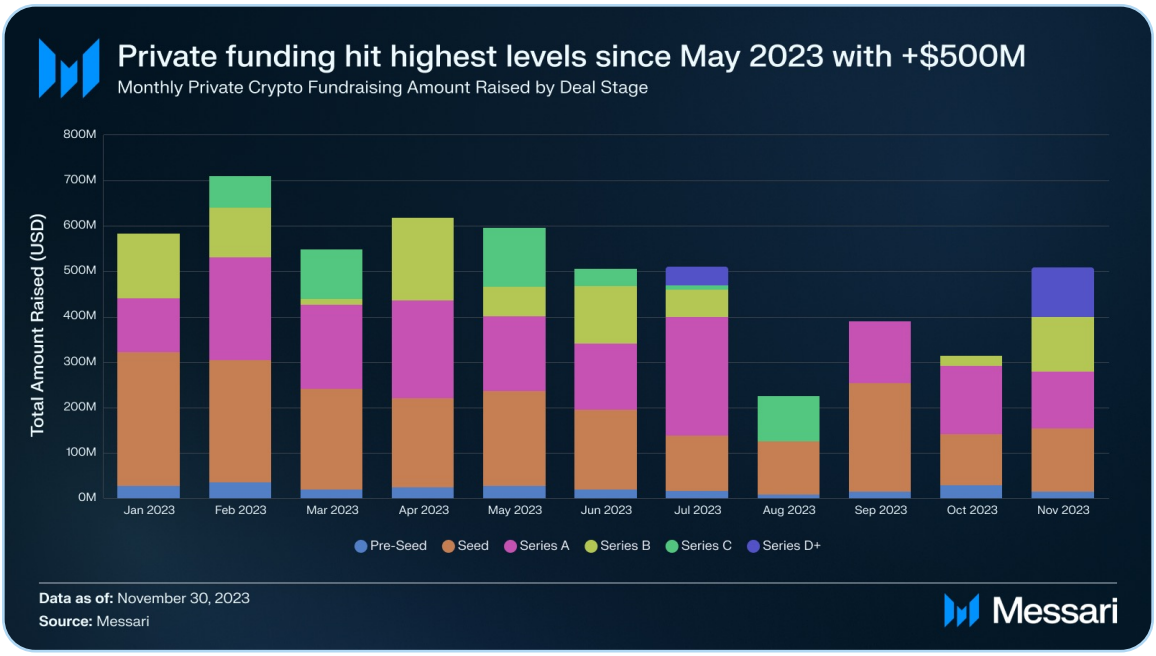
What's on deck for 2024? The liquid crypto markets remain a jungle of technical and counterparty risks, high transaction fees, and ruthless competition. Next to that jungle is a veritable valley of death that is the private crypto venture markets.

VC markets in general have been decimated by the Fed's whiplash-inducing monetary policy of the past several years. Crypto infrastructure has been hit even harder by fraud and widespread regulatory crackdowns. New users and customers are sidelined from touching "long-tail" crypto until they get some much-needed legal clarity, while old users and customers cut spending and ride out the winter as best they can. That's led to vicious demand destruction: service revenues go down, burn rates go up, budgets go down even more, and so on.

To add insult to injury, AI is the hot new Chad of tech. We're the Virgins. Again. (As I explain in Chapter 1.8, I think that's a silly meme and false choice. AI and crypto pair well together.)

Despite all this, I'm still pretty bullish for *new* crypto venture investors. The funds with a 2023 vintage will likely outperform the S&P in the medium- to long-term, and many may even have a fighting shot at outperforming the BTC/ETH benchmarks by virtue of this year's anomalously low entry prices. The liquid markets have roared back to life, and there are some signs of a venture turnaround as well.

Private VC funding (seed through Series D+) hit its highest levels since May with more than $500 million of announced deals (track them all in our fundraising screener):



Here's a partial list of crypto funds I'm keeping an eye on this year:

- **Multicoin:** I had a three-part series written about their legendary 2021 performance. (It's actually pretty good. One, Two, Three.) Though it's unclear how their LPs managed the absolutely vicious 96% SOL drawdown in 2022. Even if Multicoin's AUM rallies hard again this year, I'm not sure there have been many bigger rollercoasters for fund LPs.

- **1confirmation:** Nick Tomaino is one of the most intellectually honest crypto investors I've met. He wrote candidly about the benchmarking issues I addressed above, the need for better accountability in crypto investing, and was one of the few contrarians to call out the Sams. First SBF, then Altman. He's walked the walk too, even sharing his fund's DPI, a rarity in venture capital markets.

- There were a few "bullish at the bottom" investors whose tweets have aged well in hindsight. **Framework** (Vance), and **Placeholder** (Burniske) come to mind as two who posted specific calls AND are not simply up-only permabulls. (Even those bullish at the picotop will likely prove prescient long-term, though.)

- **a16z** and **Paradigm** might be offsides in terms of the marks on their private portfolios, depending on how much capital they deployed into the top of the market in 2021, but I don't want to bet against Chris Dixon, Matt Huang, and their teams. I'm actually somewhat relieved they (may) be flat or temporarily underwater on certain vintages. That makes them excellent fighters for the industry in D.C., and their policy teams are A+.

- **Syncracy Capital** has beaten the crypto market since inception by quite a bit. Three former Messari analysts are on the team there, including co-founder Ryan Watkins. In full disclosure, I'm an LP and will shamelessly shill anyone who helped build Messari and continues to make me money after they leave. They are one of

the few new liquid funds I know of that is above the BTC/ETH benchmarks since inception.

For day-to-day monitoring, I use Messari's asset and fundraising screeners. Nearly every day, I join the thousands of crypto investors looking to keep tabs on what the "smart money" is up to. We've got alerts, custom views, and AI-powered reports that help spot signs of life as we emerge from hibernation. Our full-year state of crypto venture report will be out in January, but you can use the tools now to start keeping track. (We released them this quarter, ICYMI).

1.5 IPOs and M&A

There are three companies that come to mind as big winners in crypto's war of attrition, by virtue of their positioning, teams, and access to capital: Coinbase, Circle, and Galaxy Digital.

Coinbase continues to be the most important company in crypto. The most valuable, tightly run crypto exchange in the U.S. warrants its own section (6.1, with the other top exchanges covered in sections 6.2 and 6.3.) It's unlikely Coinbase will see major competition in the U.S. public markets next year, though one of its top partners, Circle, may soon join them with a 2024 IPO.

Circle CEO Jeremy Allaire shared at Mainnet that his company did $800 million in revenue and $200 million in EBITDA in the first half of 2023 — a number that matched the company's full 2022 numbers and could swell further under a "higher for longer" interest rate environment. They are also well-positioned to capitalize on any forward progress with U.S. stablecoin policy or a boom in international stablecoin growth. How the company gets valued will depend almost entirely on the credit the market is willing to give the company for its products and tech growth story versus its "we earn interest on your float" economics.*

I used to think DCG would be a promising IPO candidate because of its diversified mix of services. But the company is under siege and probably off the market for a long, long time. At a minimum, DCG will have an uphill battle building back its institutional rep following a scathing fraud complaint from the New York Attorney General's office, ongoing bankruptcy litigation (and public shitshow) surrounding its lending subsidiary Genesis, and the rapid liquidation of a number of its core assets over the past 12 months (GBTC shares, CoinDesk spinout, etc.).

In the meantime, another New York-based crypto financial conglomerate has seen its stock rise, both figuratively and literally. Galaxy Digital's venture portfolio, trading desk, mining operation, and research outfit could help it take DCG's place in the industry's narrative: Mike Novogratz's company is already publicly traded (on the Toronto Stock Exchange) and commands a $3 billion market cap. That's enough liquid public equity to allow Novo's team to pursue an aggressive consolidation strategy in 2024 if they so choose. Some prime assets will inevitably become distressed amidst the ongoing venture capital stress, and Novo's already got a full investment banking advisory team in-house.

Aside from this cohort, I wouldn't hold my breath for any other breakout crypto IPOs. I doubt the window is open to others before the 2024 election. As such, the path to liquidity in crypto under the current regulatory regime remains through the token markets. Good thing you're about to get a full 100+ pages on those tokens.

*(*Tether is even stronger financially, having regained its market share since the SVB collapse this March…but don't expect its S-1 anytime soon.)*

1.6 Policy Meta

I have some stuff to say about Senator Elizabeth Warren and SEC Chair Gary Gensler in later sections. We'll get to these fine people soon. Don't worry.

But for starters, we need to zoom out. America has the technical talent, the financial markets, and the policy playbook to win the global crypto market and to ensure that the U.S. runs the financial and technological powerhouses of the 21st century. But I don't think we have enough cypherpunks to save us this time around.

The past 30 years are more than just the formative years of the Millenials among us; they provide hints, and the backdrop, for what we might expect with respect to crypto policy in the short and medium terms. Of the events and changes most impactful for crypto in these past decades, one historical analogue to our current struggle, and two mega-trends, are the most important to focus on:

1. **The Crypto Wars (of the 90s):** The first thing you should know about crypto policy, young Padawan, is that we've been here before. The original crypto wars of the 90s included unfair fights with hardasses at the NSA, legislative proposals for a literal government chip inside all of your devices that would unlock them on demand, and a popular, developer-led grassroots rebellion against government overreach. This is where the term "cypherpunks write code" comes from. You should read this book on the crypto wars, or at least this paper, which speedruns through encryption's history. It's a great underdog story, though this victory seems unlikely to be repeated with *our* crypto due to deep cultural changes in America.

2. **Complacency & Woke Shibboleths:** Unfortunately, Gen X got old and teamed up with the Boomers to do some pretty awful and unconstitutional sh*t ever since then. Today's "crypto" is a major threat to the "surveil and control" national order. And when we look at our younger protagonists (Millennials and Zoomers), the problem is they simply might not care enough to fight. They're accustomed to eroded civil liberties in a post-Patriot Act, post-COVID world. They've never lived **without** an inward-looking national security apparatus flailing wildly after a 20-year, $7 trillion global military misadventure. And many of them have even shrugged off the Twitter Files, and Big Tech's censorship industrial complex. Peter Thiel and David Sacks wrote the prediction piece on the dangers of campus cultural uniformity in the early 90s, SBF merely reminded people what we already knew, the conformity may be performative, but it's now pernicious..

3. **The End of American Hegemony:** The thing you really need to understand when you combine #1 and #2 is that there is a large chunk of government officials who genuinely believe that 90s era tech policy was a mistake and that the miracle of the open internet — and the economic growth that it spawned — has been a net detriment to American society. Tech has emerged as a convenient scapegoat. While there is some merit to the concerns that we hollowed out our manufacturing base and over-financialized our economy, it is a bit grotesque that many look at the closed internet of China with envy and only see a "missed opportunity to curb disinformation." We aren't the only superpower anymore, and because rival Big-Brother bureaucracies like China's appear to be working in some areas, our leaders

want to grab more control, too.

Our culture has weakened, our gerontocracy is delusional, and we have powerful rivals this time around. We have to play a different game and focus on "moneyball" elections instead. There is good news on this front: we're going to win. (Much more on how that will happen in Chapter 5.)

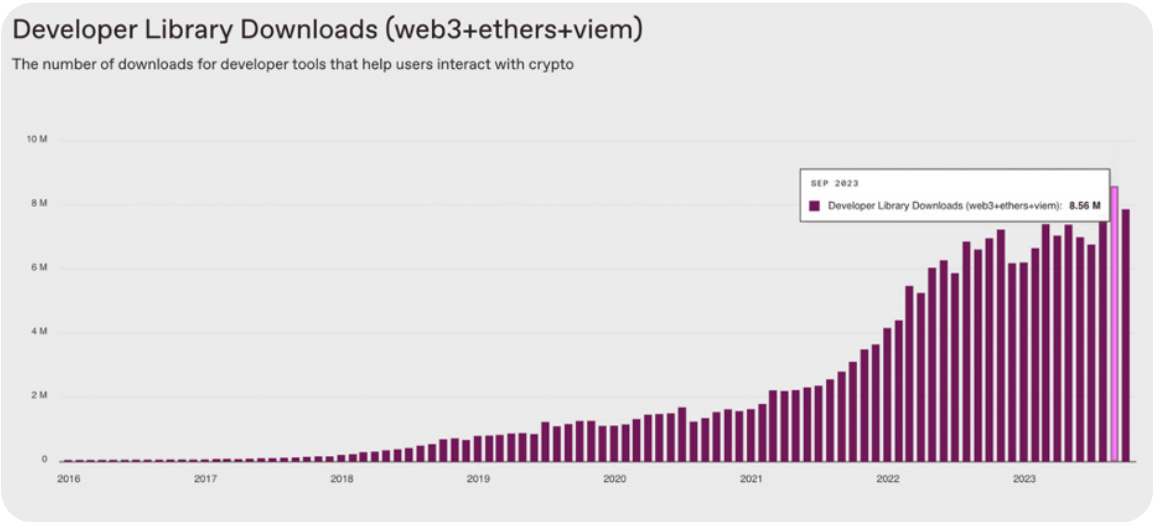
(I know you might think these trends are totally unrelated or at best tenuously connected to crypto, but they also said that about Pepe Silvia. We're fighting an existential information war.)

1.7 Can Devs Do Something?!

Despite the deep crypto recession, dips in trading volumes, and regulatory headwinds, crypto developer activity held up well this year. At the midyear point, Alchemy found that the number of smart contracts deployed on EVM chains saw an increase of 300% QoQ, while crypto wallet installations reached a new all-time high.

Electric Capital found that, by October, monthly active developers contributing to open-source projects had dropped precipitously year-over-year, but chalked it up to a variety of factors: the regulatory chill cast over the open-source ecosystem following this year's Ooki DAO ruling; more innovation and development at the application and infrastructure layer; and the general bear market tendency to remain a bit cagier about competitive threats.

a16z's State of Crypto Index is perhaps the best glimpse at overall market health. Its tracking also highlights the 30% drop in open-source developers, but it also includes a number of mitigating data points as well: developer library downloads hit a record in Q3, and active addresses and mobile wallet activity reached new record highs. Is that the spark that ignites a blaze of breakout crypto apps in 2024? If I could invest blindly into crypto based on a single chart, it's this one:



(Source: a16z)

Just wait until the AI devs realize that crypto is the yin to their yang. That's when the party will really get started. Speaking of which...

1.8 AI & Crypto: Money for the Machines

In an age of digital abundance and generative AI, tech that provides reliable, global, and mathematically guaranteed provenance and digital scarcity will be critical.

Think of deep fakes: crypto will be invaluable for timestamping and verifying devices and data. Without crypto, good luck verifying whether certain images or text come from AI or non-AI sources, or from D.C. or Beijing. And good luck preventing generative DDOS attacks without the fees required by public blockchains.

AI's rise is a "threat" to crypto in the way that mobile was a threat to the internet. It's absurd on its face. Progress in AI will only increase demand for crypto solutions. We might argue whether AI is a net good or bad for humanity (in the same way we debate whether iPhones are net good or bad...but still know they have obviously been a net good), but AI is *great* for crypto, and I for one, welcome our machine overlords.

I come bearing gifts of the perfect machine money: bitcoin.

I really don't feel the need to overthink this, but I liked (as usual) Arthur Hayes' post on the subject this summer. The two most critical inputs for any AI are data and compute power, and as such, it seems likely that "AI will transact in a currency that preserves its energy purchasing power over time." That's bitcoin in a nutshell.

For what it's worth, others may critique this as overly simplistic given that two likely AI use cases, micropayments and smart contract execution, still haven't panned out much on bitcoin. And AI agents will least-cost-route to the optimal blockchains (lowest cost and latency) when they are deployed, not necessarily settle for bitcoin's friction thanks to its proof-of-work mining. Dustin thinks it's more likely the whole "energy denominated money" thing is backwards: AI agents may be more likely to buy gas tokens (the relevant computation resource) directly.

Messari has been all over the crypto projects most likely to benefit from the boom in the AI x Crypto narrative, and this was one of my favorite mini-tracks at Mainnet 2023. Do yourselves a favor, and watch Dustin's 101 session, Why AI needs Crypto, and Why Crypto needs AI.

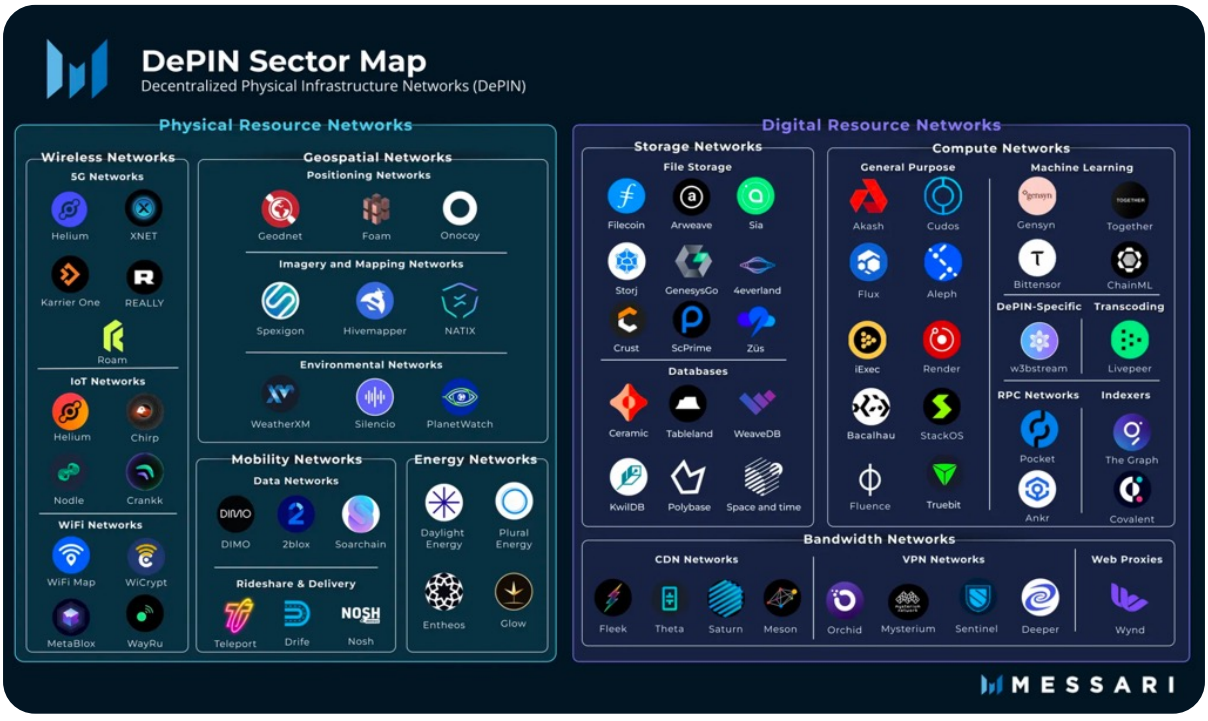
[Required Reading: Decentralizing Machine Leaning, Growing Synergies in AI and Crypto]

1.9 Three New De's: DePIN, DeSoc, DeSci

I am permabullish on decentralized finance (DeFi), but I'm not necessarily "overweight" as I think other market segments will outperform over the coming year. I do think some of the top DeFi protocols in the sector (particularly in the decentralized exchange space) are due for a rebound after a flat year of trading volumes, but it's not clear to me that DeFi's unit economics and product-market fit will be enough to offset the hellish regulatory headwinds that lie ahead. And then there's a matter of what type of assets are driving DeFi volumes. This year's spikes were largely driven by memecoin rallies, not breakout new applications or adoption. Maybe I've just spent too much time considering the DeFi doomsday scenarios in D.C. (more in Chapter 8.)

My eyes are wandering to several critical, non-financial sectors of crypto. I like DePIN (Physical Infrastructure Networks), DeSoc (Social Media), and DeSci (Yeah, science!) because they feel like they will be less driven by rampant speculation and are all oriented around solutions critical to our industry well beyond finance.

Sami helped popularize the DePIN moniker last year, and no one has been better at mapping the landscape or outlining how these hardware networks can scale to truly compete with their centralized counterparts in Big Tech. Cloud infrastructure services are a $5 trillion market cap sector in the legacy markets, and DePIN sits at just 0.1% of that. Even if you assume 0% of online services leverage DePIN as their *primary* stack, the demand for decentralized redundancies alone could cause a boom in demand. A 1% "insurance premium" to eliminate Big Tech deplatforming risks would lead to a 10x in DePIN utilization rates. It doesn't take much to move the needle, especially with AI-driven demand for GPUs and compute in general.



There's a similar opportunity in social media, where the incumbent players made $230 billion in revenue last year (half from the Meta family of companies alone), while a

vanishingly small percentage of creators make enough money to make content creation worthwhile. We've seen signs of this changing (YouTube's relentless growth, Elon's revenue sharing) and a glimmer of potential breakout DeSoc apps (Farcaster, friend.tech, and Lens), but it *feels* like the early, barely imperceptible moment in the beginning of a J-curve of adoption versus a false start. Friend.tech shared $50 million with its creators in its first several months post-launch, which is one way to create an audience. I think DeSoc in 2024 follows the "DeFi Summer" boom of 2020.

Finally, there's decentralized science. Some 50% of the DeSci projects we track were built in the past year. One of the best OG crypto investors I know has been dedicating 100% of his time here. It's a market where crypto incentives make sense: trust in our scientific establishment may be at all-time lows, and the current system is riddled with bureaucratic inefficiencies, poor data methodologies, and piss-poor incentive schemes (peer-reviewed papers that lead to tenure!), whereas crypto has already demonstrated a proven ability to fund…science experiments! At a massive scale. Token sales and DAOs were built to revolutionize how we do research, and there is enough interest in longevity, rare disease treatments, and space exploration alone to drive development in this sector.

You can invest directly in DePIN, and you can start power using DeSoc apps today. But I don't yet know of a way to lazily express a DeSci investment thesis. (VitaDAO?) If you think of any, let me know. My DMs are open.

[Required Reading: Our DeSoc, DePIN, and DeSci Enterprise reports.]

1.10 Messari Analyst Picks

TBI

Biggest winner	$GBTC, SOL
Biggest loser	Illiquid VC marks, and why can't I quit ZEC?
Holds	BTC, ETH, SOL
Likes	You are reading this report, right?

Maartje

Biggest winner	RNDR
Biggest loser	Parted ways with CRV
Holds	BTC, ETH, RNDR
Likes	DePIN

Dustin

Biggest winner	SOL, OLAS, NOS
Biggest loser	USDC
Holds	SOL, OLAS, NOS, LIKE, HBB
Likes	*loves* AI x Crypto (specifically inference coprocessors and onchain agent/cognitive frameworks)

Kunal

Biggest winner	RUNE, AKT, TAO
Biggest loser	PEPE
Holds	ETH, TIA, RPL, AKT
Likes	EigenLayer and restaking protocols. Demand for security drives value for L1 assets, and EigenLayer significantly expands ETH's security market. ETH and LSTs are the primary public instruments offering exposure to EigenLayer.

Sami

Biggest winner	RNDR, AKT, TAO
Biggest loser	Not buying more TAO
Holds	BTC, ETH, SOL, HONEY, TAO, RNDR, AKT, LPT
Likes	DePIN and decentralized AI will become crypto's killer apps. ZK coprocessors will enable crypto apps to reach parity with Web2 apps in terms of functionality and performance.

Ally

Biggest winner	SOL,TIA, RNDR, MKR
Biggest loser	MATIC
Holds	SOL + ecosystem tokens, ETH + memes
Likes	Networks and apps with comparatively less bots/Sybil activity. Innovation and trajectory of consumer apps

Steph

Biggest winner	PEPE
Biggest loser	MARBLES
Holds	BITCOIN (HPOS10), TIA, ETH, BTC, SOL
Likes	Infrastructure and memecoins

Kel

Biggest winner	SOL
Biggest loser	Not selling ETH fast enough
Holds	SOL, Solana ecosystem tokens + NFTs, LIKE
Likes	Solana ecosystem projects. Token valuations are probably overheated in the short term, but the reality is most have only warmed up to Solana recently – I expect further inflows from this type of person on a medium to long term timeframe.

Seth

Biggest winner	RNDR, SOL
Biggest loser	ALCX
Holds	BTC, ETH, SOL, RNDR, LPT
Likes	Bringing offchain compute and state to onchain applications. Key management infrastructure.

Toe

Biggest winner	AKT
Biggest loser	HAMS
Holds	AKT, TAO, SOL + Solana ecosystem, DYDX
Likes	DePIN finding product-market fit, Solana protocols with fresh charts, perp DEXs (VRTX, AEVO, Hyperliquid), ZK coprocessors, some DeFi (Ethena Labs, OSMO, SOMM), and taking profit.

Mihai

Biggest winner	RNDR, SOL
Biggest loser	ATOM
Holds	BTC, ETH, SOL, RNDR
Likes	Zero-knowledge machine learning. Key management solutions. Scaling solutions.

JTVL

Biggest winner	GBTC
Biggest loser	ATOM, not riding the RWA train
Holds	BTC, ETH, SNX, PENDLE, LBR, GNS, LINK, LQTY
Likes	More yields onchain from RWA and LSTs should bring more onchain yield trading, buy the picks and shovels. LSTFi and perps will remain growth areas and the latter especially are reasonably priced. Denominate your wealth in satoshis, embrace the store of value.

Nick

Biggest winner	AKT
Biggest loser	SYN
Holds	AKT, DYDX, ILV, SYN
Likes	Mobile applications, EIP-4844, ETH chain abstraction, re-staking and LSTs, and election-related meme coins.

Peter

Biggest winner	SOL, Mad Lads
Biggest loser	My boss's friend.tech key
Holds	SOL, BONK, ETH, COIN
Likes	Solana ecosystem

Red

Biggest winner	COIN
Biggest loser	XMR
Holds	BTC, ETH, XMR
Likes	Alt-VM Ethereum rollups for capturing Ethereum users and liquidity, without the baggage of the EVM. Bitcoin programmability for developer experimentation and trust-minimized access to BTC liquidity. AI to lead the DePIN narrative.

Micah

Biggest winner	COIN, PEPE
Biggest loser	LYX
Holds	BTC, ETH, SOL, AKT, RNDR, LYX, $COIN
Likes	ZK-coprocessors, perps, bitcoin programmability, abstraction.

AJC

Biggest winner	BTC
Biggest loser	Chasing meme coins
Holds	BTC, ETH, LINK, ARB, Milady, WINR, GMX, GRAIL
Likes	SocialFi/reputational layers (friend.tech), perp DEXs and onchain options capturing market share from CEXs, capital flowing from Ethereum to Arbitrum ecosystem and other L2s post-Dencun, ETF approvals for BTC and ETH, and GambleFi.

Mike

Biggest winner	BTC.D and Remilia NFTs
Biggest loser	Round tripping Racer friend.tech keys
Holds	BTC, ETH, SOL, Remilia NFTs
Likes	New cycle coins: TAO, TIA, and SOL. Crypto culture keeps winning: Remilia NFTs and SocialFi / Gambling / Prediction-Markets 2.0 (it's all the same thing).

For the sake of clarification, the term "Holds" in relation to specific crypto tokens or assets is used solely for analytical purposes. The inclusion of any asset in the "Holds" section does not reflect the analysts full holdings - please see our analyst disclosures here for specifics and our general disclaimer in Section 10 for more.

Messari

All Your Crypto Needs, **One Platform**

Messari Enterprise provides market intelligence data, tools, and research designed to empower informed decision-making and simplify your workflow. Our platform is tailored for businesses, compliance teams, builders, and investors, guiding you expertly through the crypto economy.

Gain Access To:

- Unlimited Watchlists, Screeners, and Charts
- Real-Time Key Developments Feed
- Fundraising Data Screener
- Diligence Reports
- Token Unlocks
- Real-time Key Developments and Governance Alerts
- Advanced daily & weekly AI Digests
- Daily Market Data & News API access
- CSV Downloads
- Access to Enterprise-Grade Research
- And All Pro features

Visit **messari.io/enterprise** to learn more or contact **sales@messari.io** to schedule a demo.

Schedule A Demo

CHAPTER 2

TOP 10 PEOPLE TO WATCH IN 2024

2.0 Where Are They Now

It's no fun writing about the same people every year, so I've included a mostly new cast of characters to watch in 2024.

To be honest, most of them probably don't want to be included on this list at all, as there is something like a 30% probability historically that inclusion here will lead to jail time, deposement, very serious legal allegations, bankruptcy, or a massive hack.

Previous "People to Watch" include FTX's Sam Bankman-Fried (jail - convicted), Terra's Do Kwon (jail - awaiting trial), 3AC's Su Zhu (jail - awaiting trial), the Tornado Cash founders (jail - awaiting trial), DCG's Barry Silbert and Gemini's Winklevoss twins (accused of *civil* fraud in New York...so far), and Binance's CZ (guilty plea - sentencing in February).

As for last year's top duo, CZ and Coinbase's Brian Armstrong, I wrote that "as their fortunes go, so goes crypto in 2023." They may have been obvious picks, but sometimes, the obvious take also happens to be correct. Don't overthink it.

The same thing can be said for much of this list: the survivors coming out of a deep bear market are worth watching simply because they are resilient. Obvious, but worth reinforcing.

The week before CZ and Binance entered their guilty plea, I wrote in this report draft: "I'm 44% sure CZ would weather the storm via 1) a record-setting billion dollar fine, and/or 2) rapid decentralization of Binance via the BNB ecosystem."

It's not guaranteed that CZ will skate away with zero jail time, but I was right about the fine (second-largest U.S. government fine in history after opioid epidemic peddler, Purdue Pharma) and the immediate pivot to BNB in his bio. Now, we'll see what he does for an encore once the legal dust settles.

2.1 Larry Fink (BlackRock) & Cathie Wood (ARK Invest)

I, for one, have enjoyed the Larry Fink memes, even if I'm cautious about what widespread Wall Street ownership will mean for Bitcoin.

BlackRock entering the crypto ETF fray with not one, but two applications for BTC and ETH spot products, is a signal that these institutional vehicles are long overdue and imminent: the world's largest asset manager joins the ETF race with a 575-1 record. Fink's journey from skeptic to crypto convert in under five years may have some relation to Paul Tudor Jones' 2021 epiphany that 86% of bitcoin purchased at the 2017 peak remained HODL'd through the 2018 trough, and the asset has an unblemished record of resurging following boom/bust periods. Fink's gushing commentary on bitcoin will be played on a loop in January if BlackRock launches an ETF. "Tokenization of assets can revolutionize finance." "It's digitizing gold." "It's an international asset." "The underlying technology is fantastic." And that was just one interview.

But Larry can get in line. All eyes will be on ARK Invest's Cathie Wood first. ARK stands at the front of the ETF application line with a "final deadline" that expires on January 10. At that time, regulators must either reject or approve her company's ETF, likely opening the floodgates to approvals for the majority of proposed products. Can you imagine BlackRock, Fidelity, WidsomTree, Franklin Templeton, Invesco, Grayscale, Bitwise, Valkyrie, VanEck, and ARK *viciously* competing with each other to sell BTC even HARDER than all of their competitors?

Cathie makes the top of the list based on the ETF calendar and as a reminder to check out ARK Big Ideas 2024 when it comes out in January. The 2023 presentation still holds up well.

2.2 Jeremy Allaire & Dante Disparte (Circle)

As I wrote in the last chapter, Circle has been killing it in the high-interest rate environment. Although USDC has ceded some market share back to rival Tether, the company's decade-long compliance-first thrust has catapulted it to the top of the 2024 IPO pile. They've now got a headstart in lining up institutional bidders, with the likes of Fidelity, BlackRock, and Goldman Sachs already invested.

Circle might be the company to benefit most from the passage of U.S. stablecoin legislation next year, as I'm not sure anyone has spent more time with global policymakers, regulators, and bankers, than Jeremy and Dante. Close government and banking ties are prerequisites for winning the regulated stablecoin game, and they've got that in spades domestically (they tightened up their long-term partnership with Coinbase) and internationally where 70% of USDC adoption resides thanks to partners like SBI Holdings in Japan, Mercado Pago in Latin America, Coins.ph in Asia Pacific, and opportunities in Europe abound with their fledgling euro stablecoin in the post-MiCA world.

Ironically, Circle's only real hiccup this year stemmed from its banking partners' woes in Q1. It was SVB's largest depositor. Circle needs protection from the banks!

I also include Jeremy and Dante on this list to call out that we shouldn't simply replace the old gods (SBF, CZ) with the new (Brian, Jeremy).

I've had about enough of the hero worship in a decentralized industry, and as much as I respect and personally like Jeremy and Dante, their incentives (and fiduciary responsibilities) are to take their digital dollar company public, NOT to fight the most intense privacy battles that lie ahead of us. Where they push back and where they relent will help determine the future of crypto's dollar-denominated status quo. Trust them, but verify.

2.3 Kristin Smith (The Blockchain Association) & Michael Carcaise (Fair Shake PAC)

The Blockchain Association ran the table in 2023, retaining the who's who within crypto as members, and even reunifying some of the warring factions that had previously split off as members in 2020-2022. The BA's Policy Summit lineup was staggering — a mark of its influence — and its importance as an organization has never been higher in the face of a relentlessly hostile regulatory backdrop (a new dystopian Treasury surveillance proposal dropped at the event while I was writing this section). If you're a member, donate to their PAC. If you're not a member, apply.

While the BA is charged with holding the line in 2024 with respect to current legislative proposals and regulatory battles, it's our up-and-coming super PAC, Fair Shake, whose fortunes will dictate how the industry fares in the U.S. long term. Fair Shake is the long-needed political operation we've been lacking, and it proved in 2022 what it could do with modest resources, winning 17 of the 18 congressional races in which it supported pro-crypto in the general election. Fair Shake has attracted the capital and whale donors that have historically been missing from our DC equation. They'll 5-10x their fundraising compared to the 2021-2022 cycle, and be one of the top ten super PACs in the country this cycle.

(My inclusion in CoinDesk's "Most Influential List" was essentially earned from repeating variations of "send Kristin and Mike money" about 11,674 times on X this year.)

2.4 Senator Elizabeth Warren (and her Minions)

The Biden White House and its banking regulators are full of staffers who despise the crypto industry. People who would prefer to kill crypto outright while they believe they still have the chance and who truly believe our industry presents more net harm than potential good to the public. That open hostility is thanks largely to one person: Senator Elizabeth Warren.

Unfortunately, she will continue to wield outsized influence for at least another year.

Last year, I came to realize that there were two major misconceptions among general crypto enthusiasts regarding Warren. One is whether she is an effective politician, and the other is whether it is a good use of time or money to campaign against her re-election. I address the latter issue in Chapter 5 (short answer: she's untouchable electorally, but we can neutralize her through indirect means). Whether she's an effective politician I'll address here.

A cursory look at Warren's track record shows that she hasn't sponsored much legislation that's actually passed into law. The impression a layperson is left with is that she is all bark, no bite. But that misunderstands what has been her explicit mission from Day 1: place personnel in high places within the D.C. bureaucracy and pull the party further to

the left.

How did she amass such power?

Warren's long-term progressive bonafides in financial services are well known, which put her in a position of outsized influence in the 2020 election when she ran against Joe Biden in the crowded Democratic primary. While she faded quickly in the race, Warren was able to strike a bargain with Biden on her way out, knowing full well that an endorsement would help him shore up the Progressive flank in a tight race against Senator Bernie Sanders.

Warren's endorsement of Biden came with significant strings attached: she wanted a say in the senior economic staffers and financial regulators who would ultimately enact Biden's financial policy. And she got it, in part because Biden did not have a deep financial policy bench to begin with. Today, across the administration and Biden's inner circle, you'd be hard-pressed to find a regulator or committee without close ties to Warren and her staff.

Some of Warren's influential allies:

- **SEC Chair Gary Gensler:** Warren coordinates softball questions for Gensler before his Congressional Oversight hearings and remains his biggest (only?) political cheerleader in a town that generally despises him, and they've maintained a close relationship for a decade (at least one Gensler family member interned in Warren's office).

- **FDIC Chair Martin Gruenberg:** Warren was a not-so-behind-the-scenes advocate for the FDIC's "Chokepoint 2.0" strategy that deplatformed multiple crypto startups and inadvertently sparked a regional bank run earlier this year. She and Gruenberg helped assassinate Silvergate and Signature Bank for their crypto associations. SVB was simply collateral damage.

- **CFPB Chair Rohit Chopra:** Perhaps Warren's top nuclear weapon, the Consumer Financial Protection Bureau she helped create and once led, has not yet been fully activated. Chopra seems to be getting closer to making moves that would reconsider the liabilities that centralized platforms face in the event of user hacks or accidental crypto transfers, and he has at least one extremely savvy crypto staffer who hates the industry and knows how and where to turn the knife, if only she's given the chance.

- **Deputy Treasury Secretary Wally Adeyemo:** Credit where it's due, this dude walked into the Blockchain Association Policy Summit and called the industry a "clear and present danger to national security" to our faces, a day after writing to Congress with a request that would have made Dick Cheney blush. Treasury wants an unprecedented expansion of surveillance powers with respect to crypto, and Wally asked for it in order to improve his prospects for Treasury Secretary in the next administration. The proposal rhymes closely with Warren's proposed DAAML bill, and his letter was addressed to...you guessed it: Warren's Senate Banking committee.

- **Former National Economic Council Deputy Director Bharat Ramamurti:** Former Chief of Staff for Warren and our most hostile opponent within the White House. This is where the calls came from inside the White House to dissuade Congressional leaders otherwise inclined to work on bipartisan crypto legislation.

- **Current National Economic Council Deputy Director Jon Donenberg:** When Ramamurti left the administration at the end of September, some former Biden White House insiders told me to "wait and see" as Biden would soften his anti-crypto stance soon after. But like clockwork, Jon Donenberg, Warren's then Chief of Staff, promptly replaced Ramamurti just days later. Do you get it now?

Warren's opposition to crypto is so effective *because* it's mostly indirect. The White House and major financial regulators won't even field *phone calls* from the industry because of her pressure, and they rebuffed all meeting requests with the 40+ founders who visited the Capitol during Coinbase's "Stand with Crypto" campaign this September.

Even *House Democrats* who have the audacity to work across the aisle face negative campaigns from the press and her many administrative proxies. Case in point: House Financial Services Ranking Member, Maxine Waters, whose 180 on the bipartisan Stablecoin and Market Structure bills immediately followed calls from Warren's White House staffers (more in Chapter 5). As a senior House Democrat leader explained in private this fall, a lack of support from Waters is a death knell for 2024 legislative hopes, as it would: a) signal to the broader House Democratic caucus that even bipartisan crypto bills shouldn't be broadly supported in a floor vote; and b) give the Democrat-controlled Senate and its crypto-hostile Banking committee the air cover needed to fully ignore any House-passed bill.

Senator Warren wants a central bank digital currency, not stablecoins. She coordinated with short sellers in order to assassinate crypto-friendly banks. She gushes over the SEC's regulation by enforcement status quo. She scapegoats the industry for its negligible role in terrorist financing (compared to government policy and traditional payments). She is playing for keeps, and as the shadow commander of U.S. financial policy (Biden himself is a complete non-factor), "President" Warren is our most formidable foe.

Since she's building an anti-crypto empire, I spent some time helping to build our rebel alliance. We'll see who wins next November, but I don't think she's going to like the outcome. Watch.

2.5 Elon Musk (and his Stans)

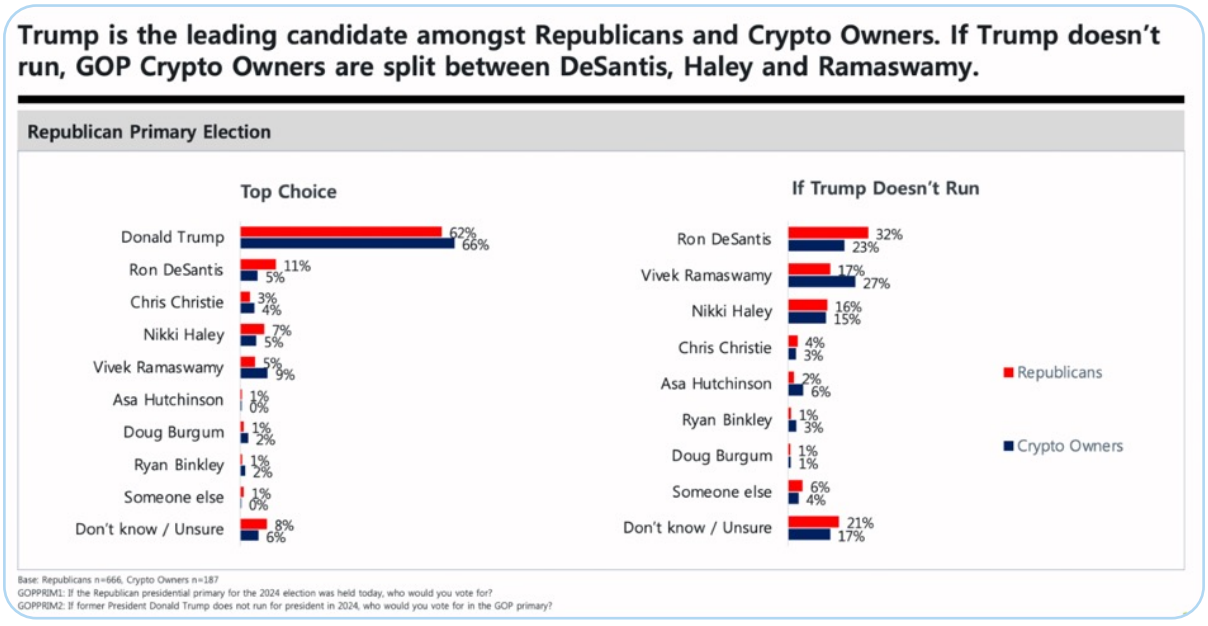
There weren't three more important iconoclasts to emerge this past year in (crypto-adjacent) politics than Elon Musk, Tucker Carlson, and Vivek Ramaswamy. (Narrative violation!)

The future of X may be in doubt due to an advertiser boycott, but Elon's buyout of Twitter exposed undeniable government pressure on free speech that the courts have agreed was unconstitutional. His rapid "replatforming" of Tucker Carlson, following Carlson's fall from grace at Fox News, led to an order of magnitude rise in exposure for Carlson and his contrarian political positions. And to the extent Obama was the Facebook president and Trump was the Twitter president, Vivek could be the first X president (or at least highly influential in a second Trump administration or in 2028): his greatest hits are curated long-form videos and posts on X.

In general, it's silly to feel threatened for pointing out the obvious: all three of these men are a net positive for crypto, and rooting for their success should not be controversial for our industry.

Vivek's thoughtful and thorough approach to crypto policy has sparked other leaders like RFK Jr. and Ron DeSantis to follow suit. We have a major and legitimate presidential candidate who can speak extemporaneously for 30 minutes on the nuances of crypto and its positive role in society. This is a good thing.

A November Harris poll pegs Vivek as voters' second choice for the nomination (behind Ron DeSantis) if Trump drops out of the GOP primary for any reason, and he's the top choice among crypto owners. I hosted him at Mainnet for a reason.



(Source: The Blockchain Association's HarrisX Polling)

Amongst mainstream media figures, Tucker Carlson has single-handedly changed how we discuss things like foreign wars, censorship, and government spending when the national

conversation otherwise seems to be tightly controlled. Tucker is also positive about crypto being a check on the state's power. That, too, is a good thing.

And, Elon alone has kept our space industry competitive with China's, done more to advance clean energy than any other living human, and — I will die on this hill — is the **only** reason that most crypto discussions are still permitted on X. We can't really argue counterfactuals, but I hope you'll agree that open discourse on Crypto Twitter is a good thing.

I respect people who don't like (or even respect) these gentlemen, but I have zero respect for people who can't understand or respect *why others like them* or would think such wrongthink is deserving of condemnation. We're in big trouble as a society if we lose our smartest voices of dissent on both the right and the left, and I happen to think Elon will be on the right side of history with his free speech crusade.

I worry much more about people who care more about looking good while doing evil, than I do with ruthlessly blunt countercultural figures. Especially since the Bolsheviks still walk among us.

2.6 Michael Sonnenshein & Craig Salm (Grayscale)

While the rest of the DCG empire is in turmoil, Grayscale has been printing money and winning or settling its highest-stakes legal battles (h/t Craig Salm). The company will end the year with ~$35 billion in AUM, representing $700 million in incredibly high-margin annualized fees. Grayscale's newer trust products beyond GBTC and ETHE seem to be following a hype cycle reminiscent of 2017 or 2020. The LINK product is up about 8x YTD (shares trade at 3x their underlying NAV), and its Solana product is up 4x since its May debut (shares trade at 4x NAV). Their eye-watering premiums might attract similar private investors who aim to replay the "Grayscale Trade" with new trusts. (Hopefully, without leverage.)

I wrote that the Winklevoss twins and Barry Silbert would be among those to watch in 2023. That proved true as their once-private legal battle degraded into a multi-front war that now includes the New York Attorney General, the SEC, and the Eastern District of New York, reportedly. There are more questions than answers with respect to how this saga will unfold in the new year.

We'll cover questions specific to DCG and Genesis in Chapter 6, but Sonnenshein is on this list for two reasons: 1) Grayscale is a great business, but its future is a complete mystery. Does the NYAG want Barry and DCG (Grayscale's parent) permanently barred from the securities business? Will DCG be forced to divest? Will Barry have to remove himself from the board? Do the sins of the father and sister company impede GBTC's ETF conversion? And 2) that sets up the equivalent of Season 6 of crypto's *Succession*. Could Sonny be the unlikely successor that inherits the Grayscale kingdom, like crypto's Tom Wambsgans, as Ram thinks?

Sonny has emerged as an industry leader. I think he's one of the good ones. But this fantasy of a Grayscale spinout is a waste of time.

Having seen Barry operate firsthand in complex transactions (the sale of SecondMarket, the formation of DCG, the creation of the Grayscale side-door listing, etc.), Most people still underestimate him. He's unkillable. The odds of Barry settling the fraud allegations against him and DCG out of court are 90%+, and the odds that Barry comes out ahead in a prolonged battle with Genesis creditors is 90%+ (he's simply better at navigating the bankruptcy process and has more leverage). The odds that Grayscale spins out or Barry loses control of his crown jewel are approximately 0%. (Either way, Sonny is in the catbird seat.)

By the way, here's a live look at people who disagree with me on this.

2.7 Nic Carter & Matt Walsh (Castle Island Ventures)

Crypto Twitter remains undefeated when it comes to entertainment value. Balaji made waves at the beginning of the year for losing a $1 million bitcoin bet (at least it wasn't a McAfee bet). Cobie predicted the CZ red notice before exiting Twitter entirely. And Inversebrah and Gabe still exist, which are noteworthy feats in and of themselves.

But few investors have been as impactful or as entertaining as Matt and Nic this past year.

Nic's prolific writing has always impressed, and his defenses of bitcoin's ethos, Proof-of-Work mining, and stablecoins have been go-to resources over the six years I have followed him. He's a truly original thinker who wrote the first thesis on crypto governance models (many years ahead of its time), went to war with the bitcoin maximalists that had previously adored him, and promoted what might be my very favorite crypto conspiracy, the bitcoin "lab leak" theory, which stipulates that the invention leaked from an NSA cryptography lab.

He hit a new peak this year. Nic went viral for exposing the rot within the banking regulators pushing "Chokepoint 2.0" in D.C. His long-time advocacy for Proof-of-Reserves led to the first legislative proposals for that custodian regulation. And he was integral in counter-narrating the inane Wall Street Journal propaganda surrounding crypto's role in the October 7 attack by Hamas on Israel: his decentralized bounty program rewarded data sleuths for correcting the record on the actual illicit figures that had been reported.

Just a hot, hot hand and one-man crypto media outlet. Not bad for someone the media referred to as a "prominent bitcoin fan," which I guess is a neg you bestow on a superior writer who runs circles around you in your profession as a hobby.

Not to be outdone, Matt Walsh exposed the ridiculous backstory behind SEC darling, Prometheus, a "registered" "digital asset securities" brokerage with alleged CCP

connections, no real volume, and an inexplicable (kidding, it's Warren-istic corruption) invitation to testify in front of Congress as an exemplar of crypto compliance. Matt was also the first person I heard ring the alarm on SAB 121, a brazenly snakey accounting rule designed by the SEC to block Wall Street firms from supporting crypto custody.

You should subscribe to Castle Island's *On the Brink podcast*, as it's the best in the game right now. It's the only one I listen to weekly.

2.8 Lucas Vogelsang (Centrifuge), Denelle Dixon (Stellar) & Christine Moy (Apollo)

When it comes to bridging the gap between Wall Street finance and crypto startups, these three stand out as early leaders. The question is whether their early leads will equate to 2024 growth or whether the "real world asset" (RWA) meme is simply another false start — this cycle's version of "blockchain not bitcoin" (2015) or "tokenized securities" (2018).

Lucas's Centrifuge has been an early leader in the RWA space, with the highest token market cap, highest market share by private loans outstanding, and lowest ratio of default to active loans out of the three leading RWA credit protocols (Maple and Goldfinch being the other two). They've got $250 million in active loans, the majority of which are thanks to a large partnership with BlockTower Credit and Maker, in which Maker has issued DAI loans backed by real-world instruments managed by BlockTower.

Denelle's Stellar has garnered early interest and support from financial institutions who view her project as a safe playground for tokenized Treasury experimentation. Franklin Templeton's $330 million tokenized Treasury play (and WisdomTree's smaller pilot) make up the large plurality of tokenized Treasuries, and the largest liquid instruments that any Wall Street firm had actually offered onchain, including stablecoins (PayPal's pyUSD is still just a third of the size of the FT products), and Denelle thinks there is more to come in 2024.

Then there's Christine Moy, whom I have wanted to include for a few years but haven't for the fact that she's always been too far on the "Wall Street loves crypto" circuit, which always feels "five years away" and generally uninteresting. Christine formerly led JPMorgan's blockchain team (perhaps the unit that has shipped the most actual crypto product in Wall Street circles so far and has already settled $1 trillion tokenized treasury trades with its Onyx team). She now runs Crypto, Data, and AI Strategy at investment giant Apollo. I'm not sure many people have a deeper combination of crypto and Wall Street networks, and Christine is ubiquitous. I finally saw the "real-world asset" potential in Singapore, when she showed me the Apollo-JPMorgan "Project Guardian" proof-of-concept that she had worked on with several crypto projects. More on that next chapter, but it feels like we're on the cusp of crossing the chasm into regulated finance. Maybe not in the U.S., but perhaps in more forward-thinking countries like Singapore.

2.9 Dan Romero (Farcaster) & 0x Racer (friend.tech)

In the off-chance that the advertiser ban at X kills the company, what will happen to Crypto Twitter? Odds are it will move to Farcaster, thanks to Romero's early curation of their user community and careful UX iteration. Lens* which recently launched its V2, and whose founder Stani made this list last year, is a close second. But Dan is the first one to build a product that looks and feels like a game-ready substitute for X if the latter platform ends up getting seized by the Harris Administration on January 21, 2025, or I finally get yanked for a Gensler mean tweet.

And yes, I know the hype has chilled, but friend.tech founder 0xRacer deserves credit for cracking the code on DeSoc gamification and preserving Dunbar's number for online fan groups. I'm not sure how many people will pay to hold a membership token that merely gets them access to a merit-based or closed group of peers, but the friend.tech model could be transformative for a world that craves OnlyFans intimacy for non-sex work use cases. Congratulations to 0xRacer for building an OnlyFans for crypto's sapiosexuals.

(*I'm an investor in Lens already, and I'll be investing across this category going forward.)

2.10 The DeFi Gang(s)

Ok, this one is a bit of a cop-out, but I couldn't pick just one founder from the "DeFi Summer" cohort who led the 2020 boom and have all stuck around to see (pivot?) their projects through to mainstream adoption. It is worth highlighting that essentially all of the "DeFi 2.0" counterparts are dead or mostly dead. The truth is, if you're looking for DeFi 2.0, you're looking for Solana-based teams: entrepreneurs like meow (Jupiter), Lucas (Jito), Mert (Helius), Armani (Backpack/Mad Lads), vibhu (DRiP), Edgar (MarginFi), Cindy (Drift), Bartosz (Cube), etc.

Out of the OGs, I like watching Kain and Antonio duke it out on X regarding governance norms (Antonio's dYdX is brute-forcing the protocol's migration to a Cosmos chain whereas Kain has allowed decentralized governance for Synthetix to flourish from a very early stage.) And I like watching Rune grapple with the various chess moves in Maker's decade-long master plan known as the "Endgame" while considering the pros and cons of real-world assets as collateral, while Rob goes all-in on RWAs at his new company, SuperState. I even enjoy the LINK marine's ongoing viciousness towards me for serenading Sergey when he went overtime during his 2020 virtual Mainnet presentation. (Sergey - join us in person in 2024, and I'll play for you live!)

These gangs are in different phases of life. The Solana kids are partying, and the Ethereum dads are debating protocol politics at the country club.

Conclusion:
That's a lot of TradFi, RWA, and policy folks, and a few crypto natives. That reflects the time we're living in. As crypto seeks to cross the chasm and avert political disasters that

lead to a closed-sourced fintech 2.0 redux, the battlefronts are in the true halls of power. 2024 will dictate whether we make it to the big leagues or are relegated to arguing over toys at the kids' table.

(For what it's worth, the more token native analysts agreed with almost all of these picks, but would have added Jesse Pollak from Coinbase for his work on Base and Coinbase Wallet, and given a bit more love to the Solana and Celestia crews.)

CHAPTER 3

TOP 10 PRODUCTS OF 2024

3.0 Killer Apps

I'm trying something new this year. That's right, it's a NEW section, with lots of pictures. I am giving this as a gift to you and to me.

We always talk about how "bear markets are for building," and I want to share the killer product experiences that I had this year (or that my team has been infatuated with).

First and foremost, there's the work the Messari product team has done this year, which I'm not sure is always so visible for those who just casually peruse our home page for price updates or think of us as a crypto research company with killer newsletter headlines.

(*If you savages have the audacity to read this 200 hour report, find it valuable, have money, and don't pay for one of our products, ~~I will kill you~~ [edit from legal: I will keep trying].*

Individuals can go Pro, Protocol teams / foundations / communities should check out our Protocol Services. Enterprises should set up a demo and trial our API. A number of big crypto companies didn't think our compliance-oriented products were "useful," and they're now bankrupt and their founders are in jail. SAD. On the other hand, our customers are THRIVING.

Choose wisely.)

Re Messari

I'm proud of the work our team has done this year for four core user groups: professionals, long-term investors, compliance teams, and crypto "community relations" leaders.

Messari Research is linked throughout this report, but that's a mere fraction of what we've delivered in 2023. Check out our:

1. **"Intel" Upgrades:** We monitor high-signal activity, a comprehensive range of "off-chain" events, and send custom alerts for hundreds of assets. Technical, commercial, and regulatory developments, governance proposals, token unlocks, funding rounds, and AI-curated news summaries are all available on our hosted service, and via API. The AI tools we are building are mind-blowing - good stuff coming in Q1.

2. **Asset Diligence:** No one has the depth of data that we have for crypto's top assets (i.e. the ones that move the needle for today's investors and major platforms). Our project pages got a major facelift in 2023, and we have meaty, standardized diligence reports for nearly 200 top crypto assets. Investors, governments, exchanges and their compliance teams use these dashboards and reports to ensure they have a complete picture of the who, what, when, where, and how of a given project. You can access the full library and request new reports with a 72-hour turnaround time.

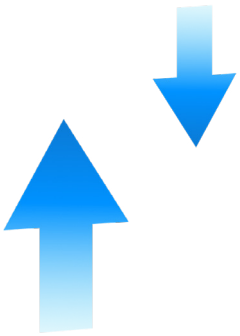
3. **Deals, Investors, and Asset Screeners:** We overhauled the Messari screener, and added our deals and investor libraries (more entity types coming soon) to what is

the most powerful investment filtering and sector analysis tool in crypto. The back-end, the front-end, the taxonomy, the available data sets, the performance, etc. all got 10x upgrades this year, and we added an AI Digest to our "watchlists" product.

4. **Quarterly Reporting:** We do comprehensive quarterly reporting for 50+ top projects under our Protocol Services umbrella, and distribute these updates for free to all of the major financial data giants. We developed these reports to show how unnecessary SEC "disclosures" are in many cases: as a third party pulling data directly from public channels and open-source blockchains, we do 90% of the work a "public filer" would be expected to do. First principles transparency is better than EDGAR dumps.

5. **Subgraph Development:** We've also been the most active subgraph contributor as a core partner to The Graph. We're continuing to support new protocols and add their key metrics to our product. Much more coming on this front in 2024.

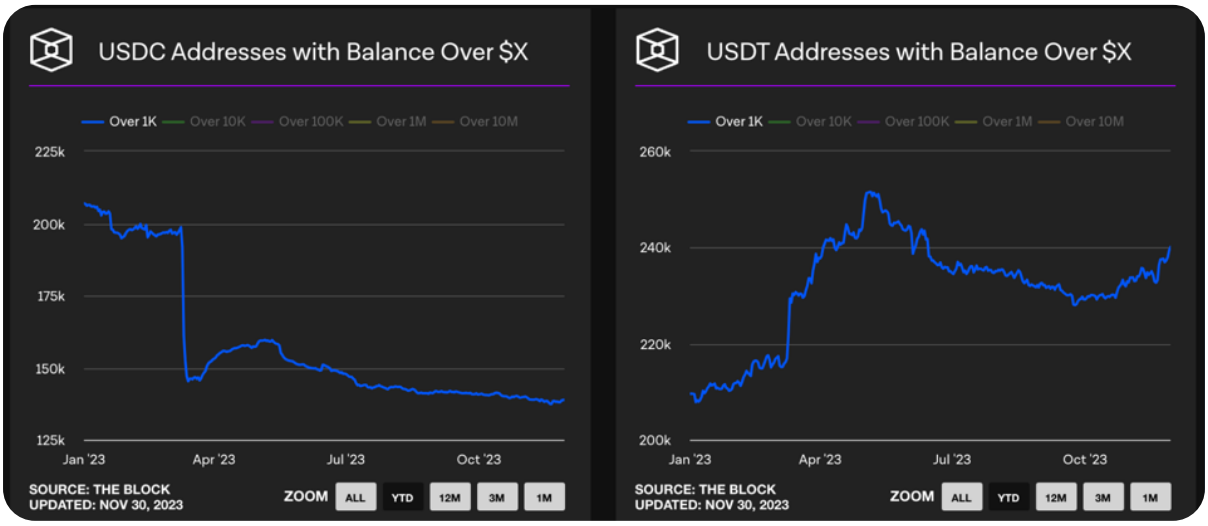
Enough about us, though. Who else shipped product this year?



3.1 USDT on Tron

Tether has long been a reserve / quote / settlement currency for overseas crypto exchanges, but Tether CEO, Paolo Ardoino, said in a recent interview that a full 40% of USDT demand was now coming from store of value and payment use cases, particularly in developing countries. With 99% of the global stablecoin market pegged to the U.S. dollar, and ongoing regulatory headwinds in store for the dominant U.S. digital dollar (USDC), USDT on Tron has emerged as the world's top crypto payment network.

I didn't have USDT dominance on my bingo card for the year, but Justin Sun (who made my 2020 people-to-watch list) has pulled off the improbable, and facilitated crypto's first truly globally important app. USDT on Tron is helping crypto realize its financial inclusion potential, and one of the most telling indications that power users and consumers rotated-out of U.S. bank affiliated stablecoins can be seen by the number of USDT vs. USDC wallets holding $1,000+ balances. USDC lost 33% of that type of user this year, and USDT appears to have picked them up on a nearly 1:1 basis. Ball don't lie.

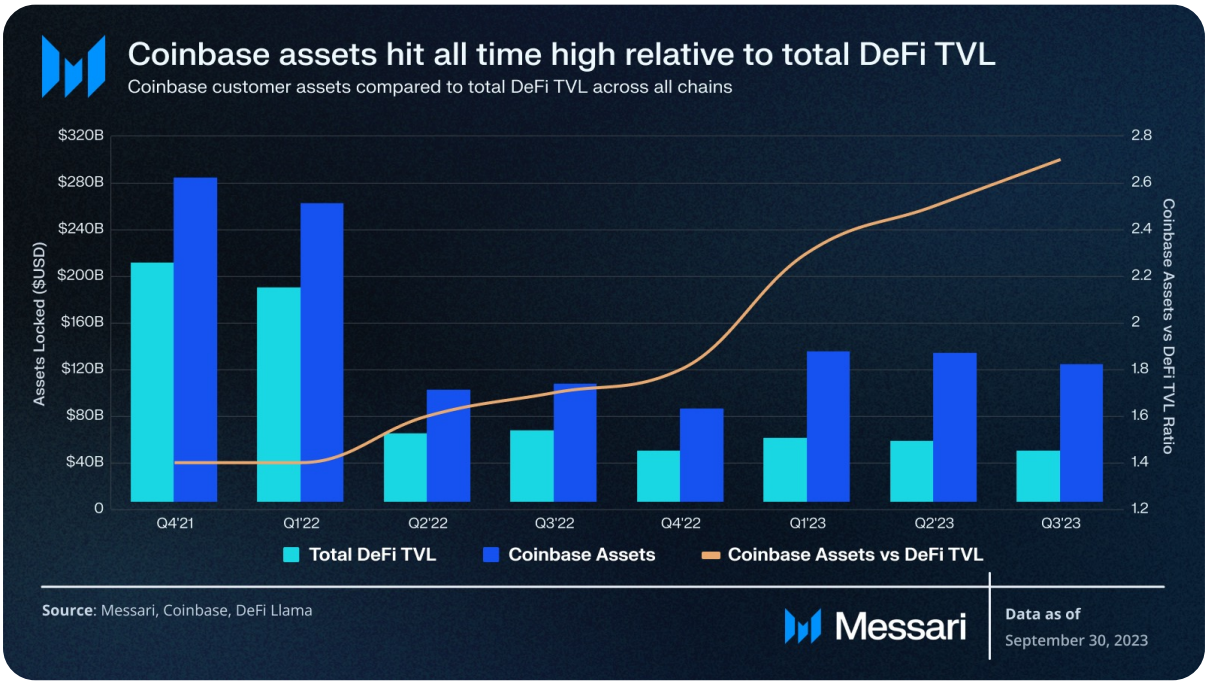


(Source: The Block Data)

[Required Reading: State of TRON Q2 2023]

3.2 BASE from Coinbase

Coinbase's entrance to the rollup market was a big crossover event for onchain finance. The Base bridging experience in the Coinbase wallet app is intuitive and (for a welcome change) doesn't fill me with terror every time I complete a bridge transaction. The speed and UX of Base helped pave the way for friend.tech's sensational launch during "onchain summer." And as a company, Coinbase has 80% more "TVL" in custody than DeFi has across all blockchains.

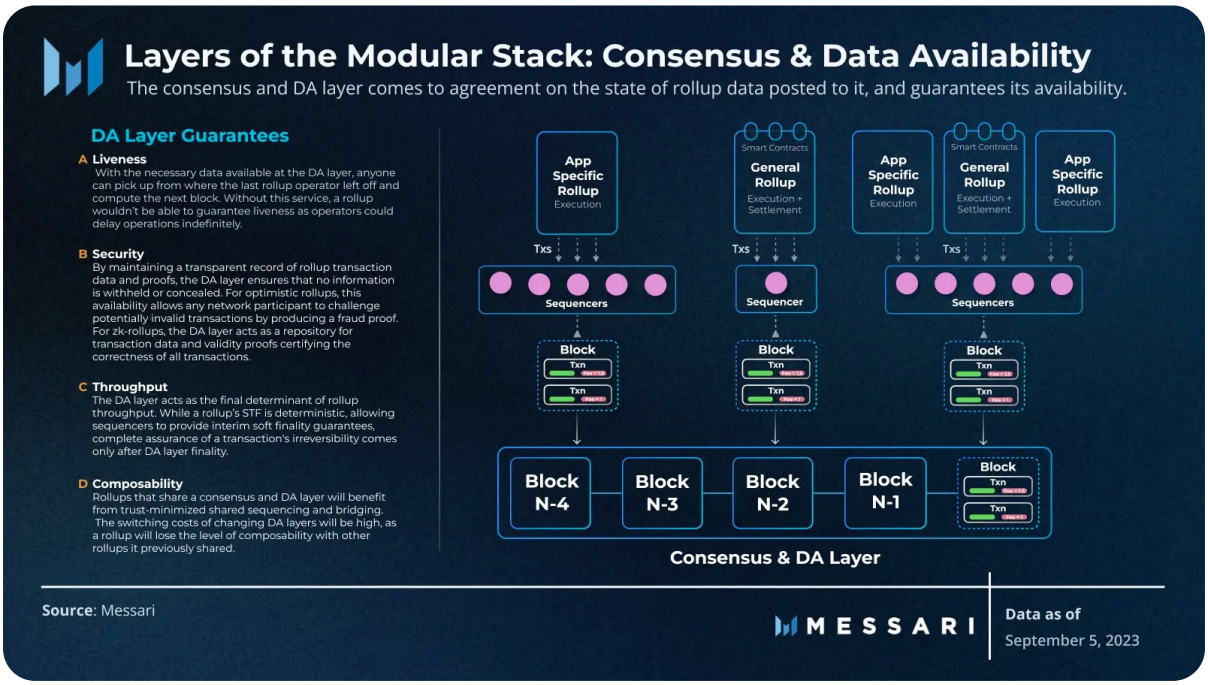


Coinbase doesn't need (or want) a token for Base (or so they say), but they have something just as good - a Coinbase "sidechain" that gives them a (low) take rate on all network transactions and that leverages USDC as a native asset (which they have an economic interest in promoting). Base blurs the line between Coinbase's centralized and decentralized services, and keeps Coinbase users within the Coinbase orbit, even when they navigate away from the exchange itself. EVM-forked BNB Chain came first, but the Coinbase go-to-market for Base seems like the model that newer exchange-affiliated rollups from Kraken and OKX will pursue as well.

[Required Reading: Pump Up The Base, Base: Establishing a Legitimate Layer-2 Presence]

3.3 Celestia

Celestia is one of the hottest token projects of the year, launching with the perfect pitch (modularity) at the perfect time (the uptrending market this November). Celestia is simple: it provides data availability and consensus for modular blockchains.

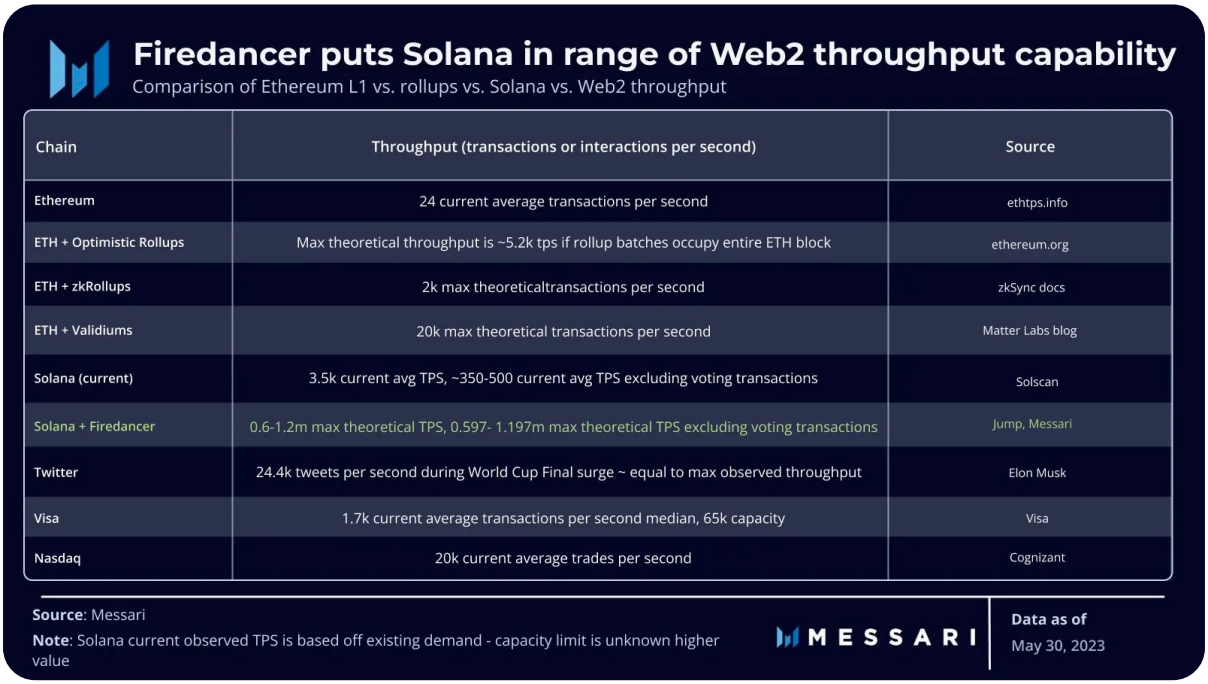


Unlike on Ethereum, where rollups need to factor in high data posting costs to the already crowded L1, by specializing only on consensus and data availability (and not on execution), rollups and other novelly constructed networks that launch on Celestia face lesser base layer congestion (and costs). Eclipse is among the first, with an upcoming launch targeted for Q1. As another high-profile chain built with the Cosmos SDK, Celestia's momentum may also be a boon for Cosmos. Is this the year Cosmos finally breaks out of its slumber?

[Required Reading: Celestia Token Launch and Valuation Dynamics]

3.4 Firedancer

The Solana validator client developed by Jump Crypto aims to enhance Solana's scalability, reduce latency times, improve client diversity, and boost throughput by 10x, making it possible to produce one million transactions per second or more on Solana. I remember the "TPS wars" of the early L1 days, and generally have an "I'll believe it when I see it" response to these sort of lofty proclamations. But over the summer, we (ok, Kel) called Solana the "contrarian bet" vs. Ethereum's "modular" and "rollups-centric" approach to scaling, and Firedancer has a lot of people fired up for the future. This is the yin to Base and Celestia's yang.



Firedancer puts Solana in range of Web2 throughput capability

Comparison of Ethereum L1 vs. rollups vs. Solana vs. Web2 throughput

Chain	Throughput (transactions or interactions per second)	Source
Ethereum	24 current average transactions per second	ethtps.info
ETH + Optimistic Rollups	Max theoretical throughput is ~5.2k tps if rollup batches occupy entire ETH block	ethereum.org
ETH + zkRollups	2k max theoreticaltransactions per second	zkSync docs
ETH + Validiums	20k max theoretical transactions per second	Matter Labs blog
Solana (current)	3.5k current avg TPS, ~350-500 current avg TPS excluding voting transactions	Solscan
Solana + Firedancer	0.6-1.2m max theoretical TPS, 0.597- 1.197m max theoretical TPS excluding voting transactions	Jump, Messari
Twitter	24.4k tweets per second during World Cup Final surge ~ equal to max observed throughput	Elon Musk
Visa	1.7k current average transactions per second median, 65k capacity	Visa
Nasdaq	20k current average trades per second	Cognizant

Source: Messari
Note: Solana current observed TPS is based off existing demand - capacity limit is unknown higher value

MESSARI

Data as of May 30, 2023

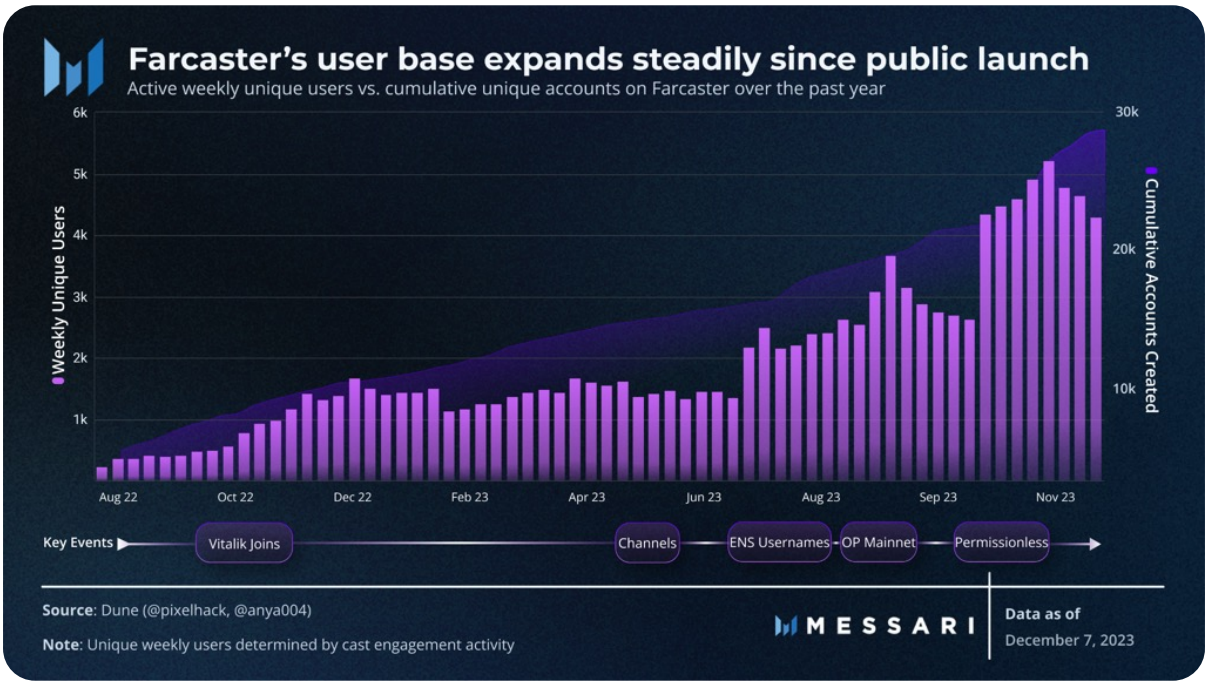
Jump demoed the capabilities at Solana's Breakpoint conference and released the Firedancer testnet this fall. Solana is *fast.* It's close to parity with centralized exchanges (as an individual DeFi user you immediately feel the difference), and the UX improvement could attract more participants and developers to Solana. It's not an "either/or" thing either: Coinbase will also support Solana (and Bitcoin's lightning) as part of their mission to bring transactions under "one cent and one second."

(To get a flavor of the potential for Firedancer, just test out projects like Jupiter, which allow traders to do things like dollar cost average into positions cheaply and automatically. Imagine Jupiter's speed at 10x scale.)

[Required Reading: Solana – Firedancer Overview And Unlocks]

3.5 Farcaster

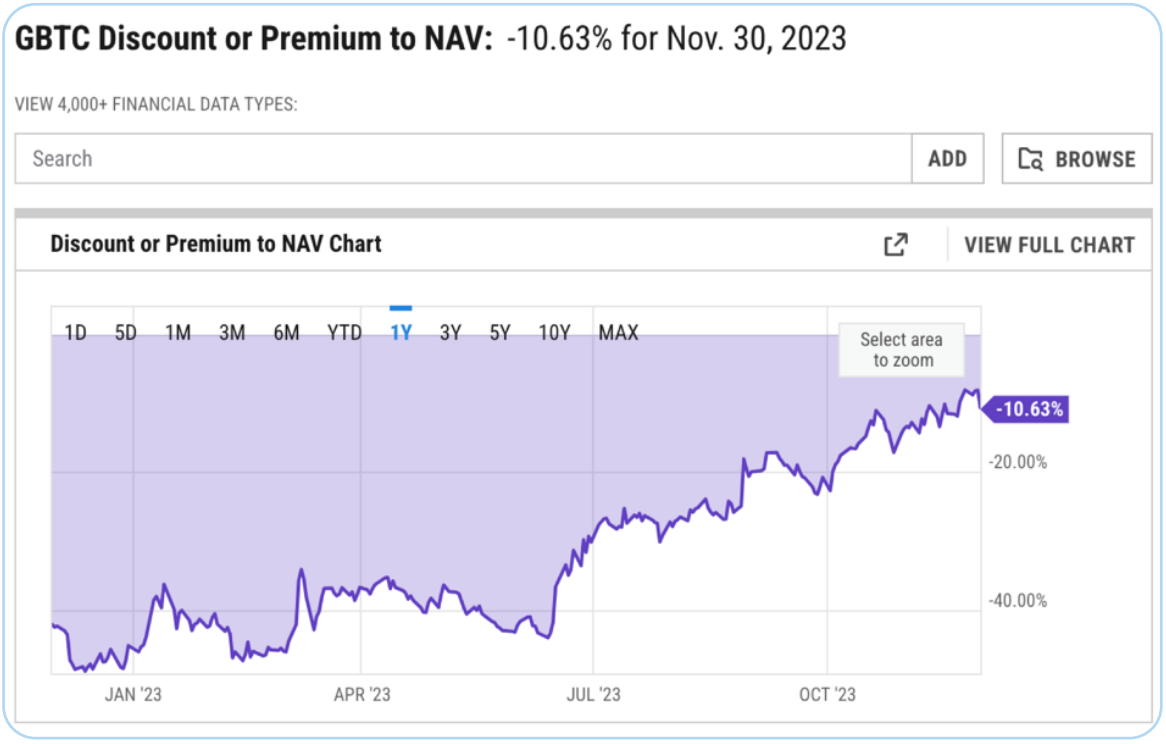
Farcaster is slick. It's the closest thing we have to the look and feel of a clean, Web2 social application, with a hybrid back-end architecture that uses onchain contracts for identity management and an offchain peer-to-peer network for social interactions. The Farcaster experience is the result of a maniacal early focus on curating the early user base, which is one reason they count regular posters like Vitalik and Balaji. About 40% of user interactions take place on thematic channels rather than their standard feed, which shows how they've improved upon some core X features, too. It's early days for DeSoc, but I will say that if X goes down, Farcaster's Warpcast is the first app I'd pull up. (I'm also overdue to try some of the updated Lens apps, and plan on doing so over the holidays. I'm open to suggestions.)



[Required Reading: Farcaster's User-Centric Growth]

3.6 GBTC

Surprise! Grayscale's SEC victory helped close what was at its peak an $8 billion gap in the market value of the Bitcoin Trust's shares vs. the fair market value of their underlying bitcoins. Barring unforeseen setbacks that cause the SEC to remove GBTC from its ETF approvals list, the NAV gap should soon close completely, and GBTC will, overnight, become: a) the world's most liquid bitcoin investment product for institutional entrants, b) ~75-100+ bps cheaper to hold as an investor, and c) the first product of all time to spark three market bubbles (GBTC was created in the fall of 2013, the levered Grayscale trade was born in 2020, and a 2024 ETF approval *should* be pretty bullish) AND one credit contagion. (Read more in Chapter 6.)

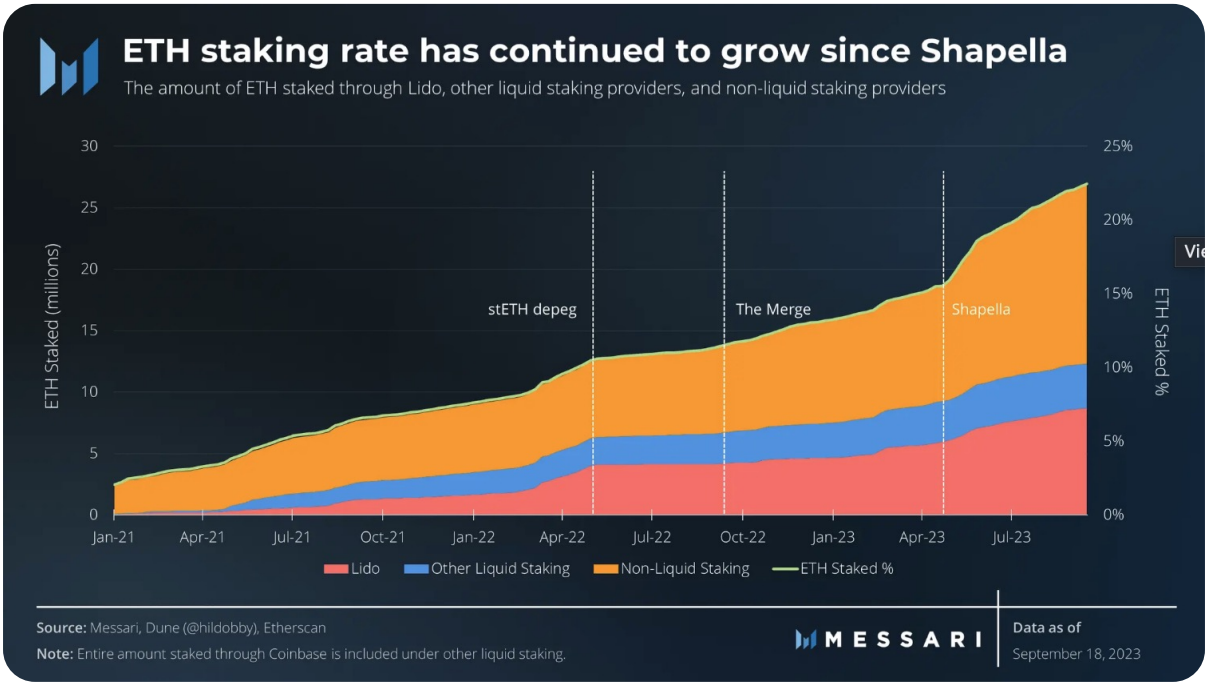


(Source: YCharts)

[Required Reading: The Grayscale-Gensler Stalemate]

3.7 Lido

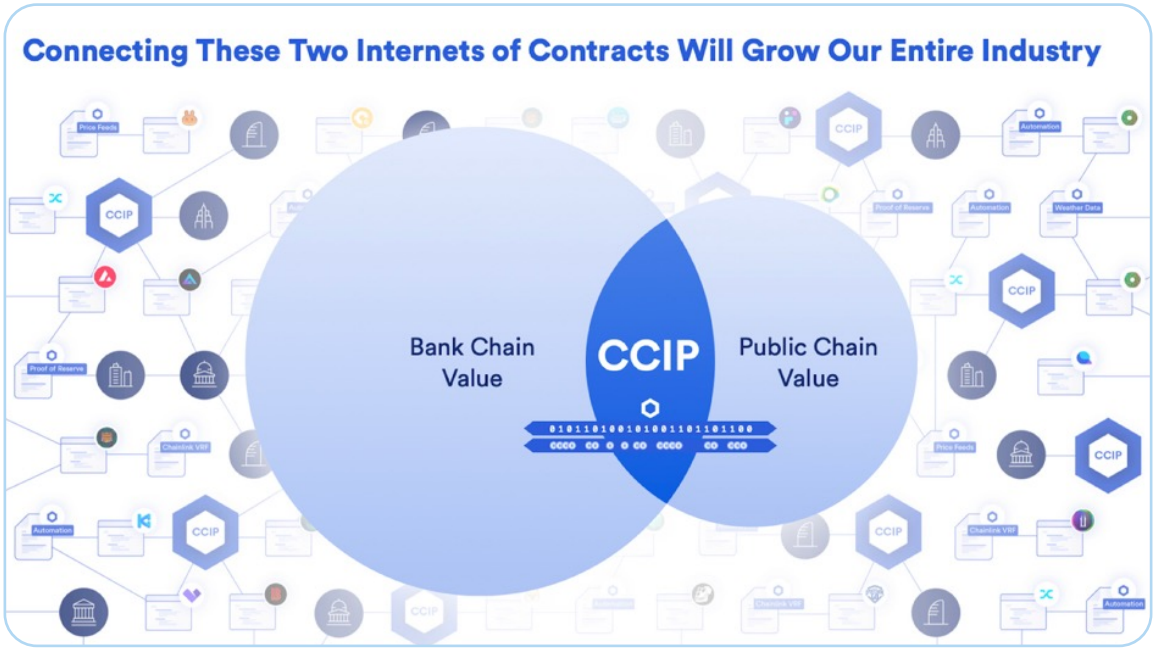
The ETH staking ratio now sits at 24% of the network, and liquid staking pioneer Lido has been so successful, they're passing laws to slow it down! Lido's outsized market share is causing headaches for core developers concerned that a 33% stake of the validator market might impact Ethereum's decentralization and overall economic security. So far, Lido hasn't tipped that magic staking number (thanks in part to Ethereum user activism), which has opened the door for centralized competitors like Coinbase, and alternative decentralized staking services like Rocket Pool to gain share. But this is one of the highest growth areas of DeFi in 2024, and the derivative use cases of stETH (like interest bearing stablecoins) are very exciting.



[Required Reading: Overdone Stake]

3.8 CCIP

Chainlink's Cross Chain Interoperability Protocol (CCIP) launched across Ethereum, Optimism, Polygon and Avalanche this summer, and rapidly attracted developer interest for those who wanted to send messages securely and privately between chains, and make "Simplified Token Transfers" that eliminate the need for customized code in token pool smart contracts. Chainlink also created an Active Risk Management (ARM) network to detect malicious cross-chain activity and protect user funds, a biggie given our collective proficiency at getting catastrophically hacked. Early partners include Synthetix (cross-chain liquidity), Aave (cross-chain governance), and Swift (bridging real-world asset tokens into DeFi). These big bank chain partners present the most exciting (and underappreciated) opportunity. *(Watch Sergey's keynote at Smartcon.)*

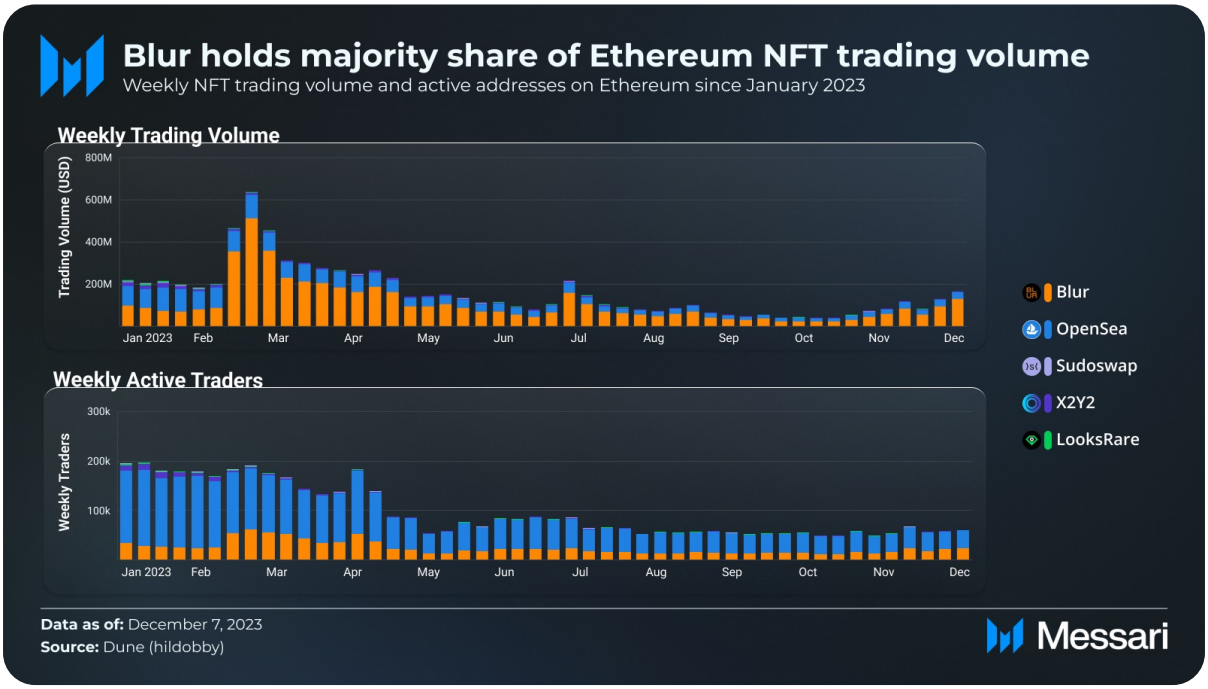


(Source: Chainlink)

[Required Reading: Speaking in Tongues - Profiling Cross-Chain Messaging Protocols]

3.9 Blur, Blend, Blast

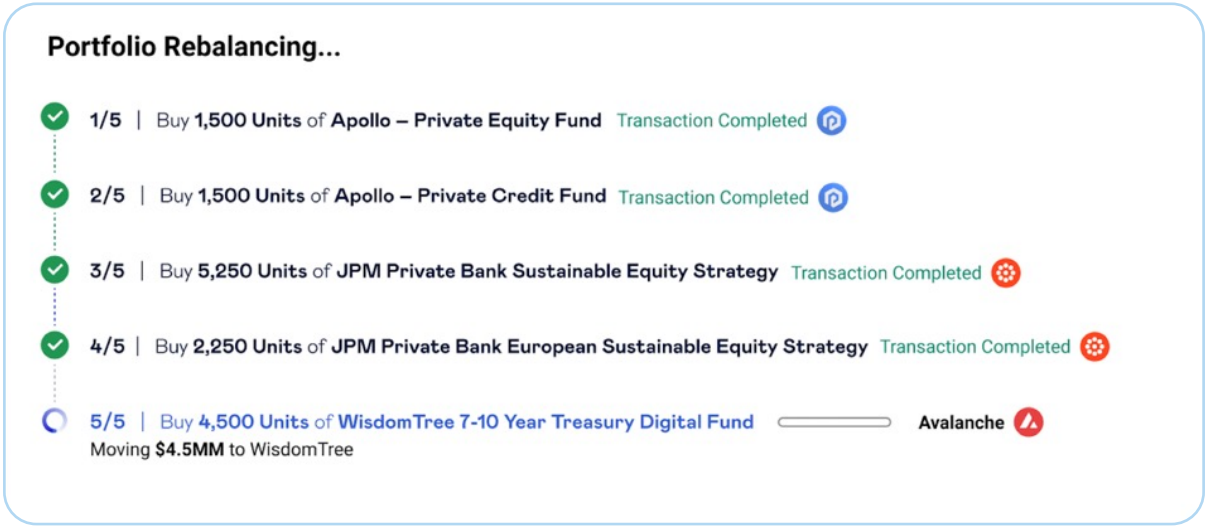
Sushi may have been crypto's first vampire attack, but nothing drained the lifeblood from the NFT markets quite like Blur and its family of NFT financialization products. (*I say that as an investor in both Blur and OpenSea.)* Blur completely shook up the Ethereum NFT ecosystem this year with a trader-friendly UX that bored a hole in the armor of OpenSea's creator-friendly quasi-monopoly. Blur's protocol incentives and innovative degen lending products like Blend have rubbed some people the wrong way. But the NFT primitives they are shipping are important building blocks for the long-term vibrancy of the NFT market. NFTs have been a real Blast this year, but I'm hopeful heading into 2024.



[Required Reading: NFT Lending, Marketplaces and Institutional Adoption]

3.10 Project Guardian

Project Guardian is the best looking Crypto Mullet of 2023 (banking in the front / crypto in the back). Remember when I wrote in Chapter 1 that I'd love to see low-fee, auto-rebalancing index products in crypto? Well one got built...for TradFi. JPMorgan and Apollo worked with Avalanche, LayerZero, Axelar, Oasis, Provenance, and others to create a product that would allow asset managers to tokenize funds and better manage rules-driven active portfolios. Green jacket, gold jacket, who gives a shit. The underlying assets don't matter, but the tech is here, it works, and it might be possible to offer in a regulatorily compliant way sooner than I thought.



(Source: The Project Guardian Demo)

The index product PoC was an eye-opener thanks to its potential integration paths to public blockchains and leverage of DeFi primitives. This was the first time I've ever gotten excited about a TradFi crypto product, which is saying something!

Conclusion

We've only scratched the surface here. We have a LOT more alpha to drop on new crypto products and protocols in the new year. But you gotta subscribe.

Keep shipping, and subscribe to Messari Pro (individuals) or Enterprise (teams) today. The team only lets me write this report if we move product, so show me the money!

Messari
Enterprise

Access all of our industry-leading data sets and tools.

Intel

Key Developments	✓
Governance	✓
Newsfeed	✓

Diligence

Asset Diligence Reports	✓

Rankings

Assets	✓
Exchanges	✓
Protocols	✓
DAOs	✓
Tools	✓
Pools	✓

Data Tools

Asset Screener	✓
Deals Screener	✓
Investors Screener	✓
Trading View Charts	✓
Chart Explorer	✓
Chartbook Library	✓
Chart Overlays	✓
Watchlists	✓

Research

Quarterly Reports	✓
Pro Research	✓
Enterprise Research	✓

Alerting

Key Developments	✓
Governance	✓
Diligence Report	On Demand
AI Digests	✓

CSV Exports

On Chain Data	✓
Market Data	1D Granularity
Deals & Investors	✓
Key Developments	✓
Governance	✓

API Access

Market Data	1D Granularity - down to 5min On Demand
News	✓
Key Developments	On Demand
Governance	On Demand
Diligence	On Demand
Research	On Demand
Assets	On Demand

Newsletters

Unqualified Opinions	✓
DAO Breakdown	✓

Visit messari.io/enterprise to learn more or contact sales@messari.io to schedule a demo.

Schedule A Demo

CHAPTER 4

TOP 10 CRYPTO MONIES OF 2024

4.0 Bitcoin & Other Digital Monies

For years, I've been of the opinion that "bitcoin" and "crypto" are two completely different financial innovations: bitcoin is a new form of digital money secured by novel technology, while other crypto projects are decentralized technologies secured by a novel type of asset.

That may seem pedantic, but I think the ordering is important.

Bitcoin truly is digital gold, transmuted from physical energy sources and a peer-to-peer global competition for computing power. By contrast, Ethereum, DeFi, DePIN, etc., are fundamentally financial platforms that would work just fine in semi-centralized contexts. But they *also* work on a decentralized basis thanks to the tokens that undergird them, which help align diverse, global stakeholders. In important respects, these non-money crypto tokens have less in common with bitcoin than other digital "monies" (e.g., stablecoins or RWAs) that sit on top of them.

If you're in crypto for the tech, we'll have plenty of sections covering the apps and infrastructure that go beyond money in the chapters ahead. But as a starting point, we'll first cover the mega-trend towards digital money, starting with bitcoin, stablecoins, and CBDCs.

[Required reading: State of Bitcoin Q3 2023]

4.1 Bitcoin is the Godzilla of Finance

Digital gold has never had more tailwinds. I teased some of the market structure dynamics at the very beginning of this report, but it is worth going into further detail here.

Thoughts and prayers for the bears when:

1. **A spot bitcoin ETF is finally approved.** This January could begin a new era of institutional adoption. ETFs are about accessibility (click "buy" with existing Wall Street counterparties and workflows) and state signaling (the SEC would be blessing bitcoin's right to exist and flourish in the U.S.). The spot ETFs are properly hyped and may still be underestimated in their importance. Mike Novogratz made the point at Mainnet that "Wall Street products get sold, not bought," and giving incentives to the world's top financial salesman to hawk bitcoin will, indeed, prove to be a bonanza for the industry. (Raoul Pal and Scaramucci agreed.) More financial veterans will begin to see the same stats that investors like Paul Tudor Jones have seen for years now: bitcoin holders simply don't sell, and the light bulbs will start going off all across Manhattan.

2. **Concerns about currency debasement run high.** Bitcoin took a lot of flak for "not performing well" during the high-inflation period of 2022, but I've always found that to be a silly critique. It did phenomenally well in 2020-2021 as a *predictor and*

frontrunner of inflation and, more importantly, of monetary debasement. It's once again the "fastest horse" among global debasement hedges as central banks begin to think about restarting QE. Many economists believe the only way out from under our crippling national debt is through a multi-year period of high inflation. Debasement is inevitable.

3. **The accountants are on our side.** Favorable accounting changes from the Financial Accounting Standards Board (FASB) now allow public companies to hold bitcoin on their balance sheets at market value, enhancing its legitimacy as an asset class, and removing what had been an unfair millstone around the necks of corporate treasurers. This is underappreciated, especially now that Michael Saylor's MicroStrategy is sitting above its cost basis on a mammoth bitcoin position. More corporates will begin to come around, especially after the SEC approves the spot ETF.

4. **The bitcoin "protest vote" is real.** Bitcoin's decentralized nature, limited supply, and culture make it a potential beneficiary of libertarian political movements, especially in countries like Argentina, where Austrian economist Javier Milei just won a landslide election after promising to abolish the perennially failing Central Bank of Argentina. I think bitcoin's role in protests (vote with your wallet) could emerge in dozens of countries with economic distress and political unrest driven by financial policy. Yes, that includes the U.S. leading up to the 2024 election. As individuals seek alternative stores of value and declare financial independence, bitcoin may gain traction as a political statement.

5. **We canceled a country last year.** I still don't think most people appreciate the long-term ripple effects we will feel from our aggressive use of financial sanctions against Russia. You can't seize another country's assets en masse and still maintain blind faith in the dollar system and its viability as a neutral global reserve. I wrote about Zoltan Poszar's "outside money" thesis in last year's report, and it holds up remarkably well. Poszar believes we are entering a period of prolonged high inflation, and mass movement away from the dollar as a reserve currency as more trade settles in euros, renminbi, and gold rather than dollars.

6. **The trend towards digital cash is obvious and unrelenting.** As the world transitions toward digital assets and a cashless society, bitcoin is likely to capture demand from those who want assets that are difficult to surveil and seize. Stablecoins, for all their potential, can't really offer that. In the aftermath of the Terra/LUNA collapse, it's unclear whether we'll ever be able to bootstrap a purely algorithmic stablecoin. If you want full control over your money, bitcoin is still the best game in town.

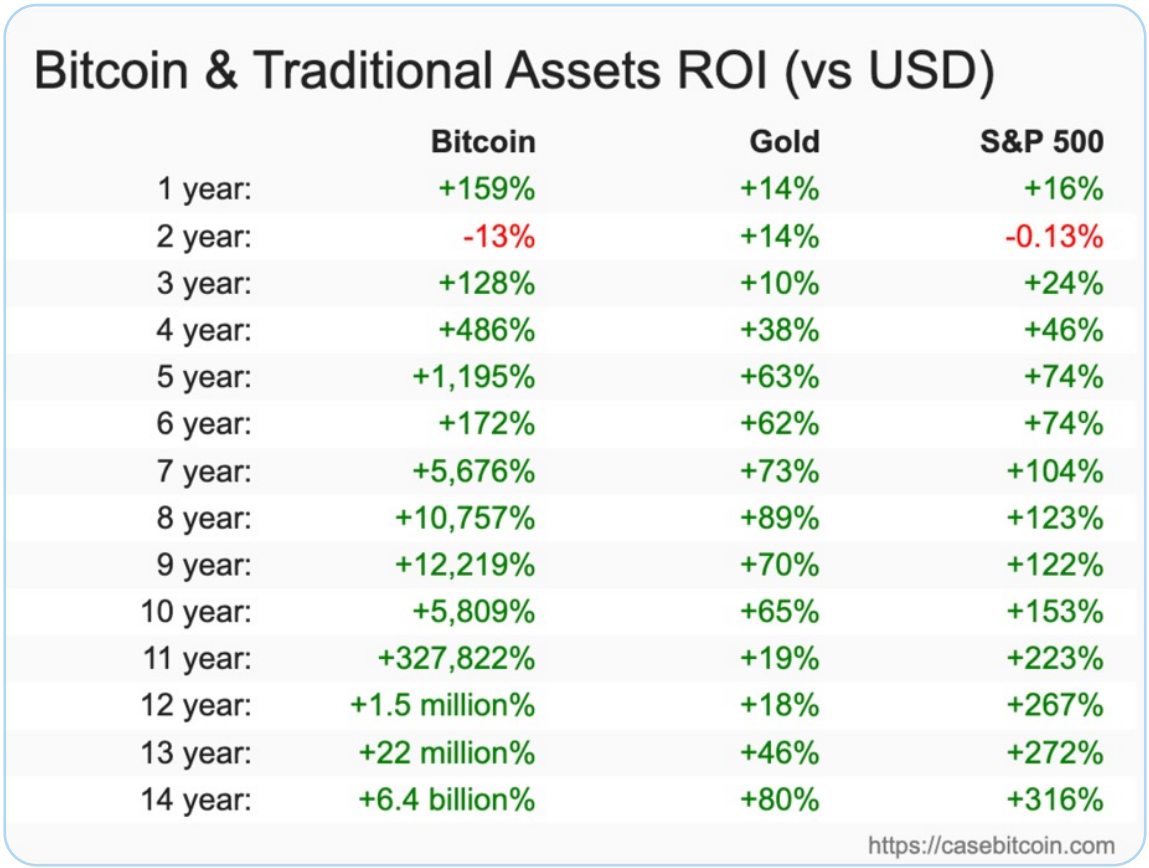
7. **Bitcoin's upcoming halving reinforces its scarcity and 21 million coin meme.** This resonates with investors seeking a hedge against monetary expansion. The quadrennial halving event, which will next occur in mid-2024, is free, powerful marketing. It's less about the positive supply shock (a halving from 3% to 1.5% is less impactful than the 2012 halving from 25% to 12.5%), and more about the simplicity and consistency of the message. Central bankers may command the attention of the Wall Street traders glued to their Bloomberg terminals, but there's

no need for high priests with a monetary policy this simple.

8. **Negative catalysts from "whale sellers" are diminished.** The closing of the GBTC ETF "NAV discount" (more later), the utter destruction of the crypto lending markets (lower cascading liquidation risks), and the delay in the distribution of bitcoin to Mt. Gox bankruptcy victims (again), cut back on areas of obvious potential selling pressure. There has never been a more diamond-handed bitcoin holder base.

If you run over a baby lizard with a truck, and it shrugs off the blow, then grows ten times larger; and then you run it over again, and the now adult-sized lizard once again 10x's in size; and then you do that a couple more times and the same thing keeps happening, you're not dealing with a lizard, you're dealing with Godzilla.

Bitcoin in 2024 = Godzilla.



Bitcoin & Traditional Assets ROI (vs USD)

	Bitcoin	Gold	S&P 500
1 year:	+159%	+14%	+16%
2 year:	-13%	+14%	-0.13%
3 year:	+128%	+10%	+24%
4 year:	+486%	+38%	+46%
5 year:	+1,195%	+63%	+74%
6 year:	+172%	+62%	+74%
7 year:	+5,676%	+73%	+104%
8 year:	+10,757%	+89%	+123%
9 year:	+12,219%	+70%	+122%
10 year:	+5,809%	+65%	+153%
11 year:	+327,822%	+19%	+223%
12 year:	+1.5 million%	+18%	+267%
13 year:	+22 million%	+46%	+272%
14 year:	+6.4 billion%	+80%	+316%

https://casebitcoin.com

(Source: CaseBitcoin)

4.2 Bitcoin Security Model & Assumptions

From the above, you can probably gather that I like bitcoin.

But that doesn't mean *I don't like* to poke my finger in the eye of the bitcoin religious community (the maximalists) every once in a while by reminding them bitcoin's security model might be broken long-term. This is generally not a controversial position amongst rational people: Hasu, Nic, and I among others have talked about this openly as a known risk for half a decade at least.

It's fairly straightforward: at some point in the not-so-distant future, the rate of new bitcoin issuance to miners via coinbase ~~Coinbase~~ rewards will be very low relative to the size of the market those miners are actually securing. Onchain transaction fees must increase over time in order to offset the predictable decline in bitcoin seigniorage over the halving schedule, but we haven't seen any evidence of that happening historically.

Bitcoin's entire transaction security model depends on economically aligned miners who compete for marginal revenue that is greater than their marginal cost of energy and mining equipment CapEx. As such, you get only three options for long-term survival: applications that pay a lot of fees emerge on top of bitcoin, creating ongoing incentives for miners; there will eventually be an amendment to the 21 million bitcoin "soft cap" to ensure bitcoin miners some minimal per block seigniorage; or bitcoin mining will eventually switch over to Proof-of-Stake.

Otherwise, the network fails (the fourth "option").

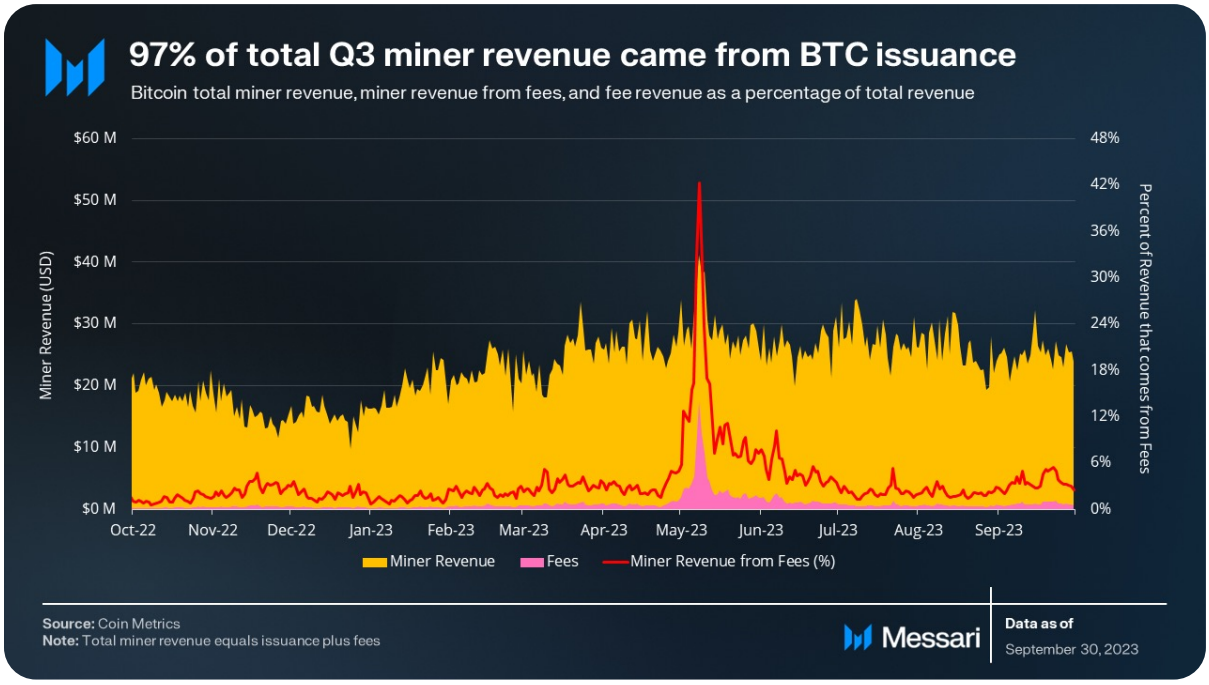
I'd assign a roughly equal probability to all four outcomes:

1. **Apps generate fees:** We'll cover Ordinals and Inscriptions later on, but bitcoin had a couple flash-in-the-pan applications in 2023 that hint at future potential for bitcoin native applications. I wouldn't bet the farm on this happening, since Ethereum and other smart contract platforms have many years worth of a headstart and more flexible programming languages. But I appreciate Udi and Eric trying. (Eric also had the best two minute clip of the year, for what it's worth.) That said, initiatives to utilize bitcoin as a DA layer for sovereign zk rollups could marry the mature smart contract development environments with bitcoin blockspace and drive fees.

2. **Soft cap, with ongoing Proof-of-Work:** I think I was the earliest person to write about this in a meaningful way, but I'm happy to review alternative evidence. As I explained in mid-2015 (jfc where'd the decade go), all bitcoin really needs to do is remain less inflationary than its fiat brethren and stored value competitors. The network could reach consensus on an inflation rate that is just below the next strongest reserve currency or the annual mining output of the gold industry (~1.5%), and bitcoin would still win. In the process, those subsidies would guarantee that bitcoin would always win as a payment rail over centralized competitors like correspondent banks and card networks, because transaction fees could remain artificially low.

3. **Hard cap, migration to Proof-of-Stake:** it's conceivable that bitcoin transitions to a

Proof-of-Stake environment in which holders are incentivized to stake BTC in order to collect onchain transaction fees themselves. This is blasphemy to bitcoin maximalists, but it is also functionally indistinguishable (as a thought experiment) from what would happen after all seigniorage runs out in 100 years if fees do not rise. Using today's (ballpark) annualized figures, a network that stores $600 billion of value and settles $3 trillion of annual transactions probably needs more than $250 million of hardware CapEx to maintain its security. As bitcoin further financializes (ETFs, Wall Street custody, rehypothecation, etc.), it becomes more likely that the "economic majority" within the bitcoin network rotates in the direction of PoS.



4. **Irrelevance:** A lot of people who are newer to crypto don't really understand how toxic the infighting within bitcoin was in 2015-2017 during the "blocksize wars." It's one of the primary reasons Ethereum took off in parallel, and we've seen relatively little innovation on bitcoin ever since. This is perhaps the biggest reason to be long ETH, despite my analysis in Chapter 1 that there are faster horses to bet on if you want digital gold (bitcoin) and exposure to smart contract platform's value creation (the non-ETH field of L1/L2 tokens).

The next bitcoin halving is mostly a marketing event for bitcoin's (temporary) hardness. It's going to be great for the memes, especially since it might fall on Tax Day 2024, and it'll be a milestone to mark our survival and resilience. But just know that it's also probably an illusion, as I doubt we can go much lower than 75 bps of annual seigniorage and maintain a healthy, secure network.

That's no longer ten years away. It's two.

4.3 Bitcoin Mining More Important Than Ever

I would prefer that a bitcoin fee market develops or that we fork the protocol to maintain a minimum viable level of seigniorage to ensure we keep Proof-of-Work mining as bitcoin's security model. The same reason so many people hate bitcoin mining — its energy intensity — is the reason we like it!

It's a contrarian, resilient, complementary model to what is otherwise the Proof-of-Stake default prevalent in essentially all other crypto networks. Mining is an industrial sector at its core, which helps keep bitcoin block production away from the financial incumbents who work for the state. The energy intensity of bitcoin is the top attribute that makes the network less susceptible to nation state-level capture.

I do believe that's why authorities truly hate Proof-of-Work mining. It's got nothing to do with climate change or local energy market dislocations, and everything to do with the fact that energy competition makes financial regulation much more difficult. You can be pro-environment and pro bitcoin mining. If you think these are at odds, you're being conned amidst a long-term information war aimed at destroying bitcoin itself.

And boy do the statists lie. And lie. And lie. And lie.

The reality is that bitcoin mining (at least domestically) helps reduce methane emissions, balance grids, and incentivize building new renewable capacity before it can necessarily be connected to local power grids. Refer to Jerry Brito for more on how to fight this incessant FUD.

4.4 Private Transactions: Protocols, Coins, or Pools?

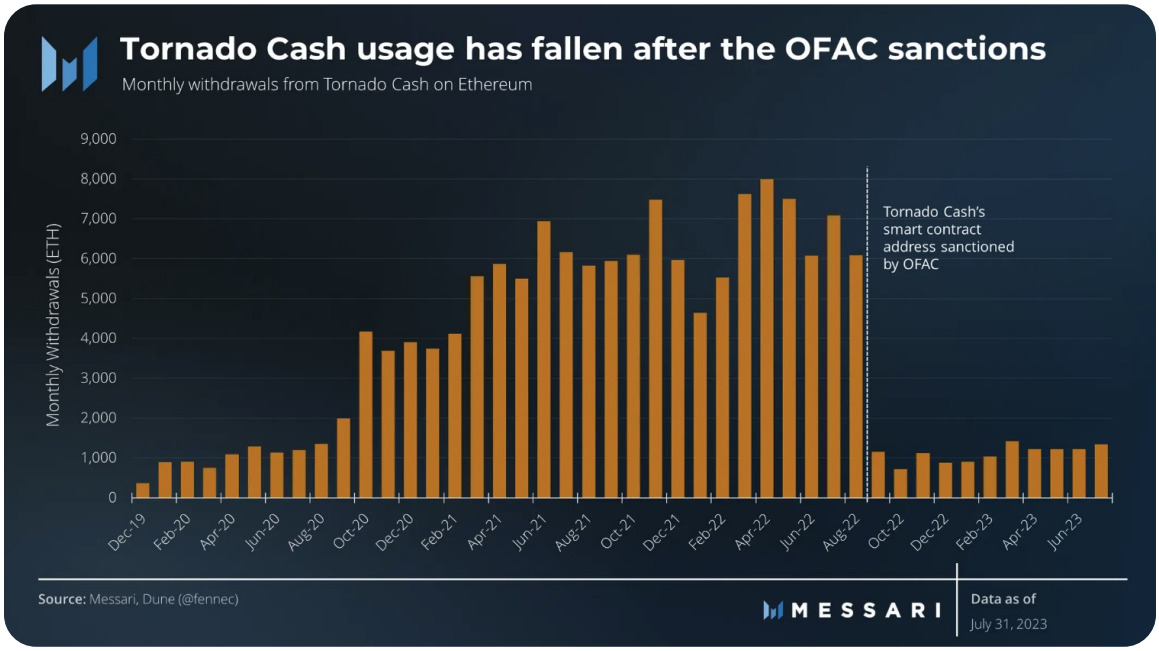
We face an extreme uphill battle when it comes to private crypto payments in the future.

The Tornado Cash *protocol* sanctions and *developer* arrests remain two of the most alarming things to have happened within crypto over the past two years, and things only got worse this year. The industry's challenge of OFAC sanctions on constitutional grounds isn't going so well, as both Coinbase and Coin Center lost their initial lawsuits and must now appeal to higher courts. They (and other supportive policy groups) remain confident in the merits of these cases, but it appears that judges so far have determined the existence of a protocol-affiliated DAO and/or governance token is enough to create a sanctionable entity.

That leaves three (potentially) legal paths for the industry to pursue truly private transactions.

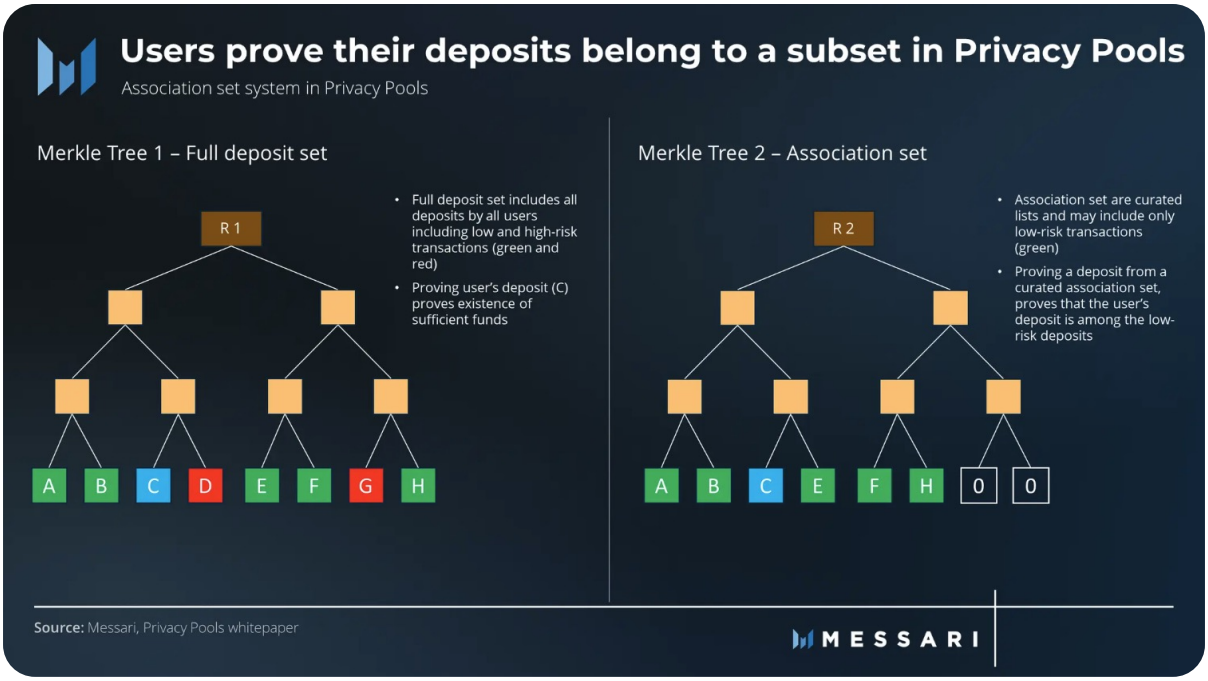
1. **Tokenless Tornado Cash:** Such a protocol would include contracts that are non-upgradeable on day 1, avoid relayers, and include no tokens, DAOs, or ongoing developer support for the associated front-ends. That would knock out some of Tornado Cash's "bad facts" and give us a mulligan on the protocol, which clearly

found product-market fit as a privacy-preserving service. There's an EIP to enshrine this sort of service directly into the Ethereum core. And Solana has explored something similar.



2. **Privacy Chains:** Monero is the largest privacy-focused blockchain by quite a bit, despite the fact that most enthusiasm for strong privacy has moved over to technology based on zero-knowledge proofs. That hasn't really translated to success for Zcash, which has struggled mightily when it arguably should be having a moment. I think this is a failure of marketing (government hostility is beating the privacy narrative), momentum (ZEC price has only gone down historically), and go-to-market (in hindsight, bitcoin's halving schedule wasn't repeatable as a launch mechanism). The unfortunate reality may be that a zk-first blockchain was either too early or better implemented at the application layer on top of a larger chain. I don't want to throw in the towel on Zcash as a project, but it's certainly contrarian to continue betting on Zcash and its blockchain as the winning model for private transactions. Much more likely that a privacy-first rollup wins the market given the liquidity already available within that ecosystem. (Aztec?)

3. **Privacy Pools:** A new protocol proposed by Ameen Soleimani, Vitalik, and researchers from Chainalysis and academia, would create a new hybrid approach to privacy and compliance. I think the approach could get pickup as institutions grapple with the challenges of preserving data privacy and IP protections while transacting on public blockchains. The model allows users to prove that their funds come from specific verified subsets of deposits, allowing them to provably avoid commingling funds with addresses tied to suspected illicit activities. Any entity can curate a privacy pool, making the framework flexible across a wide range of jurisdictions without necessarily breaking the fungibility of the underlying network tokens.



The U.S. Treasury is already clearly feeling emboldened by the initial result, as it just sanctioned another mixer, and has embraced a move towards enhanced surveillance laws that can only be described as hellishly dystopian.

My belief is that humans have the right to transact freely, in a peer-to-peer manner, without full and constant surveillance of any government. In the U.S., we have explicit constitutional protections that affirm that inalienable right, but we may have to iterate our privacy models a couple of times before the courts settle on one they agree should be protected. The Biden administration won't agree to any of them, and it's not clear a GOP Treasury would be much better. The iteration and final, workable crypto privacy model will likely have to wind through the slow grind of the courts for several more years.

[Required Reading: How Tornado Cash Works, Privacy Pools]

4.5 - The New TINA Trade: Stablecoins

Why invest in BTC or ETH, when you could invest in long-term Treasuries whose multi-year rout now rivals the dot-com bust and 2008 financial crisis? (Balaji was right!)

(Source: Semafor)

Seriously though, I don't understand the appeal of a 60-40 stock-bond portfolio in a market with so much default risk around sovereign debt, commercial real estate debt, consumer debt, and corporate zombie debt. Why would you invest in *long-term* Treasuries when no one else wants to buy them, and you know you can get liquid exposure to short-term T-bills that pay 5% via stablecoins? Zoltan is *this close* to recognizing that the ideal portfolio isn't 20-40-20-20 (cash, stocks, commodities, bonds), but 40-40-20 (interest-bearing stablecoins, stocks, and crypto).

Stablecoins are the most explosive growth area within crypto. Our first truly killer app, stablecoins, settled $11 trillion onchain in 2022, and has bucked the trend and continued to grow this year. They do nearly 10x the payment volume of PayPal (no wonder the company launched a stablecoin this year) and are closing in on Visa's payment volumes. There are nearly five million blockchain addresses that transact with stablecoins every week.

You must read Brevan Howard's masterful mid-year report on the state of the market and Nic's Token2049 and Mainnet presentations to understand how the offshore eurodollar market and onshore digital dollar market are likely to evolve in 2024. There are basically five major stablecoins / categories in the market right now: USDT (fully reserved offshore eurodollars), USDC and pyUSD (fully reserved onshore digital dollars), DAI (and other collateralized stablecoins), new algorithmic stablecoin models, and central-bank digital currencies.

The abbreviated sections below won't do the overall market justice, but I'll try.

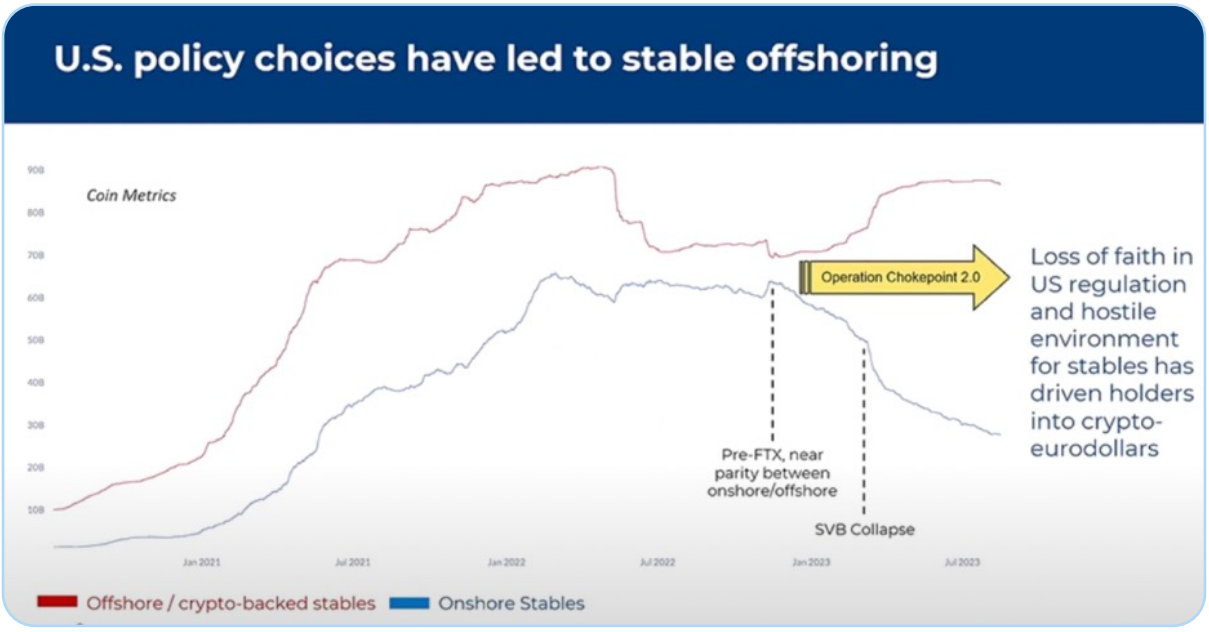
4.6 USDT

Given how quickly the U.S. dollar has been losing purchasing power, a synthetic digital dollar backed by $0.90 of T-bills, $0.05 of gold, and $0.05 of BTC might be the ideal currency for countries struggling with bank crises and high inflation. Gold is too luddite to fully back a modern currency, bitcoin is too volatile, and Treasuries come with too much seizure risk and even blow-up risk to rely upon 100%. But add all three to a basket, and you've got a killer product.

Hey, that kind of sounds like USDT!

Tether is the oldest, largest, and most critical digital eurodollar, and it serves as a critical piece of global liquidity and market infrastructure for crypto. Despite all of its prior controversies (reserves, commingling, uses, etc.) and reserve questions (audits, collateral assets, custodians), it's had a banner year following the regulatory crackdown in the U.S. With more crypto activity moving offshore and bank runs at crypto-friendly regional banks like SVB, Signature, and Silvergate earlier this spring, Tether's performance has bucked the trends.

At the time of writing, Tether had breached a new all-time high of $89 billion, while its primary competitor USDC sat at half of its previous peak. (If only U.S. stablecoin issuers could be better protected from the systemic risk these banks present to the crypto markets!)



(Source: Nic Carter)

For years, I have written that concerns about Tether are greatly exaggerated. I'm not blind to the risks, and I understand the domestic skepticism around the business. Tether's performance does seem too good to be true, but that's mostly because it boggles the mind how U.S. financial policy could be so ass-backwards that we hand a eurodollar monopoly to an overseas crypto exchange which now sits as one of the largest foreign purchasers of U.S. Treasuries. That kinda makes you think though, doesn't it?

The U.S. government's rhetoric feels more like kayfabe. Tether has survived for as long as it has *because* it plays nicely with global authorities, and there's a quiet understanding that the company will surreptitiously cooperate with the U.S. authorities long-term when it really needs to. Maybe they'll get a fine in 2024. Maybe. But I doubt there is much risk beyond that, as I find Vince McMahon's rhetoric more believable than the bluster out of D.C.

With Tether, the U.S. government wins, off-shore exchanges win, global crypto-dollar consumers win, and crypto investors win. But domestic crypto exchange and stablecoin operators lose.

The Tether team wins the most. Thanks to rising interest rates, Tether now books nearly $1 billion in earnings per quarter and holds $3.2 billion in excess reserves, including $1.7 billion in BTC, with the expectation they will use some of their "excess profits" in the future to purchase even more. From a profits per employee standpoint, it's one of the best businesses of all time, and I think it stays that way for years to come.

4.7 USDC

I've already written a bit about Circle and USDC, so I don't want to repeat myself, so much as highlight one chart that shows you everything you need to know about USDC's year in 2023. It highlights the threat and opportunity that lies ahead for Circle as the private stablecoin issuer closest to the U.S. government.

(Source: Kaiko)

"Backed by audited deposits in U.S. bank accounts" is only a competitive strength if your banks don't go under, and there's reliable access to them at all times. We didn't have that earlier this year, and it caused enormous damage to Circle and USDC, even

though the company had nothing to do with the compliance mishaps at Silvergate, the mismanagement at SVB, and the political assassination at Signature (more on this next Chapter).

Although USDC bounced back to its peg within weeks (and never faced a single redemption issue with its customers), the psychological safety that was supposed to come with U.S. banking relationships has not returned, and it seems unlikely this will reverse absent a change in tenor on crypto from the Biden administration. As bullish as I am on Circle and its early lead domestically, I am not yet convinced that U.S. regulators won't continue to hold them down while opening up avenues that reward the Wall Street incumbents to catch up first.

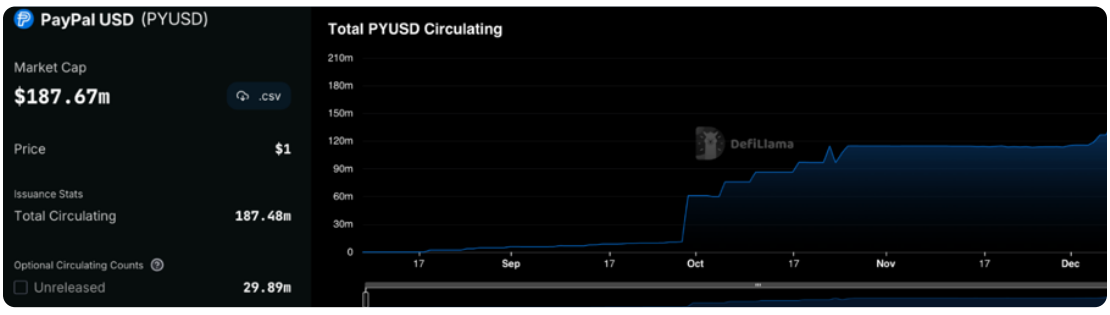
The silver lining for our most tightly regulated crypto dollar is, ironically, that it is still the dominant quote currency in most DeFi markets. USDC remains top dog in DEX volumes, CDP collateral, and money market borrows. The ETH-USDC pool on Uniswap is essentially the backbone for all of DeFi.

4.8 Paxos, Binance & PayPal Dollars

Paxos has locked in a potentially game-changing partnership with PayPal and the pyUSD stablecoin that powers PayPal's family of apps (including Venmo) - a big win in a mixed year for crypto's original New York Trust Company.

PayPal has been crypto forward for years and even has the distinction of being one of the only crypto payments firms that's well covered from potentially devastating attacks from the CFPB. The pyUSD launch was a pleasant surprise, but not a shock. It makes sense that the OG of internet payments would come around to offer a stablecoin in a rising interest rate environment. If the risk/reward skewed negative in the ZIRP environment of 2021, the sentiment would completely reverse in a year of 5% yields that would last "higher for longer." I interviewed Jose Fernandez da Ponte (PayPal's stablecoin pyUSD lead) and Paxos' Walter Hessert at Mainnet 2023, where they made the initial announcement.

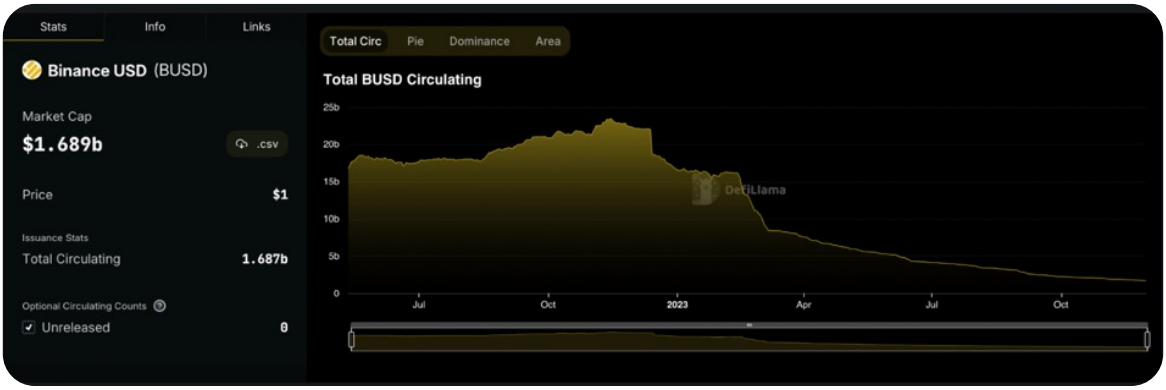
In the month that followed, pyUSD 10x'd in market cap to $115 million. It fully flatlined after PayPal received a subpoena from the U.S. SEC Division of Enforcement. But it's now back on the move. On December 8, we saw the first new issuances ($12 million) for pyUSD in a month.



(Source: DeFi Llama)

It wouldn't be the first time Paxos had a hiccup with a major partnership.

It had a huge setback and slap in the face from the New York Department of Financial Services back in February, thanks to its partnership with Binance and the Binance USD stablecoin. Following that action, Binance USD's market cap plummeted 90% from $16 billion to $1.6 billion at the end of November. Following the announced settlement with the DoJ and other financial regulators, Binance announced that it would end support for its BUSD stablecoin on Dec. 15, 2023, effectively killing the product.



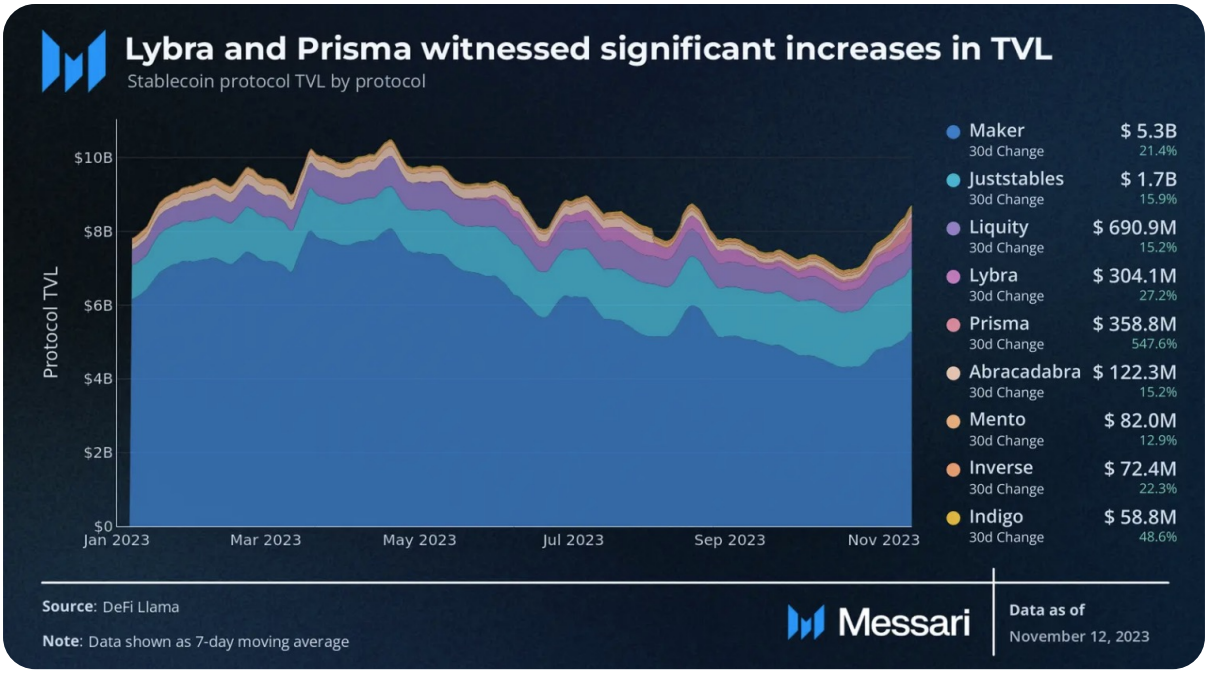
(Source: DeFi Llama)

To add insult to injury, Binance hasn't shut down its stablecoin operations, but instead simply moved them to other eurodollar partners. It started with TrueUSD, which has tripled in size since February, and more recently Hong Kong regulated issuer, First Digital, which will absorb 100% of the remaining BUSD at Binance by end of year. U.S. regulators quite literally stole this business from Paxos and sent it to Hong Kong. There's no two ways about it, and it's a small wonder that Paxos is now focusing its attention in Singapore, Abu Dhabi, and Mexico instead.

4.9 Crypto-Collateralized Stablecoins

I'm not going to front-run some of the reports we have coming out in Q1, but we've got some meaty research coming out on crypto's spectrum of crypto-collateralized (Dai) and algorithmic (Frax) stablecoins, and the economics, prospects, and hidden gems for each. I'm gonna hold back a little alpha here and direct you to subscribe for a little delayed gratification.

A little teaser: crvUSD, Lybra and Prisma are two of the newer collateral debt position (CDP) protocols that seem most promising. They allow liquid staking tokens, such as Lido's stETH, as collateral that users can mint stablecoins against while continuing to receive yield from their underlying staked ETH positions. That helps offset fees and onchain borrowing costs, even if these new models are still fairly capital inefficient and collateral constrained (TVL is capped by the size of the liquid staking token market).



Algorithmic stablecoins are pretty out of favor right now, but I remain excited about their potential in 2024. I believe we'll see some breakouts given the general unreliability of the U.S. regulators, and the need to move away from a rapidly debasing dollar as our only alternative. More flatcoins, fewer fiat coins?

4.10 CBDCs & Other Memecoins

There are two types of central-bank digital currencies: wholesale (between financial institutions) and retail. Almost all CBDC pilots to date have been "wholesale" CBDCs, which revolve around transactions between financial institutions: the Monetary Authority of Singapore (MAS) is trialing a CBDC for settlement of commercial bank payments, the Swiss National Bank is piloting a CBDC to settle digital securities transactions, etc.

But I take the retail-focused CBDC projects about as seriously as I take DOGE and PEPE. They are fun to play with and talk about, and they'll have a similar amount of near-term impact on the world. That's a good thing, too, because the way that global bankers are talking about these tools of surveillance and financial control is a bit too erotic for my liking.

Unless a Messari subscriber at one of the big banks can convince me that: a) CBDCs will be relevant *anywhere* before 2030, b) there is any hope of non-banks interfacing with them and building payment apps with them, and c) these proposals will have any degree of constitutional privacy protections baked into them — I'm going to continue ignoring them and linking lazily to the most recent cliff notes from all around the world:

- BIS Project Tourbillon says it can provide KYC and payer anonymity with its "eCash 1.0" and "eCash 2.0" prototypes. Paper released November 29.

- The Bank of Korea is piloting a CBDC program with 100,000 citizens in 2024.
- Russia is piloting a basic retail CBDC payments program in 2024 with 13 banks and a limited group of its users.

- The e-CNY is one exception to watch: it has processed over $250 billion of transactions with 120 million wallets created since 2020 and now includes Standard Chartered, Hang Seng Bank, and HSBC as pilot program partners.

There are two core concerns with CBDCs, aside from ending individual financial privacy in favor of granting authoritarian governments the sort of unlimited global surveillance powers that would make Orwell turn in his grave:

1. **They could disintermediate banks:** Ironically, this is the best risk for crypto! Elizabeth Warren would prefer a retail CBDC that eliminates the Federal Reserve Banking system and destroys a bunch of local and regional banks. Fortunately, Fed governors are wise to the risk already and have highlighted the role banks play in local economies and in preventing government overreach.

2. **They wouldn't be easily exportable:** It's unclear how much demand there will be to export CBDCs (which may be easier to seize, monitor, or otherwise manipulate by the issuer) versus public-private stablecoins which will likely prove more fungible and serve the role of a true digital cash and bearer asset.

Former CFTC Chairman and current Digital Dollar Project lead, Chris Giancarlo spoke with me about CBDCs at Mainnet. He insists that my skepticism that privacy safeguards would ever get added to future Fed-issued CBDCs was overdone. Indeed, some of the folks at the Boston Fed are closely aligned with the early MIT bitcoiners who worked on Project Hamilton.

Ripple announced the launch of its CBDC platform earlier this year, and it seems to be in an interesting position to fork the XRP Ledger that's core to its product to assist smaller central banks especially. It's got a hell of a hook to dangle in front of these bankers, too: an in-the-clear XRP token, which has already been used extensively as a carrot in its other institutional on-demand liquidity programs (with correspondent banks and remittance giants) as a low-cost "bridge" currency between multiple currency pairs. I never thought I'd live to see the day where I wrote that, but that's what a $100 million, multi-year court victory over the SEC will net you. You can read our report on the State of XRP Ledger in Q3.

I do take retail CBDCs seriously in one sense: I think they will be about as interesting and effective as the government's foray into healthcare IT. I like the idea that CBDCs will prove to be so painfully bad compared to private sector driven crypto protocols that we should welcome them and let them expose themselves as inferior goods.

Conclusion

If it's a helpful framing, I think of Tether-Circle-Paxos-Maker-JPMorgan on the stablecoin issuer side in the same way I think of Binance-Coinbase-Kraken-Uniswap-Nasdaq on the crypto exchange side. All are strong businesses, but they sit in different positions based

on their approach to regulation and decentralization.

- Binance and Tether are the global cowboys, who play ball with regulators when they must, but otherwise leverage huge balance sheets, white-shoe law firms, and regulatory arbitrage to scale outside of the U.S. regulatory perimeter.

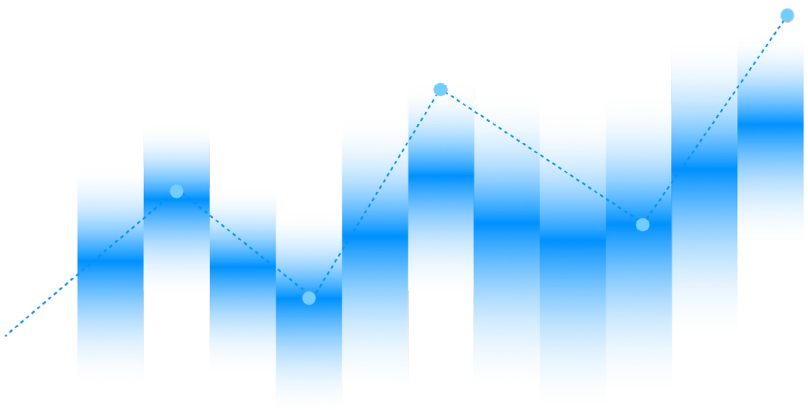
- Coinbase and Circle are the slow-and-steady U.S. incumbents that would benefit greatly from federal legislation but still have true crypto values embedded in their DNA.

- Paxos and Kraken played by all the rules, but they chose to emphasize a state versus federal strategy (ironically, Kraken by avoiding New York, and Paxos, by leaning into it), and ultimately began ramping up internationally after they got screwed over at home.

- Maker and Uniswap have created the category for decentralized stablecoin issuance and decentralized exchange, but they are now confronting the harsh realities of how they'll have to interface with global authorities now that their projects have scaled.

- JPMorgan and Nasdaq are quietly poised, waiting eagerly to pounce whenever the regulated crypto floodgates open — be that 2024 or 2034. They can afford to wait patiently, and their size, reputations, and regulatory status will help them catch up to (some of) the crypto upstarts.

We'll cover the exchanges in depth in Chapter 6 on CeFi. But first, let's make a pit stop and discuss everyone's favorite topic in crypto: policy.



CHAPTER 5

TOP 10 CRYPTO POLICY TRENDS FOR 2024

5.0 Trigger Warning

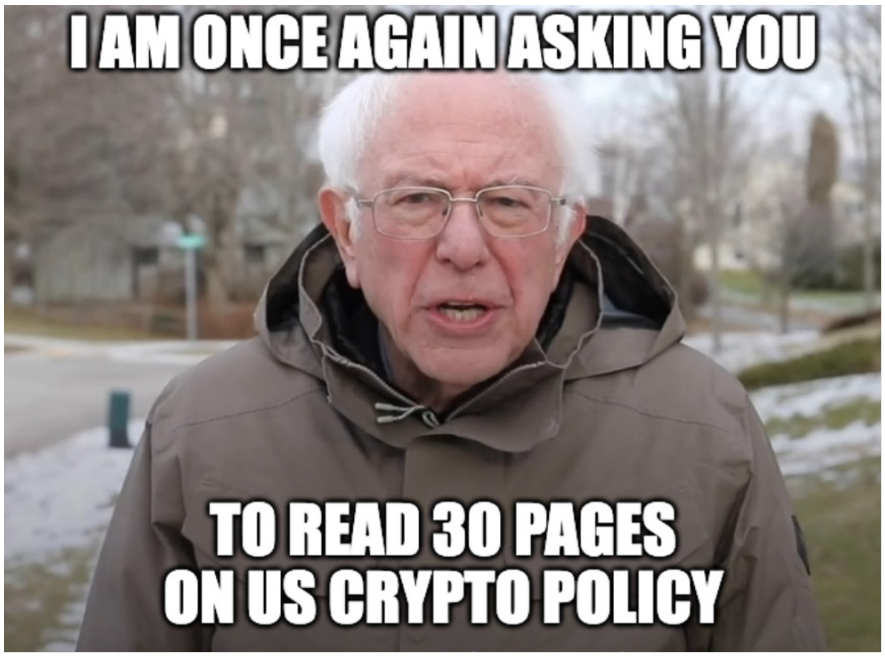
Crypto is political now. (Always has been.) So I'm starting this chapter with a trigger warning:

There are controversial snippets in this section that dive into partisan politics. If you are left-leaning, you may not be happy with my conclusions. My goal is not to stay neutral but to elucidate the state of play in D.C., informed by significant investments of time, energy, and money in The Swamp. There will undoubtedly be places where some of you disagree, but I've had editors of all different political persuasions help with this section to keep the analysis tight, even if it's net unfavorable to one political party.

I wrote this chapter for people who want an unfiltered perspective about what it will take for crypto to win in the U.S. I'm also writing to widen the Overton window of political speech for crypto investors and entrepreneurs heading into a pivotal 2024 election. I continue to believe, as I wrote the past two years, that the U.S. is crypto's most important and winnable battleground, if only enough industry leaders have the will to fight.

If you disagree with me, that's fine. Just know that many crypto policy pros in D.C. agree with my assessments, even if they can't say so publicly for various personal or professional reasons.

(Note: If you are not in the U.S., you may be dismayed that I am not covering your region thoroughly enough, which is why I included some additional third party links at the end of this chapter which do a good job of covering the global crypto policy landscape.)



5.1 Politics is Downstream of Culture

Enacting laws in the U.S. is difficult by design, and bills have a tendency to move only when there is a broad, bipartisan political will to tackle a given problem.

There are two tailwinds you need to pass new laws.

First, the populace in general — or a vitally important group of constituents — must be adamant about the need for action on a given issue. It takes enormous energy to pass *any* legislation, so the issue must be big.

Second, it must be politically safe for the two parties in Congress to work together on a solution, since it is next to impossible otherwise to obtain a super-majority of support in the Senate. We don't see much legislation on issues where there is a high degree of emotional polarization among voters (gun control, immigration, abortion, etc.), precisely because any given position is unlikely to be politically safe for both sides. One way to help reduce the chances of emotional entanglement is to remove the demagoguery, which is why you will hear policy folks in D.C. frequently refer to crypto as either "non-partisan" or "pre-partisan." It's a strategic decision to use neutral and euphemistic language.

At $1.6 trillion in market cap, crypto certainly registers as "material" both as a risk (consumer protection advocates want better oversight in the markets after last year's disasters) and as an opportunity (political leaders see the economic potential of this new technology and don't want that growth and job market offshored due to crippling regulatory uncertainty).

For a period of 2022, there appeared to be some positive momentum and bipartisan consensus that common sense crypto legislation (particularly the DCCPA or "Stabenow-Boozman") would be a net positive for the U.S. Unfortunately, that sentiment turned on a dime after one of the DCCPA's leading proponents and D.C. political donors, Sam Bankman-Fried, self-combusted. He took down much of the industry and millions of investors with him in an egregious fraud.

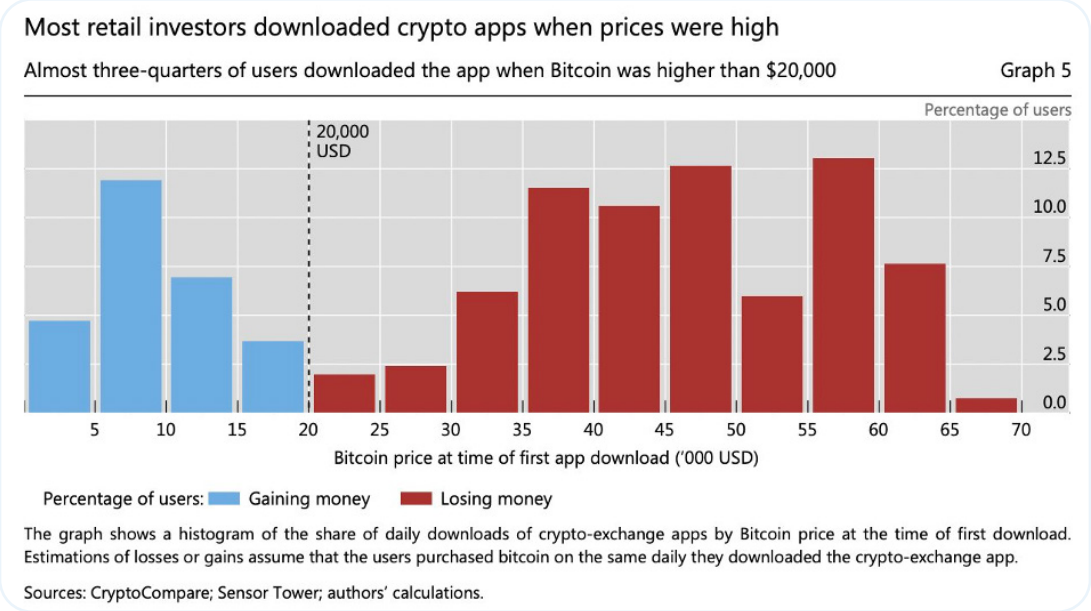
In the aftermath of such a huge scandal, we face four primary *cultural* challenges:

1. **Bear Market Blues:** Although we have technically been in a bull market all year, we're still in a rotten place with respect to public sentiment, especially in D.C. The GOP position on crypto has remained largely unchanged (focused on free, fair, safe markets and U.S. leadership), but Democrats have become hard liners on consumer protection issues after multiple frauds hurt millions of crypto investors in 2022.

2. **National Security:** We're on the wrong side of the civil liberties / national security divide. Our leaders have grown accustomed to the "third-party doctrine" that allows for dragnet surveillance of all financial activity through the banking system, and they continue to lean heavily on our global sanctions regime and reserve currency status as a foreign policy cudgel. It's one thing for crypto to get beaten up over things like tax compliance, consumer protection, or even financial stability. But we do NOT want to be on the wrong side of the national security apparatus. Senator Warren inflicted real political damage by scapegoating us after the October 7

Hamas attacks in Israel. It was a brazen smear that deflected from her party's foreign policy failures. But it left a mark.

3. **Our Size is Not Size:** Contrary to some industry battle cries, we don't have a very large or particularly healthy army right now. More like the Continental Army at Valley Forge. A majority of crypto users may still be underwater on their investments or stuck awaiting the resolution of bankruptcy processes in which they are claimants. Others have simply moved on to emerging fields like AI. We often tout the number of U.S. crypto investors, but many of them aren't necessarily happy to be here. It's a stretch to hope that crypto *ownership* will lead to single-issue *advocacy*. (*Note: I wrote this section before the Blockchain Association presented polling that fully confirmed this at their annual policy summit.) This BIS data is a year old, but it's probably still directionally accurate, and a majority of U.S. crypto holders are still underwater when bitcoin trades below $40,000.*



(Source: : BIS via Paddi Hansen)

4. **Pitching the Gerontocracy and the NoCoiners:** There are sizable gaps in the technical understanding of our leaders regarding crypto. Often that is due to age (the average House Democrat crypto ally is nearly 15 years younger than their antagonist colleagues), but the gap is just as frequently about perverse incentives.

   Congress can use emerging AI tools like ChatGPT, but they often can't or won't own crypto due to potential conflicts of interest. Fewer than 2% of Congressmen own crypto, a rate that's an order of magnitude lower compared to the general population. Many Congressional offices and financial regulators even force their staff to liquidate crypto if they cover the industry professionally (though they have no issue owning equities they influence through legislative action…). That explains a lot! How can you appreciate crypto's potential if you've never had an aha moment with a crypto app? The U.S. adversely selects financial regulators with a pre-existing bias against the industry.

But it's not *all* headwinds. We have three big things going for us:

1. **Distrust in the Bureaucracy:** At least one party (the GOP) believes that many of our D.C. institutions have been weaponized for political purposes. They are sympathetic to the crypto community's arguments to this effect, and there is bipartisan disgust at the SEC leadership, in particular. Chair Gensler's habit of ignoring Congressional oversight requests and brazenly overreaching on his statutory authority has rankled some pretty powerful people. GOP representatives have questioned whether Gensler had his eye on the right ball, given he met with Sam Bankman-Fried in 2022 and missed the FTX fraud, while ignoring Coinbase CEO Brian Armstrong's repeated entreaties to meet constructively. Gensler has admonished the industry while industry leaders, the financial press, Congress, and even fellow Commissioners have called bullshit on his "invitations."

2. **The Constitution (and the Courts):** There's a civil liberties component to crypto that resonates well with some of the GOP members of Congress. Leaders like Majority Whip Tom Emmer are inclined to support crypto as an open, private alternative to dystopian central-bank digital currencies. And recent court rulings that have repeatedly deemed federal financial regulators (again, the SEC, in particular) as "arbitrary and capricious" are creating cracks in the administrative state's armor. There are major battles ahead that involve self-custody, peer-to-peer transaction privacy, and due process for crypto users that circumvent the financial system, and which we can use to undermine the third-party doctrine.

3. **The Return of the Bull:** It is more difficult politically to crack down on crypto when individual investors and institutions (especially TradFi) are all making money. The economic potential for crypto is still massive, and a booming U.S. crypto market will lead to jobs, economic growth, and digital dollar proliferation. Stablecoins can keep the dollar strong and stable: their supply is auditable in real-time, movements are fully transparent onchain, and redemptions require KYC at exchanges that integrate with the regulated financial system. Stablecoin issuers are also massive buyers of Treasuries at a time when we need more buyers. Given today's market tailwinds, time is our friend.

If we can get crypto legislation passed when we have market momentum, staunch bipartisan support (most of the GOP and a growing cohort of younger Democrats), and the conservative courts on our side, we may yet have a vibrant U.S. crypto ecosystem.

Don't get your hopes up yet, though. The political chessboard is messy.

5.2 How a Crypto Bill Becomes a Law

There are multiple paths to victory, but we'll probably need to wait until 2025 or 2026 to get there. To understand why, let's go back to the basics of how bills become laws.

1. **Remember Schoolhouse Rock:** The two chambers of Congress, the House of Representatives and the Senate, need to agree on and mutually pass a bill before it heads to the President. The President can then sign the bill into law or veto it. If a bill is vetoed, it can still be enacted into law with a Congressional override via a 2/3 majority of both chambers of Congress. Bills that make it through both chambers of Congress usually get signed into law, particularly when at least one chamber is controlled by the same party as the President.

   (Fun fact: there have only been two veto overrides in the past 15 years. Trump's veto of the 2021 NDAA, in which he clamored to remove Section 230 protections for tech companies on national security grounds; and Obama's 2016 veto of JASTA, in which the House and Senate unanimously passed a law to end immunity for sovereign sponsors of terrorism — in that case, Saudi Arabia's liability for its role in the 9/11 terrorist attacks.)

2. **Introduction:** There's a lot that happens in the halls of Congress before a bill ever gets a vote. A bill can be introduced in either the House or the Senate by any member of Congress, whether they are in the majority or minority party. For the most part, the only bills that are taken seriously are those introduced with a bipartisan group of "sponsors" or (less frequently) a unanimous vote by members of the chamber's majority party. Most other bills are simply "messaging bills" introduced to score political points and raise awareness on issues, but with little real chance of advancing into law.

3. **Committee Jurisdiction:** Once introduced, a bill is referred to the committee(s) related to its subject matter in the chamber where it was introduced. In crypto, the most important committees in the Senate are Banking (Elizabeth Warren's turf) and Agriculture (home of the "Stabenow-Boozman" bill FTX championed); while in the House, the relevant committees are Financial Services (Chair Patrick McHenry, House Majority Whip Tom Emmer, Ranking Member Maxine Waters, American Hero Ritchie Torres), and Agriculture (GT Thompson is Chair).

   Senate Banking and House Financial Services have oversight over most of the financial regulators and are the ones who do hearings with Treasury (Chair Janet Yellen), the Fed (Chair Jerome Powell), the FDIC ("Operation Chokepoint" architect Chair Marty Gruenberg), and the SEC (Chair Gary Gensler). Agriculture committees in both chambers oversee the CFTC (Commodities and Futures), which regulates the crypto futures markets and could oversee large chunks of the spot markets as well.

4. **Committee Reviews:** The relevant committees are responsible for reviewing and amending bills before they are brought to a full vote. Committee Chairs are selected by the chamber's majority party. They wield considerable power as they decide which bills get moved to a committee vote. Most bills die in a committee

without ever reaching the floor for a vote. Part of the review process will typically include hearings to gather information, debate the bill's merits, and listen to expert testimony. But often, hearings are acts of partisan political theater. Amendments can be proposed and voted on during the committee review stage, and there is usually a great deal of deference to committee Chairs and Ranking Members (senior-most committee members in the minority party).

5. **Committee Markup:** Members of a committee can propose changes to draft bills, which may go through multiple revisions before a final version is approved by a majority vote in the committee. In Q3 2023, several crypto bills passed out of House Financial Services: The FIT 21 Act ("market structure" regulation covering exchanges like Coinbase), the Clarity for Payment Stablecoins Act (determines state versus federal oversight rules for issuers like Circle), the Keep Your Coins Act (affirms protections around self-custody and personal wallets), the CBDC Anti-Surveillance State Act (Whip Emmer's block on the creation of a federal CBDC), the Blockchain Regulatory Certainty Act (exempts blockchain developers and service providers, who don't handle customer funds, from specific registration and reporting obligations), and the Financial Technology Protection Act (proposes creating a Treasury Department working group to study and report on terrorists' use of emerging financial technologies and report on its findings)

   On the Senate side, everything productive (the comprehensive Lummis-Gillibrand bill) is currently stalled by Senator Warren and Senate Banking Chair Sherrod Brown. On the other hand, there are some dangerous bills getting traction, including Warren's DeFi surveillance bill (DAAML) and Senator Mark Warner and Mitt Romney's similar, but bipartisan "CANSEE" bill. Both are messy, arbitrary, and unconstitutional proposals that would amount to de facto bans on peer-to-peer crypto in the U.S. Those aren't my words, they're the far more sober Coin Center's.

6. **Floor Debate and Vote:** If a bill passes the relevant committee, it is scheduled for debate and a vote on the floor of the chamber where it was introduced. Members of that chamber can propose further amendments during this debate. A simple majority vote is required for the bill to pass in the House, but 61 votes are required for most legislation in the Senate. We could see some "clean" House floor votes on crypto bills in the next few months, though it's unlikely.

7. **Conference Committee:** If both the House and the Senate pass different versions of the same bill, a conference committee is formed to reconcile the differences between the two versions and agree on a final bill. This is where we'll end up if we get any progress on any of the major bills under consideration today. There is often horse trading between leadership in different chambers and committees, and there's at least one possible (likely) trade to be made on stablecoin legislation given Senate Banking's advancement of the SAFER Banking Act.

8. **Omnibus Hell:** The first seven steps of this process are commonly referred to as "regular order." In other words, it's how laws are supposed to be passed. But it's also possible (and somewhat easier) to pass narrow legislation through amendments to large "omnibus" packages as well. If crypto legislation gets pulled into an omnibus bill, only bad things can happen, thanks to the hostilities in the Senate. The

industry's recent scapegoating over the October 7 Hamas attacks is a perfect case in point: bad headlines up the risk that a terrible, reactive, crypto-killing surveillance bill gets rammed into "must-pass" legislation like the annual National Defense Authorization Act. Such a scenario would map closely to how we previously lost a major battle in the 2021 Infrastructure Bill, a loss we'll be feeling for years.

9. **Passage & Presidential Signature:** Even if a "clean" bipartisan crypto bill passed both chambers, it is still possible we could see it vetoed, given how hostile the Biden administration (and its Warren acolytes) has been towards the industry. That said, anything that gets out of the Senate under Banking Chair Sherrod Brown, is likely to be signed into law. Likewise, there is no chance the President would veto an omnibus package brought to his desk by the Democratic Senate majority. So the highest potential pieces of crypto legislation are bad amendments appended to "must-pass" packages. This is why vigilance is so critical over the next 13 months.

10. **Implementation:** This is really just the *beginning* of the process. We haven't even touched on the implementation of new laws! That's where crypto lawyers and policy pros make their real money: contributing to the rulemaking process, ensuring that financial administrators don't overreach on their Congressional authority, and offering legal support when necessary.

Until this year, crypto had basically only experienced step 10 (new rulemaking and legal challenges) and steps 8-9 (with the disastrous "crypto broker reporting" requirements that were inserted in the 2021 Infrastructure Bill). Will we finally get something through the Congressional sausage-making process (steps 1-7) in 2024?

Slim chance. But not zero.

[Required Reading: Market Structure Bill Comparisons, Stablecoin Bill Comparisons]

5.3 Congressional Sausage Making

If you made it through the quick civics lesson in the first two sections of this chapter, you have a sense for how difficult it will be to pass any crypto legislation. But I know (hope?) you're reading this report fireside with some spiked nog, so I'll skip the *really in-the-weeds* policy scenario planning and cut to the chase: the probabilities and most likely paths to crypto laws in 2024.

Major Legislation:

1. **"FIT 21" (House) and "Lummis-Gillibrand" (Senate), also called Market Structure**

   <5% chance of passing

   Both bills provide clarity over regulation of the crypto spot markets, custodial exchanges, and asset issuers, and would settle jurisdictional issues between the CFTC and SEC. They would prohibit the commingling of customer funds

and certain conflicts of interests, address cybersecurity risks, authorize new self-regulatory organizations, and likely usher in something that resembles SEC Commissioner Hester Peirce's Safe Harbor.

But Senate Democrats want too much deference to the SEC under any market structure legislation. They're demanding expansive language that would capture all of DeFi and their "responsible parties" (including developers) under rules traditionally meant for entities that hold and exchange customer assets directly. Democrats won't move legislation that carves out DeFi, and GOP leaders aren't keen to reward Gary Gensler for his bad behavior. They're at an impasse.

It's too bad, too, as there are some great improvements to the status quo in these bills. You can read our analysis or Justin Slaughter's full take on X.

2. **"Clarity for Payment Stablecoins" (House) and "Lummis-Gillibrand" (Senate)**

   25% chance of passing

   The path to stablecoin legislation is more clear, though still unlikely. Both chambers' bills include language that would require USD-stablecoin issuers to back "payment stablecoins" with highly liquid reserves on a 1:1 basis and comply with disclosure, redemption, and capital requirements. Both bills provide a path for banks and non-banks (e.g., credit unions, fintechs) to issue stablecoins, subject to federal approval and oversight, and also provide a path for issuers approved by state regulators (e.g., the New York Department of Financial Services). The degree of deference to the Federal Reserve remains the major point of contention. (Our full analysis is here.)

   Democrats fear that a state-run oversight process would create a race to the bottom in regulatory standards and lead stablecoin issuers to venue shop for the states with the mildest oversight requirements. They want stricter regulations for entities providing custodial services, language promoting financial inclusion, and authorization for a CBDC study, which would likely be a non-starter for the GOP.

   But if there's a horse trade to be made, it's on stablecoins. That's because Senate Banking recently advanced a separate bill focused on cannabis banking reform, the SAFER Act. SAFER is likely dead on arrival in the House without concessions on stablecoin legislation in the Senate, and a barter could help crypto win twice. Stablecoin clarity would (obviously) help Paxos, Circle, and U.S. banks win market share back from offshore "eurodollar" competitors like Tether. But the SAFER Act could *also* help end the FDIC's "Chokepoint 2.0" attack on crypto (more below): the latter would prohibit banks from terminating customer accounts without "valid reasons" beyond "reputational risk."

3. **DAAML and CANSEE (similar Senate bills)**

   *40% chance that a *watered down* version gets passed*

   Both DAAML and CANSEE would effectively end DeFi in the U.S. by imposing

unworkable anti-money laundering and sanctions law requirements to open-source software contributors and non-custodial peer-to-peer networks. They would grant broad powers to the Treasury Secretary to determine who "controls" a protocol or who earns exemptions from AML requirements. They would criminalize activity related to publishing certain types of code, or even potentially coerce speech by forcing developers with no custodial relationship with their users to write code required by financial regulators.

My friends in D.C. tell me I'm too pessimistic on these, but I think the odds are far too high for odds of negative surveillance-oriented legislation to get crammed into a "must-pass" bill like the National Defense Authorization Act. It doesn't seem like a binary outcome (will this happen), so much as a matter of degree (can we effectively whittle down the negative language proposed in DAAML and CANSEE, so they are workable, and minimally damaging). The odds of compromised legislation go up if Chairman Patrick McHenry (who has been excellent for crypto) is willing to make concessions to his colleagues on his way out: he announced his retirement last week.

In the aftermath of reports that crypto has helped fund Hamas, Iran, and North Korea, the bills have enough bipartisan momentum that I don't think we can be certain that even our staunchest defenders will hold the line for crypto if they are appended to broader bills. We're an easy horse to trade if we don't muster the financial clout to fight. The reality is that a good chunk of Congress may prefer to choke off illicit crypto even if it means killing innovation. We've got to hold the line on these bills and prepare for court battles otherwise, as DeFi is simply incompatible with certain elements of our global surveillance apparatus.

4. **FLASHBACK: Crypto Broker Tax Reporting**

Passed in 2021, initial rulemaking proposed in August 2023

Back in 2021, the Congressional Budget Office claimed that billions of dollars in incremental tax receipts could be generated if only crypto brokers submitted tax reports to the IRS like their TradFi counterparts. This "pay-for" was stuffed into the bipartisan Infrastructure Bill via a shoddily drafted "broker rule" that became an unexpected lightning rod for Congressional leaders who had previously not thought much about the crypto industry.

Anyone who has ever reported tax liabilities by manually parsing thousands of crypto exchange trades, knows that this rule would have been somewhat welcome if it merely focused on exchanges like Coinbase and Kraken. Tracking cost basis and gains and losses, and streamlining tax reporting is a nightmare most of us would gladly outsource to the venues within which we trade.

But Congressional leaders — largely at the insistence of the White House — were adamant that DeFi also needed to be captured in the broker rule language, lest the administration lose track of the emerging peer-to-peer marketplaces that sit alongside their centralized competitors. Many of us argued that Congress' final legislative text was intentionally broad, designed to capture decentralized

exchanges as “brokers” responsible for submitting tax reports to both the IRS and their users. This August, the Treasury finally confirmed our fears.

The “Proposed Rule” ostensibly requires DeFi application builders to maintain centralized control of sensitive user information for tax reporting purposes, even if they do not collect such information today. It undermines privacy and imposes significant burdens on small businesses and developers (for limited financial upside). Also, the letter of the law may even inadvertently *require* decentralized applications to *add centralized custody* in order to comply with tax withholding requirements.

Patently absurd.

We know that the Treasury’s expansive interpretation is inconsistent with Congress’s intent, as there have already been proposed legislative fixes that clarify and tighten the faulty language (e.g., the bipartisan Keep Innovation in America Act), not to mention a bipartisan colloquy at the time the Infrastructure Bill was passed.

But it doesn’t matter. Let this be a warning to all: any law that can be abused, will be.

5. **Minor Legislation:** A few smaller legislative fixes could be on the table next year, though they seem too small on a standalone basis to make it through Congress as part of regular order, especially in an election year.

   The most sensible and promising pieces of “quick fix” legislation are the bipartisan PROOF Act, which would require digital asset custodians to obtain attestation from independent auditing firms that their customer deposits are fully backed at all times, and the bipartisan Uniform Treatment of Custodial Assets Act, which would reverse the SEC’s Staff Accounting Bulletin 121 (“SAB 121”) guidance that directed banks and other public companies to treat cryptoassets held on behalf of customers as balance sheet liabilities. Doing so would make it impossibly expensive for banks to enter the crypto custody business, due to the punitive, SEC-mandated capital reserve requirements.If you’re petrified right now, this isn’t all as bad as it sounds.

I don’t mean to sound sanguine, but we are less than a year away from a fairly consequential election, and retrenching and living to fight another day isn’t a bad strategy. No law is better than bad law, and expensive court battles are preferable to negotiated surrenders that cripple the long-term viability of crypto in the U.S.

It may be difficult to pass new laws in 2024, but it is next to impossible to repeal bad old ones. Faced with bad options, we parry with the regulatory state, leverage the courts, and win at the ballot box next November in order to give ourselves some breathing room.

Ideally, we pass crypto legislation during “Secret Congress” and not at a time when we are a political punching bag thanks to our cascading credit failures and fraud cases.

5.4 The Relentless Hostility of the Money Regulators

There are three major points of leverage the federal government has over crypto market participants: (1) they control access to banking services, (2) they make the tax reporting rules, and (3) they enforce anti-money laundering (AML) laws.

We've seen the power of all three leverage points so far this year, and we have no reason to believe that 2024 will be any less harsh.

Crypto Banking

> *"Awful nice bank you've got here, be a shame if something happened to it."*
> -FDIC Chair Marty Gruenberg (probably)

The government lied about the failures of SVB and Signature Bank earlier this year. I mean that literally. They were caught on tape lying about bank solvency just months before the collapse.

The issues were caused primarily by the whiplash effects of the Fed's unpredictable interest rate policies, where regional banks like SVB faced colossal "unrealized" losses on long-term bond portfolios (purchased when Fed rates sat at record lows), only to be forced later to rapidly realize those losses once depositors got wise to the balance sheet gaps. The Fed lied, and banks died, as Balaji explained in epic detail.

But it was the regulators' simultaneous pursuit of Chokepoint 2.0 towards crypto companies that provided an accidental spark (and eventual scapegoat) for the worst banking crisis (by deposits) since 2008.

I'll again point to Nic Carter's full report on Chokepoint 2.0 (though it's important to note that this operation was also well documented by white-shoe law firms later on), where he accounted for the government's multi-step, multi-month, multi-agency effort to de-bank major crypto platforms from Silvergate, SVB, Signature Bank, and First Republic Bank.

Basically, sitting Senators worked in cahoots with short sellers to threaten existing banks with investigations, forced them to kill or significantly pare back otherwise healthy crypto customers (including highly liquid stablecoin issuers, who are *excellent* bank clients), and discouraged them (via officials at the Fed, FDIC, and OCC) from taking crypto deposits on "safety and soundness" concerns. They blocked the new entrants outright from Fed Master Accounts and National Trust Bank Charters, citing the risks that the government itself created.

It sounds like a conspiracy theory, but the operation was merely a redux of an explicitly named program Operation Chokepoint (not 2.0) that FDIC Chair Martin Gruenberg had led under the Obama administration. Back then, the administration extralegally targeted firearms dealers, payday lenders, and other legal, but politically disfavored, industries.

This year, they targeted crypto firms. The operation has had its desired effect. We've heard directly from big banks that they have been instructed from the highest levels of their institutions to avoid crypto companies, even businesses like Messari, whose

business models are as benign as it gets. (We're not handling customer funds, processing payments, or flipping tokens.)

It's not like banking had been *easy* to come by over the years (as outlined last chapter, Tether's rise highlights the industry's long-time solution to that intractable problem), but it was never this bad.

Even Dodd-Frank co-author Barney Frank said the quiet part out loud: the destruction of Silvergate's SEN and Signature's Signet (crypto exchange settlement services) was the goal. Pressure had been mounting for years, but the FTX bankruptcy finally gave regulators a perfect crisis they couldn't let go to waste.

We can't say that any of this behavior is surprising!

Gruenberg's confirmation for a second stint at the FDIC was considered laughable in circles familiar with the original Operation Chokepoint. It's not like these folks were winning ethics awards before the 2023 banking crisis. Gruenberg has a history of poor management and lax oversight of the out-of-control frat that is the FDIC.

Some Congressmen are asking questions, but it is too little, too late.

Crypto Tax

We covered the broker issue in the section above, but there are multiple ways that the federal government is turning the tax screws on U.S. crypto companies and their users:

1. If you use DeFi, services may soon have to collect identifying information and tax reports on your use of their "front-end" interface, even if they never take custody of your assets..

2. If you never touch on/off ramps or even stablecoins but simply conduct ETH to other token DEX transactions from a self-hosted wallets, you're on the hook for self reporting all of those gains and losses, with no de minimis exemptions. The IRS hates you.

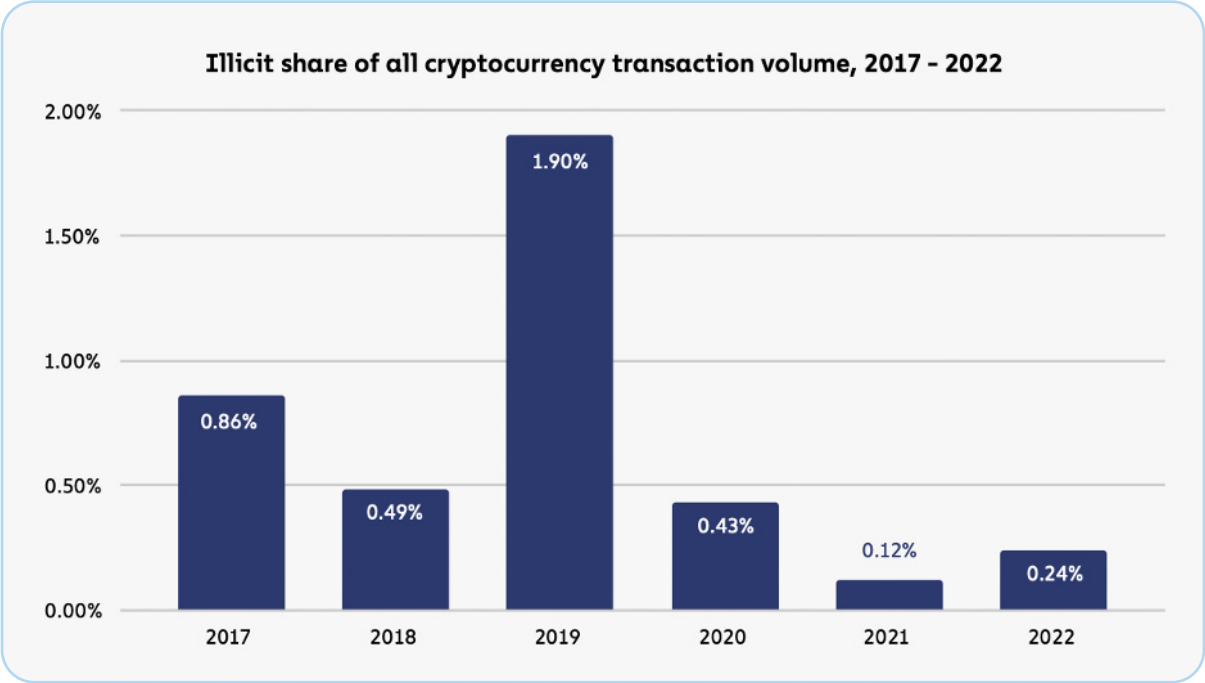
3. If you fail to accurately report liabilities or simply dispute cost bases that your service provider submits to the IRS (this happens All. The. Time.), you better watch out because the government is getting more aggressive with tax enforcement and asset seizures.

I'm not sure if you've noticed, but the U.S. government is absolutely *starving* for cash, too. They went after Microsoft, the world's largest company, for $29 billion in decades-old back taxes, enough to pay for... less than a week...of our government's current deficit spending. They're coming for your crypto, and you should think about all available options to protect it.

Crypto AML/KYC Compliance

They got Al Capone on tax evasion, and they got CZ for breaking anti-money laundering laws.

Calling a national press conference to announce a $4 billion fine is one way to show that you are doing your job, I guess, but I'm unconvinced we're getting the big things right. Crypto crime accounts for basis points of global GDP and a barely higher percentage of crypto volumes:



(Source: Chainalysis)

About 1.3% of U.S. GDP in general is laundered through traditional financial rails, and a much higher percentage is laundered using cash (of a much larger denominator). Crypto crime is a red herring that allows financial authorities to believe they are doing a good job.

Don't get me wrong, we *should* put fentanyl dealers in jail (my preferred solutions would be more medieval), and we should root out terrorism and limit nuclear proliferation. Obviously.

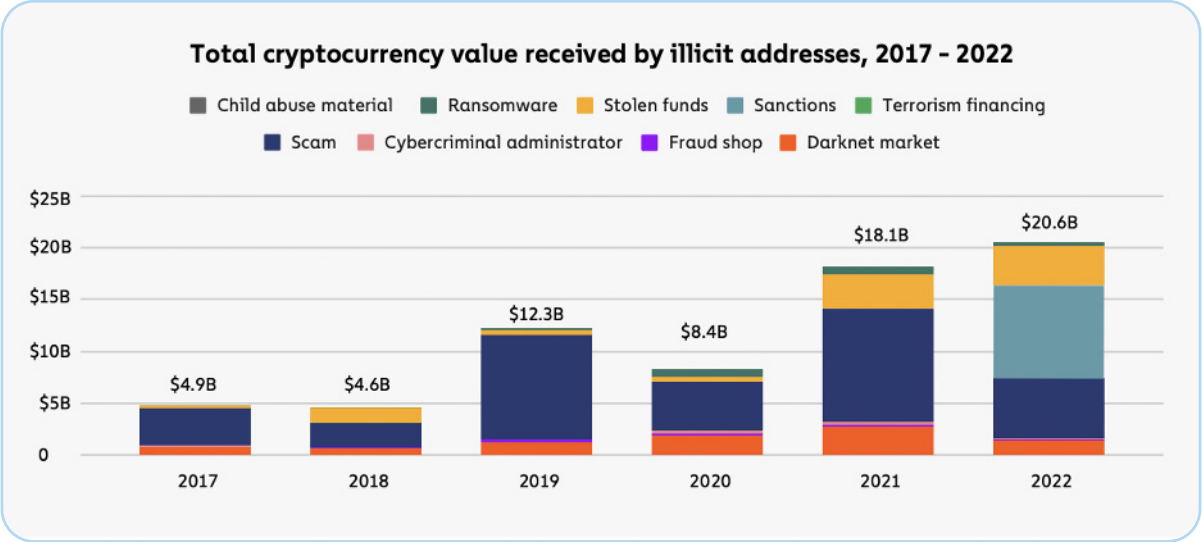
But crypto is actually significantly *better* at minimizing illicit transactions compared to the legacy banking system because blockchains provide a permanent digital record of transactions that allow for a full and permanent inspection by law enforcement personnel. That permanence ensures that crypto exchanges go above and beyond in monitoring for suspicious activities on their platforms because they know that any errors they make will be easy to trace in perpetuity.

But what is the reward for our superior compliance?

We give them the open financial records that make us easier to hit. They use this transparency against us to cripple tech that can help broaden access to financial services globally, even when the supranational FATF itself recognizes their human rights blind spots. Not great!

If we hadn't sanctioned the sixth largest economy in the world in 2022, "crypto crime"

would have dropped 40%, instead of “increasing” — statistics without context are meaningless.

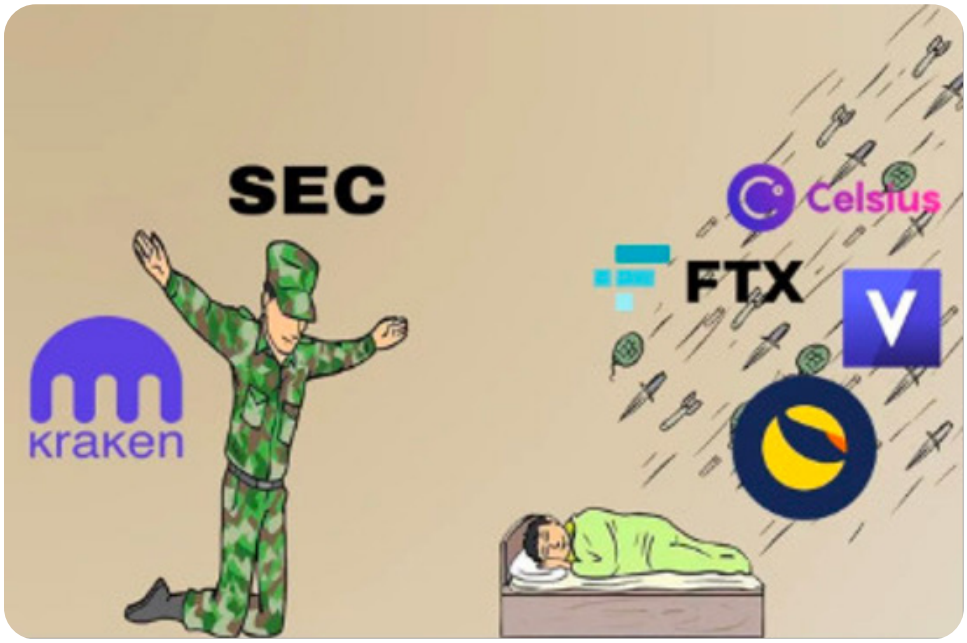


(Source: Chainalysis)

A global, open-source tech like crypto is not responsible for the geopolitical games of the state. I’m glad that we have some groups calling this out and fighting against their overreach.

5.5 The Relentless Hostility of the Protectooors

I don’t know about you, but I have never felt more protected in my entire adult life than I do by the SEC under Chair Gary Gensler.



I know Gensler will likely enjoy this section. (*"Yes, yes, and they can do nothing about my cunning opposition. Excellent, Smithers."*) But it's worth highlighting exactly how terrible this man is, and has been, for the long-term competitiveness of the U.S. capital markets.

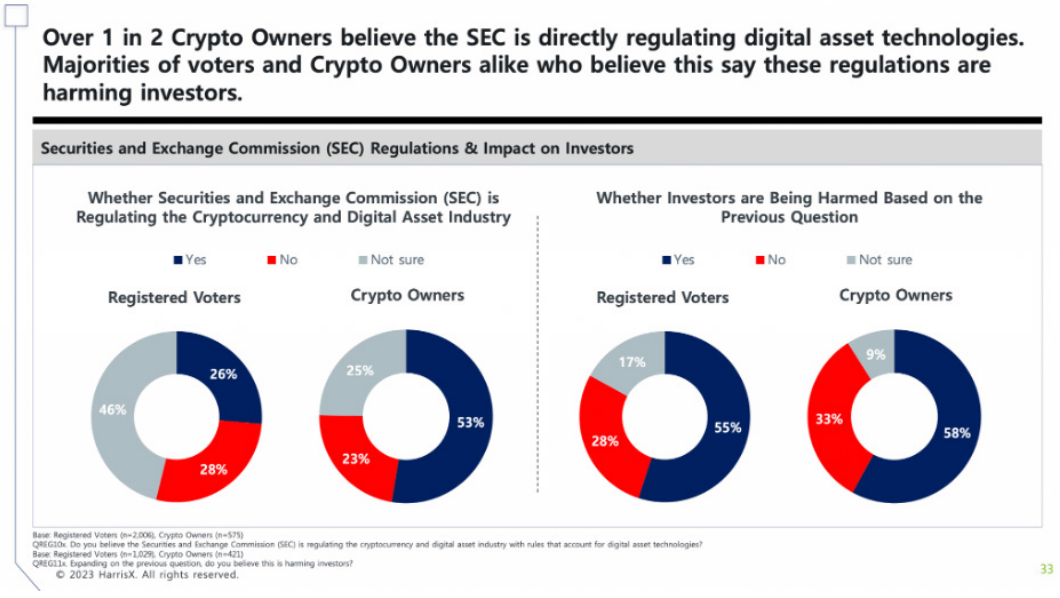
The SEC is rotting from the head, as dead fish do, and may be sanctioned for corruption soon, if you would only believe the conspiracy theorists in the <checks notes> federal courts. Here's what you need to know about Chair Gary Gensler:

1. **He's Undermined the SEC's Mission:** I always feel compelled to remind people — including those at the SEC — that the agency's mission is to promote capital formation, protect investors, and ensure that the U.S. capital markets are fair, efficient, and competitive. Messari shares that mission, but Gary Gensler never has.

   Gensler's patented line "the rules are clear" has become a meme, yet he has had no explanation for his inconsistency on ETH, an asset for which the SEC approved a futures ETF this fall, while refusing to acknowledge that the asset itself was not a security. The courts provided conflicting guidance this year on how tokens fit under the Howey test, mostly slapping down the SEC's long-held assertion that these tokens are de facto securities. Gensler has even threatened to go after airdrops that decentralize crypto protocols because of their embedded "incentive structures" for contributors.

   While this is frustrating, it's not rocket science. Streamlined registration or a Safe Harbor would be possible if only the SEC were committed to solutions rather than enforcement. Tell us, Gary, how do onchain disintermediated assets and their peer-to-peer networks function under the SEC's view of the markets? (They don't.)

   The good news is that voters understand that the SEC is hurting investors:



(Source: HarrisX)

2. **He's an Incompetent Cop on the Beat:** Again, not my words! His oversight committee's words. But they're well earned. Gensler has whiffed on every

substantive crypto issue that's come across the SEC's desk and has pursued high-profile, low-impact cases instead. With FTX, Gensler met Sam Bankman-Fried, missed his fraud, and then sued the carcass of the company. With Grayscale, he blocked its ETF conversion application but allowed the toxic GBTC product (an SEC reporting company with selling restrictions!) to take down the entire crypto market as bad collateral. It took a federal judge (Democratically appointed) to overrule his blockade as "arbitrary and capricious."

And don't get me started on the SEC complaints against bankrupt or defunct entities (Genesis and Gemini, Bittrex, BlockFi). In the world of financial firefighting, Gensler only shows up to pick through the rubble after the camera crews have already arrived. He's never saved a soul or even pretended to try to put out raging infernos.

Millions of investors have been hurt by this SEC and its Chair, and I'm tired of pretending it's an institution that still deserves respect. I hope my friends have the time and resources to take their cases to the Supreme Court and blow the SEC back to 1933.

3. **He's Self-Aggrandizing:** Pretty much from Day 1 at the SEC, Gensler has been focused on one thing and one thing only: continuing to climb the political ranks in D.C. From the heroic, planted profile pieces in the mainstream media (with glamor shots), to the gimmicky Office Hours with Gary Gensler productions, to the focus on celebrity enforcement actions that keep his name in the news, to his pivot to AI (along with every other tech influencer), to his counter-programming of Congressional hearings and other high-profile events, Gary is always looking out for number one.

4. **He's a Bad Faith Operative:** Gensler has lied about the "registration process" for crypto companies. Meanwhile, a single random "digital asset securities exchange" called Prometheus was approved by the SEC — just in time for its founder to proffer pro-Gensler, pro-Warren talking points in testimony before Congress. Prometheus' background is... interesting.

   "Come in and register" has, I think, set a record for level of snakey duplicity out of a government regulator. He doesn't actually care whether he has the Congressional authority to regulate crypto, as he knows that by the time this is adjudicated in the courts, he will be long gone. No one pointed out the inanity of current SEC overreach quite like his fellow Democrat, Ritchie Torres. "If I purchase a pokemon card is that a security transaction?"

There are reams of ethical questions Congress has about Gensler beyond crypto, but I'll let the elected partisans pick those fights, and stay in my crypto lane in the interest of time. If you want to know what else Gensler is wrong about more generally, I give my proxy to Hester Peirce and her vast library of dissents.

There is another major financial regulator we should talk about, too: the CFTC. I've appreciated the CFTC's current leadership, but hardly think shifting crypto oversight there would be a panacea either. The CFTC has blocked innovation in prediction markets

within the U.S. in the past. Their Ooki DAO enforcement action has wreaked havoc on innovation within the U.S. DAO ecosystem. We still don't have onshore perps, and it seems unlikely we will any time in the near future, as the CME still dominates our futures markets and DeFi projects are being chased offshore or shut down via enforcement.

If anything, Gensler (the former CFTC Chair!) is the poster child for why we should not blindly trust *any* government regulator to operate fairly or reasonably if given overly expansive (or ambiguous) statutory authority to exercise oversight on a given market. That's particularly true when we consider how broadly U.S. agencies' influence can extend beyond the U.S. Indeed, a recent IOSCO report has Gensler's fingerprints all over it.

We're fighting a global policy war, locally. We really need to get these important details right.

*(**Aside:** It's a little ironic, isn't it? Every regulator that bothers to learn about the tech gets excited about it and ends up defecting to help advance the industry in the private sector.*

Senator Warren and Rep. Alexandria Ocasio-Cortez (AOC) led an effort earlier this year to make it harder for crypto firms to hire former government officials to guide their lobbying efforts, after finding hundreds of government officials had moved on from public service with Treasury, the SEC, the CFTC, other financial regulators, and Congressional offices, to crypto firms. Maybe we shouldn't force the people who know anything about crypto to leave the room.)

5.6 The Courts Are Our Friends...Sometimes

The regulatory situation is so stacked against us that it's tempting to fight every one of our battles in court.

The trouble is that this strategy is expensive and high-stakes. Few teams can afford to wage such lengthy, expensive battles.

Ripple claims to have spent more than $100 million on just the first round of their case with the SEC, which, after 2.5 years, was resolved (mostly) in its favor, but still faces an SEC appeal. Grayscale successfully sued the SEC for refusing to approve its spot ETF conversion application, but not before the SEC's delays crippled dozens of Grayscale counterparties, including its sister company Genesis and parent company Digital Currency Group (more on that next chapter). And Grayscale's procedural victory still hasn't led to an actual ETF conversion, even though the SEC missed another deadline! Coinbase sits in limbo: the damage that its SEC Wells Notice has done is unknowable, but it certainly hasn't been helpful historically to delay new listings and products while global competitors eat into your market share.

And those are our early *winners*!

For every Ripple, there is a LBRY, an actually useful project, with an actually useful token, which lost in court and was forced to unwind after years of litigation. (Read Hester

Peirce's scathing dissent, even if it won't bring an American innovator back to life.) For every Grayscale that's paving the way forward for institutional adoption, there is a Kraken getting slapped down and permanently suspended from offering competitive staking services to its U.S. customers.

The problem is that it almost never pays to fight the government. At best, it's trench warfare. At worst, we are weighed down by our weakest links when it comes to court precedent.

Take Ooki DAO: a perfect example of "bad facts making bad law." The default judgment around Ooki this spring created a nightmare for decentralized governance participants in the U.S. Plaintiffs, attorneys and regulators alike now have legal air cover to pursue DAO delegates, voters and even passive tokenholders as general partners in unincorporated associations, if they interact with any DAO. In other words, a decentralized-in-name-only financial platform blew up an entire emerging legal construct.

Similarly, I worry that the Tornado Cash case may strengthen the Patriot Act and Bank Secrecy Act rather than neuter them. We are putting enormous pressure on ourselves to win in the highest levels of court against opponents who, in certain instances, have literally unlimited resources (as with the Fed and its battle with Custodia).

They're called "prayers for relief" for a reason. And while we should take advantage of our strongest cases and a Supreme Court that seems willing to brush back regulatory overreach, we don't want to be stuck throwing Hail Mary's forever.

But if Democrats hold the White House and Senate this November, we will be. (Here we go!)

5.7 Swinging the Senate

As I explained in the section on Senator Warren in "People to Watch," most of the pressure on *Representative* Waters to vote against the FIT 21 bill came from the White House via Warren proxies. The Lummis-Gillibrand market structure bill sits in Senate Finance Committee purgatory in the meantime, and it will never see the light of day as long as Warren and her fellow anti-crypto comrade, Chair Sherrod Brown, preside over that committee.

It would be nice if Senator Warren retired. We can all agree on that.

But what we'd like and what we can get are two different things, and as such, all attention should be on displacing Warren's allies and marginalizing her impact on financial policy rather than tilting at windmills to convince the solidly blue Massachusetts to elect another senator.

If you want crypto to survive in the U.S., you'd better get to know some new names.

In the case of the 2024 election, the whole ballgame is about swinging the Senate to GOP

control. Yes, we should also keep our GOP friends in the House supported, and back the rare progressive allies in whichever chamber they emerge. But the party in control of the House in 2024 won't matter if the Democrats hold the Senate, and Sherrod Brown and Elizabeth Warren retain control of Senate Banking.

When it comes to the upper chamber, I find myself reciting names with Arya Stark reverence before I go to bed: Sherrod Brown, Jon Tester, Katie Porter, Ruben Gallego, ~~Joe Manchin.~~

Those are the most vulnerable Senate Democrats we must ensure are sent to the private sector in 2024. With Joe Manchin announcing he would not seek re-election in 2024 for what is otherwise a deep red West Virginia Senate seat, the GOP must pick up just one more seat in order to retake the majority, swinging control on key oversight committees and the final say in White House political appointees. If this happens, the Chairs of Senate Banking and Senate Agriculture swing to the right and Warren gets relegated to the back bench.

Still, her staff connections in a second Biden Administration would remain.

On that point, crypto proponents would do well to support the GOP candidate for President as well. Even if President Biden were to drop out of the race for some reason, there are no good alternatives for us on the Democrat side, as any presumptive nominee would likely need to make the same assurances and commitments to Senator Warren that Biden had to in 2020. Her tentacles would choke any financial administration, but Senate control could at least keep the worst financial appointees in check.

I've heard valid concerns that He-Who-Must-Not-Be-Named was no fan of bitcoin, and it is true that Treasury Secretary Mnuchin attempted to ban self-hosted wallets as a parting shot towards the industry in January 2021. But that is all the more reason to support the most powerful proxies we can in the Republican field, including any financial regulator who hasn't completely burned bridges with the former President (Chris Giancarlo, Hester Peirce, Brian Brooks?), as well as any high-profile potential cabinet members or Vice Presidential candidates (Vivek).

To be explicit, there is zero chance that a Biden redux and Warren Senate will lead to anything other than the end of the U.S. crypto industry through 2028.

If keeping crypto in the U.S. matters to you, there is no alternative. The Democrats, as currently constituted, will kill the industry and dance on our graves.

I am not naive. Though I helped popularize the concept of a "single-issue crypto voter" in 2021, I know that for 99.9% of voters, crypto will not register on a list of top five issues that inspire them at the polls. So instead of "activating a base" that doesn't exist, we're left playing a game we hate: moneyball politics, Super PAC funding, and a focus on high-impact elections.

I will be voting for and financially supporting whoever the GOP nominees are for the Presidential and Senate races. If you'd like to focus more broadly on bipartisan pro-crypto candidates in House and Senate races, I recommend contributing as much as you can to

Fair Shake PAC. We can hold the line a little longer, but we can't afford to lose next year.

5.8 Stand with Crypto: Engagement vs. Kowtowing

There are few words I despise more at this point than "engagement."

It's a made-up word that reeks of mediocrity, bureaucracy, and the reductive, life-wasting empty chatter only possible amongst those incapable of actually building things.

The crypto industry's default (largely libertarian) position is that we should only regulate crypto financial services businesses that handle other people's money (private keys) and otherwise build open-source tech that anyone can use, without encumbrances.

In that world, peer-to-peer software would be protected speech, and crypto ownership would be fully protected property under the U.S. Constitution. Any time spent in D.C. kowtowing to policymakers to assert rights that already exist is not only counterproductive but degrading. Time spent lobbying for new law is time spent negotiating our own surrender, and instead, we should stand and fight on principle.

I'm oversimplifying this, perhaps, but only slightly.

The ethos of the community is largely in line with some combination of Erik Voorhees' Permissionless call to action and Bill Gurley's *All-In Summit* takedown of the regulatory state. You must take 30 minutes to watch both of these talks over the holidays if you haven't already, as they get to the essence of many of the industry's early builders' ethos.

Voorhees, one of the bona fide libertarian OGs of crypto, discussed the "peaceful rebellion" of building permissionless systems that replace the rule of law (ineffective and arbitrarily applied) with the rule of math (consistent and precise). Gurley, a legendary venture capitalist, discussed regulatory capture and explained how incumbent corporate interests influence policy and regulation to provably benefit themselves at the expense of citizens. He ends with a line that evoked a standing ovation: "The reason Silicon Valley has been so successful is because it's so f*cking far away from Washington DC."

There's just one problem: this presents a false choice.

Given the reputational setbacks we have suffered this past year, some degree of political [ring]- kissing is necessary to survive and advance. We can't realistically walk away from all "engagement" in DC when many leaders are ready to legislate *punitively* on our industry. The choice to opt out entirely from these conversations — with an aging, technically challenged gerontocracy at the helm of our nation's institutions — would be suicidal, even if participation in the discussions themselves is stultifying.

We are not only up against the big, incumbent banks in our policy fights, but the incumbent regulatory state itself. And regulators f*cking LOVE intermediaries.

Policymakers believe that banks, exchanges, and other centralized financial services providers help the state with tax compliance, suspicious transaction monitoring, consumer protection, etc. These entities can be held accountable to achieve specific public policy

goals. Of course, the degree to which they are *actually* helpful, or to which such policy directives are cost-effective, does not change the faith that policymakers have in institutions as useful appendages of the state.

Permissionless systems are a threat to the entire regulatory state because they are by definition intermediary-less. Regulators lose information, they lose control, and they arguably lose their need to exist if they can't identify the responsible parties that help maintain these systems.

If I've done my job in the sections above, it should be evident that U.S. regulators view crypto as a threat. The overreaching rules on "broker" tax reporting requirements. The unconstitutional proposals floating around Congress that would extend the "third-party doctrine," compel speech, and deputize software developers to enforce KYC / AML regimes. The DeFi regulation report from IOSCO, an international securities meta-regulator (run by the SEC), that aims to create a new legal definition, "responsible party," for permissionless systems from thin air.

All of these proposals would effectively kill crypto in the U.S. because they would make compliance technically impossible: all sorts of ecosystem participants would face some version of the SEC's "come in and register" duplicity.

Engagement helps combat strawman attacks from bad-faith enemies. *"Yes, tax compliance, national security, market integrity, bank stability, and consumer protection are important public policy goals. I'm not fighting you on that. However, you can't apply old rules to new technologies. True intermediaries like Coinbase and Kraken should be regulated. But we'll also need explicit protections for software developers, DeFi, and self-hosted wallets in any legislation that moves forward on purely Constitutional grounds."*

There are ways to get involved directly: call or meet with your Congressional representatives (check out Stand with Crypto), donate to crypto-friendly incumbents (I had a good list in 2022 that I'm updating), and comment on proposed rules (leverage AI to generate comment letters if you must). Or live life on easy mode, and delegate and financially support the work of organizations like Coin Center, the Blockchain Association, and Fair Shake.

We know the system is rigged against us today, but if we don't show up, we don't even have a seat to defend ourselves. The war will be long, but it's one we can win. And even small victories will add up over time.

5.9 We Need to Set Higher Standards

At some point, we need to look in the mirror and accept that we are all ultimately responsible for the culture within crypto. As I wrote 18 months ago, Salvation Lies Within.

Too often, it's felt like a shitty, get-rich-quick industry with a high-time preference. There are too few people willing to call out bad actors because the incentives to do so are terrible. It is reputationally, economically, and, at times, legally risky. There are

nearly no leaders within the industry who have been willing to work on cross-industry standards setting, lest they align with the "wrong partners," put themselves at a relative disadvantage to competitors, or make the sensible disclosures that could later be held against them in court.

Still, I think it's important we try to advance standards and to work on self-healing in parallel to our regulatory, political, and legal fights. This is the front of the information war that we can actually win quickly, if adults commit to sitting down and working through some options. Some examples:

1. **Proof-of-Reserves:** Reserve and liability attestations for crypto custodians would be easy wins for the industry. It is difficult (not impossible) to fake periodic proofs-of-reserves. We should know which exchanges hold which assets, and we should be able to monitor those flows onchain or through independent auditors on a regular basis. There are legislative proposals to this effect, but nothing prevents us from moving on this today and demanding this standard from all of our crypto custodians.

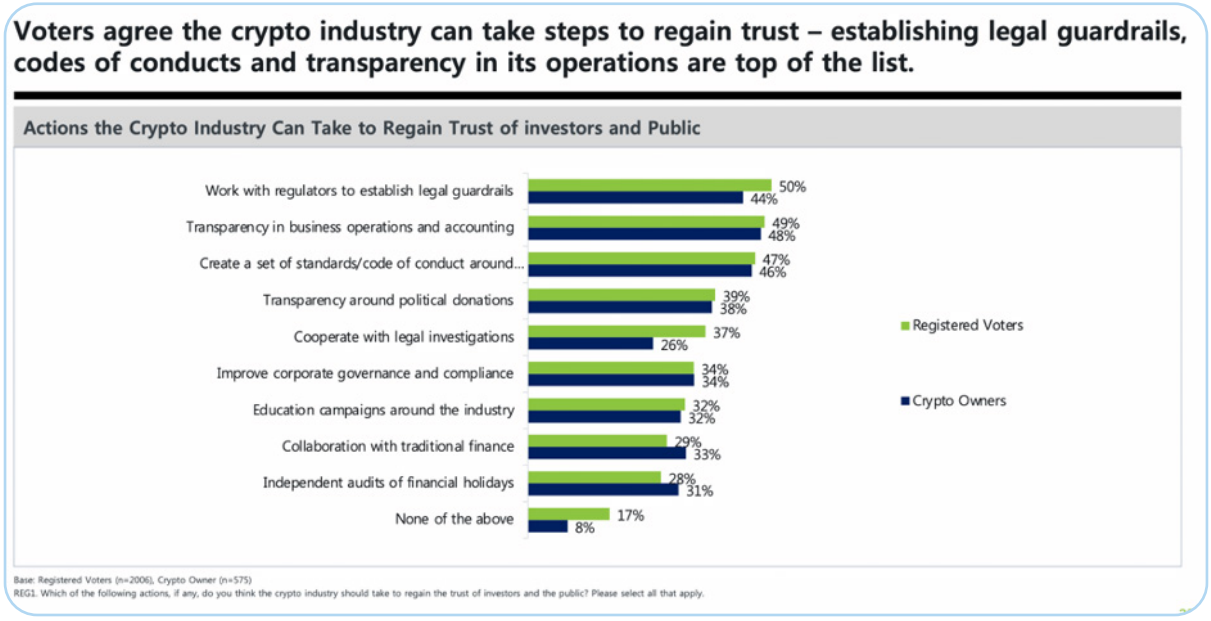
2. **Related Entity Disclosures:** Crypto exchanges and custodians should clearly mark where there are conflicts of interest and related-party transactions, and they should face higher disclosure demands with those "special counterparties." It would have been impossible for FTX to borrow against its own FTT token so heavily and have its related fund, Alameda, fleece its customer piggy bank, with any degree of ongoing related-party disclosures. The Alameda and FTT connections and conflicts were parading around in plain sight. We should have known the details. Likewise, GBTC investors should have known that the GBTC shares subject to strict selling restrictions were actually *pledged collateral* central to multiple bankruptcy disputes and were ultimately liquidated on the open market driving the product's discount to fair market value to nearly 50%.

3. **Token Disclosures:** Token creators will need to get used to some form of disclosure standards in the years ahead. MiCA makes this inevitable in Europe. Similar regulation will extend throughout Asia and eventually hit the U.S. through something similar to the Safe Harbor. Our founding mission at Messari was to create a crypto "EDGAR" library and protocol reporting standards that would solve the industry's token transparency problem and would serve as a backbone for universally accessible project information: user analytics, tokenomics and insider transactions, governance votes and processes, technical developments and risks, security audit results, key integrations (bridges, wallets), etc., — all of which can and should live in an open library. We're working on this, and encourage you to check out our Protocol Services for details.

4. **User Training in Lieu of "Accreditation":** The SEC's antiquated accredited investor standards don't seem to make much sense in a world with AI, an open internet, and financial regulatory double standards such as ubiquitous sports betting and lottery play. That said, we haven't really done ourselves any favors in standardizing user training and good crypto security and hygiene. The *Bankless* guys have done a good job structuring "homework" in their newsletters to help people manage their own crypto holdings and participation, and companies like Rabbithole and Quests

have attempted to gamify training. But there haven't been any universal efforts on this front. We'll likely have some audiences receptive to rethinking accreditation standards (Hester Peirce asked: "Why do we so casually toss aside people's liberty when it comes to their financial decisions?"), but our odds of success drop mightily without clear safety nets. Even former SEC Chair Jay Clayton (no crypto shill) created the Investors' Bill of Rights, which advocated for investing more time and money in a) user education, b) investor qualification, c) real-time transparency, and d) disclosures for various types of investors. A four-year, $250,000 debt-financed, non-dischargeable degree should serve as accreditation.

5. **Front-End Heuristics**: When you authorize a third-party app to your GitHub account it tells you how many users it has, as a heuristic for trust. We should be doing the same thing with wallets and other crypto plug-ins, total call count for a given function, number of wallets using a given contract, etc. The age and security history of projects should be easier to discern, and users could explicitly acknowledge the risks associated with decentralized protocol participation and self-custody. We could perhaps normalize personal responsibility again, if we... disclaimed that users be careful and responsible, and assured them they would have no recourse if they weren't.



(Source: HarrisX)

I will be working on standards-setting in 2024, in large part because, a) I am, as they say, "sick of this shit", b) I want us to be amazing and as far beyond regulatory reproach as possible, and c) I know that the only time standards-setting work happens is before the go-go days of a bull market pick back up.

5.10 MiCA & TFR: Europe's "Leadership"

I never understood the propensity for European technocrats to boast about how "innovative" they are with respect to crafting tech regulations. It's always struck me as a bit of an own goal.

I don't know, maybe I'm not supposed to say that.

I do appreciate the effort at creating clear crypto regulation in Europe, but if the results are unworkable for many applications, what exactly is the point of "clarity"? The recently passed Markets in Crypto Assets Regulation (MiCA 1.0) and Transfer of Funds Regulation (TFR) are definitely a mixed bag.

That was a large portion of the debate on our MiCA panel at Mainnet a couple of months ago, where some of the top crypto policy professionals weighed in on the European regulatory state of play. I'd encourage you to watch this session in full, as it breaks down how this "innovative" regulatory package could actually prove to be a millstone around the neck of EU crypto innovators for years, maybe decades, to come:

"Europe was the first major market to adopt comprehensive crypto regulation. It was [also] the first major market to cripple its crypto industry and forfeit its global competitiveness."

A few high-level takeaways from MiCA and TFR:

1. **Comprehensiveness**
   a. Pro: It's the first legislation for what EU regulators call cryptoasset service providers (CASPs) and token issuers. It recognizes utility tokens as a distinct class of assets outside of the securities realm; liability for CASPs with respect to hacks of operational vulnerabilities, and certain token disclosure requirements;

   b. Con: The regulations will top out at more than 1,000 pages when all final rules and clarifications are incorporated, and that's before "MiCA 2.0" and other future proposals that cover areas like DeFi and NFTs.

2. **Travel Rule Implementation**
   a. Pro: No information disclosure requirements for purely peer-to-peer transfers, a big win, as an earlier version of the legislation would have effectively banned self-hosted wallets (which cannot comply); CASP-to-CASP information sharing required as recommended under guidelines proposed by the supra-national Financial Action Task Force (FATF).

   b. Con: No transaction minimum for TFR information sharing, plus CASP to self-hosted wallet information requirements.

3. **Stablecoins**
   a. Pro: Clarity for issuers, which could encourage the creation of long-awaited EUR-stablecoins (99% of stablecoins are USD-denominated)..

b. Con: EU CASPs might be prohibited from providing yield/interest on top of stablecoins (reduces the incentive to offer them) and may face caps on issuance. If issuers do not seek authorization, they won't be eligible for trading on EU-regulated exchanges. That would take USDC/USDT out of EU-regulated exchanges and knock professional investors out of EU-domiciled exchanges to more liquid offshore entities. (Breaking when this was going to print: Societe Generale listed the first bank-regulated euro stablecoin on Bitstamp.)

4. **DeFi Coming Soon**
   a. Pro: There is hope that an open approach to DeFi (clear supervision, tax, DAO incorporation rules, etc.) would allow Europe to lead on "embedded supervision" and experimentation with automatic compliance monitoring versus the data collection and verification default common for centralized services (a pilot program for "embedded supervision" was greenlit in 2022).

   b. Con: DeFi developers and technical governors could eventually be on the hook for DeFi regulation, as there is no first amendment protection in Europe and there are certainly no illusions that "code is protected speech."

5. **Miscellaneous**
   a. Pro: Non-EU companies will have strict marketing restrictions for EU users, but exemptions for "reverse solicitation" (where EU users actively seek out foreign services), good for global incumbents like Binance who have a healthy head start; also, no ban on Proof-of-Work (PoW)...yet, but some are leery that mandatory environmental disclosures could lead to those restrictions eventually.

   b. Con: Commenting on crypto assets in (social) media for profit (directly or indirectly) without disclosure could be considered market manipulation.

I understand why European regulators are puffing out their chests a bit at MiCA. It is a regulatory milestone under which they believe engaging in frauds like FTX would have been impossible or at least significantly harder. But I'm more circumspect, and I fear we are entering a time when global compliance among various conflicting regimes will prove impossible. The future belongs to the countries which commit to technological superiority and innovation, not who creates the crypto version of GDPR's website banners.

Conclusion:

Regulators worldwide are probably not going to kill crypto (or AI, or social media, or biotech, or...), but they can make our lives miserable for a considerable period of time. We just need to hold the line for a bit longer and defend the free and open internet of finance.

Remember: Politics is downstream of culture. Politicians pick personnel. Personnel is policy. Policy is quasi-permanent. Win the cultural information war, and we win the ballgame.

(For those looking beyond the U.S. and Europe, this is a good resource. PWC also has some good resources on the global regulatory picture for crypto and the global tax picture. These are a year old, but I assume will likely be refreshed for 2024. EY also has some good overviews of the potential paths to compliant DAO engagement, which I'll elaborate on in Chapter 10.)

Messari Protocol Services

Bridging the Divide For Crypto Projects and the Community

Messari Protocol Services offers leading crypto projects comprehensive solutions, including in-depth research, standardized financial reporting, and a platform for disseminating key fundamental information.

Visit **messari.io/protocol-services** to learn more or contact **sales@messari.io** to schedule a demo.

Schedule A Demo

CHAPTER 6

TOP 10 TRENDS IN CeFi

6.0 State of CeFi

"A lot of holes in the desert, and a lot of problems are buried in those holes."
-Nicky Santoro, Casino

As centralized crypto financial services go, 2023 was a mercifully quiet year compared to last year. Sure, there were a bunch of bankruptcy workouts, a couple of high profile arrests, plea deals, settlements, and one conviction (so far), not to mention a number of fines, and rounds of layoffs at the titans of crypto, but it *seemed* manageable compared to the credit contagion of 2022. Most CeFi companies buried the bodies of yesteryear, and got back to the boring ground and pound business of crypto infrastructure.

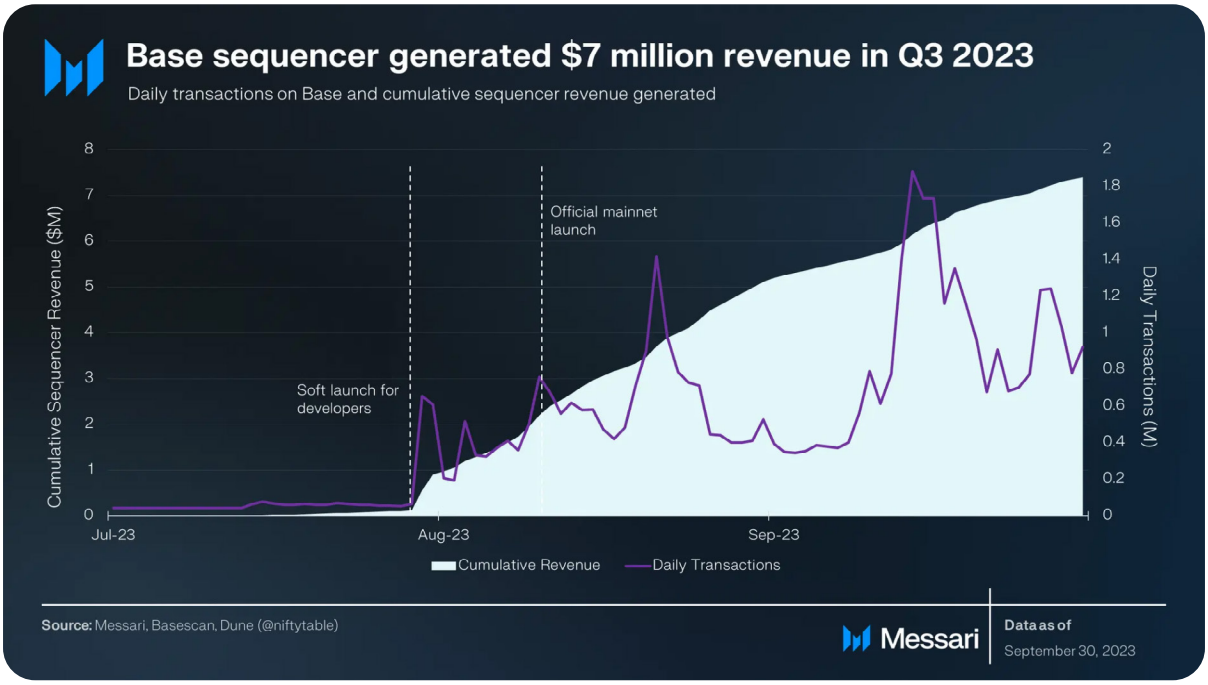
Coinbase crushed it in a difficult market, and their shareholders won big. Binance lived to fight another day, albeit under new leadership. OKX, Kraken, and ByBit were net winners, but many other exchanges lost ground. Exchange volumes hit their lowest levels since late 2020 in September, and piss poor sentiment, delistings, and regulatory chokepoints all played a role in contracting the CeFi landscape.

But we seem to be back on the upswing. What doesn't kill us makes us stronger.

6.1 What. A. Year. For. Coinbase.

Coinbase is operating at an otherworldly level right now, and remains the best positioned company in crypto.

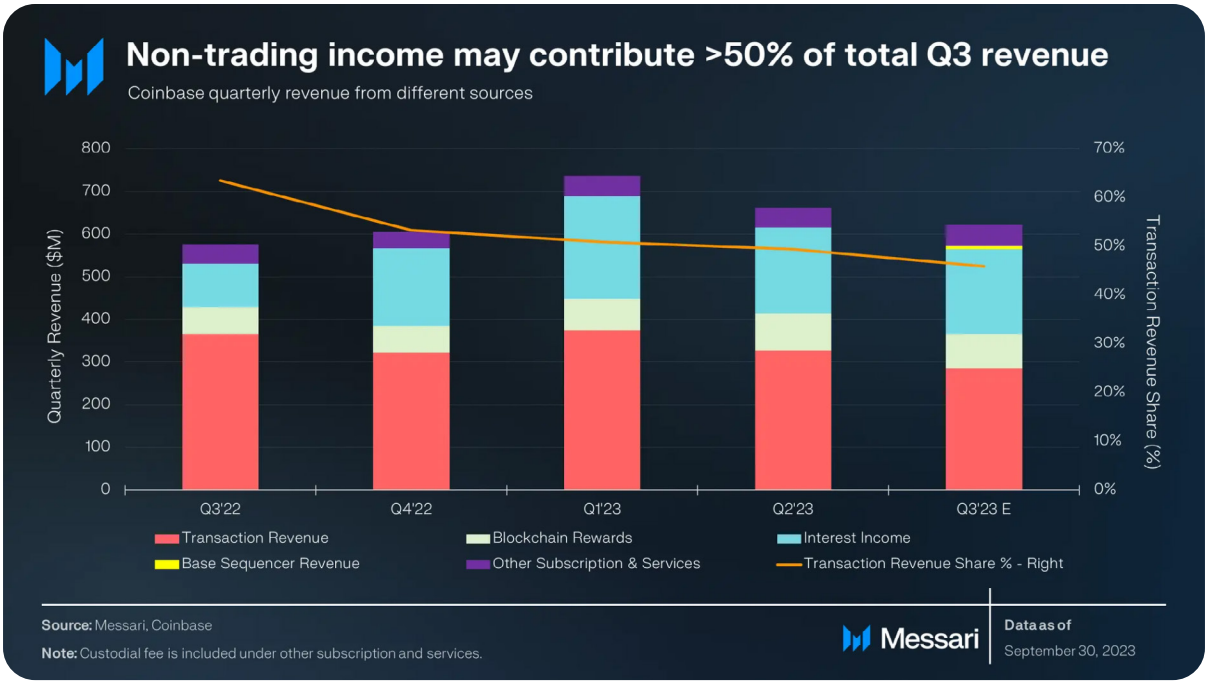
They weathered the post-FTX storm and several rounds of layoffs, sued the SEC when they needed to take the gloves off and go to war, secured license after license in an international expansion whirlwind, deepened a core strategic partnership with Circle regarding USDC issuance, and launched Perps. They also shipped a successful L2 in Base (which generated $7 million in revenue in its first quarter and powered the app of the year, friend.tech), made multiple slick upgrades to their self-hosted wallet (and"wallet-as-a-service" expansion play), and launched Project Diamond, an onchain RWA platform.



(Source: Spoiler Alert – Coinbase Q3 Revenue Estimates)

They also paid down debt at favorable prices, beat earnings expectations multiple times, and benefited from a mix shift in revenue that now has the majority of Coinbase's earnings coming from non-trading activities. In a low volume environment with brutal regulatory headwinds, the company is operating at break even. Imagine what will happen when an ETF gets approved, and their custody revenue alone doubles overnight.

Retail revenues will still drive the business forward in bull markets, but this is a company built for ZIRP speculation and high interest (and staking) environments alike today. They've got the cash horde and informational advantages (Coinbase Ventures has been the third most active industry investor this year) to pursue inorganic growth (M&A), once consolidation plays emerge as crypto startups start running out of money.



(Source: Spoiler Alert – Coinbase Q3 Revenue Estimates)

I told Brian on stage at Mainnet that his company was performing so well that I felt like I was kissing his ass. But what am I going to do, lie about it?

They haven't just been on the pulse, they have been the pulse of crypto. And they avoided the catastrophic errors that so many other crypto incumbents fell prey to this cycle.

Coinbase certainly isn't infallible, and they've still got to win their high stakes U.S. court cases, ward off competition from the emerging Wall Street players hellbent on eating their lunch, and do what they can to steal share back from Binance internationally. None of that will be easy. But I don't think there are many operators in crypto who wouldn't trade positions with Coinbase right now if they could. The company is a juggernaut, and I hope the intensity and creativity stays as high as it's been this year.

[Required Reading: When it comes to $COIN, Kunal beat the Street all year.]

6.2 Binance in ('2)4

"we see the bad, but we close 2 eyes."

Has there ever been a more expensive chat message in the history of the world?

Ever since we read this line in the CFTC's complaint against Binance back in March, we knew it was just a matter of time before the DoJ shoe dropped, and the U.S. authorities extracted their pound of flesh from CZ and his company. For a long time, I assumed early Binance compliance shenanigans would result in a billion dollar fine, but no jail time. That wasn't directionally off, but I underestimated the size of the fine and could yet turn out to

be overly optimistic about CZ's prospects for staying out of jail completely with his plea deal. There are a few silver linings to Binance's settlements with the U.S. government and guilty plea for money laundering and sanctions law violations.

1. **It could have been worse**. Much worse. I'm not sure we could afford the black cloud of a "shadowy global exchange" hanging over the industry's head much longer. It started to feel like an existentially bad outcome was on the horizon. Binance was accused of some bad behavior, but what they copped to likely wasn't nearly as bad as it could have been. The end result is that Binance is still chugging along and dominating global exchange volumes. Their 150 million global users (!!!) seem happy.

2. **We have "surveillance sharing agreements."** These institutional compliance agreements might finally pave the way for institutional entry to crypto. Surveillance sharing was always cited as a missing bit of market infrastructure that blocked the approval of spot crypto ETFs. Now the major ETF applicants have formal agreements in place with Coinbase, and an independent compliance monitor may give the U.S. regulators comfort that Binance's global operations are on the up and up. CeFi has been legitimized overnight in a way it's never been before.

3. **The U.S. giants can actually compete.** Coinbase and Kraken are still facing (frivolous) lawsuits from the SEC. But the Binance resolution re-leveled the competitive playing field a bit after years in which American companies sat at a structural disadvantage to their overseas counterparts. You could tell how much this bothered Brian Armstrong and Jesse Powell based on their public comments following the announcement. It doesn't make the U.S. regulators behavior towards the industry ok, and it doesn't reverse the market share losses the U.S. leaders suffered in the process. But at least the American rule-followers don't feel like *complete* suckers for building at home anymore.

4. **Customer funds are SAFU, but tax filers?** One of the things I expect out of the Binance settlement is an enormous amount of customer pain for Binance's American users who failed to correctly report their crypto holdings or gains. Binance may have just handed the DoJ and IRS a honeypot of naughty little boys and girls just in time for Christmas. As someone who pays taxes and hates every second that's wasted on the horrifically complicated cost basis tracking and reporting of crypto, I am marginally happier knowing that low hanging fruit tax evaders will be pursued before I'm asked about my intraday accounting of $5,000 of LP pool tokens.

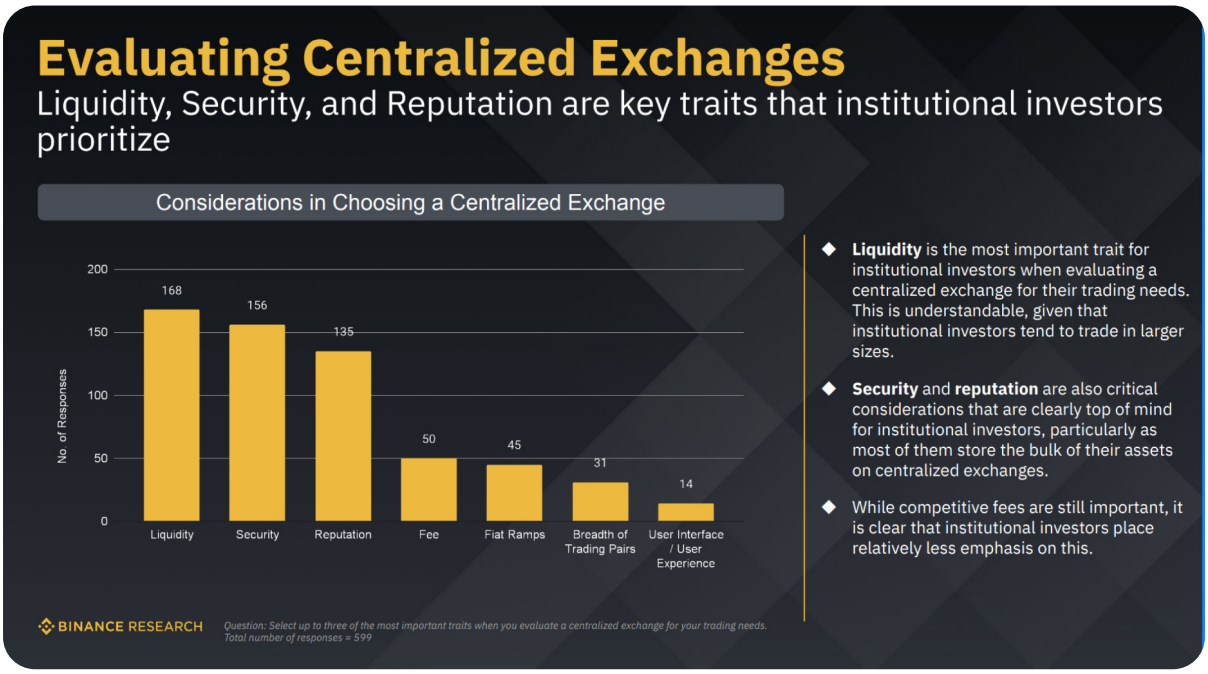
5. **The Beginning of the End.** FTX's bankruptcy felt absolutely gutting because I knew that we were in for a relentlessly awful twelve months. The FTX bankruptcy was the "end of the beginning" of the crypto bear market last November. Getting the Binance settlement behind us finally feels like the beginning of the end, and is probably responsible for 51% of my bullishness going into 2024. A weight has been lifted, and we can move forward.

It sounds weird to say, but I'm also pretty excited for CZ's next act. It sounds like he's interested in DeSci, and anytime you get to start something new, it's liberating. Assuming

his sentencing is light and smooth this February, this is probably the best possible outcome for someone who ran headfirst into the U.S. empire and didn't get Epsteined in the process.

6.3 The "Other" Net CeFi Winners

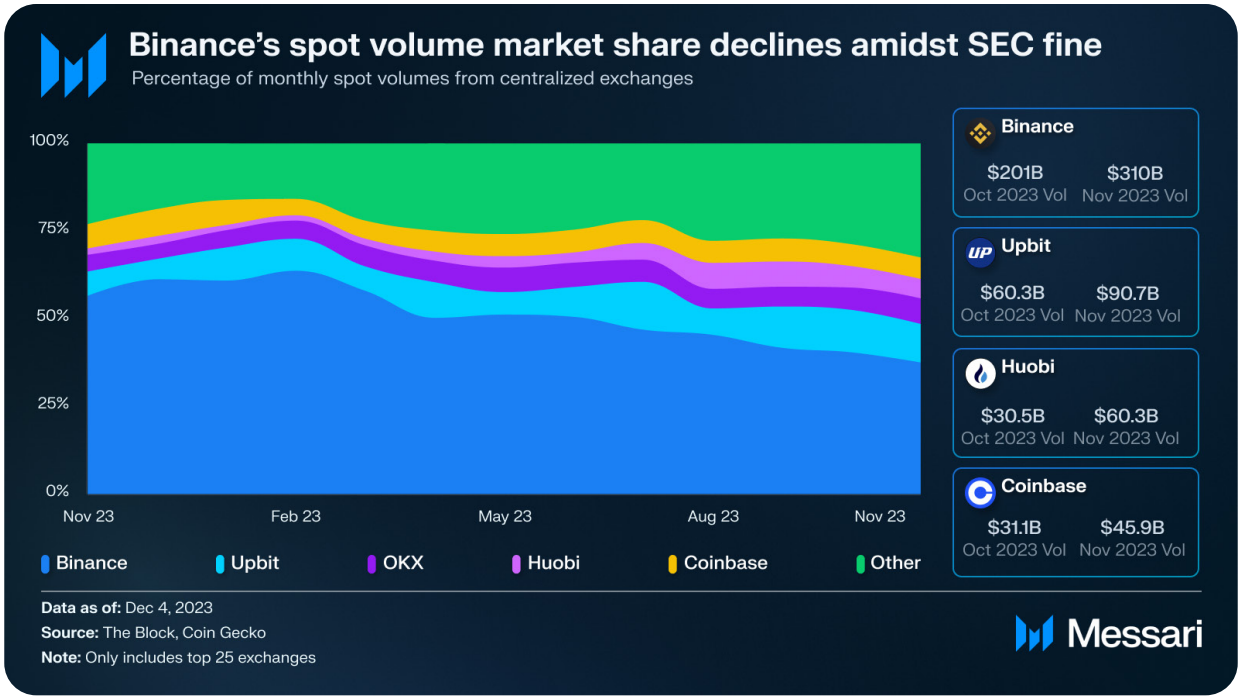
If you want a quick peek at who's most likely to pick up the slack from Binance, you can just look at Binance Research's institutional customer survey results from earlier this year. The most important factors for new entrants when selecting CeFi services were liquidity, security, and reputation. I'm sure that gets truer by the day when considering the U.S. regulatory position on crypto right now.



(Source: Binance)

Outside of Coinbase, three players stood out for their market share gains this year, all on the exchange side: OKX, Kraken, and Bybit.

Binance lost 25 points of market share in international exchange volumes this year, primarily to Kraken in Europe, and OKX and Bybit elsewhere. Some of this was due to traders diversifying away from Binance due to regulatory concerns (though Bybit has had some rumored interest from regulators as well). We'll see if the exchange can recoup some of their customer losses now that they've put their U.S. concerns in the rear-view mirror.



(Source: Market Liquidity Brief)

I don't have time to write up every *single* global exchange platform (and there are many other good ones like Bitfinex, Bitstamp, Upbit in Korea, Bitso in Mexico, etc.), but I would point out that the exchange tokens (for those that have them) have held up pretty well as both a historical performance report card and signal of strength heading into 2024. Huobi's HT token halved, and BNB and LEO flatlined, but the others rallied YTD with the market's comeback. It's all priced in!

What about the dedicated custodians? Binance Research's survey results showed that nearly 60% of institutional investors prefer to store crypto on exchanges, while just 20% preferred non-exchange custodians like Anchorage and Fireblocks. I could go out on a limb and say that this gap will likely narrow, but I will admit I was surprised to see Coinbase run the table as the custodian partner for most of the spot bitcoin ETF applicants.

It's not surprising that investors prefer the one-stop shop convenience of bundled custody and exchange services, but it does lead to some head scratching when you consider recent history (FTX flameout). The crypto custodians may be the big winners if we get some bills passed.

6.4 The ETF Race(s)

For those who believe the spot bitcoin ETF may be a “sell the news” event, I would only ask one question: if not marketing spend (direct to consumer ad dollars and institutional sales to key distribution partners), then how else will these firms compete for ETF AUM in January?

Issuer *(Ticker)*	Company	Asset	Exchange	Custodian	Index/Pricing Provider	SEC Next Deadline	SEC Final Deadline
"Physically" Backed							
Grayscale Bitcoin Trust(Re-file)*Conversion (GBTC)*	Grayscale	Bitcoin	NYSE	Coinbase	Nasdaq	~10/13/23	Unknown
ARK 21Shares Bitcoin ETF(Re-filing) *(ARKB)*	21Shares & ARK	Bitcoin	CBOE	Coinbase	S&P Dow Jones	1/10/24	1/10/24
iShares Bitcoin Trust *(IBTC)*	BlackRock	Bitcoin	Nasdaq	Coinbase	CF Benchmarks	1/15/24	3/15/24
Bitwise Bitcoin ETP Trust (Re-filing) *(BITB)*	Bitwise	Bitcoin	NYSE	Coinbase	CF Benchmarks	1/14/24	3/14/24
VanEck Bitcoin Trust(Re-filing)	VanEck	Bitcoin	CBOE	Gemini	MVIS	1/15/24	3/15/24
Wisdomtree Bitcoin Trust(Re-filing) *(BTCW)*	Wisdomtree	Bitcoin	CBOE	Coinbase	CF Benchmarks	1/15/24	3/15/24
Invesco Galaxy Bitcoin ETF(Re-filing) *(BTCO)*	Invesco & Galaxy	Bitcoin	CBOE	Coinbase	Bloomberg	1/15/24	3/15/24
Wise Origin Bitcoin Trust(Re-filing)	Fidelity	Bitcoin	CBOE	Fidelity	Fidelity/CoinMetrics	1/15/24	3/15/24
Valkyrie Bitcoin Fund(Re-filing) *(BRRR)*	Valkyrie	Bitcoin	Nasdaq	Coinbase	CF Benchmarks	1/17/24	3/19/24
Global X Bitcoin Trust(Re-filing)	Global X	Bitcoin	CBOE	Coinbase	N/A	11/21/23	4/19/24
VanEck Ethereum ETF	VanEck	Ethereum	CBOE	N/A	MVIS	12/25/23	5/23/24
ARK 21Shares Ethereum ETF	21Shares & ARK	Ethereum	CBOE	Coinbase	N/A	12/26/23	5/24/24
Hashdex Bitcoin ETF *Strategy Change (DEFI)*	Hashdex	Bitcoin	NYSE	N/A	CF Benchmarks	1/1/24	5/30/24
Hashdex Nasdaq Ethereum ETF	Hashdex	Ethereum	Nasdaq	N/A	N/A	1/1/24	5/30/24
Franklin Bitcoin ETF	Franklin	Bitcoin	CBOE	Coinbase	CF Benchmarks	1/1/24	5/30/24
Grayscale Ethereum Trust *Conversion (ETHE)*	Grayscale	Ethereum	NYSE	Coinbase	N/A	12/6/23	6/18/24
Invesco Galaxy Ethereum ETF	Invesco & Galaxy	Ethereum	CBOE	Coinbase	Bloomberg	12/23/23	7/5/24
iShares Ethereum Trust	BlackRock	Ethereum	Nasdaq	Coinbase	CF Benchmarks	~1/13/24	~7/26/24
Fidelity Ethereum Fund	Fidelity	Ethereum	CBOE	Fidelity	Fidelity/CoinMetrics	~1/21/24	~8/3/24

Note: Dates are estimates and deadlines, so they may come earlier. Bloomberg

Source: Bloomberg Intelligence, SEC.gov

(Source: Bloomberg, courtesy of James Seyffart)

You want to hold assets that Blackrock, Fidelity, WidsomTree, Franklin Templeton, Invesco, Grayscale, Bitwise, ARK, Van Eyk, and Valkyrie are all tripping over themselves to sell HARDER than each other. And that’s exactly what’s going to happen with bitcoin as soon as the ETF floodgates open. With billions of dollars of fees on the line, there will be enough shilling to make even the most cringe crypto YouTube personality uncomfortable.

A spot bitcoin ETF is a product whose time has long-since come. Institutional money managers are going to love the fastest horse / digital gold narrative, bitcoin’s sharpe ratio, the knack for both explosive growth years (performance fees!) and volatility (trading fees!), and all of the other bull case bulletin board material I already wrote about in previous sections.

I haven’t thought deeply about the other ETF issuers to be honest, or the timing of the other spot crypto ETFs (ETHE) now that the SEC has broken the seal on ETH futures ETFs as well. A few rapid reactions, though:

1. We know that fees on these products are going to come down rapidly, and the

market is about to get a whole lot more liquid.

2. As the primary custodian for most of the ETF issuers, Coinbase is bound to see billions of dollars of new custody demand overnight.

3. Michael Saylor, who owns 25% of MicroStrategy, gets to keep the $5 billion of bitcoin his company now owns (and the $1.6 billion gain they've notched on that levered bet so far) even if $MSTR loses some of its "sort of an ETF" luster. Saylor played an all-in wealth creation game on easy mode. Respect. (He's still buying, btw.)

As exciting as the prospects of the ETF approval are, I'm still a bit sad thinking about what could have been. The SEC created a financial weapon of mass destruction and full-blown crypto credit crisis with their refusal to convert Grayscale's GBTC product much earlier, and it blew up Three Arrows Capital, BlockFi, Voyager, FTX, Genesis Capital, Gemini Earn, and maybe even Grayscale's own parent, Digital Currency Group, in the process.

Let me explain (for the fifth year in a row.)

6.5 DCG and the Fall of Rome?

Grayscale *should* be first out of the gates, and they and their GBTC shareholders *should* be the biggest winners of this long-overdue milestone. But their biggest threat to an ETF uplisting may be tied to the high stakes drama at their parent and sister companies, DCG and Genesis.

If FTX was guilty of garden variety fraud thanks to its founder's delusional and machiavellian mission to become a trillionaire and U.S. President, then DCG's struggles last year were more tragic: they had good businesses, tons of liquid assets and earnings power, and a good reputation, but they were eventually choked out by a mix of bad timing and bad counterparty risk management surrounding the very product that made them kings, GBTC.

I'm not sure I've read a worse legal complaint than the New York Attorney General's civil fraud allegations against Digital Currency Group (DCG), its prime broker Genesis, and its executives "for defrauding more than 230,000 investors, including at least 29,000 New Yorkers, of more than $1 billion." (Crypto exchange and custodian Gemini was also included in the complaint for allegedly misrepresenting the riskiness of the Gemini Earn investment program at the center of the fraud allegations. The evidence cited against both groups look...not great.*)

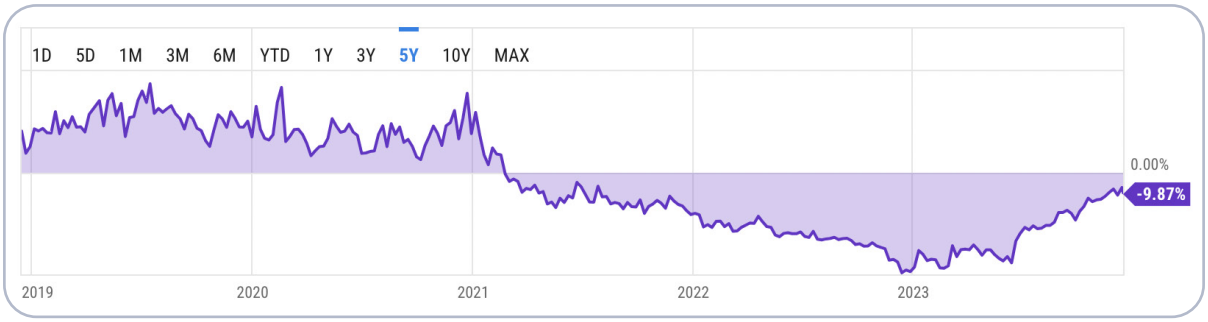
I'll try to catch you up (once again) at 3x speed.

DCG created asset manager Grayscale and its Bitcoin Investment Trust product in 2013. Given Barry Silbert's expertise in private markets (his first company SecondMarket was a trading platform for private shares in companies like Facebook), the Trust was the first vehicle to get publicly quoted through a "side door" listing mechanism called Rule 144.

You can read the details about this "side-door ETF" in previous Messari reports here, here, and here. The details are technical, but what you need to know is that GBTC was the only game in town for public market bitcoin exposure for many years.

The Bitcoin Trust allowed investors to create new shares using bitcoin deposits, but didn't have a redemption mechanism to convert shares back to bitcoin *because the SEC sued them to cease their redemption program* in 2014. (lulz). As a result, GBTC shares could trade above or below NAV (net asset value) as share supply was locked, but demand for GBTC shares vs. spot bitcoin varied over time. For years, GBTC traded at a premium as it was the lone public bitcoin equity instrument available to many investors. Demand exceeded supply, but supply couldn't quickly adjust to demand given the side door path to offering GBTC shares.

Hedge funds piled into this "arbitrage" trade with leverage in 2020 and 2021, betting that they could create new shares, flip them to public markets investors while the NAV premium existed, and redeem shares for bitcoin if the share price ever fell to a discount, in particular once a spot ETF was approved that allowed for daily redemptions. But few anticipated that the GBTC share premium could flip to a *deeply negative discount* for an *extended period* of time. Alas, it was a bloodbath in 2021-2023. The GBTC share price reached a 50% discount to NAV last December.



(Source: YCharts)

Grayscale successfully sued the SEC this summer for blocking its ETF conversion on "arbitrary and capricious" grounds. Though the ruling may have come too late to save DCG, as the damage from the GBTC-related credit contagion was already done. That's because GBTC investors praying for an ETF approval (which would allow for a share redemption at par value), were already blown out of their levered GBTC bets in mid-2022.

GBTC was the "widowmaker" trade that took out 3AC (among others), and 3AC was a large Genesis Capital borrower. The bad GBTC-collateralized loans to 3AC were among the *largest* assets at Genesis. When 3AC went bankrupt, Genesis suddenly had a $1 billion hole to fill in its balance sheet. It looked to its parent DCG for help. Given the earnings power of DCG and its subsidiaries, and its known balance sheet, it seemed reasonable that DCG could plug the hole, even though it was massive.

DCG and Genesis worked out a deal whereby Genesis could unload its bad 3AC loans (and bankruptcy claims) to DCG, in return for a 10-year promissory note that doubled as a "capital infusion." In reality, it appears to have allegedly been an empty accounting trick. DCG didn't have the cash or liquid crypto assets to back the note. Instead, their companies' earnings power (which was considerable) would be able to pay down the

commitments to Genesis.

In reality, it turned out that DCG was itself a borrower from Genesis. The firm allegedly borrowed large sums of money from its subsidiary in order to finance stock buybacks and purchases of GBTC shares back when they traded at a steep discount to NAV. The GBTC share repurchases were publicly disclosed in Grayscale filings. The DCG share repurchases were unknown at the time, but disclosed later in the Winklevoss complaints against DCG.

The NYAG (and Gemini) alleged that Genesis and DCG fraudulently misrepresented the nature of the promissory note as a "current asset" (in this case a liquid asset with less than a year of duration) to Genesis creditors, in order to avoid a bank run on Genesis and firm up confidence in the lender after a public black eye from the 3AC bankruptcy. And there's been conjecture that DCG may have "bailed out" Genesis in June 2022 in an attempt at the time to avoid getting pulled into a Genesis bankruptcy (where they ended up anyway). There are some bad facts in the NYAG complaint (written statements from executives) that look difficult to explain away at first glance.

I recommend Vijay's synthesis of the situation here to get fully up to speed on the related party transactions, and what exactly has been alleged by the NYAG. Ram even made the Enron analogy. I also recommend Laura Shin's interview with two Genesis creditors. Or you can read the NYAG complaint itself, and decide what you want to believe while the case makes its way through the courts.

I'm not going to speculate much more on how this plays out, other than to say that I've seen the documents, I've read the complaints, and I know how much money is on the line. I do think there's maybe a 90% chance that all the parties end up settling and living to fight another day (perhaps after they pay hefty fines) now that asset prices are once again ripping higher. More importantly, I doubt that the tangled relationships in this saga will complicate and drag out Grayscale's ETF conversion application with the SEC (GBTC shareholders would be the only ones who would be punished by that outcome).

The wrinkle is whether the NYAG's complaint against DCG, which seeks to permanently ban Barry and DCG (and Genesis and Moro and Gemini) "from engaging in any business related to the issuance, offer, distribution, exchange, promotion, advertisement, negotiation, purchase, investment advice, or sale of securities or commodities within or from this state" ultimately has teeth. There are existential ramifications for DCG, Genesis, and Gemini, but could authorities technically force a sale or spin out of Grayscale from DCG, given their shared governance?

I doubt it.

Genesis is dead, its wealth management division HQ was shuttered. DCG just sold CoinDesk to crypto exchange Bullish, and many of DCG's investment assets appear to have been sold off or pledged as collateral to Genesis or its counterparties. That leaves Grayscale as the crown jewel of DCG, along with Foundry (the operator of the world's largest bitcoin mining pool). It's tough to imagine DCG as a going concern without Grayscale, so I wouldn't expect this fight to abate for years if push comes to shove. It's simply not happening.

Honestly, I could write another 20 pages on this saga, and how it might unfold, but I already did that when it mattered last year. My optimistic resolution did not come to pass. Instead, I'll cut this short and wish a very Merry Christmas to all of the lawyers and bankers involved.

**A couple of disclaimers:*

1. Gemini and Winklevoss Capital are small investors in Messari;

2. I own GBTC shares, which represent interest in the Grayscale Bitcoin Trust. Grayscale is owned by DCG, and is a sister company to Genesis.

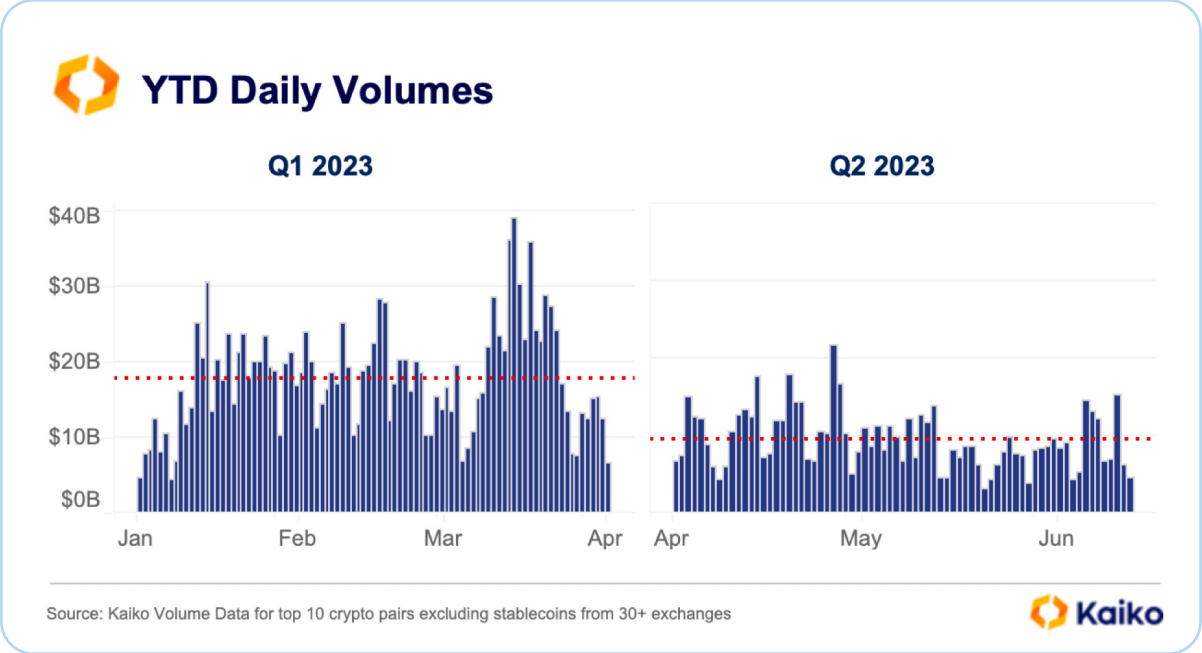
3. I was the first employee at the DCG parent company when it spun out from Barry Silbert's previous venture, SecondMarket. I worked with the two execs singled out in the NYAG complaint, Barry and Genesis CEO Mike Moro from 2014 to 2017. I have no financial relationship with DCG or any of its affiliates (aside from GBTC shares), and haven't since I left.

*4. Last December, I wrote some thoughts about how DCG, Genesis, and their creditors may have recapitalized and avoided this public sh*tshow. Obviously, none of what I had outlined as a potential path to a private resolution manifested. I've been passively watching the spectacle play out along with the rest of you all ever since.*

6.6 Banking Choke Points

I've already covered "Operation Chokepoint 2.0" thoroughly in previous sections, but it's worth double clicking on one item in particular that's a less obvious medium-term setback for the industry: the destruction of the SEN and Signet services has significantly hampered liquidity within the industry, and signaled to major U.S. market makers to get the hell out of crypto markets in the U.S. Two of crypto's largest market makers in Q1, Jane Street and Jump Trading, pulled liquidity from US crypto trading platforms within weeks.

"We don't want regulated financial firms banking crypto companies" was a message well received, and it helped wreck market depth by 30-50%, essentially overnight.



(Source: Kaiko)

In any other country, what Senator Warren did in reportedly conspiring with short sellers to assassinate crypto-friendly banks and apply extrajudicial pressure on other regulated financial institutions was a miscarriage of justice. Unfortunately, in the modern U.S., it didn't even register as a scandal, it was just a Wednesday.

I do think it's important to set the record straight on this, though.

Silvergate, in particular, was a great supporter of the industry, and will go down as one of the most important companies in our young history. They didn't deserve the death penalty for Sam Bankman-Fried's crimes, and they shouldn't have met their demise at the hands of a conflicted and politically motivated Senator. They liquidated their business in an orderly manner, and didn't need a taxpayer bailout (via the FDIC) to wind down operations.

That's because their business model and reserve risk management practices were actually pretty good, and they offered exactly the type of (close to fully-reserved) banking we should be fighting for now as a replacement to our fallen comrades.

Fortunately, we have Caitlin Long's Custodia Bank, which has been grinding out progress in her multi-year litigation to secure a Fed Master Account despite the stiff opposition of the Federal Reserve, their dirty games, and a (literally) unlimited legal budget due to the way the Fed is able to fund its own operations.

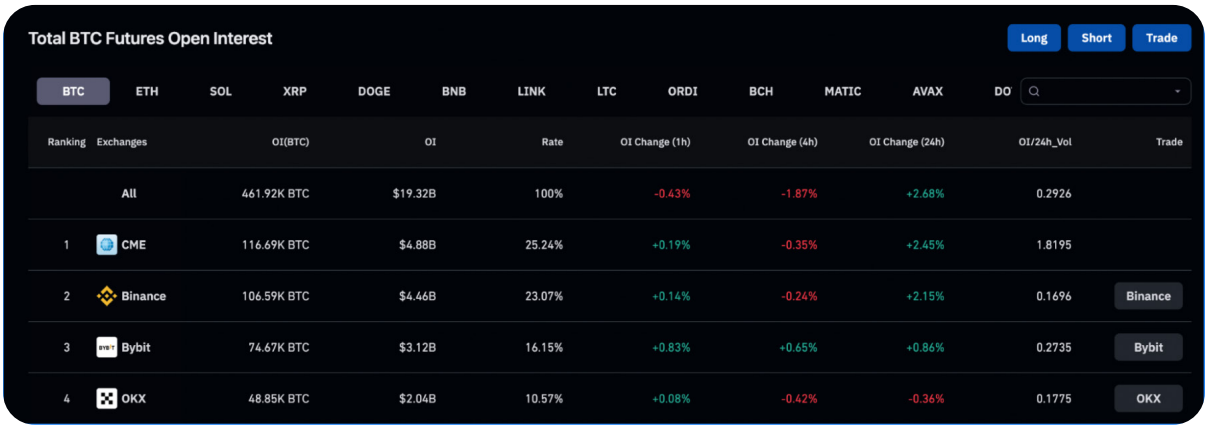
Custodia now accepts dollar deposits and offers bitcoin custody services for business customers, but there's a long way to go to reclaim the banking services we lost this year.

6.7 CME vs. Perps vs. dYdX

The bitcoin futures markets are rocking ahead of ETF speculation, and sit at their highest level of open interest (OI) since early 2022. CME futures may have taken the lead amongst institutional investors in OI, but perpetuals as a product still dominate more than 75% of the global crypto futures OI and more than 90% of volumes. Binance, Bybit, and OKX take down the lion's share of bitcoin perp volumes today, and even crypto options platform Deribit is primarily a perps-driven business. The products crowd out every other major trading product given their 24/7 nature and the high leverage rates on most major exchanges.

It's unlikely CME will compete as effectively with the perp giants outside of bitcoin, as I don't see many scenarios where the ETH futures ETFs pick up market share vs. their imminent spot alternatives. With just $20 million in AUM across the ETH futures ETFs that launched this fall, there's not a whole lot of need for high volume CME markets. That will likely be the case for every other asset for which CME ultimately lists a market as well, and it's much more likely Wall Street firms will lobby to trade perps than wait on the sidelines for U.S. regulators to greenlight the CME markets on a multi-year lag.

I'd also expect dYdX, which already outpaces BitMEX and Kraken in certain markets (ETH and SOL), to continue to win market share vs. its centralized perps competition. dYdX's outperformance could just be the beginning. I'll have more to share about this in Chapter 9, but dYdX's migration to a Cosmos app chain should speed up performance, and unlock another banner year amidst limited DeFi competition.



(Source: CoinGlass)

6.8 Compliance Tools - Tax and AML Forensics

I wrote that my base case for 2023 was that the IRS would create hell for crypto investors. I'm sure that's probably happening at scale (or is about to) given the treasure trove of information the Feds now have from their settlement with Binance, and Kraken's relenting on the IRS's dragnet demand that Kraken turn over data on 42,000 high-volume user accounts. (Coinbase had turned over similar records in 2017 following a court order that is still being challenged in court on constitutional grounds.)

Broker reporting requirements always struck me as somewhat sensible and inevitable, but following the coming implementation of the crypto "broker rule" tax reporting requirements, they are now definitely here. While I will miss manually reconciling cost basis and trades across three exchanges and a bunch of DeFi applications, I am thrilled to get a professional and accurate tax form at the end of the year next year from the firms I have been using for years.

If tax reporting is a nightmare, then AML reporting is a hellscape. With major DeFi hacks by North Korea and the sanctioning of Tornado Cash, 2022 was not a great year. While I believe the industry's compliance tools and norms continue to get stronger each year, 2023 may have been even worse from a headlines risk standpoint, thanks largely to some ill-advised marketing by blockchain forensics leader Elliptic. What was meant to be an advertisement for how blockchains help industry players identify and catch illicit actors, turned into a public billboard that was used to argue for the industry's destruction. Elliptic clarified the data, but the damage was already done.

I don't need to repeat myself from Chapter 5: I think TradFi and our horrific .gov government sites are at far greater risk of technical exploits or missing rogue payments. But they're screw ups aren't broadcast via open accounting ledgers, so they don't make the front page of the newspaper. Ours do.

I'm looking forward to Chainalysis' annual crypto crime report. You can read last year's to get a sense for how much better things keep getting year in and year out when it comes to crypto compliance. The vulnerabilities we have are identified quickly and patched, and we're slowly creating an army of opsec militants, which is probably a long-term positive for society.

6.9 Compliance Tools - Diligence

Some of Messari's top power users work in compliance.

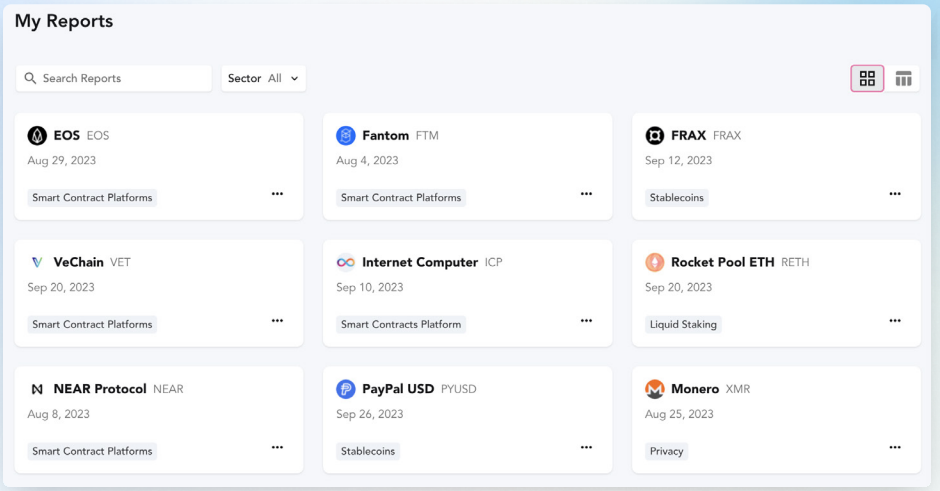
How listing decisions get made, how tokens get supported once they are integrated into a crypto platform, and how investors get comfortable allocating client capital (or voting their tokens) all come with certain duties of care. We already highlighted some of these tools in Chapter 3, but we have the most comprehensive library of asset diligence reports on the market and track off-chain developments, "corporate actions," legal and regulatory developments, and community governance for hundreds of global crypto projects.

There will definitely be reporting requirements for the crypto industry in the years ahead. Whether that looks like Hester Peirce's Safe Harbor or MiCA's enhanced token disclosure rules is besides the point. We know what types of information need to be aggregated in order to reduce the flaring information asymmetries that exist in crypto today, and we're already building the tools that will be ready when policymakers define the final rules.

Messari

Messari Diligence Reports: Your Compliance Hub for Thorough Asset Diligence

Delve deep into the history and inner workings of assets and protocols with Messari Diligence Reports. Our structured, in-depth analyses distills must understand information into one consolidated view, streamlining your diligence process for informed integrations, investments, and educational pursuits.



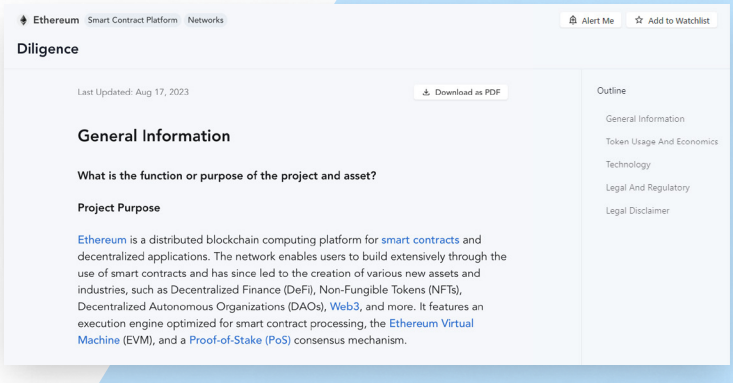
Professional, In-Depth, Unbiased: The Trifecta of Crypto Asset Diligence

+ **Professional Asset Analysis**
  Uncover the full history, structure, and features of any asset or protocol. Explore core project details, legal and regulatory risks, economics, and technology with structured, in-depth reports.

+ **Streamline Decision-making**
  Facilitate integrations, investments, and internal education with comprehensive reports used by leading exchanges, custodians, funds, and institutions.

+ **Asset and Protocol Integration**
  Accelerate your asset universe growth and unlock new interactions for your users with precise protocol integrations analysis.

+ **Real-time Notifications**
  Receive instant alerts when there are notable changes to your diligence reports, streamlining your compliance workflows and ensuring you're always up-to-date with the latest developments in your assets and protocols.



Other Features

+ **Unbiased Perspective**
  Gain an unbiased perspective spanning from a project's background to its technical integrations, ensuring peace of mind in your asset and protocol incorporations.

+ **Personalized Dashboard**
  Effortlessly access purchased reports, included reports, or swiftly acquire new reports through a personalized dashboard, tailored to meet your diligence needs.

+ **Downloadable Reports**
  Access diligence reports directly on the Messari platform or download them via PDF, providing flexibility in how you interact with critical asset information.

6.10 Everyone Else in TradFi

The opportunities for TradFi within crypto are obvious: they have regulatory advantages (and compliance moats), a knack for investing enormous sums of human and financial capital when they sense opportunity, and perhaps most importantly, a clean slate that comes from waiting for permission for many years on the crypto asset class's periphery.

In tech, a late mover bias may be a liability. But in finance, it's a competitive advantage: one that Gary Gensler himself harped on back when he taught at MIT and suggested that crypto's incumbents might be too far gone to remediate their listings sins and come into compliance as regulated exchanges.

Beyond the ETF race, Fidelity is the TradFi firm with the highest potential to lead the field in 2024 and compete most aggressively with Coinbase. They've been deep in the industry for a decade, field a large and talented team, and would have launched their excellent services with much more fanfare had their go-live not coincided with last November's FTX trainwreck. My base case assumption continues to be that all assets on the planet eventually trade on open blockchains, so incumbents' entrance to crypto is merely a matter of time, scale, and asset types. Some firms might be tempted to stay on the sidelines with initial service offerings for a bit longer, and pay up for M&A opportunities rather than false start again on home grown platforms.

If we see a sustained price rally, Wall Street will go shopping.

Conclusion

CeFi and institutional crypto might need to be a whole separate report for me in 2024. I have glossed over a lot at precisely the same time many institutions are re-considering their entrance into the space. June midyear report, perhaps?

Until then, there's more to be excited about in the liquid crypto markets. The rest of this report is about those bubbling opportunities.

CHAPTER 7

TOP 10 TRENDS IN LAYER-1 NETWORKS

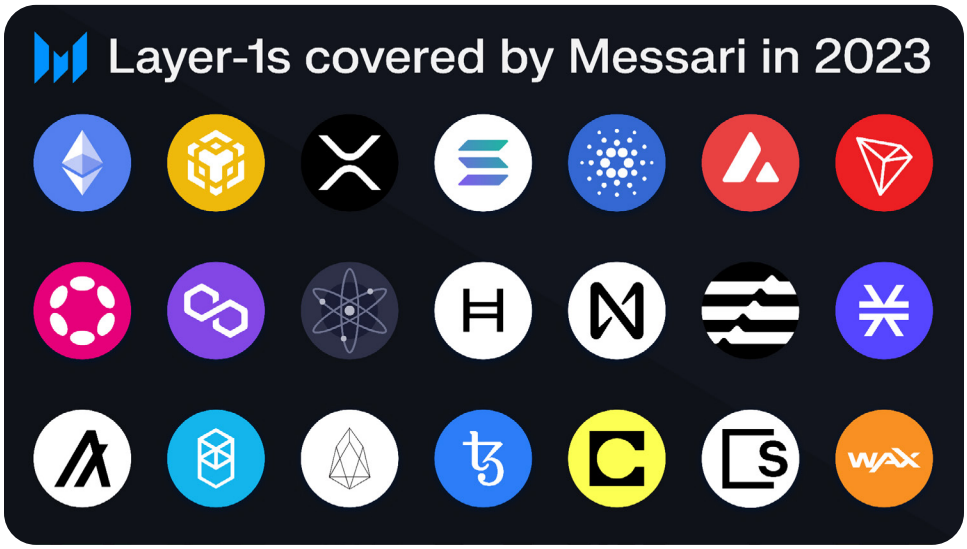
7.0 Networks & Interoperability

This is the first year I've opened this section with a general comparison of crypto networks vs. a headfirst dive into the state of Ethereum. I mean no disrespect - Ethereum had a big year with its long-awaited Shapella upgrade, and its "rollup-centric" vision of the future is picking up steam. But we live in a multi-blockchain world today, and compatibility and interoperability are more important than any one network or roadmap.

That's a good thing.

Fortunately, Messari happens to produce some of the world's top research on networks not named Ethereum. (We're all over Ethereum, too...this isn't zero sum.)

Who's going to be important to keep an eye on in the new year? These reports should help catch up on all of the networks that matter in 2024. (If your project is missing, get in touch!)



Ethereum Q3'23	BNB Chain Q3'23	XRP Ledger Q3'23	Solana Q3'23	Cardano Q3'23	Avalanche Q3'23	TRON Q2'23
Polkadot Q3'23	Polygon Q3'23	Cosmos Hub Q3'23	Hedera Q3'23	NEAR Q3'23	Aptos Q3'23	Stacks Q2'23
Algorand Q3'23	Fantom Q3'23	EOS Q3'23	Tezos Q3'23	Celo Q3'23	SKALE Q3'23	WAX Q3'23

7.1 Ethereal Network Dominance

At this point, many Ethereum purists may not like me very much. First, there was my flagrant disrespect in the opening chapter (ETH will lag BTC and other L1s, if not both next year), and now I'm burying ETH as a mere "peer" in the category it helped create and define? The gall!

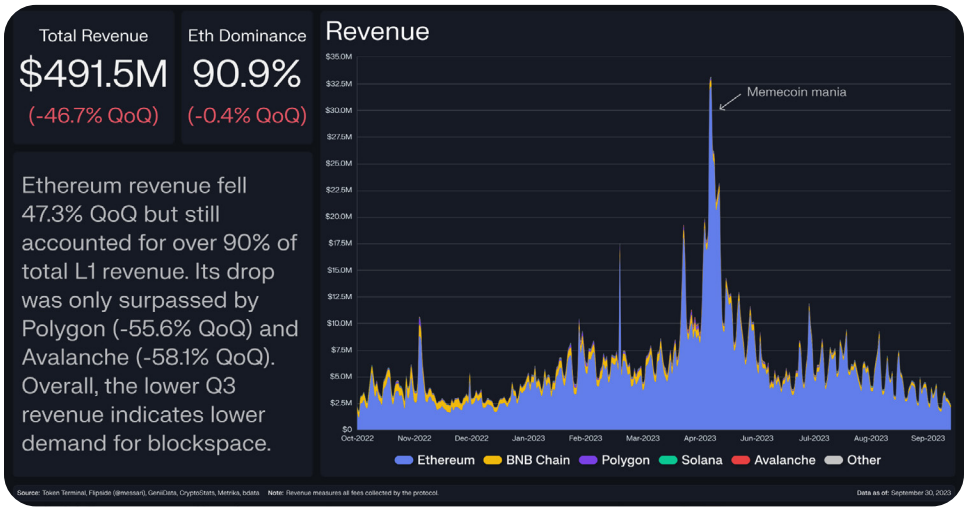
While this was Ethereum's best year yet, and it has proven to be the strongest network by community size and revenue generation (aka fees), we are still in crypto's adolescence, and I have never been more confident that smart contract blockspace is a commodity product.

Most developers will build on the lowest cost, highest performance blockchains, and to the extent they interact with Ethereum, it will be through rollups and bridges. That is not my critique, but rather Ethereum's long-time, explicit direction. Devs and applications will decentralize away from Ethereum, and network token value will likely follow, dispassionately, because no one sings folk songs about database software.

Consider this: the top network for stablecoin settlement is Tron; the top network for tokenized on-chain assets is Stellar; the top network for DePIN is Solana; and the top networks for DeFi are suddenly up for grabs (Maker's "NewChain" could be a Solana fork, dYdX has moved to Cosmos, and most DEX volumes already settle primarily on rollups and other L1s).

It was fitting that Project Guardian's institutional partners hardly referenced Ethereum at all: the big, smart, and powerful money will route around rent-seekers, and will view Ethereum's security model much differently than the crypto faithful (i.e. they won't think it's necessary).

Ethereum does have an advantage in one market segment, though. They crushed it during the meme token rally this spring:



(Source: State of L1s Q3)

If we're talking about fundamentals for network tokens, there's one supply side dynamic that matters (inflation and token burn rate), and two demand side metrics: fee generation and the "expected demand for security."

I've come to believe that network fees (in PoS networks at least) don't matter as much as everyone thinks they do. Even if they do matter long-term, I agree that we are debating their importance prematurely. So let's look at the demand for security model instead.

[Required Reading: The State of L1s Q3 2023]

7.2 Value Accrual and Security in a Multichain World

There are different ways to think about value accrual and fundamentals across various crypto market segments. In DeFi, it probably is fee generation (similar to financial services). In "Layer 1" blockchains, there are additional factors outside of network fees that resemble commodities.

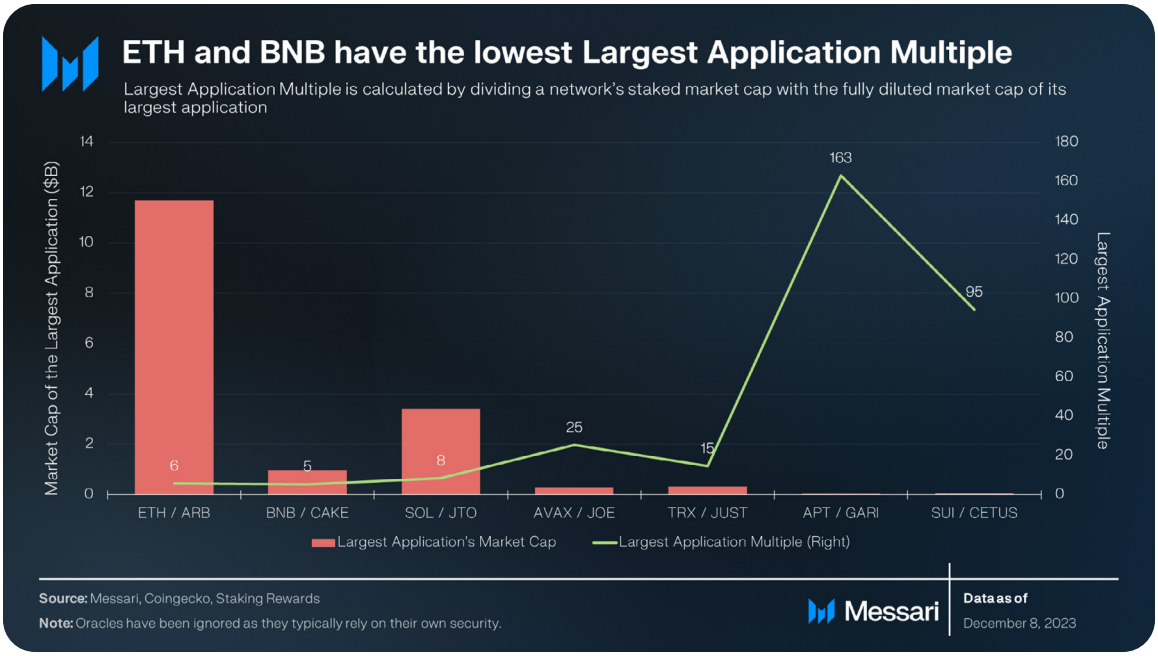
Base chains (Layer 1s) secure all the smart contract apps and rollups deployed on top of the network. Within these apps, the native base chain token can have significant demand as collateral, rollup gas token, or generally as money in addition to transaction fees. Ethereum is a clear example, with over 33% of the entire supply of ETH locked in smart contracts. Modeling out the aggregate demand sinks of the base asset against inflation is the most comprehensive valuation framework - albeit a difficult one.

We introduced a simpler framework earlier this year, which zeros in on the security demand of the largest apps on top of a given chain - the "Expected Demand for Security Model" (EDSM).

In brief, as app protocols or rollups see valuation growth relative to their base native tokens, the application becomes a major customer of the base chain's security (staked market cap). While there is no exact fundamental ratio, the base chain must scale security to serve those users.

Thus, the ratio of the base native token's market cap to the market cap of the largest *app protocol* onchain can be used as a directional valuation multiple. Chains that have relatively low valuations compared to their largest application can generally be expected to appreciate meeting the security demands of the app protocol.

To illustrate, look at the staked market cap of Ethereum (security supply), and you'll see that it's a relatively low multiple of Ethereum's largest application by market cap (Arbitrum), especially when compared to younger chains. That makes some intuitive sense: as demand for Ethereum blockspace picks up and the ecosystem matures, its relatively high network fees will cause some application demand to dissipate (i.e. Ethereum blockspace demand flattens or declines). This is similar to earnings multiples in publicly traded stocks: market leaders trade at lower P/E's than up-and-comers. Even if the market leaders are still growing quickly, their ceiling is lower.



(Kunal published this report the day after we dropped the Theses last year, which shows you why you need to subscribe for the good stuff.)

If we look at fully-reserved stablecoin EDSM, Tron and Ethereum trade at cheap valuations. Again, this isn't surprising, as more stablecoins are expected to bridge to other chains (rollups or alt L1s), and Tron is unique given the many ties between Justin Sun-affiliated apps and overall Tron TVL. The EDSM suggests that Tron is either undervalued, or the market is heavily discounting what they believe to be a high, but relatively noisy, percentage of activity on that network. There will be improvements that can be made to the EDSM over time, but my bet is that this remains a weak signal for traders, and a high signal model for developers and other builders who are considering where they should consider deploying applications.

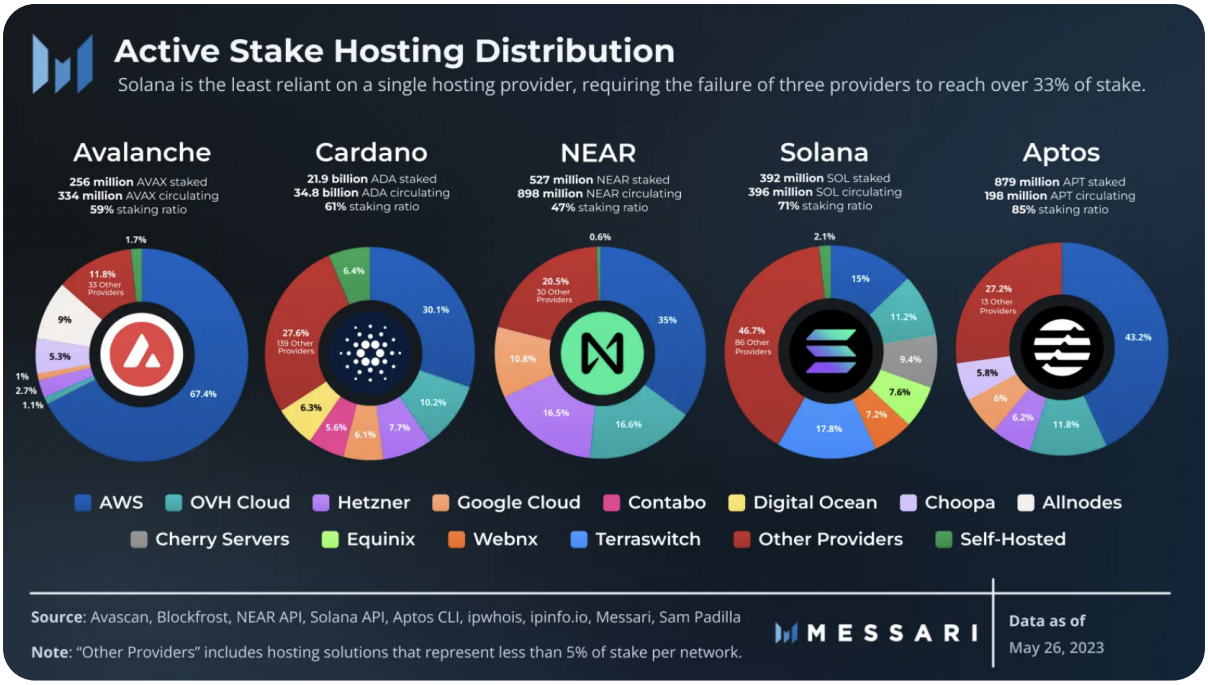
[Required Reading: The EDSM, Quantifying Demand for Security]

7.3 Network Decentralization

I'm slaying a bunch of sacred cows in this chapter.

My hunch is that the decentralization of crypto that really matters is market share among interconnected blockchains. Technical points of centralization still matter, but overreliance on AWS within one crypto community is more tolerable than overreliance on Ethereum by the *entire* community at this point.

We should still track infrastructure concentration closely for signs of centralization risk, especially after Hetzner's ban on crypto operations in August 2022, but I don't think it's worth panicking over whether AWS accounts for the majority of hosted stake for the 10th most popular, two year old L1 network.



In the future, we'll have fully permissioned bankchains, and broadly decentralized public chains...and everything in between. The job of application developers is to determine which network tradeoffs they are going to make for their particular use case.

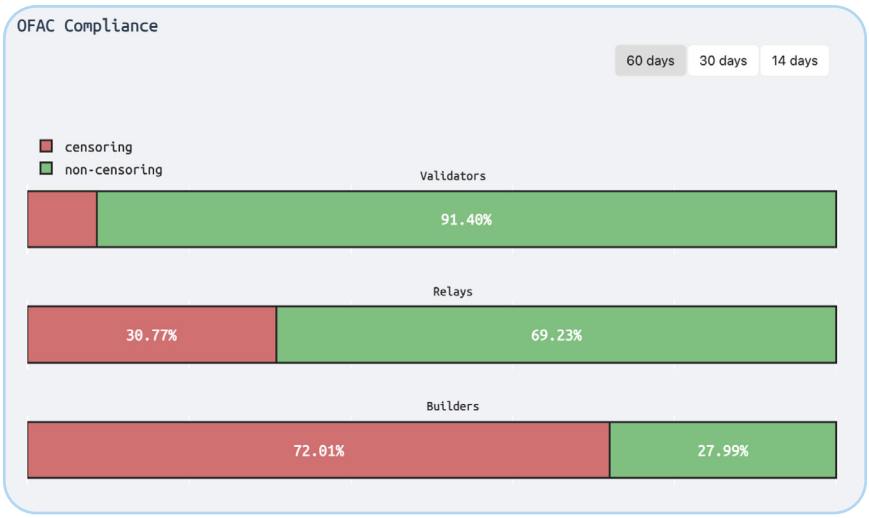
For most networks, centralization concerns are overblown. When they arise, economic concentration and geographic concentration matter just as much, if not more.

[Required Reading: Evaluating Validator Decentralization]

7.4 The Evolution of Censorship Concerns

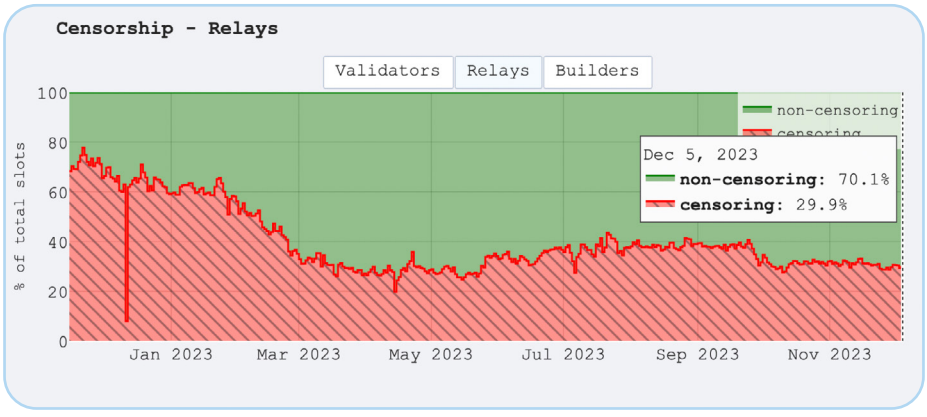
Centralization concerns essentially boil down to two core issues: (1) does a certain vector of centralization lead to network performance issues that put applications at risk of outages, and (2) will centralization create censorship challenges.

One of the interesting things about the disentanglement of block building, relaying, and validation in Ethereum is that it cleanly separates censorship challenges between three different layers of the Ethereum transaction processing stack.



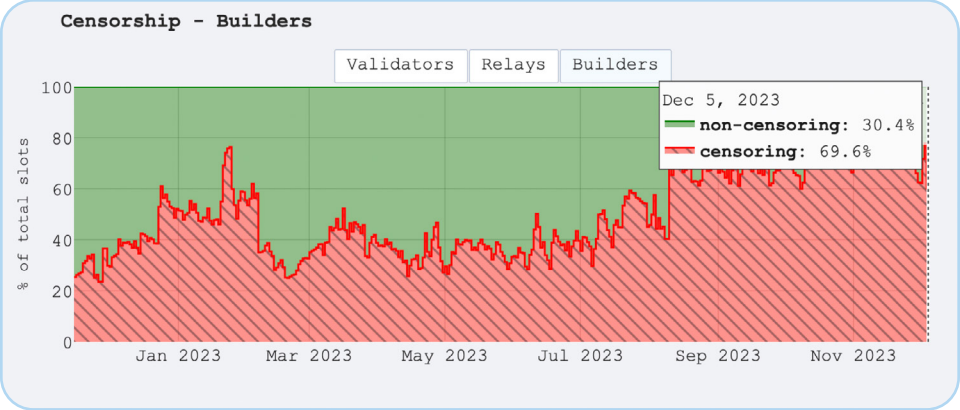
(Source: Censorship Pics)

After the U.S. Office of Foreign Assets Control (OFAC) sanctioned Tornado Cash addresses last summer, major Ethereum relays began to censor transactions. The problem only abated once Flashbots open-sourced its market dominant relay, and allowed permissionless relays like Ultra Sound, Agnostic, and bloXroute to become more competitive.



(Source: Censorship Pics)

Today, it's block *builders* who have increasingly begun to censor transactions. I'd expect some of the biggest development breakthroughs in 2024 to come in areas like mempool encryption that shield transactions from potentially censorious parties before they are included in a block. As always in crypto, we tackle these problems one at a time, when they arise.



(Source: Censorship Pics)

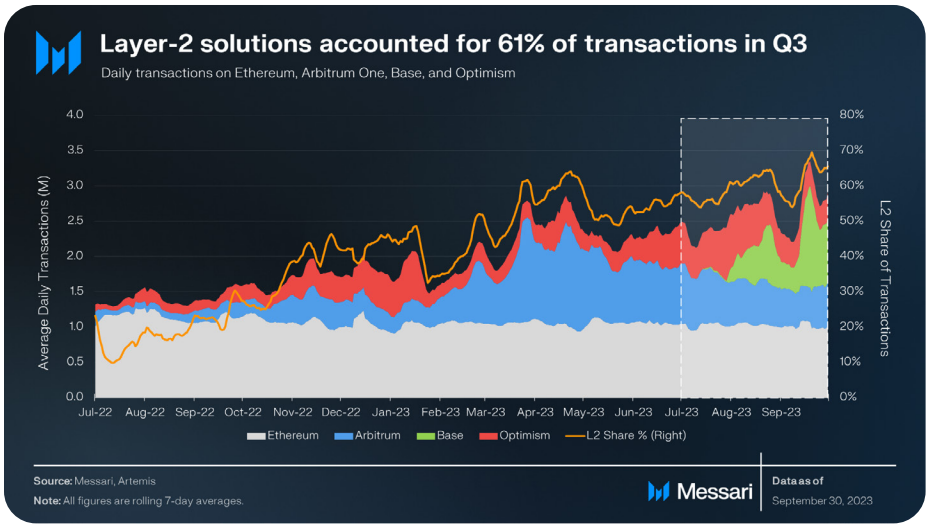
Every network will have to grapple with its own censorship challenges in the years ahead, but I do agree that Ethereum is light years ahead of other communities so far when it comes to considering these challenges and front-running (or quickly addressing) them with solutions.

[Required Reading: State of Ethereum Q3]

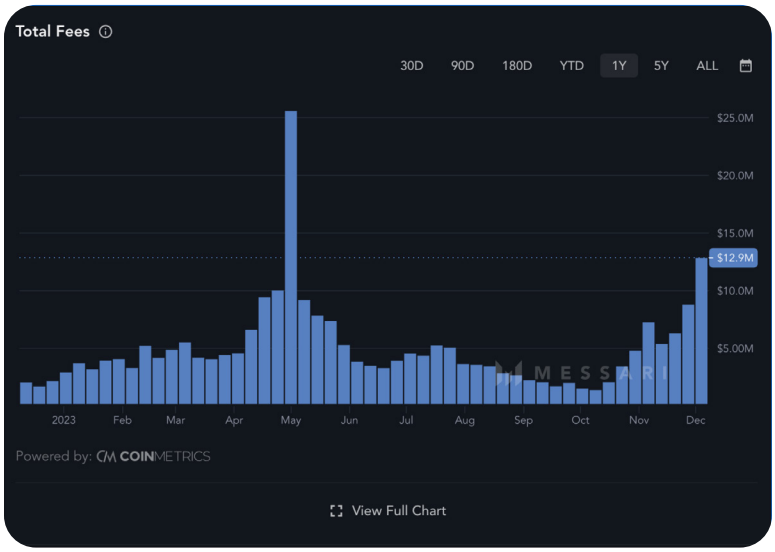
7.5 The Bull Case for Ethereum

I promise you, I'm not trying to intentionally mid-curve the case for ETH. To prove it, I'll give the best case that I can, which counters the FUD up to this point in the report.

1. **Pole Position Matters:** Ethereum has long-established network reliability, a liquid ecosystem, and a $300 billion market cap that is 10x higher than the next largest smart contract network. Ethereum's maturity helps attract rollup and app developers due to the security the network provides. As such, the ETH community is in a prime position to attract developers who have already started to build products that could meaningfully contribute gas fees and transactions to Ethereum's ecosystem.

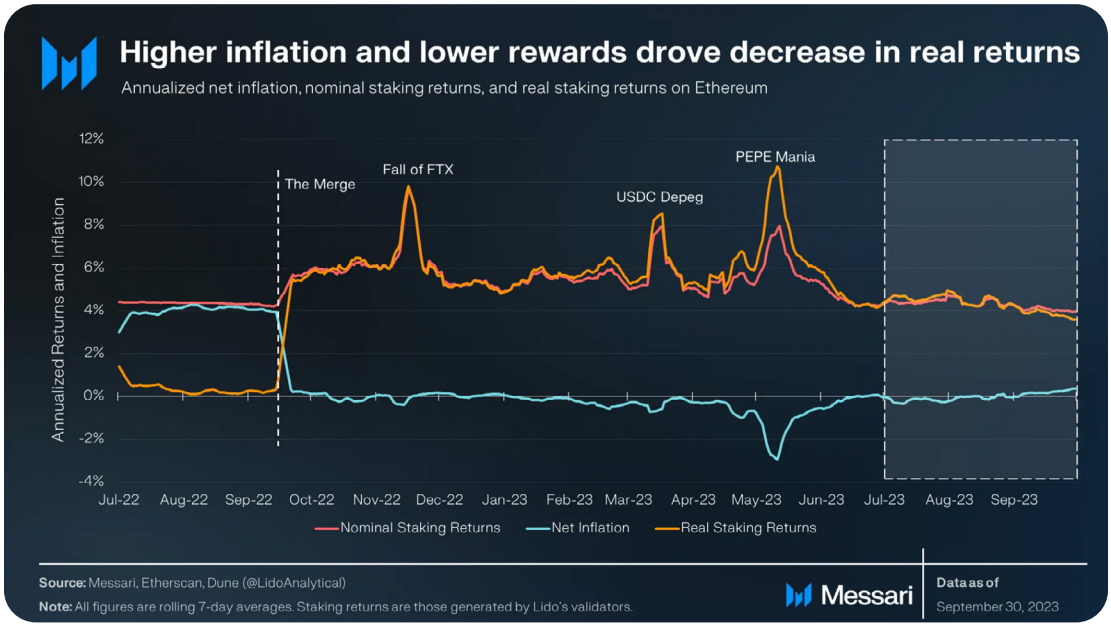


2. **TradFi is Going to Love the Pitch:** If I end up eating my words on ETH's performance in 2024, it will be because I underestimated how much Wall Street will love the ETH pitch. The high growth market leader has a clean / ESG narrative that beats bitcoin's, an ETF that will fast follow the bitcoin spot ETF, a net deflationary supply, and is generating run-rate fees (not ETH rewards, but true fees) of ~$300 million per year. Its 4-5% staking yield will also get more attractive in a declining interest rate environment.



(Source: Messari, Coin Metrics)

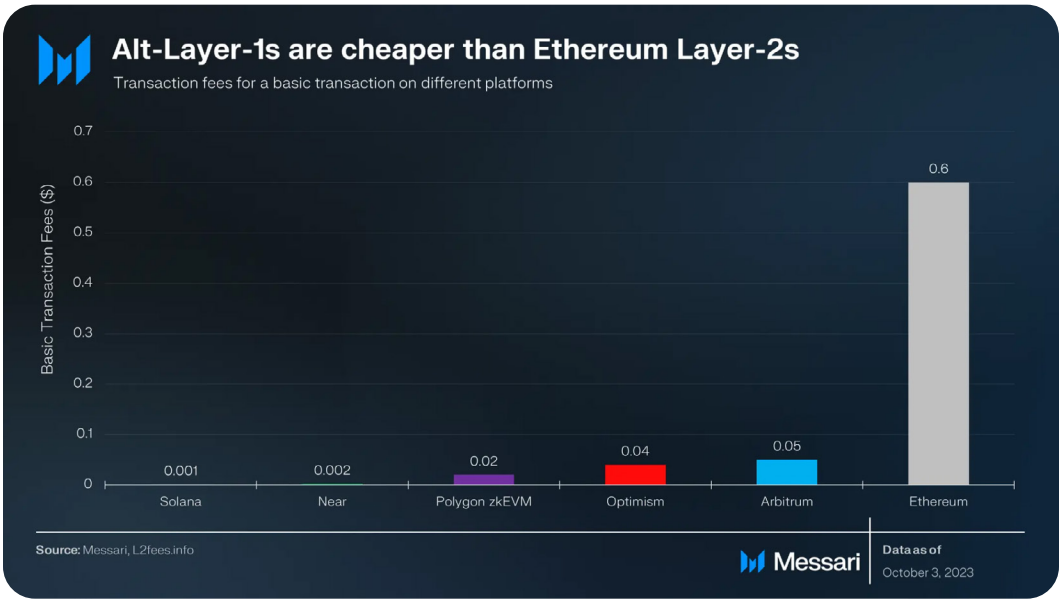
3. **ETH Is Chaotic Good:** Here's something that might be non-obvious, but the world's original decentralized investment bank thrives on volatility and chaos. If bitcoin is a bet against bankrupt central banks, then Ethereum is a bet against morally bankrupt investment banks. Ask yourself if you expect 2024 to be more or less chaotic than this year geopolitically, then look at the three spikes in Ethereum network activity:



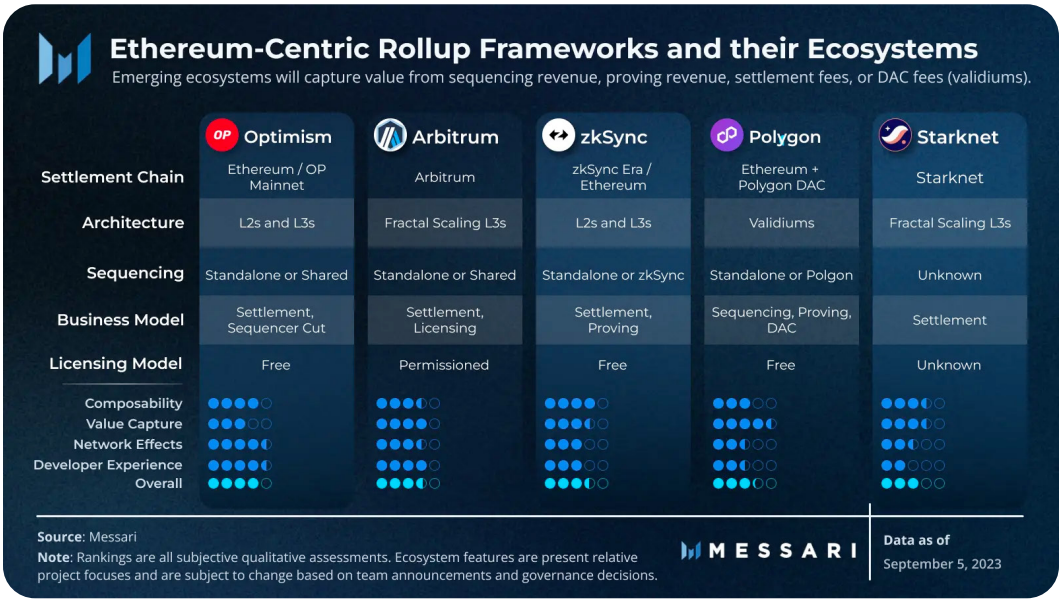
[Required Reading: State of Ethereum Q3 Report]

7.6 Dank Rollups

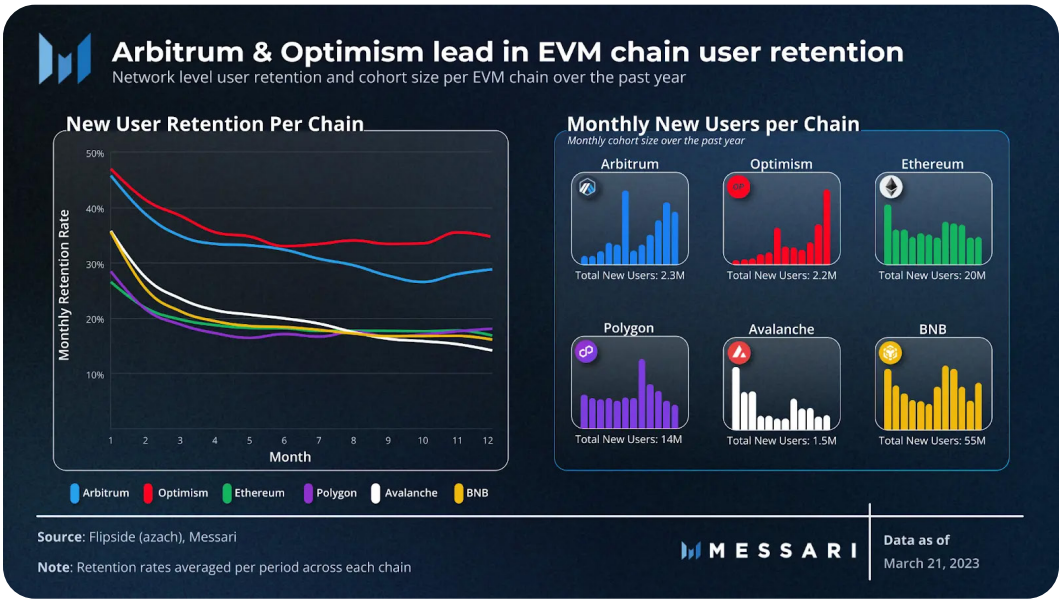
The next upgrade to Ethereum, Cancun-Deneb ("Dencun" is expected in Q1), will reduce transaction costs on rollups by 90-99% by implementing EIP-4844, or proto-danksharding. (You can read about the technical details in our linked research at the end of this section.) That could lead rollup transactions to become as cheap, if not cheaper, than alt-L1s. As such, the Dencun delivery date is one of the most important dates to watch when it comes to the ongoing blockspace wars.



It's not just about one or two rollup chains plugging into Ethereum either. We're talking about composable rollup *ecosystems* with common infrastructure, shared liquidity, and network effects. In the last year, the Optimism Superchain, Arbitrum Orbit, zkSync, Starknet, and Polygon have all announced details surrounding their Ethereum-centric rollup ecosystems, with varying degrees of developer lock-in contemplated in order to extract revenue from the use of their rollup frameworks.



Airdrops for rollup users have been pulling them over from Ethereum L1, but there's a long way to go, and retention still revolves around the availability of token incentives. The Arbitrum and Optimism communities have continued to invest heavily in short-term incentive programs that entice teams to move to their general purpose rollups.



I'm serious, people, at some point, you're going to have to subscribe to Messari's research to get all of the details you need on these networks. There is simply too much for me to cover that would adequately do the rollups space justice. I can't write 30 pages on this, but the team can. See for yourself:

[Required Reading: The Rise of Ethereum-Centric Rollup Ecosystems, The Efficacy of Token Incentive Models, User Acquisition and Retention across EVM Chains, The Rollups-as-a-Service Ecosystem, Arbitrum Ecosystem, Base Legitimacy, Scaling Optimism]

7.7 The Modular Moment

There are two main approaches to building decentralized networks: the “modular” and the integrated.” Integrated architecture refers to a system in which all of a network’s operational functions are integrated in a single protocol, followed by all operators. This includes executing transactions, coming to consensus on their order and validity, and storing the state of the chain.

A integrated architecture usually creates:

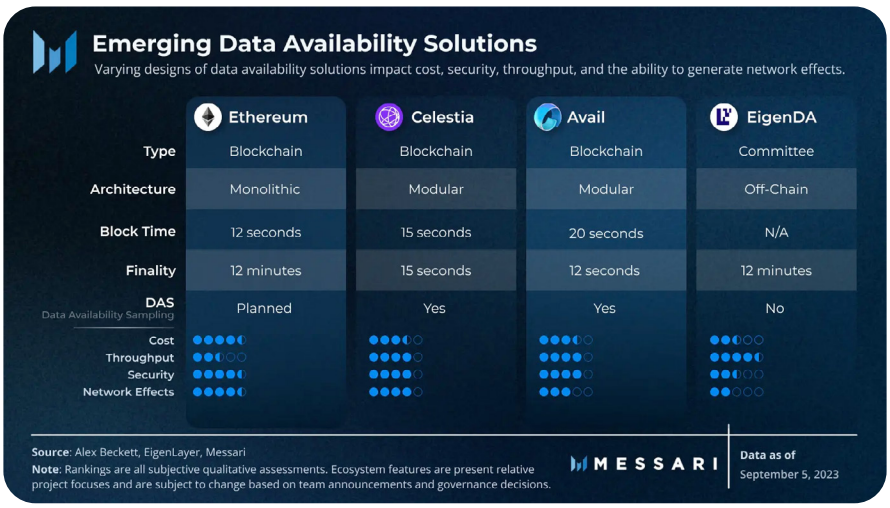
- **Slowdowns in Innovation:** A tightly integrated codebase can delay the introduction and adoption of new features or improvements, reducing the network’s ability to evolve and meet emerging demands.

- **Scalability Challenges:** Applications share execution on a traditional integrated chain which can lead to network congestion, hampering the system’s ability to handle large volumes efficiently and resulting in high fees for users. Operating nodes must participate in all aspects of the network leading to increased computational overhead.

- **Flexibility:** App developers may have different needs and priorities than what is possible within the constraints of a dedicated virtual machine. Integrated systems are also not easily reusable, so developers requiring greater levels of customizability are forced to build whole blockchains as opposed to modifying a single component to their use cases.

Given this, Ethereum went the “modular” route by implementing its rollup-centric roadmap. Rollups allow developers to separate and optimize their execution environments from the settlement, consensus, and data availability (DA) provided by Ethereum L1. Ethereum L1 is also optimizing its role for rollups with the danksharding upgrades as touched on above.

Celestia and friends take the modular concept a step further by offering a purpose built network for rollup DA. By solely focusing on this service, these networks offer cheaper fees and greater throughput for rollups than a general purpose L1. Devs can tailor their DA selection along the cost-security spectrum.



Celestia launched at the end of October, marking the beginning of the modular era outside of EVM ecosystems like Ethereum and BNB Chain. Celestia's TIA token, used for network staking and rollup posting fees, has been having a moment, jumping over 300%....

The challenge for building rollups on Celestia and other alt-DA layers will be the inevitable fragmentation of liquidity. Modular systems will never offer the same composability benefits as a shared state machine, which opens the door to competitors.

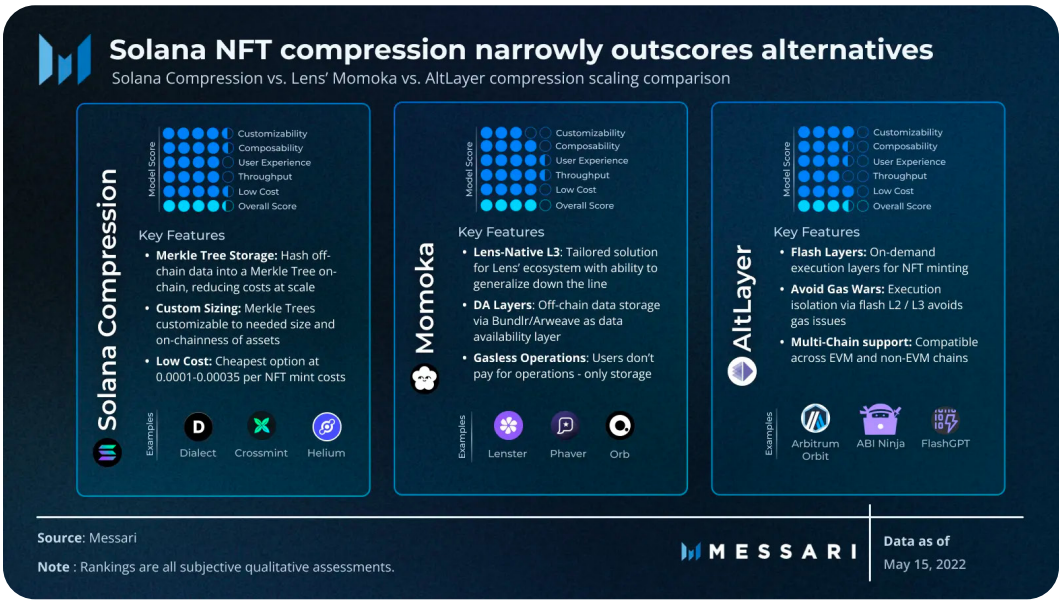
To achieve a seamless inter-rollup transaction experience, interoperability solutions will be critical to prevent ecosystem fragmentation. The end result is likely an interconnected web across various modular ecosystems where users transact without necessarily knowing which rollup or ecosystem they're in—only that their requirements are being fulfilled. Achieving this will involve shared sequencers like Astria and Espresso, current and upcoming bridging protocols like Hyperlane and Polymer, and order flow abstraction networks and intents by Anoma and Flashbots SAUVE.

[Required Reading: The Modular Blockchain Landscape, Celestia Token Launch and Valuation Dynamics, Modular Blockchains Beyond Rollups: A Dive into the Eclipse Mainnet]

7.8 Solana's Resurgence + MOVE It or Lose It

Solana was crypto's comeback player of the year. The ecosystem was left for dead by many in the industry following last fall's FTX collapse, but has since resurged. The torrid pace of new product releases, spike in onchain liquidity, and broadening availability of developer tooling has been a sight to behold.

On the tech side, upgrades like local fee markets, QUIC, and stake-weighted QOS paid dividends in 2023, significantly reducing the downtime Solana had previously suffered in 2022. And NFT compression slashed minting and management costs to Solana, which led to a boom in the DePIN sector as protocols like Helium and Render leveraged its compression capabilities.



Attention now centers around a few major initiatives going into 2024:

- Performance enhancements via Firedancer (Jump Crypto's client that brings 10x+ write throughput improvements, which I covered earlier) and Sig (Syndica's validator client that brings 10x+ read throughput improvements)

- The development of light clients through Tinydancer. One of Solana's most common criticisms is centralization of nodes due to expensive, technically-challenging hardware. Light clients keep expensive *validators* producing blocks honest by allowing low-cost *verifiers* to check their work. Don't take the Solana Foundation's word for it – Vitalik outlined this vision for Ethereum years ago in his oft-cited Endgame post.

- The deployment of the token-22 standard, which extends Solana token functionalities. Token-22 will enable new token types like interest bearing tokens, allowing for native confidential transfers of tokens onchain, and enable developers to create programs that are triggered on token transfers (e.g. programmatic NFT royalties can be enforced at the protocol level).

Tech like local fee markets and state compression enable applications that are "Only Possible on Solana," spanning sectors such as:

- **DePIN:** Projects like Helium, Hivemapper, Render, and Teleport have migrated to Solana. Render recently ditched their own blockchain to take advantage of Solana's compressed NFTs, transaction speeds, and composability with onchain order books.

- **Payments:** Solana holds promise to help power mainstream payment flows - so says Visa who expanded its USDC settlement pilot to Solana. It's possible to transact on Shopify using Solana USDC through Solana Pay's plugin, send crypto with a link using TipLink or Code, and offramp using Beam or Sphere.

- **Consumer apps:** Cheap NFT minting through compression have enabled new consumer use cases to form, such as DRiP and Dialect. DRiP partners with artists to distribute free NFTs to subscribers. Since late March, it has minted over 78 million cNFTs to 1.6 million wallets for a grand cost of 413 SOL (around $0.00036 per NFT).

- **DeFi:** Super cheap fees, fast finality, and protocols like fully onchain order books create a DeFi UX not found on other networks. Even better - a lot of these protocols do not yet have their own token. The wealth effect is real and coming to Solana with recent and upcoming airdrops from Pyth, Jito, Jupiter, and more.

With 907 projects formed in its latest hackathon alone, the odds of Solana hosting breakthrough applications are up only. The SVM has emerged as the industry's clear #2 "operating system."

Solana's achievements have helped reframe not only its own narrative, but also the general narrative around high-performance, integrated networks.

This is especially beneficial for other networks like Aptos and Sui, the two L1s born out of Meta's Diem and Novi projects. One of their many innovations is the Move programming language, which they each have their own flavor of. Move promises application developers enhanced safety and flexibility over Solidity and other Web3 programming languages. Their ecosystems are younger but worth watching. Luckily for you, we cover both (Aptos Q3'23, Sui Deep Dive).

[Required Reading: Reframing the Solana Narrative, Aptos Q3'23, Sui Deep Dive, Solana Landscape, Finality Times in Crypto]

7.9 FHE and ZK Trends

God bless our smart contract developers. They've already built incredible apps with such little computational resources. However, to reach parity with the complex, sophisticated Web2 apps we've all become accustomed to, smart contract developers need access to more compute. This will be a major theme in 2024 – increasing the computation available for onchain apps. ZK coprocessors have emerged to address this issue. Think of these as GPUs in the cloud.

When a smart contract developer needs additional computational resources that would be prohibitively expensive to access natively on Ethereum, they can tap into ZK coprocessors.

For example, imagine Aave wants to offer personalized borrow rates based on complex credit score logic. Inscribing all of that logic onchain and running through the calculations for every loan would likely result in users paying more for just getting a credit score than the actual loan itself! ZK coprocessors allow complex computations to be run offchain, and their ZK properties enable anyone to verify that the computations were correctly processed. As a whole, smart contract developers can access cheap, verifiable compute.

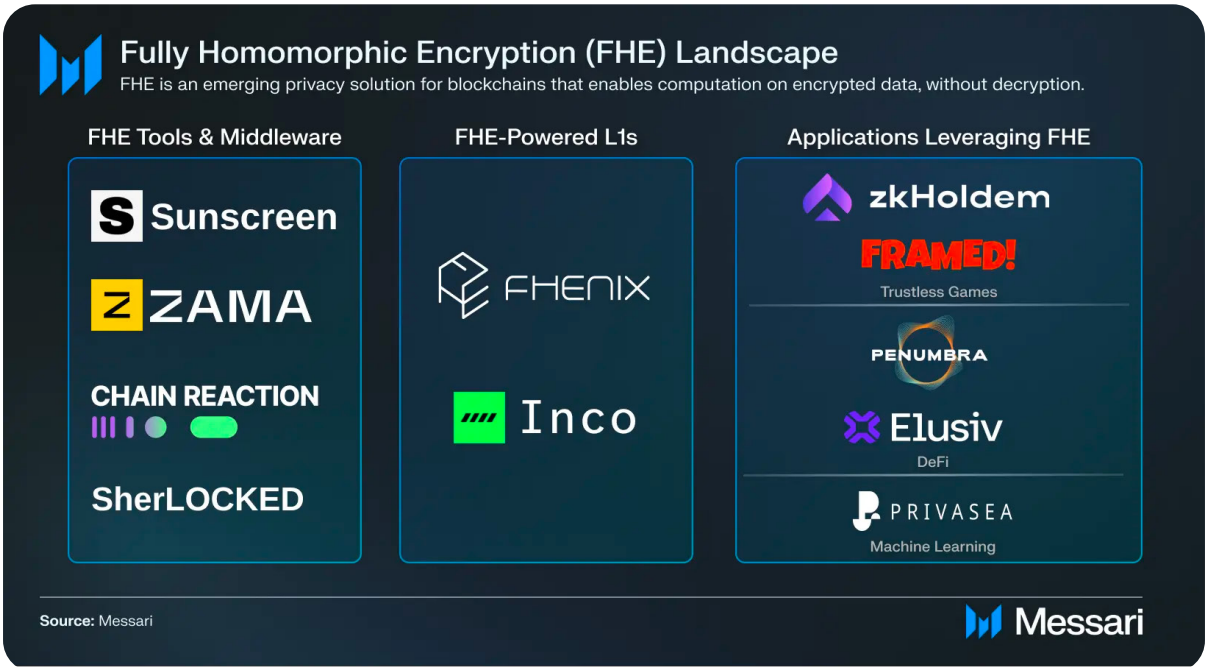
An important aspect of ZK coprocessors is that they empower app developers to shift their focus away from zk-related concerns and concentrate on other aspects of their technology stack. Devs won't have to worry about needing the infrastructure or know-how to generate zk proofs.

There's a downside to ZK coprocessors: they don't enable privacy, but rather rely on third-party "provers" to generate computationally expensive proofs. These proofs require access to input data, so in our hypothetical Aave credit score example, users would have to trust third parties with potentially sensitive and personal data. This design echoes the trust dynamics of Web2 cloud computing, with users relying on and trusting these entities to safeguard their data.

That's where Fully Homomorphic Encryption (FHE) comes in.

Essentially, FHE enables an entity to compute directly on encrypted data (yes, it sounds like black magic, but it's real).

FHE has been a topic of academic discussion since 1978, but recent practical advancements have positioned it for real-world deployment. FHE R&D has surged recently, driven by tech giants (like Meta, Google, Amazon) responding to stringent data laws like GDPR and government agencies boosting funding amid rising cyber threats. For companies reliant on targeted advertising, the capacity to compute over customer data without compromising privacy compliance is crucial.



Within crypto, FHE is set to broaden the spectrum of possibilities. The most anticipated breakthrough is an FHE-enabled smart contract platform, which would enable end-to-end encryption for public blockchains (Fhenix is working on this) and keep all *onchain data* private. Even validators would not be privy to FHE transaction data, potentially eradicating MEV and providing better privacy for businesses and individuals.

Besides FHE-enabled smart contract platforms, FHE could be used for private payments, trustless games, private voting, private machine learning, and creating a private data economy.

ZK coprocessors and FHE are powerful, new cryptographic primitives. They are in their infancy, but will be among the most powerful innovations in crypto this decade.

[Required Reading: Fully Homomorphic Encryption, Scaling with ZK Coprocessors]

7.10 The Evolution of Bank Chains

We're living in a moment where everyone wants to run their own blockchains. Successful applications are considering moving to custom blockchains on Cosmos, forking Solana, or creating their own rollups. Institutions are taking it one step further still: many are insisting on managing their own private chains, reminiscent of the companies in the early 2000s who thought they would run their own cloud.

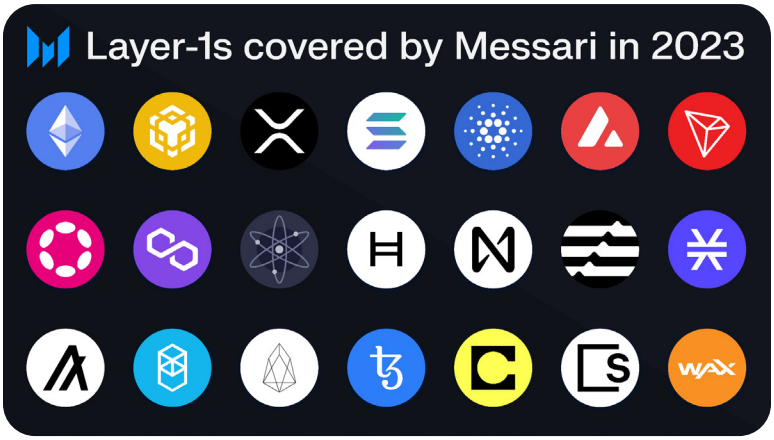
But just as intranets fell into the dustbin of history, and internal server management died at the hands of the dominant Big Tech-run cloud, purely private blockchains will eventually die off as well. Even though banks have the budgets and IT teams to manage private blockchains, there is no way they will be able to properly maintain their infrastructure as effectively as the public, open-source platforms. Even the stodgiest institutions will default to joining public blockchains as soon as we get some rules of engagement for institutional entrants (there's that public policy theme again).

The only exception (if there is one) might be JPMorgan's Onyx, which is the only bank chain I think is worth tracking at this time.

As I wrote in Chapter 5, our political success in the U.S. is not a foregone conclusion. Keeping an eye on Onyx's design and ongoing developments will be important for those who want to stay in crypto within the U.S. if things don't go crypto's way next November.

Conclusions:

I'm not going to lie: drafting this section was the first time that I felt I had met my match in wrapping my head around all of the year's developments. I'll reiterate what I've said throughout. There is too much going on to truly do justice to the core themes in crypto network development, but I hope this scratched the surface enough for you to dive in more.



Ethereum Q3'23	BNB Chain Q3'23	XRP Ledger Q3'23	Solana Q3'23	Cardano Q3'23	Avalanche Q3'23	TRON Q2'23
Polkadot Q3'23	Polygon Q3'23	Cosmos Hub Q3'23	Hedera Q3'23	NEAR Q3'23	Aptos Q3'23	Stacks Q2'23
Algorand Q3'23	Fantom Q3'23	EOS Q3'23	Tezos Q3'23	Celo Q3'23	SKALE Q3'23	WAX Q3'23

Industry Leaders Trust Messari Protocol Services

50+ top DeFi, Web3, and Layer-1 protocol teams and DAOs choose

Messari Protocol Services.

Our in-house analysts, experts in their fields, deliver independent, in-depth research reports. Simplify your financial reporting and stakeholder communications with our comprehensive Messari Quarterly Reporting.

Visit **messari.io/protocol-services** to learn more or contact **sales@messari.io** to schedule a demo.

Get In Touch

CHAPTER 8

TOP 10 TRENDS IN DeFi

8.0 DeFi is Back?

DeFi represents just under 0.01% of the approximate $510 trillion value of global financial assets. That represents some...headroom...for growth.

Last year provided evidence that onchain financial rails offering transparent and instant settlement can provide greater safety and lower fees under the same stress conditions as off-chain financial rails. DeFi held up well when Luna collapsed, when FTX went bankrupt, and when the U.S. banking system froze up.

Even the IMF estimates that DeFi applications have the lowest marginal cost of capital by 3x due to slashing operational costs (and margin!).

The move towards a more regulated DeFi might prove to be inevitable. I'm not necessarily giving up the fight, but many top projects seem to be preparing for rigorous oversight.

This will spark product changes that make it look as though we are re-intermediating finance in some cases, but the better way to think about DeFi in a post-regulation age is like a bridge: jurisdictions that require lots of intermediation for regulatory reasons may treat front-end operators like financial intermediaries, but Wall Street will also finally be able to (if not incentivized to) start some of these store-fronts themselves, and more volume will flow over public blockchains over time as a result.

It's the beginning of a gradual multi-decade technical upgrade, not dissimilar to how financial firms adapted to the internet.

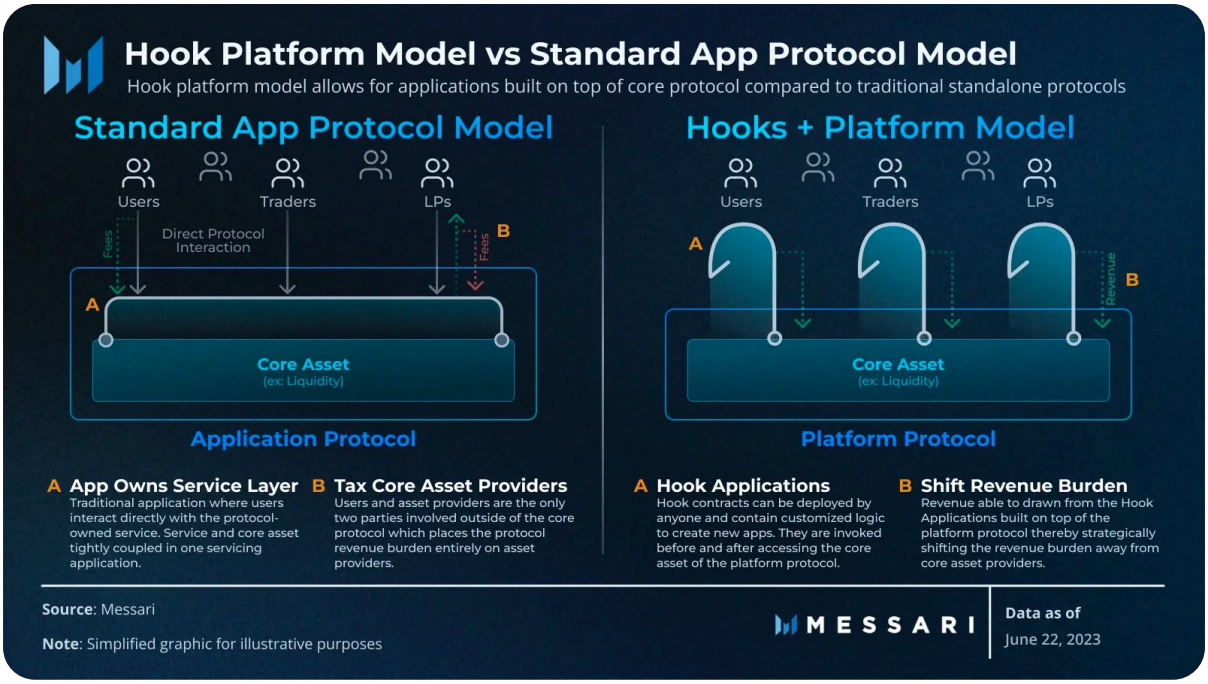
8.1 DEX Platform Updates

Uniswap's dominance in the DEX space continues - on Ethereum at least. It even eclipsed Coinbase in volumes in March (SVB crisis) and May ($PEPE boom) this year.

The automated market maker pioneer continued to lead DeFi through the bear:

- The Uniswap DAO (which governs the core DEX protocol) launched Uniswap on rollups, consolidating its lead across the Ethereum ecosystem.
- Uniswap Labs launched a mobile wallet to lock in its users.
- Labs unveiled its plans for Uniswap V4.
- Labs turned on fees for their front-end (more on this in 8.2).

V4 introduced "hook contracts," creating DeFi's first "platform moment." Developers looking to deploy new features (on-chain limit orders!) and custom trading strategies can now build on top of the core libraries. Protocols become platforms. Maker, Synthetix, Morpho and others are building on this trend heading into 2024.



Ally showed how Uniswap has retained market share across user segments. It will be difficult for any other DEX to supplant its dominant position on Ethereum and its rollups (Uni V3 is top dog in volume on Arbitrum, Optimism, Base, and Polygon) without a major differentiating feature set. (Hashflow is one that looks interesting: they have a request-for-quote model, strong backers, and will be deploying their v2 with Smart Order Routing on Solana.)

Other chains remain up for grabs: TraderJoe dominates on Avalanche, Osmosis remains #1 in the Cosmos, Orca sits atop Solana's exploding DeFi ecosystem, and PancakeSwap is still basically the only game in town on BNB Chain. I'd keep an eye on the projects below in 2024 if we see a combination of a) regulator-led asset delistings at major Western centralized exchanges, b) a melt-up in token prices following a Bitcoin ETF-driven rally, and c) the return of the "hot ball of money" trade for Solana, Cosmos, and non-Ethereum based DeFi.

	Asset	Price Current	Price 12H Change	Price 24H Change	Price 7D Change	Marketcap Current	Real Volume 24H	Sector	Price 30D Change	Price YTD Change
1	PancakeSwap CAKE	$2.41	-1.73%	-1.90%	+5.55%	$618M	$31.06M	Exchange	+9.75%	-23.85%
2	Curve CRV	$0.641	+3.85%	+2.69%	+15.05%	$562M	$64.27M	Exchange	+15.04%	+21.82%
3	dYdX DYDX	$2.98	+1.71%	+0.06%	-7.65%	$522M	$112M	Exchange	+23.31%	+163.22%
4	Osmosis OSMO	$0.746	-1.07%	-2.51%	+7.63%	$466M	$3.06M	Exchange	+46.68%	+8.52%
5	SushiSwap SUSHI	$1.31	-0.17%	-3.25%	+1.86%	$250M	$36.18M	Exchange	+35.73%	+38.47%
6	Balancer BAL	$4.24	+0.47%	+0.43%	+16.00%	$223M	$4.13M	Exchange	+16.28%	-18.58%
7	Orca ORCA	$2.52	-4.47%	-8.09%	-27.71%	$118M	$951.73K	Exchange	+46.53%	+489.81%
8	Bounce AUCTION	$16.09	-7.53%	-13.35%	+30.60%	$114M	$149.10K	Exchange	+125.82%	+302.62%
9	Kyber Network Crystal KNC	$0.741	-0.51%	+0.74%	+3.88%	$112M	$8.42M	Exchange	-6.07%	+62.78%
10	Bancor BNT	$0.778	+0.18%	+0.41%	+3.46%	$103M	$4.91M	Exchange	+35.06%	+116.35%

(Source: Messari)

[Required Reading: Uniswap V4 + Platforms in Crypto, DeFi Verticalization]

8.2 Trading Aggregators & Front-Ends

The problem with the "decentralized" in DeFi is that it has an undercurrent that suggests your community would be ok limiting its potential take rate. What we've seen repeatedly in DeFi this year has been quite the opposite.

Following the announcement of Uniswap V4, Uniswap Labs announced a 0.15% fee on transactions made on its Uniswap Labs-owned web UI and Wallet. The *company* is now making $1 million per month in front-end fees, as the new fee structure sits atop what the underlying protocol charges users on behalf of its liquidity providers. This looks like a double dip, and I hate the optics, as does Haseeb.

But I'll also defend it for a couple of important reasons:

1. **Regulatory Realism:** DeFi regulation in the U.S. is in a precarious spot, and there's a good chance Uniswap is dealing with a bevy of legal issues that force their hand. I don't think anyone is happy with the idea of "regulating front-end interfaces like brokers," but some investors are promoting this as the least bad option given the impossibly hostile regulatory backdrop, not to mention the alternative - ignoring policymakers' call to act as a broker that collects user information, reports taxes, and cooperates on KYC/AML and market manipulation investigations might not be a smart position to take.

2. **Credible Decentralization:** In light of the regulatory situation, it's healthy to cleanly separate Uniswap Labs from the protocol it helped spawn, as well as the Uniswap Foundation. Though you could see how this all would be confusing, right? The UNI supply that was initially distributed to the Labs and Foundation entities and their teams and investors has mostly vested:

Category	Allocation	Unlocked So Far	Unlocks Remaining	% Unlocks Completed	Vesting Description	Assump
Community Treasury	430.00M UNI	396.49M UNI	33.51M UNI	92%	Four year linear vesting with 40% unlocked in Year 1, 30% unlocked in Year 2, 20% unlocked in Year 3, and 10% unlocked in Year 4.	--
Team & Future Employees	212.66M UNI	171.06M UNI	41.60M UNI	80%	Four year linear vesting.	--
Investors	180.44M UNI	145.14M UNI	35.30M UNI	80%	4 year linear vesting.	--
Airdrop	150.00M UNI	150.00M UNI	0.00 UNI	100%	Retroactive airdrop made available to LPs, users, and SOCKS holders / redeemers at token genesis	--
Liquidity Mining	20.00M UNI	20.00M UNI	0.00 UNI	100%	60 day liquidity mining program from September 18, 2020 to November 17, 2020.	--
Advisors	6.90M UNI	5.55M UNI	1.35M UNI	80%	4 year linear vesting.	--

(Source: Messari Token Unlocks)

3. **Opt-outs are Available:** Users can opt out from using the Uniswap front end if they so choose, and leverage aggregators like 1inch or 0x's Matcha. Yes, the defaults will matter for most users, but this still seems ok, and it's incumbent on new entities (particularly those operating internationally) to compete away Uniswap Labs' incumbent advantage with a better product.

(Source: 0x Q3 Brief)

The projects I'm watching most closely in the aggregator space are 0x, which has now caught and surpassed its top competitor, and 1inch, after settling charges with the CFTC.

Solana DEX aggregator Jupiter is interesting for another reason: Solana traders are opting to use the community's leading aggregator in greater percentages than the leading DEX, Orca.

This could be a hint of things to come as interfaces add additional value on top of the onchain protocols they route transactions to. With additional tooling like UniswapX or Jupiter's DCA tool, interfaces can win customer acquisition battles and capture value.

[Required Reading: 1inch Quarterly, Matcha Q3 Brief, 0x Q3 Brief, Uniswap: Zero to Infinity]

8.3 Payments!

Could this be the year that Lightning finally takes off?

(Source: Bitcoin Visuals)

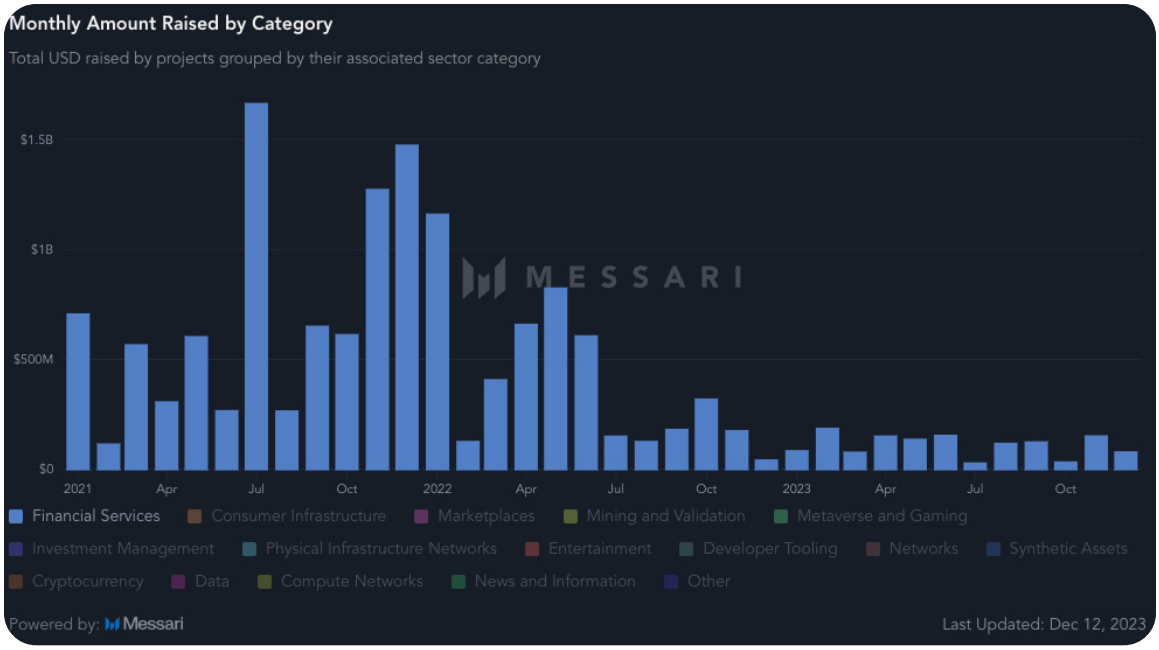
While I don't like making a habit out of betting against people like David Marcus, after five years of development, I would have expected the Lighting Network to have more capacity than TerraClassicUSD, but USTC post-LUNA collapse is still twice as large. OOF.

There are some *other* killer payments protocols coming live that will change how we transfer crypto as a 10x improved payments system vs. the traditional banking rails.

The new functionality these protocols provide can be broadly categorized as streams (continuous, real-time micropayments for content, subscriptions, token vesting, etc.), splits (smart distributed payments amongst a group of recipients according to predefined logic, like royalties), and smart payments (abstraction layers that handle complex payment logic on behalf of users. Basically all the companies raising tons of VC funding: Sphere, Decent, Solana Pay).

These are the tools that AI agents (and DePIN networks) will use to pay one another, not JPMorgan, and they serve as the financial backbone for new types of DeSoc networks (Lens V2) where synergistic actions between users are rewarded with programmatic payments.

Investment in the space fell to just under $500 million after $6.5 billion poured in the previous three years. That is a return to normalcy, not the death of the business.

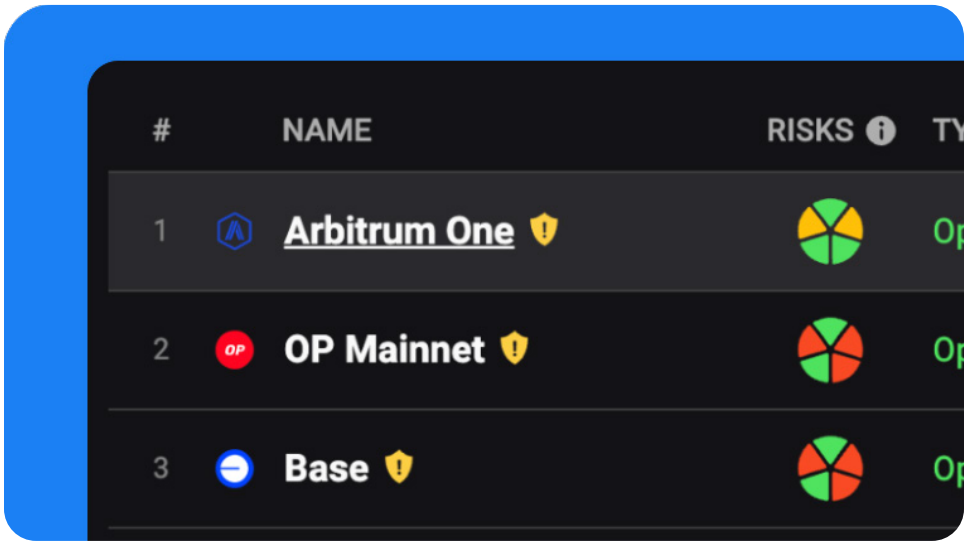


(Source: Messari Chartbooks, Fundraising Data)

[Required Reading: Web3 Payments: Catalyzing Crypto's Next Wave of Application Innovation]

8.4 On-Chain Perps

This year, DEX spot volumes averaged around 15% of CEX volumes, with Uniswap leading the way. But when it comes to futures and perpetuals - the lifeblood of the CeFi markets with 70% of all trading volumes - DEX market share is an order of magnitude smaller, averaging between just 1.5-2.0%. dYdX is even more dominant than Uniswap, with 70%+ market share in its sector, and a big year upcoming in 2024 with its v4 upgrade.



dYdX has been one of the most popular DeFi applications on Ethereum, leveraging StarkWare's L2 infra for its platform, which by itself is currently the fifth largest rollup

by TVL. That capacity should increase with the migration to dYdX V4, after the project launched its own customized, standalone Cosmos chain in October. The dYdX central-limit order book model more closely reflects the trading experience most perps traders are familiar with, so odds are good that dYdX can close some of the market share gap with CeFi given the stresses those (mostly offshore) platforms have been dealing with amidst an ongoing regulatory crackdown.

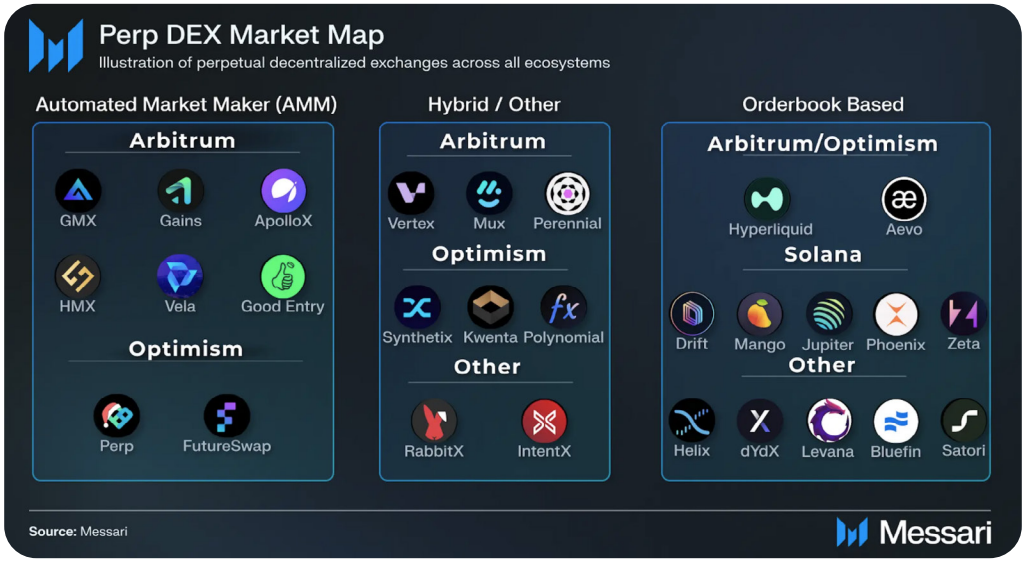
#	NAME	RISKS	TYPE	STAGE	PURPOSE	TOTAL	MKT SHARE
1	Arbitrum One		Optimistic Rollup	STAGE 1	Universal	$8.45B ▲ 6.50%	52.48%
2	OP Mainnet		Optimistic Rollup	STAGE 0	Universal	$4.59B ▲ 15.04%	28.53%
3	Base		Optimistic Rollup	STAGE 0	Universal	$629M ▲ 2.31%	3.91%
4	zkSync Era		ZK Rollup	STAGE 0	Universal	$560M ▲ 6.29%	3.48%
5	dYdX v3		ZK Rollup	STAGE 1	Exchange	$360M ▲ 6.08%	2.24%

(Source: L2 Beat)

The market already took note of the opportunity for dYdX this year: among DEX tokens over $100 million in market cap, it's been the third best performer (behind only 0x and Orca), after notching a 170% gain through the end of November. The only things holding back dYdX are a successful migration of its markets to V4, and its (still significant) token overhang (just 42% of its token supply is outstanding today).

Aside from the Solana DEXs (Drift and Jupiter, in particular), one major alternative to watch is DeFi OG Synthetix: its Andromeda Release is upcoming, will introduce cross-margin functionality, support multiple new collateral types, and a range of other trading improvements (access controls, liquidation improvements, etc.), plus an attractive change to the SNX token's fee share dynamics. It trades at a third of dYdX's fully diluted valuation, and was the fourth best DEX performer YTD.

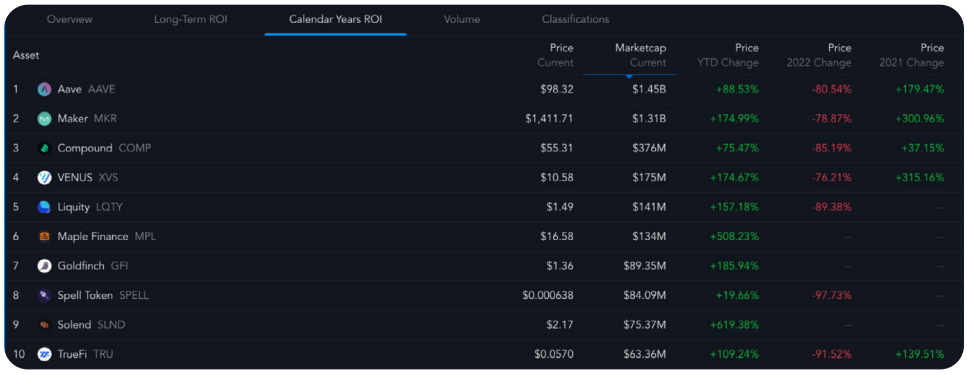
If you're going to watch one sector in DeFi this year, it should be the Perp DEXs:



[Required Reading: Analyzing dYdX Tokenomics, Perp DEX Deep Dive, State of SNX Q3, Perp DEX Token Cheat Sheet]

8.5 DeFi Lending

The CeFi lending markets wreaked havoc on crypto in 2022, and their disastrous effects on the centralized lending market (plus rapidly increasing interest rates) had spillover effects in the DeFi lending markets. But things are slowly coming back, and I'm not sure I can be friends with you if you don't think that the top 10 DeFi protocols (in aggregate) will still be worth less than the world's 216th largest bank by market cap in five years. (Synovus!)



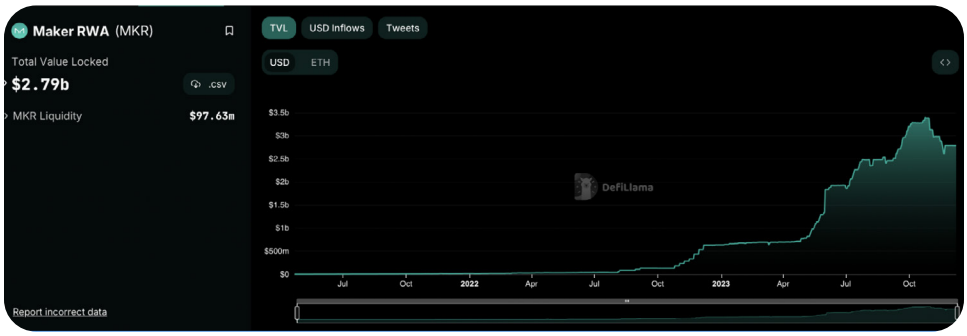
Overview | Long-Term ROI | Calendar Years ROI | Volume | Classifications

	Asset	Price Current	Marketcap Current	Price YTD Change	Price 2022 Change	Price 2021 Change
1	Aave AAVE	$98.32	$1.45B	+88.53%	-80.54%	+179.47%
2	Maker MKR	$1,411.71	$1.31B	+174.99%	-78.87%	+300.96%
3	Compound COMP	$55.31	$376M	+75.47%	-85.19%	+37.15%
4	VENUS XVS	$10.58	$175M	+174.67%	-76.21%	+315.16%
5	Liquity LQTY	$1.49	$141M	+157.18%	-89.38%	--
6	Maple Finance MPL	$16.58	$134M	+508.23%	--	--
7	Goldfinch GFI	$1.36	$89.35M	+185.94%	--	--
8	Spell Token SPELL	$0.000638	$84.09M	+19.66%	-97.73%	--
9	Solend SLND	$2.17	$75.37M	+619.38%	--	--
10	TrueFi TRU	$0.0570	$63.36M	+109.24%	-91.52%	+139.51%

(Source: Messari)

If anything, DeFi lending is the one sector where you can win thrice:

1. The trend towards real-world asset tokenization is mostly captured in two areas: yield-bearing stablecoin holdings at exchanges like Coinbase and DeFi lending protocols. For example, Maker's reserve composition has shifted towards tokenized treasuries, up from $40 million in mid-2022 to nearly $3 billion today.



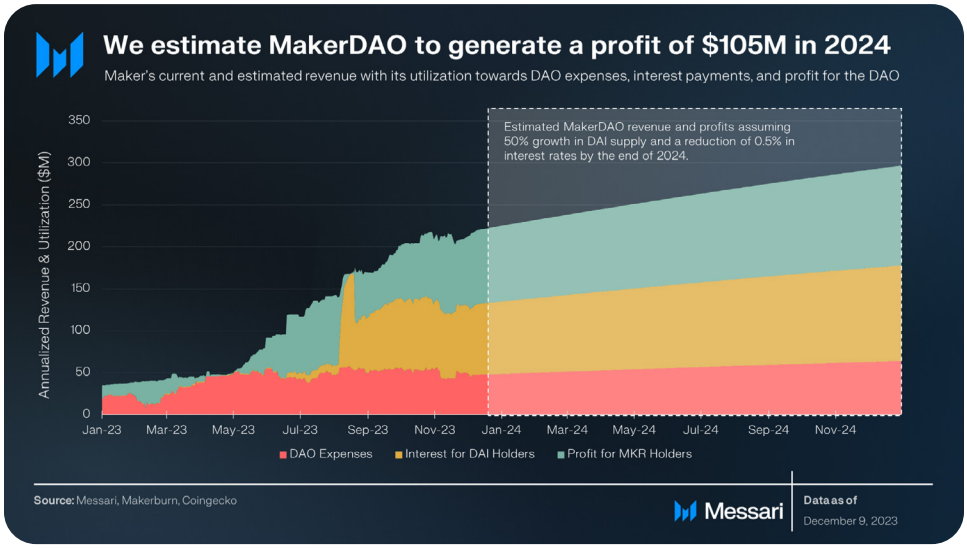
(Source: DefiLlama)

2. They're safer than CeFi lending services because they're more transparent and easier to scale globally. They held up well vs. their CeFi counterparts amidst the Luna, FTX, and SVB crises over that tumultuous 12 month period, and have kept on ticking without much fanfare.
3. LSTs have become a popular collateral type for MKR, constituting 26% of deposits. As more DeFi-native investors seek to juice their yields, having an interest-bearing collateral (like Lido's stETH) backing a Maker vault will further widen the spread between the attractiveness of CeFi and DeFi loans.

Security concerns (rugpulls, oracle attacks, bridge hacks, etc.) remain an issue, but DeFi

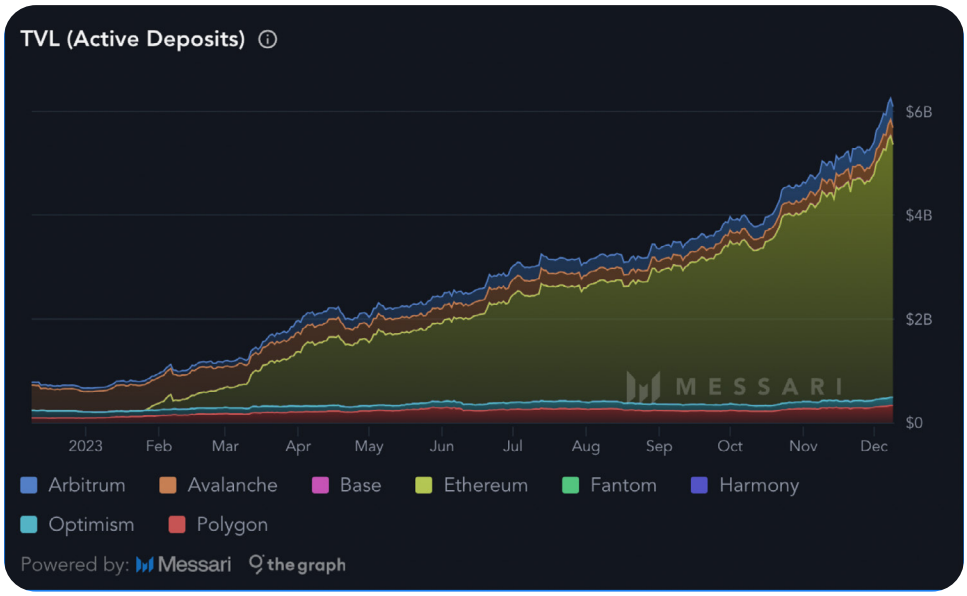
gets more antifragile over time, and the OG protocols have a Lindy effect.

Maker, in particular, feels like a "value investor" dream, to the extent any TradFi investors look to deploy to liquid crypto markets beyond the major network tokens. MKR now trades at a forward PE of...13ish? Simply incredible.



(Source: Messari)

Aave's TVL is up 80% YTD, too, driven by adoption of Aave v3 and the proliferation of LSTs as collateral assets this year. Aave V3 introduced a new efficiency mode that allows higher loan-to-value ratios for correlated tokens like ETH and stETH, further juicing staking yields. It hasn't been all sunshine and rainbows: Aave's long awaited stablecoin (expected to be a big revenue driver and new business model for the money market businesses) stumbled out of the gates, but this is hardly a stagnating project.



(Source: Messari)

[Required Reading: DeFi Business Models Converge, Meet Your Maker, Maker Mistaker, Aave v3 Goes to Ethereum Mainnet]

8.6 LSTs

Liquid Staking Tokens (LSTs) are yield-bearing IOUs issued by liquid staking protocols and have become the largest DeFi sector by TVL.

I covered Ethereum's liquid staking derivative juggernaut, Lido, in the "products to watch" section, as that might be interesting for the TradFi folks and new entrants reading this report. But Lido is an obvious pick for anyone who's deep in the crypto weeds and who understands Ethereum's emerging liquid staking derivatives market.

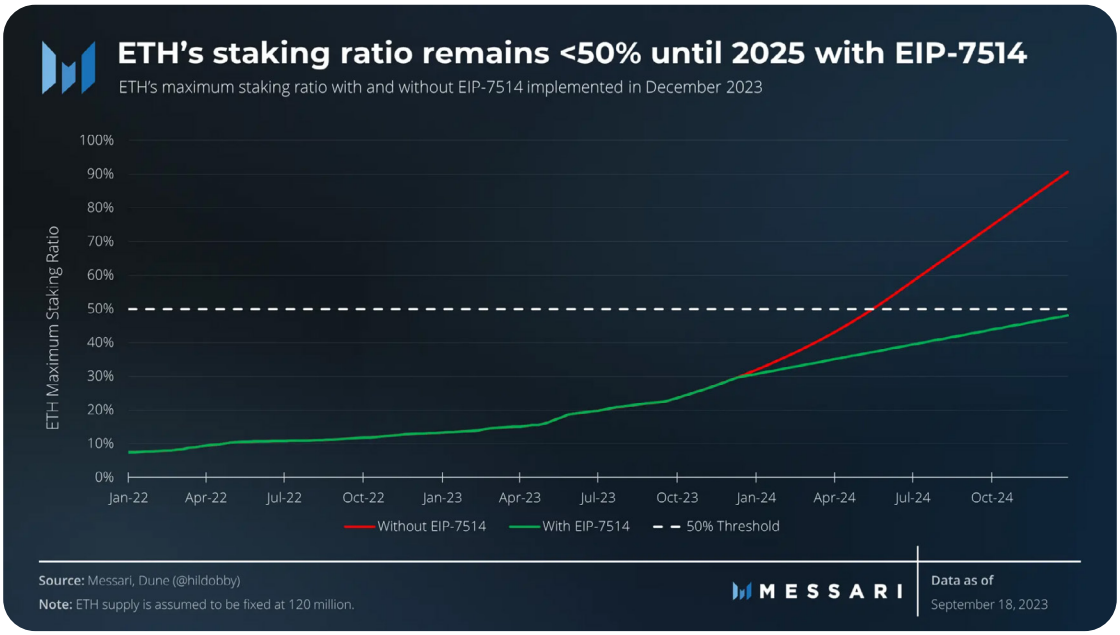
There are a number of others to watch, as well:

	Asset	Price Current	Marketcap Current
1	Lido Staked Ether STETH	$2,205.71	$20.50B
2	Rocket Pool ETH RETH	$2,421.94	$1.32B
3	Frax Ether FRXETH	$2,214.47	$670M
4	Staked Frax Ether sfrxeth	$2,353.78	$500M
5	Coinbase Wrapped Staked ETH cbeth	$2,332.82	$469M
6	sETH2 SETH2	$2,212.90	$74.81M
7	Ankr Reward-Bearing Staked ETH AETHC	$2,521.35	$56.13M

Ethereum's liquid staking market has only existed in a *fully functional environment* for a handful of months.

Before April, ETH could be delegated to a third party validator in return for a "liquid staking token" that would serve as an IOU for the contract's underlying staked ETH, but it wasn't fully redeemable. (Lido's stETH was effectively the onchain equivalent of GBTC in that regard.) The Shapella upgrade in April marked a significant milestone for Ethereum by enabling staking withdrawals from the Ethereum staking contract. This resulted in substantial capital inflows into ETH staking, as many Ethereum investors had been awaiting the opportunity to stake their assets with the assurance of full redeemability and the flexibility to withdraw at any time. Multiple catalysts still remain for liquid staking. Today, Alluvial and Ether.Fi are creating unique LST offerings and more are working to incorporate Distributed Validator Technology (DVT) to make their staking products, and Ethereum staking itself more robust.

Liquid staking tokens are a multi-billion dollar industry that supports the security of Ethereum, Solana, and other L1s. Liquid staking on Ethereum has a TVL of $15 billion (with 28 million ETH staked) and a 3.7% staking yield, staking services collectively generate revenues of $2.3 billion. It's an enormous market with the potential to grow further, and I've come around on staking issuance revenue being "real" in Ethereum (rather than a form of stock dividend) thanks to the limitations on the growth of network validators to be imposed by EIP-7514.



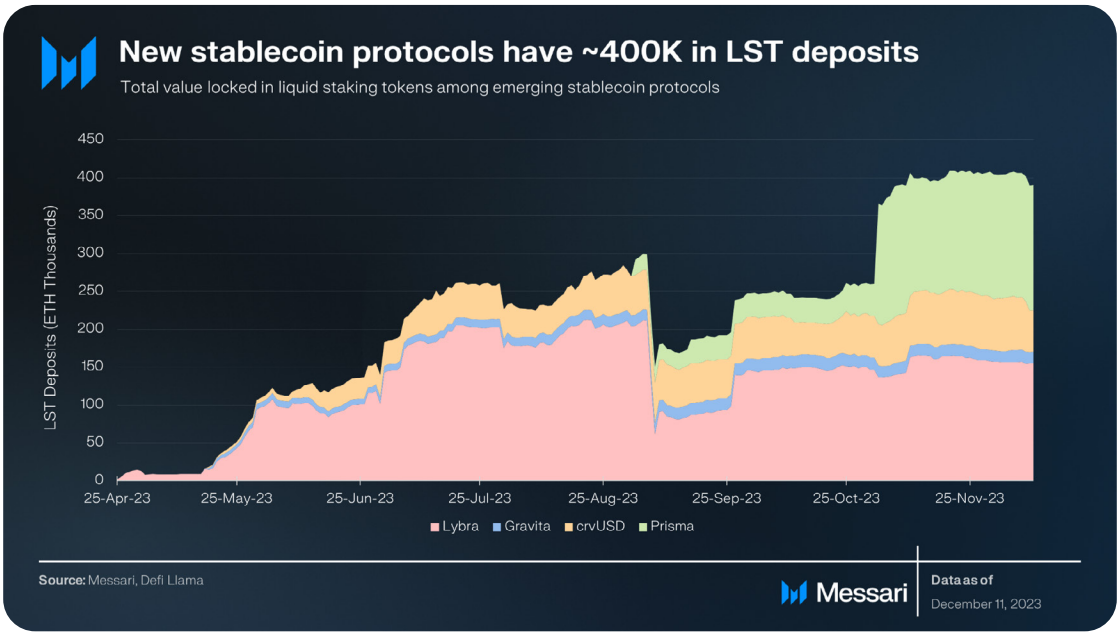
The greatest opportunity for liquid staking protocols will be in 2024 and the years ahead. If a BTC spot ETF gets approved, can ETH's be far behind?

TradFi giants are already tripping over themselves to get Gary's approval, and once it is approved, a staked ETH ETF is not much of a leap. A native yield-bearing asset with no inflation, home to the future of finance and the digital consumer economy, and being carbon-neutral on top — the investment pitch practically writes itself.

But yes, liquid staking could destroy the network with validation delays (thanks to a larger number of validators that must communicate to form consensus) and ETH holding disincentives (if LST liquidity eclipses ETH liquidity, disincentives to hold ETH may cause unpredictable outcomes). But the birth of new products like EigenLayer, a restaking primitive that enables Ethereum stakers to use their staked ETH to secure additional networks, creates counterbalances.

(Note: Vitalik has discussed his thoughts on L2s and restaking protocols and exporting demand for protocol security (an essential factor in layer 1 value accrual) at length.)

Liquid staking tokens (LSTs) are having a transformative effect across the DeFi ecosystem, too. LST deposits have accounted for effectively all of the growth in Aave deposits this year, and now represent the majority of all lending activity in the protocol. Maker is following a similar path, with liquid staking deposits surpassing ETH as collateral (stablecoins and RWAs still represent the plurality of collateral assets). And the new LST-backed stablecoin market is now exploding, amassing ~400k ETH in staked assets so far this year.



LST-finance had a moment in 2023, but it is likely only the beginning. The nearly $1 billion TVL in these protocols is yield-bearing assets. Yield is the lifeblood of finance, and these protocols unlock a new, sustainable yield source for DeFi. PENDLE, the native token of the yield trading protocol, was one of the best performing assets in 2023, up over 2,000%. Projects like Ethena and Prisma are still early in their stablecoin development and have the potential to bring new exciting solutions to LSTFi.

Will we have a Lido in every PoS network pot?

Probably. Jito, a combination of “Flashbots for Solana” (they bill themselves as an MEV infrastructure project) and “Lido for Solana” (liquid staking for Solana) just dropped a mammoth airdrop to its users in early December, and may very well be the project that sets off Solana DeFi’s Winter Summer.

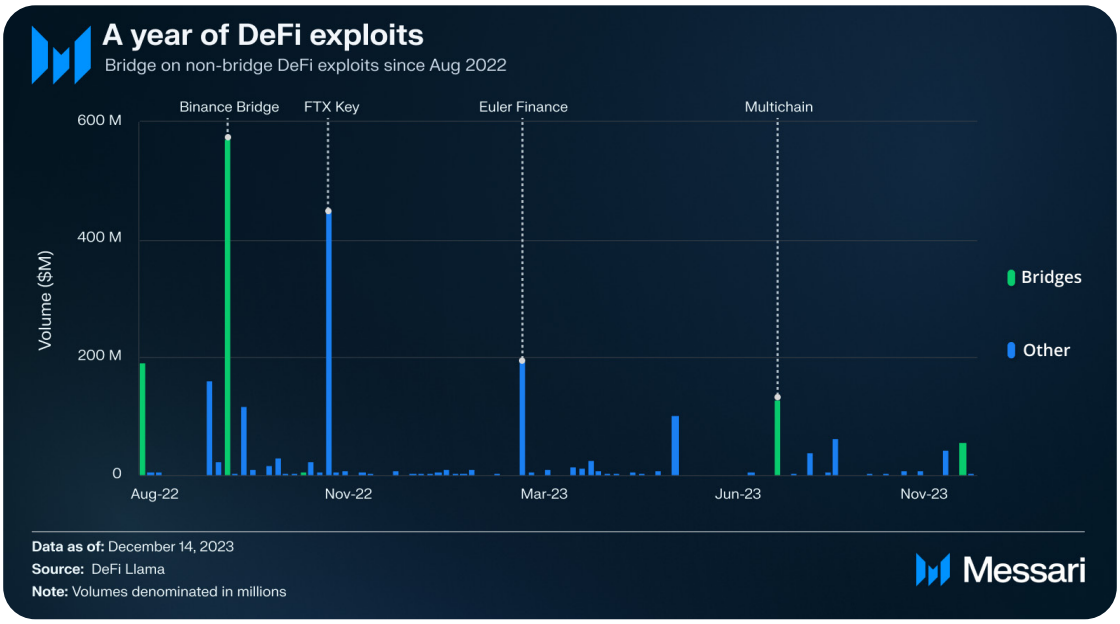
Expect leading LSTs on other networks to follow suit.

[Required Reading: Overdone Stake, Staking Since Shapella, Liquid Staking Brief, Ethereum's Ecosystem is Staking Up, Eigenlayer, Frax Enters the Arena]

8.7 Bridges & Messengers

Cross-chain bridges have been a disaster for us over the past few years.

When it comes to crypto's narrative vulnerabilities, bridges are behind only centralized exchange frauds as our biggest and most damaging black eyes. The $600 million Ronin and Poly Network hacks, $300 million Wormhole hack, and $200 million Nomad hack (among others) have accounted for nearly half of the $5.7 billion in hacks over the past six years in DeFi, with a significant chunk of those funds allegedly flowing through to the North Korean hacking group, Lazarus.



Look, it's pretty obvious we're the victims here. No one sets out to lose nine figures of assets in a smart contract vulnerability.

But the setbacks shouldn't dissuade us from building trustless bridges given how obvious it is that the future will be multi-chain. The open internet of blockchains won't be possible without better bridges and interoperability protocols. I enjoyed this Bankless interview on Thorchain, the largest DEX to offer bitcoin trading today, with about 2% of overall bitcoin spot volumes.

We've had a few positive developments in the bridge space this year. Our team covered "Omnichain Fungible Tokens" in depth (OFTs allow any application to mint and burn a single, unified token standard across various chains from LayerZero's Endpoint smart contracts). Chainlink is looking to enter the "Layer0" game with CCIP (see Chapter 3.9). And UMA's Across Protocol has taken market share from peers and first party bridges

with its fast and cheap optimistic oracle design.

I gotta hand it to the marines: I like the mental model (and narrative) around CCIP as a L0, Chainlink's bevy of core services at the data and computation layer for L1s, and Chainlink itself as an L2 (running node infrastructure to perform off-chain computations).

But Chainlink has some competition...

8.8 Oracles

As exciting as CCIP is (see Chapter 3.8 in the top products to watch), there was a late breaking addition that shifted the landscape: Pyth, the oracle network built on Solana.

Truth be told, Pyth wasn't really on my radar until it dropped its token in November. The oracle protocol has a great narrative (Solana native project + focus on RWAs + "cheaper" LINK + institutional backing from the likes of Jump + "Airbnb model for crypto market data" meme), but it's the underlying model that makes the project highly intuitive to anyone who understands the uniquely borked nature of the crypto market data landscape.

Rather than aggregate order data from crypto's exchange platforms (as is the model for TradFi incumbents like ICE, a company that is more data vendor than "exchange"), Pyth incentivizes the *market makers* to contribute trade data to assemble reliable order book and price data.

Why is this such a big deal?

Crypto exchange data (CEX and DEX) is fragmented and generally unreliable for institutional audiences. There's the long-time issues of fake volumes from loosely regulated offshore exchanges who offer no-fee trading, wash trading incentives (liquidity mining!), or manipulating their own order book data in order to climb the CoinMarketCap rankings.*

Crypto tokens also don't "list" on a single dedicated exchange like the NYSE or Nasdaq, but rather major global exchanges often compete concurrently to offer the tokens on their platforms. Because they usually double as custodial services, liquidity can migrate between platforms on a per month, per asset, and per product (perps vs. spot) basis constantly.

Oh, and most of the exchange APIs have sucked historically (though some are getting better).

When you add those things up, you get: 1) the rise of aggregators like Kaiko, Coin Metrics, CryptoCompare, etc.** who aim to address the issues above and consolidate various feeds into a single interface, providing an institutionally reliable aggregate "spot" prices, and 2) sophisticated, regulated market makers like Jump and Jane Street who connect directly to global trading venues and manage their own higher-fidelity records internally.

Market data aggregators have a couple of limitations when it comes to offering reference pricing data for certain use cases.

First, there are latency issues as you need to hop between multiple exchange APIs, and run logic on the aggregator side that can net out bad data (adding "hops" to market data intermediaries = losing money to traders with faster information). Second, because of the liquidity fragmentation issues noted above, CEX market data is often misvalued: crypto exchanges face an issue where they:

a) haven't charged for their market data APIs historically

b) want to charge for it now, but overestimate the relative value of their market data compared to their competitors (because everyone is coming off zero!)

c) individually tend to overestimate the take rate they should have on multi-exchange index products (Binance will want a fee split that reflects their trading market share, while Coinbase will want a fee split that reflects their regulatory positioning in the West).

It's a hot mess.

What does this have to do with oracles?

When multi-exchange oracle data is expensive to aggregate, slow to propagate to networks, and generally only as good as the reputations of the exchanges supporting them, it's easier for an alternative to emerge.

On the other side of the trade, market makers are usually the *payers*, not the sellers of market data. So when someone like Pyth comes along and offers to aggregate market maker data and pay them for it, it's a no brainer to the firms being approached, who are collectively able to reconstitute price feeds based on their large positions in the markets.

These lower-latency price feeds are essential for perp DEXs to function, and Pyth has slowly amassed the majority of DeFi trading apps as customers. ChainLink is in an unusual position from where it's been historically, playing catch up with a low-latency alternative called Data Streams. I'd imagine that data consumers will pay for multiple oracle solutions to mitigate their upstream bad data risks, so this might not be a winner take all market. (Synthetix uses both Chainlink and Pyth for its perp platform.)

That is assuming more DeFi protocols don't go oracle-free as it is.

Now is that worth 28% of Chainlink? Does that not give Chainlink's new Data Streams product enough credit? Is Chainlink too far ahead with multi-chain integrations and an economic model that can work at scale. That's for the market to decide.

As an investor, I don't know how to underwrite these networks (they feel expensive: Chainlink's fully-diluted valuation matches FactSet's). But as a data consumer, I'm excited they exist.

** Bitwise famously analyzed the fake volume problem in an epic report for the SEC as*

part of their bitcoin spot ETF applications. Ironically, this data was then used as evidence to justify the ongoing delays in approving the products.

***Note: We appreciate our partners like Kaiko, CryptoCompare, CoinMetrics, and CoinGecko. We're happy to work with teams who are working on some of these gnarly problems.*

[Required Reading: Oracle Free DeFi]

8.9 RWA Diversification

People want money and investments onchain.

The thing a lot of people are missing about the coming RWA boom - and why this is different from the premature 2015 ("blockchain not bitcoin") and 2018 ("security tokens") narratives around TradFi coming into crypto - is that Wall Street is not rushing in to take advantage of "tokenization" for its own back-end optimizations, so much as rushing in to satisfy demand from wealthy investors who want onchain products and will otherwise not invest into TradFi.

This is a profound realization, and once you see it, you can't unsee it.

Robinhood bridged a new generation to the stock market, but they also fueled the rise of meme stocks...and meme coins, and now those young Shibe's want to load up their IRAs with crypto ETFs, boomer ERC-20s that costs 10x more to store than the underlying crypto, but can grow tax free. We probably won't see tokenized commercial real estate any time soon, but we'll create network states that fractionalize Earth. When it comes to ushering in the era of RWAs on public blockchains, it will probably take a DeFi native, not a suit. And you'll want to follow where the DeFi natives are building.

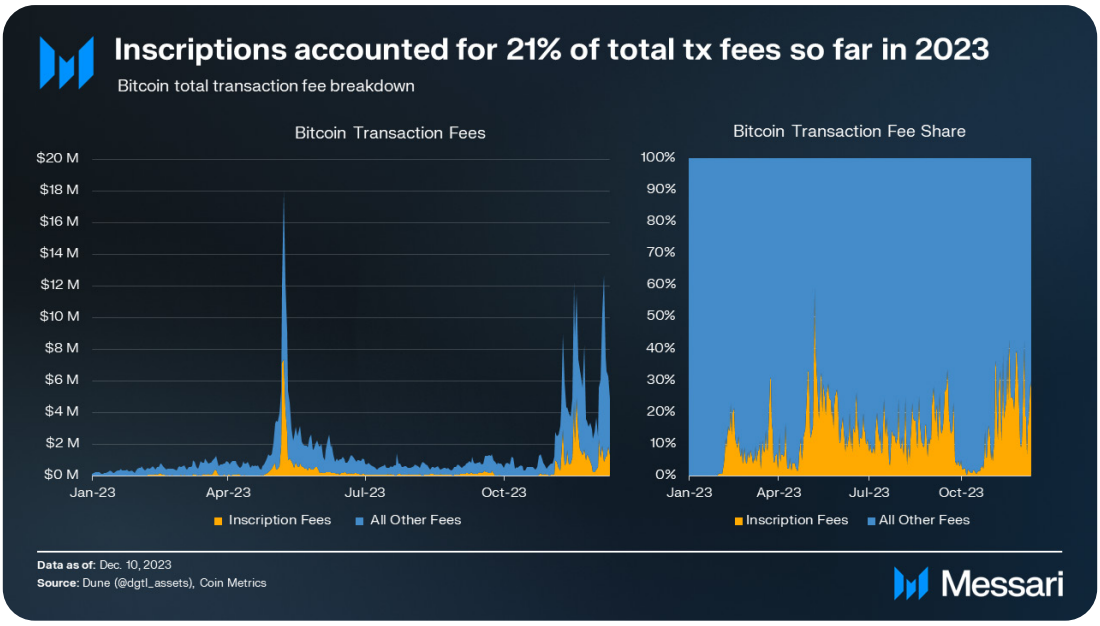
Some crypto holders will begin to sell into Wall Street's ETF buy walls in January. And when they diversify into other assets, most will prefer to buy them through Coinbase vs. JPM.

We're not stuck with Wall Street, they're stuck with us.

[Required Reading (and tracking): US Treasuries Fuel RWA Growth, RWA.XYZ]

8.10 Stacks & BRC-20s

Bitcoin is so back. We'll cover the Inscriptions and Ordinals boom in the next chapter, but for now, just know that new technical upgrades to Bitcoin core have opened the door for a vast design space of scaling and added functionality in the bitcoin ecosystem. BRC-20s, Stamps, Runes, recursive Inscriptions, and other types of new transactions have begun to flood bitcoin's mempool and spike its fees as enthusiasts and traders tested out the tech.



The corresponding fees are a possible solution to bitcoin's long-term security budget issues, but they are also a source of concern for those watching the size of the bitcoin blockchain: the number of UTXOs on bitcoin has increased 73% since the beginning of 2023 to over 140 million. BRC-20s, for instance, create new permanent transaction sets that cannot be pruned, and may ultimately affect bitcoin's decentralization as full nodes require more physical storage.

Other L1s are now facing their own 'issues' with BRC-20-inspired tokens. Avalanche, Near, Solana, and others have experienced activity spikes from Ordinals activity, and Toncoin even had an outage because of the spikes in volume these types of transactions have caused.

Bitcoin has seen a vibrant L2 (sidechain) ecosystem emerge this year, led by Stacks, which can read and respond to bitcoin L1 transactions. Stacks' upcoming sBTC and Nakamoto Release should provide access to BTC liquidity with fewer trust assumptions; their integrated consensus mechanism is unique in leveraging the full hash power of bitcoin to secure transactions. There are also several teams exploring rollups on bitcoin like Chainway, ZeroSync, and Kasar Labs.

Conclusion

Subscribe to Messari Pro for the best DeFi research in the industry. It will be a raucous and volatile 2024, and we've got you covered. Don't miss the boat.

Messari PRO

Unlock the power of informed decision-making with our **expertly designed platform**. Messari Pro is your gateway to staying ahead in the rapidly evolving crypto landscape.

What You Get:

In-Depth Data
Dive into extensive details on Assets, Protocols, Exchanges, and DAOs.

Trendsetting Research
Stay updated with cutting-edge industry trends and significant developments.

Exclusive Token Unlocks Data
Gain in-depth insights into the relationship between unlocks and their market impact.

Advanced Screener
Tailor your analysis with customizable filters.

TradingView Integration
Visualize market trends with advanced charts.

Chartbooks Access
Explore curated chart collections for deeper insights.

AI-Driven Newsfeed
Get real-time news summaries, crafted by AI for accuracy and speed.

Unlimited Watchlists
Keep a close eye on your interests with daily and weekly AI-generated digests.

Governance Daily Alerts
Stay on top of governance changes and updates.

Enjoy a discount of
30% OFF
on your first year!

Use code at checkout
THESES30

Learn more at messari.io/pro

SIGN UP TODAY

CHAPTER 9

TOP 10 TRENDS IN CONSUMER CRYPTO

9.0 Consumer Crypto

Given the absolute bloodbath this year in NFTs, I expected this chapter would be a breeze to write. *("Dead. Nearly dead. Never was alive. Dead. Next.")* But I was pleasantly surprised to find that I had 40 pages of notes and ideas regarding "consumer crypto," and actually think I made something of them. The ownership economy is here to stay.

I'm a power user of the new DeSoc platforms. I nailed some core NFT theses. (OpenSea and Blur are down viciously in a bear market, but they're still the market leaders and my two core investments in this space.) I continue to whiff on NFT trading itself, but like my three letter ENS name. I have some hope that bitcoin's fee model may become a life-sustaining force for miners. I have friends that understand crypto gaming and user-generated experiences so I don't have to. And I even know a guy trying to take over the world and start a cloud country.

We can't let the institutions steal our jpegs, and must seize the memes of production, as NFTs are the most defensible type of crypto assets we have right now. Gary Gensler may try to come after those, too, but at least he beclowns himself in the process: to both his Congressmen and fellow commissioners.

Until last year, I thought crypto consumer applications were "nice to haves." Now, I think the "toys" are actually critically important bits of infrastructure to get right. And fast. NFTs and public blockchains will be indispensable in our AI-driven future.

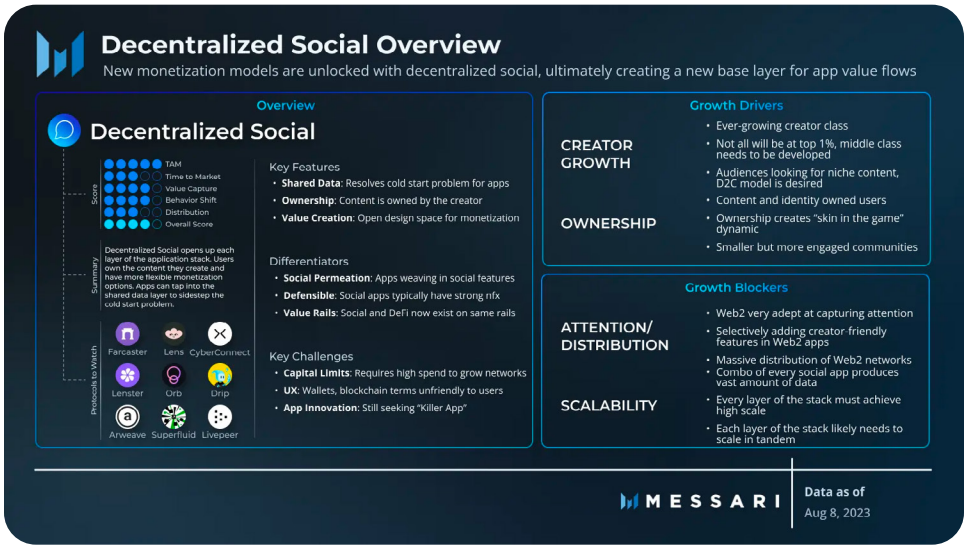
I thought this framing from Stratechery was on-point: the PC, Internet, and AI revolutions were discrete events in the history of information. We could control the PC's power to duplicate information at zero marginal costs until the internet came along; then we needed public encryption. We found a way to harness the internet's power to distribute information at zero marginal cost by creating social media and search platforms. But we have no way of controlling AI-generation just yet. We'll need NFTs and blockchains in order to track provenance.

The opportunities ahead are mind blowing, and will be lucrative to those paying attention.

9.1 DeSoc

Elon Musk bought free speech a little more time this year with his acquisition of Twitter, but the "misinformation" barbarians are at the gates, and there seems to be a concerted effort among the powers-that-be to kill the company via a coordinated ad boycott.

It's not worth risking a digital un-personing any longer. If you want bona fide protection from censorship on the social web, we need decentralized social media platforms (DeSoc) to work. And fortunately, we have several that are making good progress on this front. We already covered Farcaster in the top products section, but there are a number of DeSoc applications to get excited about: Lens, Yup (a DeSoc aggregator), DeSo (which forced me to rename the sector to DeSoc), XMTP for messaging (huge integration with Coinbase), and many more.



(Source: Exploring Consumer Crypto Trends)

DeSoc solutions solutions aren't just a "nice-to-have" anymore, but existential for free and open speech. I think we have a good shot at cracking the DeSoc nut in 2024 because the product-market fit has gotten clearer due to a confluence of factors.

1. **Portable Social Graphs:** I really felt the need for this - ironically - with the launch of Instagram's Threads, where I posted content for about 3.5 days before it died. For a long time, I worried about cancellation on the bird app for posting about things like crypto, civil rights, and actual science. But it was Threads' overnight evisceration of my X impressions that gave me pause: what happens if X bleeds slowly, and I don't invest enough time and energy in cultivating a social graph on other platforms? Do I just lose 10 years of accumulated work and network building? DeSoc solves this issue in the medium-and-long term by hot swapping the back-end of social media. This is already the norm in DeSoc: 70% of Lens users interact with more than one app.

2. **Anti-Censorship:** The portability of a social graph is an important long-term fix to prevent digital unpersoning. But in the short-term it's really all about ensuring that the crypto conversations remain unfettered. Our Progressive leaders consider

crypto a national security threat (a precursor to a speech crackdown), and they've now got the most important man in the country encouraging them to shut the sector down. I wouldn't blame you for scoffing at me last year for my crypto speech censorship concerns (you'd have been wrong, but less obviously so). Things are different now.

3. **Control over the Algorithms:** DeSoc breaks apart traditional tech stacks resulting in more interfaces for developers to build new business models and features. I think about the future of social media a bit like the world of investments today. Instead of investment products and investment managers, we'll invest in DeSoc filters and algorithm managers. Attention is our scarcest resource, and it's only going to get harder to compete for it in an AI world with infinite content generation. Imagine paying for control over a custom "for you" feed that *you* control. "Deep Focus" mode. "Breaking News" mode. "Happy Hour" mode. With happy, angry or flirty tone filters.

4. **Creator Cash:** Traditional social platforms capture $300 billion of revenue per year. Almost all of that goes to the platforms vs. the creators, which makes Big Tech's margins DeSoc's opportunity. This is always the area where crypto shines given its roots as a financial technology first and foremost, and friend.tech showed the potential for DeSoc apps to leverage economic incentives to rapidly onboard new users. But this will arguably be be the least important driver of DeSoc adoption. People have an innate desire to be connected and to feel like they own their own identity, and think for themselves. Financially rewarding that desire is merely lighter fluid.

I also wouldn't bet against Elon (or Zuck) conceding the point, though. Elon already rolled out ad sharing for creators. It will be an increasingly important part of Instagram's / Threads" business, too, and they have an enormous head start in shareable revenue. Here's Meta's Average Revenue per User (Average Revenue per User):

	DAU	MAU	Ad Revenue	ARPU
U.S. & Canada	200	269	$12,710	$48.85
E.U.	183	245	$2,810	$11.47
Non-E.U.	124	166	$3,459	$20.84
Asia-Pacific	873	1,324	$5,893	$4.52
Rest of World	657	986	$3,229	$3.35

(Source: Stratechery)

[Required Reading: The DeSoc Map, User Behavior and Engagement on Lens, Farcaster's User Centric Growth, Decoding friend.tech Metrics to Monetization, XMTP Communication]

9.2 friend.tech

I can't believe how much I have to skip in the DeSoc space, but I only have so much time, and friend.tech needs its own section after emerging as this year's breakout app.

It's possible that Lens, Farcaster, and crypto derivatives of X are the wrong starting place for DeSoc entirely. The novelty of friend.tech had to do with a combination of uniquely "crypto" attributes: small, exclusive digital tribes; economically enforced scarcity; gamification with points (and maybe later, tokens); lots of controversy, etc.

The "Nasdaq for People" allows users to create and join exclusive private chat rooms gated by "keys" that can be bought and sold via a bonding curve. Each user's bonding curve is the same regardless of profile, which means that liquidity at incremental key prices is always available, and the maximum room size for the very largest accounts approximates Dunbar's number. It also means that a bot army could quickly design strategies to "take people public" (bidding up the early supply of their keys), as soon as their X account gets connected.

They absolutely crushed the onboarding experience on both the creator and consumer side. They nailed the Progressive Web App design (instant install outside of the app stores, and one-click transactions on an embedded wallet through Privy), the Base L2 integration (highlighted the power and potential speed of rollups), and the viral "hook" (connect your X account and instantly earn fees based bot bids for your initial keys; you kept half of the trading fees on all buys and sells).

The question has been one of staying power.

Will friend.tech be a breakout app, or just a flash in the pan? Many people are underestimating the project for some pretty obvious reasons:

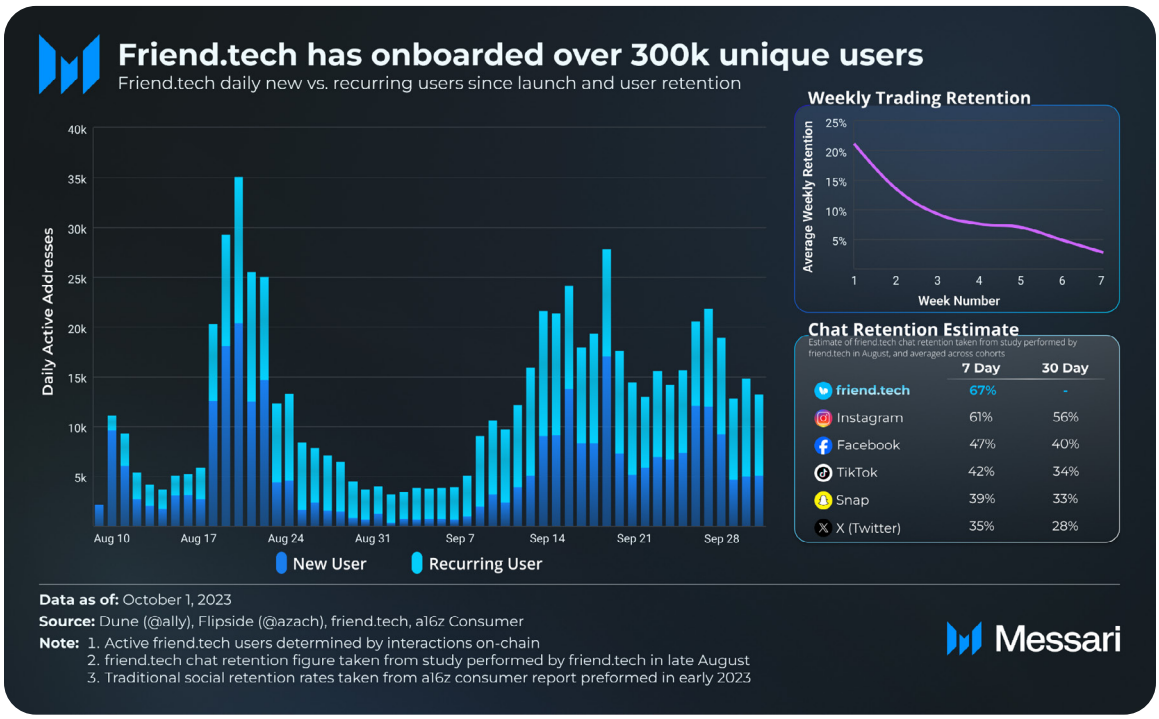
1. **People like Celebrities:** We like to collect things, and as fans, friend.tech gives us an app to collect access to celebrities and larger accounts that we otherwise wouldn't engage with. There are many who would spend $100k+ on a room key with Taylor Swift (giving the bonding curve dynamics and the exclusivity that would imply) if given the chance. friend.tech is the purest expression I've seen of financialized social capital.

2. **This is Cancel-Resistant / More Authentic Chat:** Everything you post on the internet can be broadly distributed. But by capping friend.tech rooms at the low hundreds of users, the protocol could give rise to more unkillable (at least digital) truth tellers. Smaller audiences reduce the risk of social attacks, and so long as your key prices don't go down, can you really be canceled? It's not just a hedge for those at risk for being punished commercially for unpopular speech (a la NYT journalists moving to Substack), many fans will reward authenticity ("100 true fans" sustain you if you don't "sell out").

3. **Killer Apps Have High Margins:** Technology that boosts margins is almost always good. Coinbase makes 1% on retail buys and sales. Grayscale makes 2% on assets under management. Tether sweeps all interest to itself. The difference

with friend.tech is that it shares its high trading fees with its users. There are explicit disincentives to flip keys (keep room key holders more stable), and explicit incentives for creator engagement (key fee share). Even if alternatives emerge, many will be competing on cost, which is a shitty place given that users mostly *benefit* from the high fees.

The platform has generated $50 million in fees this year so far, and at one point friend.tech's daily revenue was 10x OpenSea's. Even after a cool-down in activity, it's generating $4.5 million per month, a top 20 crypto app by almost any metric in less than six months.



*

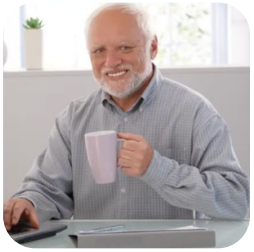
The friend.tech launch felt like a Uniswap or OpenSea moment for me. Even if friend.tech isn't the final form for this concept (gamified, liquid, token-gated fan communities), the idea won't be uninvented, and there's something special here. Though if friend.tech is like OpenSea (high trading fees and creator emphasis), that...might be bad news for the project. It's just a matter of time before a trader-oriented alternative emerges.

(Note: we've had a bunch of debates about friend.tech internally at Messari. Some rebuttals to common criticisms: "Social Media breakthroughs are hard, we've only had a handful in the last 20 years." Yes, but when they happen they are enormous. "Small accounts are making no money, trades/trading fees are not significant enough." Who cares, good creators come for the money, but most users will be consumers. "On friend.tech, the money is frontloaded so once the bulk of the money has been paid out, most creators have little incentive to stick around." This is a fair criticism that some key prices are too high / bubbly, not that the experiment will die. "Unlike NFTs, bonding curves have immediate sell value, so once it looks like a creator on FT has topped, the game theory is for everyone to immediately cash out and not be last." This ignores the stiff selling disincentives of a high fee trade."Don't make the same mistake thinking you can beat a 20% transfer tax ponzi (10% each way)." Come for the chats, not the fast money!)

9.3 NFT Market Models

Pain..

OpenSea pioneered the NFT marketplace. I compared their model last year to Coinbase's retail platform (high feess, great UX for creators, etc.) vs. a high-speed trading platform. I still think that rings true, but my, oh my, what a brutal year it was for the top dog marketplace and its sector.



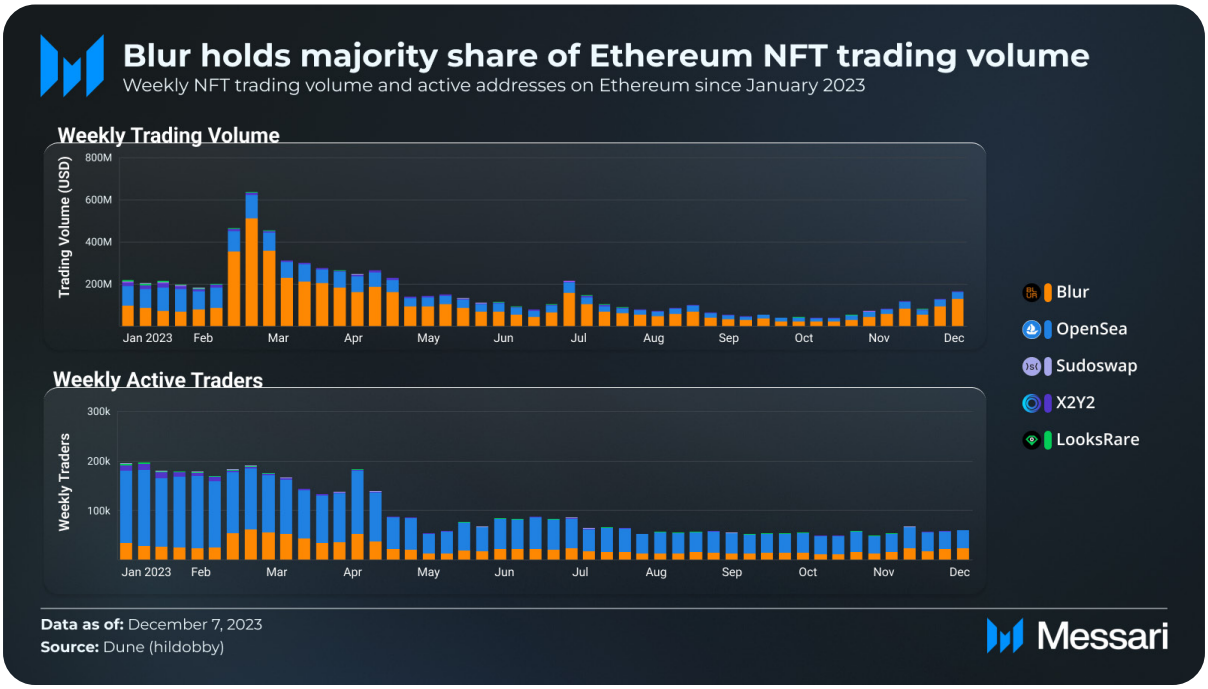
1. **The Market Sucks:** The NFT market has been caught in a death spiral I warned about last year: per project prices have plummeted because there's no theoretical limit to the number or diversity of NFT projects, and few have true value memetically or artistically. (Though we are perhaps seeing some early signs of life going into 2024.)

2. **Blur Hurt Them:** With NFT interest fragmenting, and new investment and liquidity plummeting, it was a bad time to see sophisticated trading tools introduced that made the market even *more* liquid. But that's what Blur did, and they dominated the "NFT financial infrastructure" segment (and dropped a cleverly designed token distribution scheme in the process). Blur's fee-minimized trading also pressured OpenSea to reduce creator royalties. (Interestingly, this is basically the opposite dynamic of friend.tech: NFTs are infinite, so a low fee model wins. *Specific* room keys are finite, which is why the high creator fee sharing model might be sustainable.)

(Source: Exploring Consumer Crypto Trends)

3. **The Market Forced OpenSea's Hand:** I have always appreciated OpenSea's emphasis on creating a creator-friendly marketplace, but they had to make some tough decisions this year, and even some of their biggest boosters criticized the adjustments they were forced to make around the enforcement of creator royalties.

The market correction was predictable, but its intensity was surprising. Despite all the drama and headwinds and layoffs, OpenSea remains the dominant NFT marketplace by users. It's a two player market right now, and if these two can maintain their market leadership in this phase of the market cycle, I'm confident they'll thrive upon the return of the bull.



*

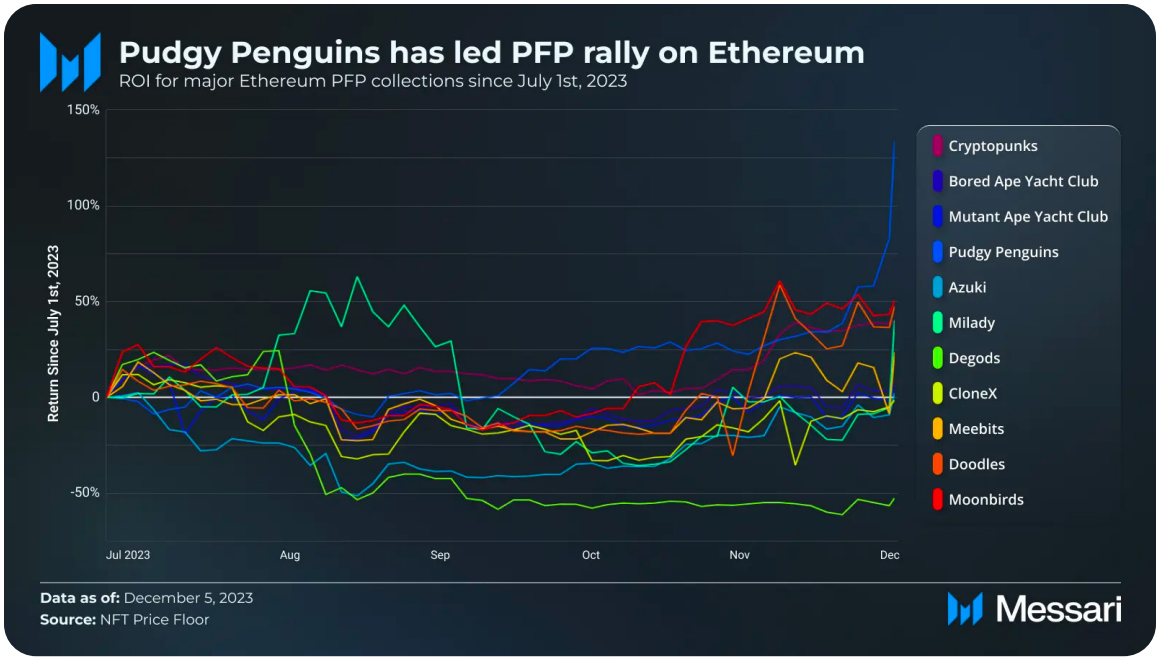
[Required Reading: Blur's Token Incentive Model, Aggregators in Web3, Beyond Digital Art]

9.4 The March of the Penguins & Ordinal Theory

I'm not covering pfp projects this year. I'm sorry. I'm tapped out.

But I would encourage you to read our linked reports below. I am personally looking for projects that sit at the intersection of NFTs and AI-generated content. Securing identity and IP in the AI age is a trillion dollar market. So feed me ideas. Otherwise, let's just assume the pfp market is BACK, and we'll have more to say about its resurgence and projects to watch in January.

In the meantime, for the pfp punters looking to guess what's next, I'd check out Upshot's new AI-driven price prediction tool.



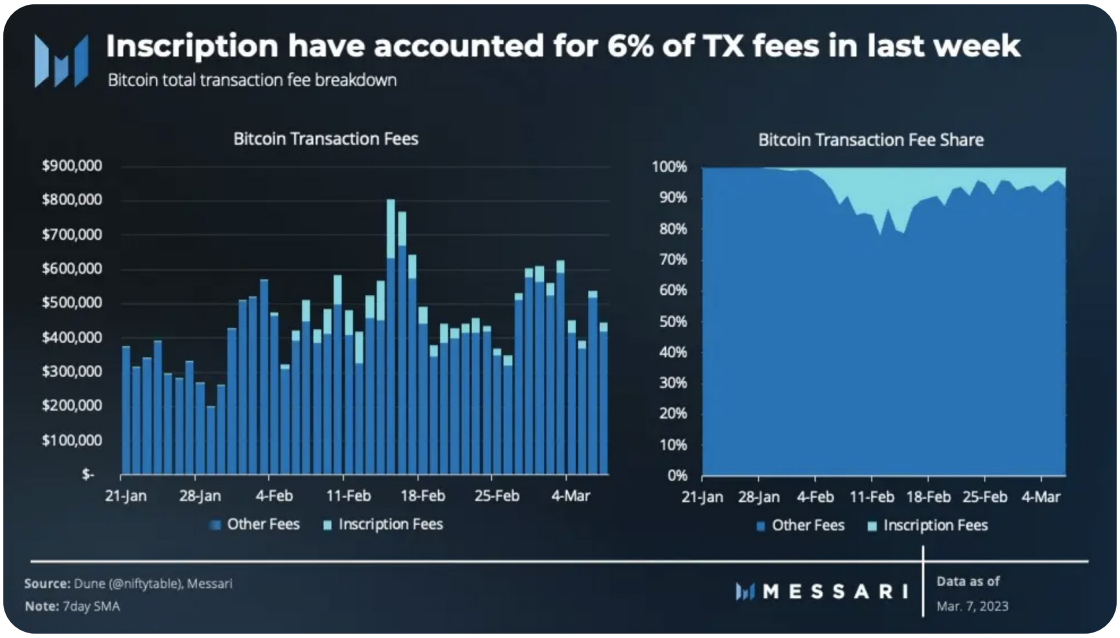
(Source: PFPs are Making a Comeback)

[Required Reading: Evolution of Web3 Communities, Digital Identity in the Advent of AI]

Ordinal Theory

I am *extremely* excited about bbitcoin's Inscription boom and Ordinal Theory. Not because I am partial to bitcoin jpegs per se, but because I think bitcoin zealots will eventually recognize that the success of these projects will be the only thing that drives fees to proof-of-work miners on a sustainable basis. Otherwise, they are choosing between a fork to proof-of-stake, an alteration of the 21 million bitcoin hard cap, or long-term irrelevance.

In other words, I think they'll come around!



Ordinals are worth a quick history lesson.

In August 2017, bitcoin underwent a soft-fork upgrade called Segregated Witness (SegWit), which separated transaction data on bitcoin into two parts: transaction data (which contains information about the sender, receiver, inputs, and output), and witness data (which contain scripts and signature data). SegWit made it easier and cheaper to store larger amounts of data on the bitcoin blockchain without radically increasing its size, and as such it was the resolution to a years-long battle over the issue of block size limits. Few will remember the drama, but it was 100x more more intense than it sounds now.

One unexpected development that the SegWit upgrade brought bitcoin was Taproot, which activated in November 2021. One of the primary features of Taproot was more advanced scripting capabilities in the witness portion of bitcoin transactions. In fact, Taproot removed the guardrails that constrained the amount of data that could be included in the witness portion of a transaction, unintentionally enabling individuals to store large amounts of arbitrary data on the bitcoin blockchain.

That brings us to this year, and the explosion of NFTs on bitcoin, including the largest bitcoin block and transaction in history, featuring a Taproot Wizard NFT. The introduction of "Ordinal Theory," an off-chain method for serializing or numbering individual satoshis (or "sats," the smallest unit of bitcoin), introduced collectibility to bitcoin and allowed users to inscribe fungible sats with arbitrary data, converting them into NFTs.

Bitcoin Ordinals grew over 300x earlier this year, leading to a predictable debate among the bitcoin religious regarding the purpose of the bitcoin blockchain; financial transactions vs. more complex data on bitcoin, and other absurdities. I think it's great. I hope BRC-20s work, too.

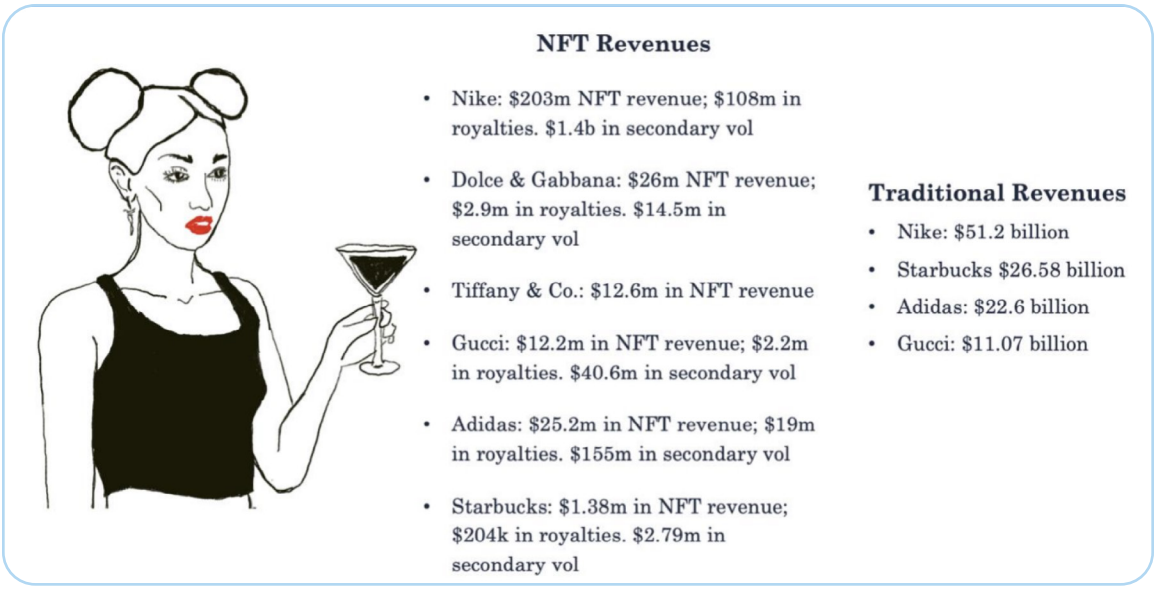
[Required Reading: Inscriptions: A Bitcoin Renaissance, Extra Ordinary Bitcoin, Ordinals & AI]

9.5 Crypto Gaming & Digital Native Brands

The gaming industry is thriving. There are ~~3.44 billion gamers globally who contribute to the $184 billion in expected revenue for the gaming industry in 2023, a figure that is ripping higher year after year. Gen Z and Gen Alpha — who increasingly view digital and physical experiences as one and the same — devote considerable time to gaming (~15 hours/week), and spent $135 billion in 2022 on virtual gaming items alone.

Of course today's game items are neither truly owned nor freely tradeable, but it's inevitable that (younger) gamers eventually demand ownership of their virtual goods.

Gaming goes through paradigm shifts approximately every 10 years, and in many respects, the rise of crypto gaming is similar to the rise of free-to-play (F2P) gaming a decade ago. Monetization enabled by crypto will become *the* dominant business model in gaming. When these paradigm shifts happen, they seem obvious only in retrospect.



(Source: It's All a Game)

[Required Reading: It's All a Game, Nike, Still the Biggest Game in Town]

9.6 Token Bound Accounts

There have been a lot of big, exciting developments this year in the NFT / digital identity realm, but the biggest was the introduction of token-bound accounts, onchain smart contract wallets that an NFT *owns*, formally proposed within ERC-6551. Opportunities abound: they're backward and forward compatible, they'll work across any rollup or EVM chain and they can accumulate assets, interact with other TBAs, and transact autonomously. Huge.

Some implications:

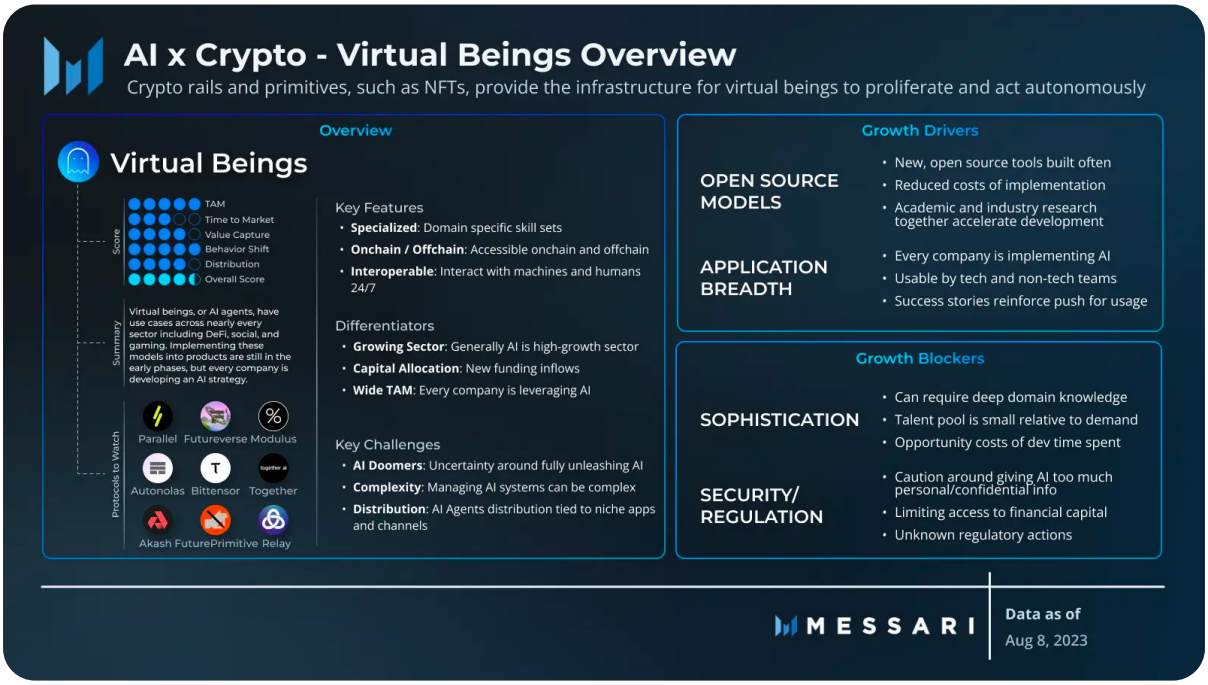
- It's a growth opportunity for marketplaces like OpenSea which was developed under the assumption users would trade standalone NFTs versus dynamic assets that can also own other things. TBAs change the whole NFT marketplace model. They're the difference between buying a "skin" and buying a digital character with a portfolio of non-fungible and fungible assets, including reputations. (I'm sure we'll run into ethical debates around selling digital autonomous "persons," but that's a fight for next year.)

- In NFT lending, TBAs open the door for the equivalent of NFT "cross-margining," which could boost liquidity and reduce liquidations and bad debt.

- It's a major development for Lens, which announced an integration of TBAs into their v2 and rearchitected Profiles back in July. Now, all the value earned from "mints" and "collects" can be accrued to the wallet of a Profile instead of directly into an owner's address. Lens is the top project to leverage TBAs so far.

- They are also highly complementary to “non-transferable” or “soulbound” tokens, which are useful in different contexts. It might be ok to have soulbound tokens sent to a TBA, but you probably won’t want an NFT social credit score appended to your public ENS vs. a Lens TBA.

I expect that we’re just getting started here.



(Source: Exploring Consumer Crypto Trends)

[Required Reading: Token Bound Accounts, Expanding NFT Utility]

9.7 Co-Creation & UGX

Building digital worlds is expensive.

Meta has spent more than $20 billion building out its metaverse in the past several years, and gaming companies spend multiples of that yearly on R&D to satisfy their insatiable users.

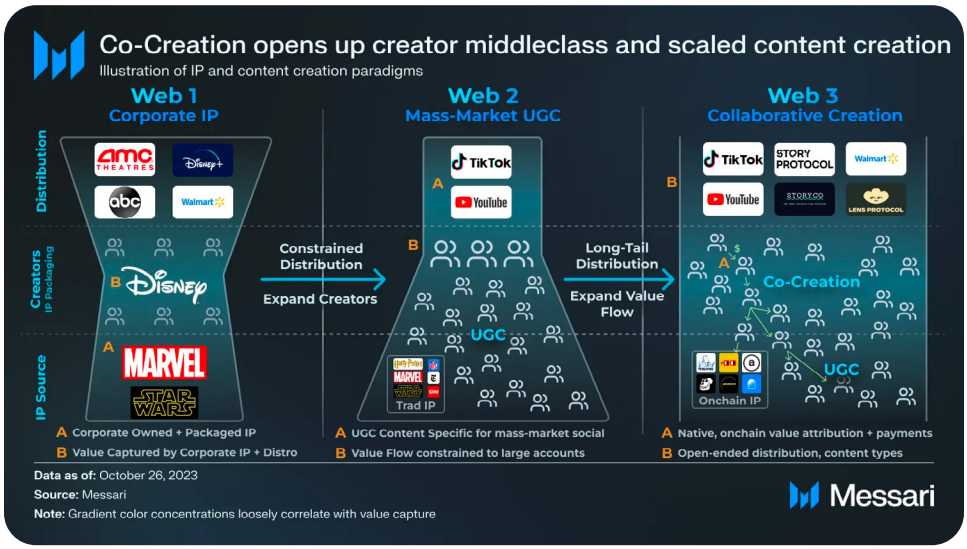
It’s hard to see how crypto communities could ever get over those massive financial disadvantages to be competitive and build digital, autonomous worlds. But autonomous worlds have the potential to break the stagnant world of game development, where big studios milk pre-existing IP due to the high risk profile of developing new IP, and the spoils for sparking such a content revolution would be massive.

(Source: Exploring Consumer Crypto Trends)

Aside from better game designers (or better partnerships with incumbent gaming giants), it's also going to take better onchain gaming infrastructure and better user-generated storytelling to disrupt the incumbent gaming giants.

Polygon and Immutable may be the early ecosystems courting the most onchain gaming development today (they've probably got ~70% market share, though it's difficult to measure precisely), while Solana is likely to pick up steam in 2024 after its recent rally. On the storytelling side, "cocreation" through platforms like Story Protocol, Shibuya, StoryCo, and Storyverse aims to disrupt mega creator platforms by leveraging NFTs and programmatic payments to broader creator ecosystems. (Gang. Gang.)

A lot of money has gone to the crypto gaming space in the past several years. We haven't seen results yet, but my bet is we'll see 5-7 onchain games hit the 100k DAU mark by 2025. The tech is there, and we're ready.



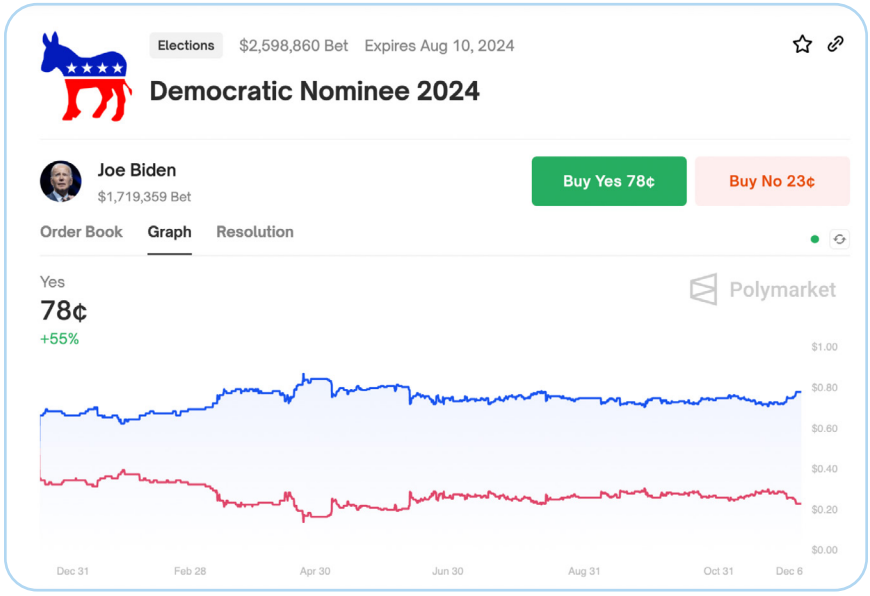
(Source: Co-Creation)

[Required Reading: User Generated Experiences, Cocreation: Landscape & Value Accrual, Business Advantages of Autonomous Worlds, Potential for Fully Online Games]

9.8 Bet-To-Play Gaming & Information Markets

I don't generally give crypto prediction markets much time or thought, but I'll make an exception for three reasons this year:

1. We're in a wild Presidential election year with lots of moving pieces. (Not just who will win, but "Will Trump be convicted?" "Will Biden drop out of the race due to health issues?" "Will RFK Jr be the only independent candidate in the race?") If crypto prediction markets don't make it big this year, then we're still probably another four year cycle too early. Polymarket did about $6 million in volume last month. I think it will do $300 million next October.



(Source: Polymarket)

2. Prediction markets are the largest and easiest subset of "curation markets," which we desperately need as a probabilistic alternative to disastrously inaccurate "independent" fact checkers or more community sentiment-driven products like Community Notes. I agree with Nick and Balaji that prediction markets will help improve data, news and ultimately, public discourse by gamifying truth.

   We'll likely be able to get more creative in terms of how zk-tech is used for things like truth verification, too, which will cut down on misinformation by enabling proof that a given statement is true (this picture came from my device at this time) without revealing any additional information. This granularity could help resolve increasingly more subjective information markets.

3. Finally, it's batshit crazy to me that we can't bet on prediction markets (I'm smarter than you), but we can bet on ourselves in things like online gaming (I'm better at FIFA). Both should be allowed, and society is worse off because we are blocked in the U.S. from doing the former by unnecessary CFTC encumbrances. The sports betting and iGaming markets are growing by mid-double digit percentages year over year, and Kel thinks "bet-to-play" models could add $10 billion per year in revenue to Fortnite alone.

(Source: [Bet-to-Play: The Real 10x Paradigm Shift in Crypto Gaming])

The market size is staggering, the gambling element makes it a perfect gray market use case for crypto, and the ability to wager on crypto games could give them a marginal benefit that helps put them over the top of other centralized gamemakers.

9.9 Network States

There's been a quip going around for a while that the three scariest words in the English language are "Balaji was right." I'm not going to walk through his many prescient bets, or debate whether his $1 million bitcoin bet earlier this year was a terrible wager or a marketing ploy to ring the alarm on our sovereign debt crisis (a discerning reader that understands anything about investing knows the answer), but I will point out that his network state thesis is playing out.

The scariest thing to me about Balaji's bet wasn't how right he's been in the past about other major events, but rather watching our President's son and the ex-President face criminal charges, witnessing a rise in anti-Semitism take hold across the U.S. and Europe with no obvious paths to deescalation, seeing a state governor debate on behalf of his President and fill in as a proxy for that President on a major diplomatic visit, and then understanding that cultural divisions are continuing to deepen further still.

In many respects, the West has already hard forked in the cloud (our legacy and social media filter bubbles are now completely divorced), so a cloud country looks like a forgone conclusion.

After starting a new global form of money (BTC), or a new permissionless internet (ETH), I don't think there is much more of a punk rock *software* play than trying to form *a new country*.

I was there in Amsterdam when he hosted the first Network State conference before Breakpoint, and the place was electric. The tailwinds for the Network State resemble bitcoin's the closest: the vision will gain prominence simply thanks to the slow digitization of everything and the inevitable ongoing declines of institutional credibility. I'd encourage you to watch the talks from the event over the holidays: I'll also do a podcast with Balaji soon.

9.10 Techno Optimism

If the rest of the world is getting pretty dark, crypto's future is still bright.

Going into a chaotic 2024, I'm trying my best to focus more attention on ideas from builders like Balaji, Elon, Vitalik, and Marc Andreessen, and turn down the volume on politics, which drained too much of my energy in 2023 (but which, again, I believe was worth the investment).

Read the Elon Musk Series by Tim Urban, Techno Optimism by Marc Andreessen, and Vitalik's thoughts on decentralized accelerationism.* Elizabeth Warren, Gary Gensler, and other luddite obstructionists (or degrowth cultists) are not going to save the U.S. or advance humanity. But the builders might. We just need to ensure there are more of us than there are of them. That's no small task, but I'm going to keep doing my part in 2024.

We'll only win if we build products that people love and advance ethos that people respect. That's why this is a good place to end this chapter.

*(*I beat Vitalik by three weeks in noting that d/acc was a good meme, please clap.)*

Conclusion

Consumer crypto is booming, even if prices and sentiment suggest otherwise.

(Believe it or not, I still left a ton of things out of this section. (DeSci, despite being a theme of the year for me up front in the intro, didn't make it.) But never fear, you can still read our research on DeSci and cover our ongoing research in this market all year, by subscribing to Messari Enterprise. After 160 pages, what on earth would stop you?)

Messari

Unlock the full potential of your business with **one platform.**

Messari Enterprise lets your team get back to work by flagging major updates in real time. Cover more assets without the risk of falling behind.

Visit **messari.io/enterprise** to learn more or contact **sales@messari.io** to schedule a demo.

Schedule A Demo

CHAPTER 10

TOP 10 TRENDS IN PEER-TO-PEER INFRASTRUCTURE

10.0 Crypto Usability Upgrades

It's difficult to overstate just how much innovation there has been in peer-to-peer infrastructure over the past two years.

We'll look back at the wallets we used in the first ten years of crypto as barbaric, and technical breakthroughs of 2023 will look in hindsight like a quiet inflection point for crypto adoption. We'll reminisce about the graft and "batshit crazy dipshittery" of DAO governance (as one crypto lawyer affectionately puts it) in an era before we had legal wrappers for these entities or proper community management tools. We'll thank the old gods and the new that DePIN built us parallel hardware infrastructure to check the runaway power of Big Tech before it was too late.

These are the good old days. Enjoy them!

10.1 Wallet-Centric Future: MPC Upgrades

If you own the world's primary crypto user interfaces, you're going to capture a good deal of value. Blockchain.com built the core of its $8 billion business by creating nearly 90 million self-hosted wallets. Metamask propelled ConsenSys to a $7 billion valuation with the original browser wallet. PayPal acquired Curv for nearly $200 million in 2021. Coinbase, Circle, and Fireblocks consider embedded Multi-Party Computation (MPC) wallet infrastructure critical growth areas for their businesses. And that's not even considering up and coming smart wallets like Safe, which raised $100 million in 2022, and manages $35 billion in onchain treasuries.

That said, the average wallet user experience has been awful for years. The status quo requires users to sign multiple transactions in which they are expected to understand complex technical inner workings in order to avoid catastrophic hacks. Wallet friction points cause users to churn out of crypto products, at best. At worst, they can be financially ruinous.

Before we get into the meat of the much-needed upgrades we've seen in the wallet ecosystem, let's do a quick refresher on 1.0 crypto wallets.

Background on EOAs
For years, externally owned accounts (EOAs) have been behind the de facto wallets on Ethereum. Metamask has allowed users to execute Ethereum transactions using a single private key since its initial launch. While functional, that's proven to create honeypots for hackers, as access to your private key (via direct access or via a phishing exploit that accidentally signs over wallet access) could unlock your entire wallet. The rigidity of our legacy wallets has also created bottlenecks to onboarding new crypto apps, as EOAs require you to buy crypto through an on-ramp, send it to a wallet, and maintain a positive balance before you can do anything onchain. New wallet infrastructure has already radically improved the UX here.

MPC Wallets
MPC wallets remove some of the risks of basic wallets with a single private key. They are also different from simple "multi-sig" wallets in that they provide some flexibility in terms of signature schemes (threshold signature security, which are important, but I don't have time to go into here) and privacy.

In early 2022, Coinbase announced they were shipping a new decentralized application wallet built on MPC tech, removing the need for users to maintain the entire burden of their own private key management. This is my favorite wallet today, and I find there is an acceptable security tradeoff when it comes to managing my true "wallet" funds (play money and payments) vs. long-term holdings (which aren't large enough to wrench me over, which is why I still have to grind through this report, so don't even think about it). The MPC wallet allows Coinbase to have its cake and eat it too, retaining user relationships for non-custodial applications, but avoiding the liabilities that would come with direct custody or facilitating activity in certain onchain applications like DeFi. It was a killer investment and terrific execution by the Coinbase team.

Most wallet providers haven't yet sought to leverage smart contract accounts (SCAs), as creating SCAs today requires significant fees on Ethereum, and most crypto apps historically have been designed for interactions with EOA wallets (or their MPC cousins). That may change in 2024.

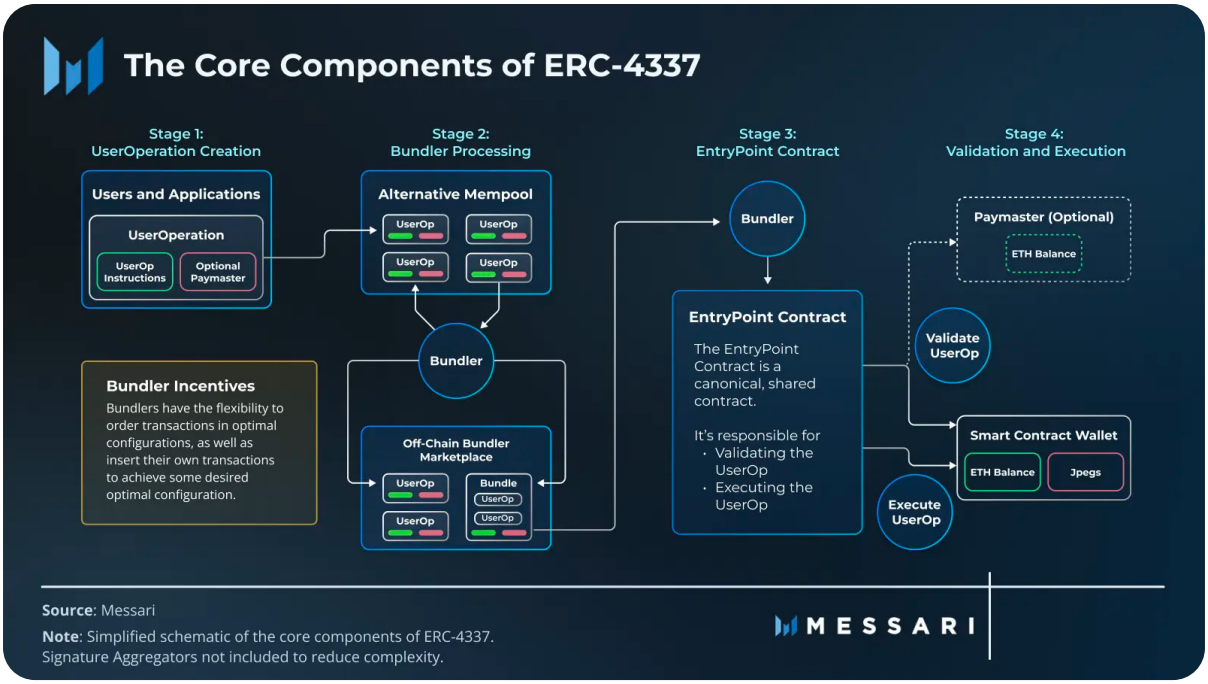
[Required Reading: Wallet Landscape Map]

10.2 Wallet-Centric Future: Smart Contract Accounts

Today, the vast majority of self-hosted wallets are simple EOA wallets or MPC wallets. Scheduled upgrades on the Ethereum roadmap could change that.

Account abstraction (AA) is a core Ethereum roadmap initiative aimed at replacing EOAs with smart contract wallets or "smart accounts." These new forms of wallets are dynamic, and allow for things like social recovery options, apps that pay for fees on behalf of users, more efficient bundled transactions, security features like spending limits, multi-factor authentication using hardware devices, single-step multi-chain operations (again, important because of the cost to creating a new smart contract wallet on Ethereum), and more. There's even one effort (EIP-7212) to support the signature scheme used by Apple that powers its biometric ID system. You might soon be able to use FaceID to confirm a Uniswap transaction!

The core AA implementation, ERC-4377, provides a standard for wallet developers, infrastructure providers, and end users to rally around in order to leverage the benefits of smart contract wallets without taking major leap-of-faith security risks with multiple implementations. Here's how it works:

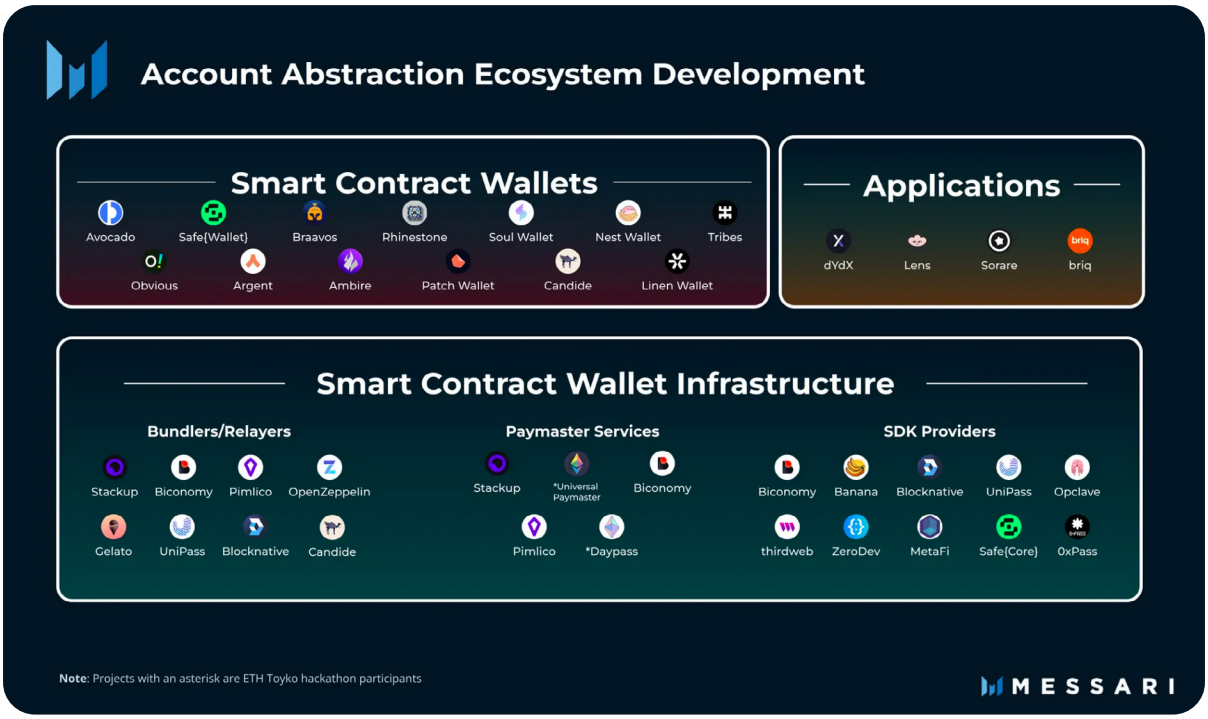


In case that graphic makes your eyes bleed, I will try to dumb it down.

When users interact with ERC-4337 wallets, they initiate “user operations,” rather than “transactions.” User operations get sent to special transaction pools where “bundlers” package them up and post them onchain. Bundlers can be centralized parties or decentralized networks, but they serve a similar function to block builders and searchers in onchain EVM transactions. They (slightly) re-intermediate crypto transactions, and open the door for service providers called Paymasters (who can pay gas costs for users), and Signature Aggregators (who can compress signature data to optimize transaction processing). The design has caught the attention of incumbent payments giants like Stripe and Visa - natural bundlers and paymasters in this new paradigm.

There isn’t a clear winner in the smart contract wallet space yet, but to date, Safe{Wallet} is the early leader. With nearly ~$35 billion in value secured on Ethereum alone, they’ve rolled their own relay network to support users, and partnered with Stripe to create an SDK that serves as a sort of app store for Safe users. Amongst other things, Safe partners can integrate fiat onramps in-app, powered by Stripe, which obviates the need to onboard to crypto through a centralized exchange. That’s a threat to the incumbent exchanges and an opportunity to DeFi projects like Uniswap which would prefer to create “SuperApp” wallets that onboard users with direct bank or credit card deposits without the requisite pitstops through Coinbase or Metamask, who are slowly moving downstream and could steal more DeFi users over time.

(Some layers like L2 zk-rollups (e.g. StarkNet and zkSync) have account abstraction available in their core protocols, but Ethereum provides account abstraction on an opt-in basis at the application layer via ERC-4337, which won’t require a core Ethereum protocol upgrade. Solana has always had native account abstraction via its program-derived addresses (PDA), and has always allowed for “program accounts,” which can store code. That capability allows for features like transaction bundling and custom multisig logic. GG, Solana.)



[*Required Reading: Towards Account Abstraction, The Account Abstraction Landscape*]

10.3 Wallet-Centric Future: Embedded "Wallets-as-a-Service" vs. SuperApps

Embedded wallets, as opposed to external, downloadable wallets like MetaMask, sit naturally within an application. This architecture was perhaps most famously used by progressive web apps like friend.tech this year, and helped create a seamless UX for users who never have to leave a new app in order to sign transactions.

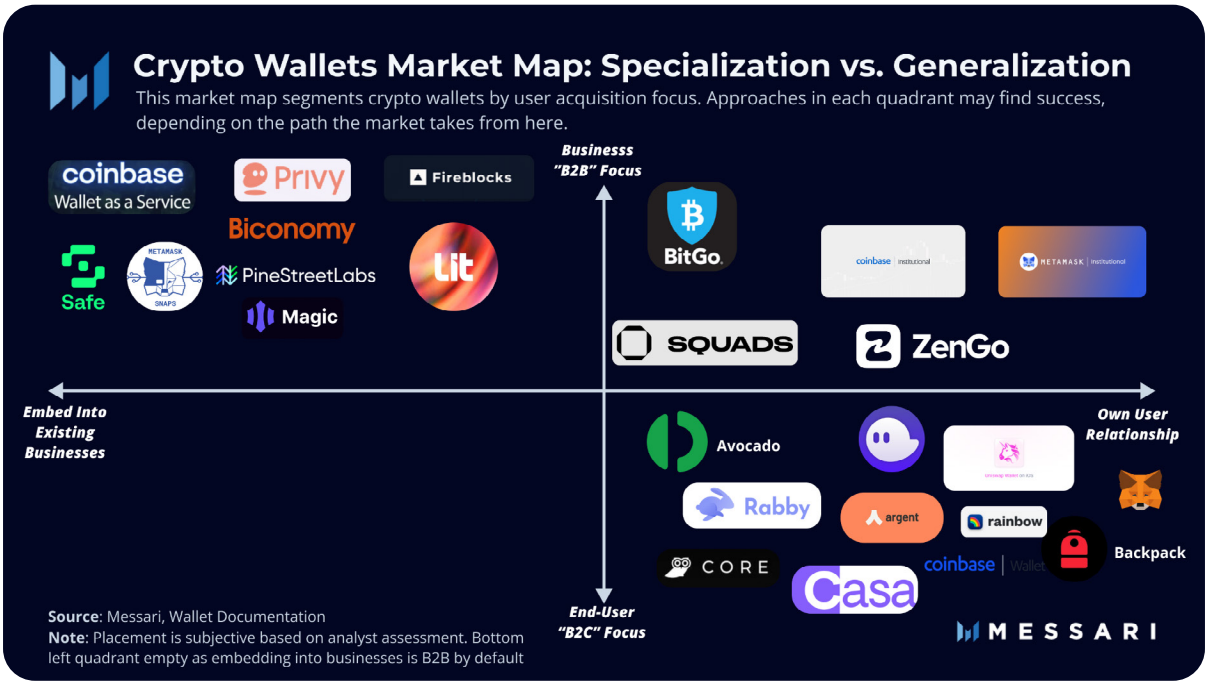
Whether you are talking about MPC wallets or smart contract wallets, the race is now on amongst the market leaders to embed their wallet tech as widely as possible.

Coinbase's MPC-based Wallet-as-a-Service (WaaS), MetaMask's "Snaps" and Safe's "App Store" allow third-parties to embed crypto wallets into their products and onboard users while outsourcing the arduous, and technically difficult, wallet creation and key management process onto the wallet designers. Those three wallet juggernauts can leverage their robust and trusted brands to capture the embedded wallet space, but things should get spicier.

Circle entered the fray with its "Programmable Wallets" release in August, and Fireblocks announced a similar MPC-based WaaS solution in September, which will power wallets for Indian e-commerce giant Flipkart.

To be honest, I'm not sure where the greatest points of technical differentiation will

emerge. The embedded wallet race feels like a marketing / BD / distribution contest rather than a technical space race, which leaves me wondering how other WaaS startups like Dfns (raised $20 million), and Privy (besides their steal of a partnership with friend.tech), will compete long-term.



Privy may have already accidentally shown the way forward: upstarts might consider pivots that swing from generalist WaaS platforms (top left) to super-app affiliated wallets (bottom right), where they'll likely find eager market-leading application partners: projects like Uniswap are working feverishly to ensure they retain control over their own user relationships, as third party wallet providers begin to blur the competitive lines.

It's not just about competitive forces, there are likely user benefits to specialized, vertically integrated "super app" wallets on a per sector basis. Uniswap could incentivize the usage and growth of its mobile wallet by subsidizing transaction fees for its users, offering unique compliance tools such as automated tax reporting for DeFi transactions, or making personalized investment allocation recommendations based on user inputs. Likewise, you could imagine something like an OpenSea wallet that incorporates unique features for game play and allows its users to natively access NFT lending platforms.

The idea of a fully integrated Instagram, Signal, Fidelity, and Bank of America is fairly terrifying, to be honest, and I think crypto apps will be no different. Many users will prefer to separate their NFTs, DeSoc accounts, DEX trading, and payments vs. aggregate them in a single wallet.

[Required Reading: Embedded Wallets]

10.4 The Ledger Recover Debacle

What's more dangerous: losing your private keys, becoming victim to a "five dollar wrench" attack, or allowing a third party hardware wallet provider to build a backdoor that allows for centralized, multi-party recovery of your wallets in the event you lose the device?

That's a debate that raged earlier this year, as Ledger battled through one of the biggest PR crises in its history. Though the criticisms of Ledger were overblown, the saga highlighted the challenges of managing the profound security / usability tradeoffs for crypto customers.

On the one hand, Ledger's new "Recover" product could make it easier for "normie" users to avoid catastrophic losses associated with user error and private key loss. The opt-in service would (for $10 per month) split up and send three "shards" of a user's encrypted seed phrase to Ledger and two of its independent partners, and allow the centralized services to recover the user key upon a user's request if they provided a National ID card.

But there was a (somewhat predictable) revolt following the company's rollout of the Recover product, as it became clear to users that it was even *possible* for Ledger to push a firmware update that could export encrypted private key data from its devices. Many people had previously been under the impression that this was purely impossible, similar to how Apple's "secure enclave" works in its iPhones. Dragonfly partner, Haseeb Qureshi, explained how this reflected a technical misunderstanding of hardware wallets (and corporate communications snafu), rather than a real vulnerability. But Ledger was forced to clarify that the Recover feature could make user keys available to governments and civil litigants under certain scenarios (e.g. criminal investigations or national security requests).

When I read all of this, my first thought was "no good deed goes unpunished." The benefit of Ledger addressing the risks of self-custody with a reasonable user recovery service probably outweigh the risks that funds are ever seized by authorities via a court order.

But as I've considered it further, I worry that this sort of thing could open a pandora's box for bad global regulatory requirements. If governments move to ban self-custodial wallets *without* Recover-like features, are these companies in much of a position to fight back? This doesn't exactly seem like a negligible risk in Europe post-MiCA and TFR. I worry about the default slowly shifting from "opt-in" to "required for citizens in [country]."

I'd much rather see a divergence between the hardware wallets available on the market, as Ripple's David Schwartz summed up: Ledger (or another company) create two separate firmware release streams, one with account recovery and one without. Ideally, users could buy devices without account recovery features, and only add the Recover firmware if they first wiped the device of all previous key material. And Ledger could make a public commitment not to introduce features that would change their default firmware streams to permit key material to leave the devices after keys were generated. This would be functionally similar to creating a non-upgradeable "ASIC" wallet.

I'm glad this drama unfolded in the midst of a bear market to be honest. I think it's important that we have these philosophical battles around user defaults and state seizure resistance while the stakes are still relatively low. I expect we'll see both new

hardware models, and a variety of new services that handle high stakes edge cases (like inheritance) in the year ahead.

10.5 DePIN Storage Wars

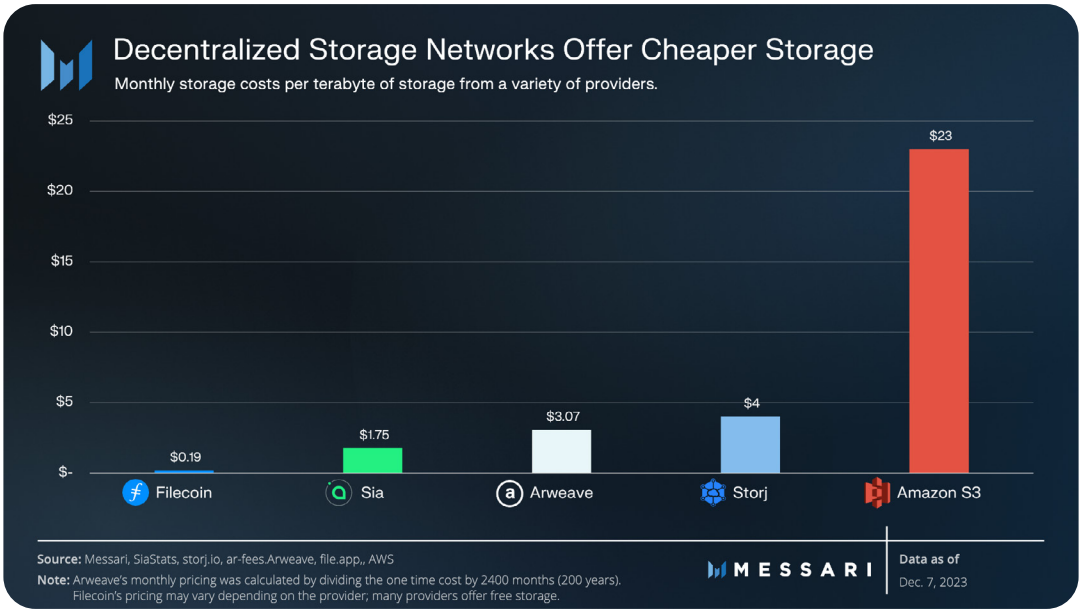
If wallets are the front doors into the house of crypto, hardware networks are the foundation. I don't think there is a more important area of long-term development than decentralized physical infrastructure networks (DePIN).

Token models have long helped align the crypto software development market, but they've been just as important in shepherding physical resources, starting with bitcoin and ethereum mining. In recent years, tokens have helped accelerate the build out of physical infrastructure networks that makes the internet itself harder to censor or shut down. DePIN spans storage, computing, wireless connectivity, energy networks, geospatial data collection and more. It's one of crypto's most vibrant ecosystems, and progress only seems to be accelerating.

We can break down DePIN into two main forks: Physical Resource Networks (PRNs) and Digital Resource Networks (DRNs).

PRNs incentivise participants to deploy *location-dependent* hardware that provisions resources to certain physical locations for energy, geospatial data, or connectivity use cases, whereas DRNs create a new l*ocation-independent* back-end for the cloud, incentivizing market participants to provision certain digital resources like compute, storage and bandwidth.

The market demand for DRNs has continued to explode (from a small base), but we have still only scraped the surface in potential adoption. The cloud storage market is $80 billion and growing 25% per year, while decentralized alternatives serve under 0.1% of the market, even though they cost 70% less than providers like Amazon S3.



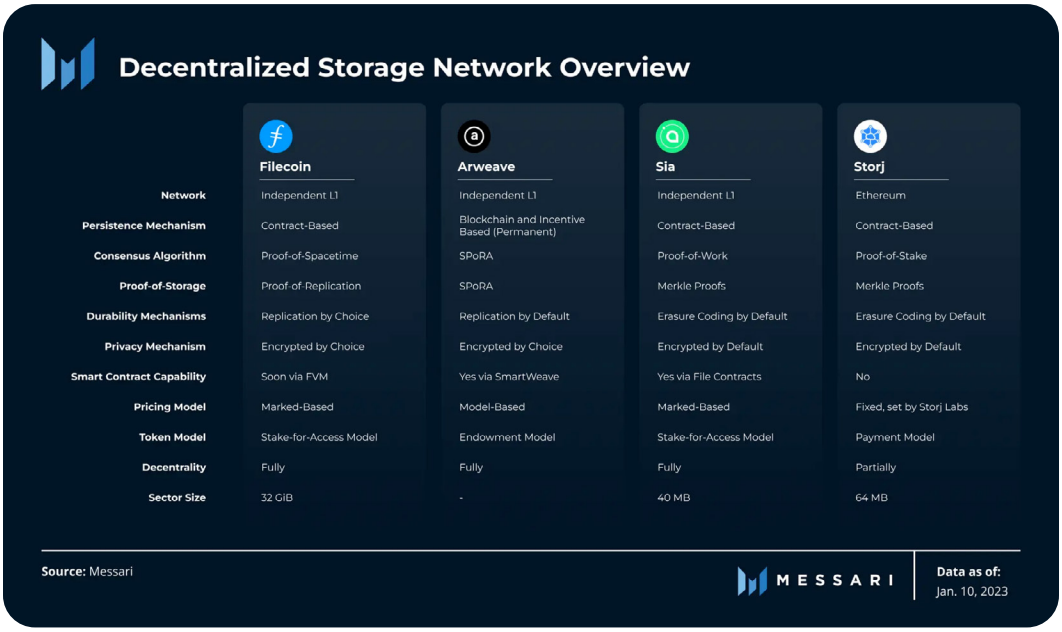
As I outlined in Chapter 1, at the very least, these networks offer a cheap "hedge" and decentralized redundancy, which may be attractive to enterprises looking to back up their services in emerging markets with subpar infrastructure or who are operating in gray market industries at heightened risk of censorship. Of the major decentralized storage providers, four are worth highlighting in particular:

- **Filecoin** is primarily geared towards providing cold storage solutions to enterprises and developers. Its competitive pricing and ease of access make it an appealing choice for Web2 entities seeking cost-effective alternatives for storing large amounts of archival data. It's the dominant storage network by capacity and utilization today.

- **Storj** is optimized for providing hot storage to enterprises, offering cloud object storage that is compatible with Amazon S3. It offers fast retrieval times and has proven effective for large video file sharing. These features have led Storj to focus on the media and entertainment industries.

- **Sia** is also positioned within the hot storage market and largely targets developers. Sia appeals to users looking for a private storage solution with quick retrieval times.

- **Arweave** is particularly attractive to NFT, metaverse, and decentralized social projects thanks to its innovative "pay once, store forever" model. Sami's modeling shows potential Arweave demand increasing 20x over the next three years. (How might that impact the token price?)



It is unlikely most businesses will ever revert to hosting their own server infrastructure in-house and managing complex hardware setups. But it's equally unlikely many of them will continue to blindly trust centralized Big Tech vendors either, especially given that in some cases, those firms have told us not to trust them. Instead, we'll see the emergence of a "hybrid cloud" where computing is managed across multiple public cloud services and integrated local and edge infrastructure. That's a boon for DePIN, a sort of mean reversion

to the historical status quo where enterprises better control their hardware.

In a tech ecosystem driven by outrageous hype cycles, the economics behind DePIN networks are easier to understand ("Airbnb for digital storage"), and their tokens are easier to underwrite. If decentralized networks eventually take 10% of the cloud market, the results in this sector will be eye-popping. You can check out the full market map of who we're watching here, though there are three areas beyond decentralized storage that I'm watching particularly closely.

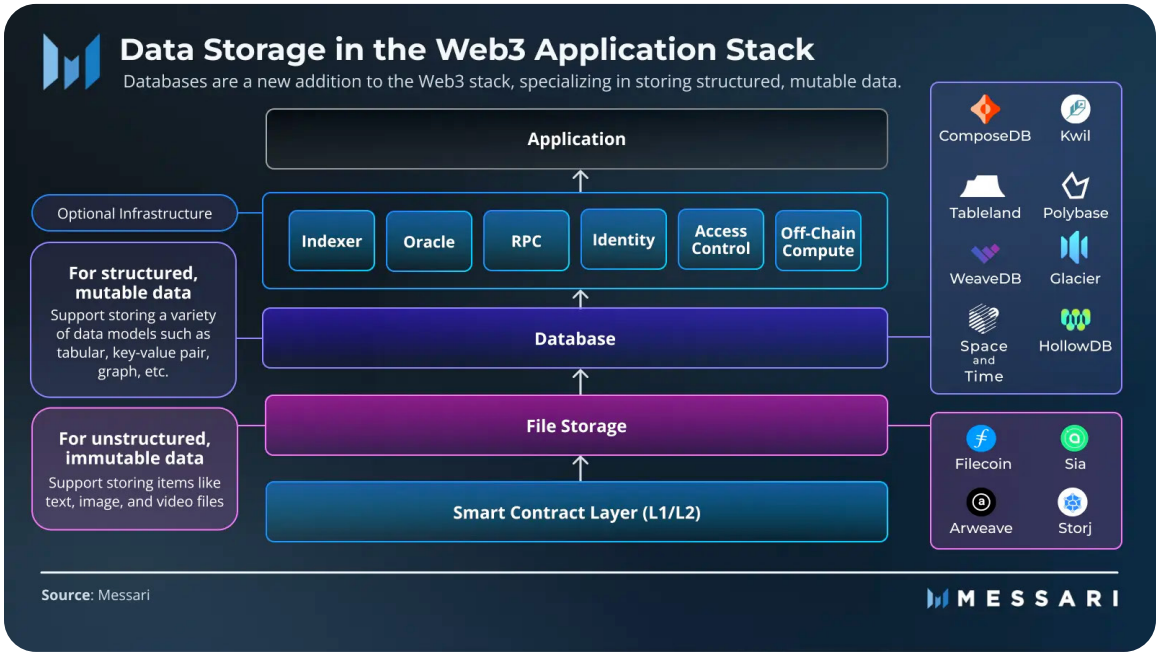
Decentralized databases, AI-adjacent crypto computing networks, and wireless plays.

[Required Reading: Navigating DePIN, Essentials of Decentralized Storage, Evolving Cloud Frontiers]

10.6 Decentralized Databases

Decentralized storage networks are only as powerful as the decentralized databases that make network data accessible.

I'm looking for breakout infrastructure projects that allow developers to build on better indexed data sets (The Graph), leverage decentralized data warehouses (Space & Time), and offer decentralized access control systems (Lit Protocol). Decentralized databases have suffered from major performance and latency issues historically, but there are glimmers of hope that these products level up significantly in 2024, and it's one of the areas of greatest opportunity in the DRN segment of DePIN. Applications in DeSoc, gaming, dynamic NFTs, and ML/AI will all depend on a proliferation of decentralized databases.

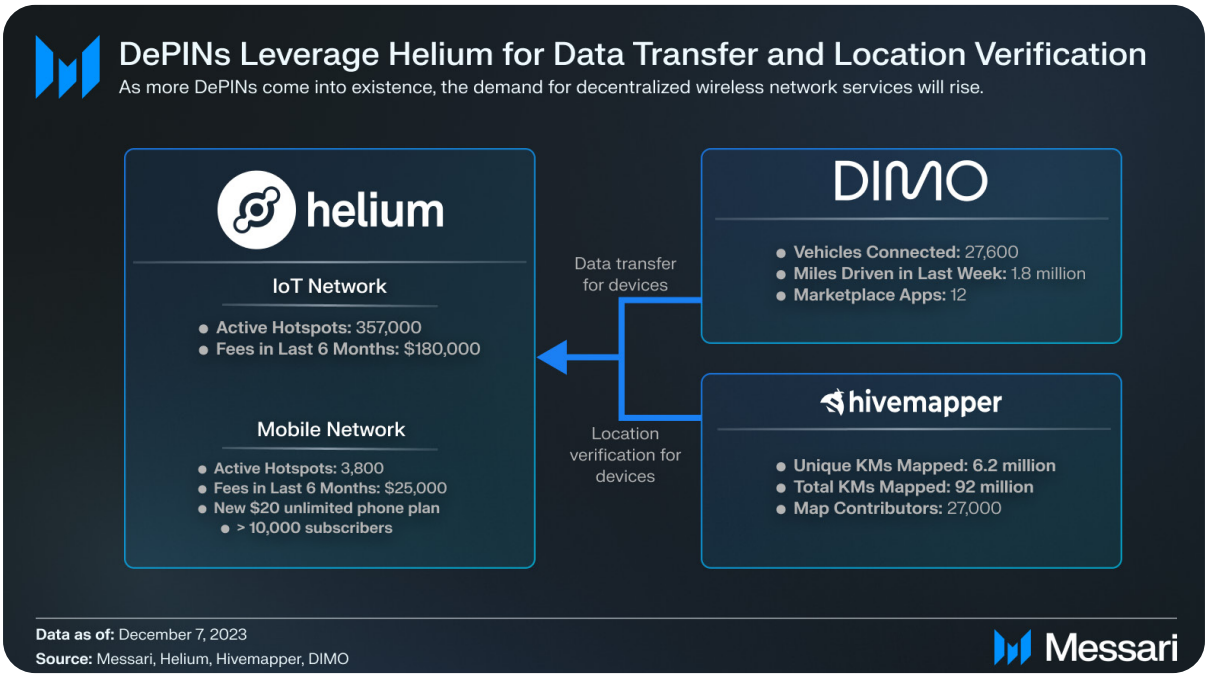


[Required Reading: Decentralized Databases]

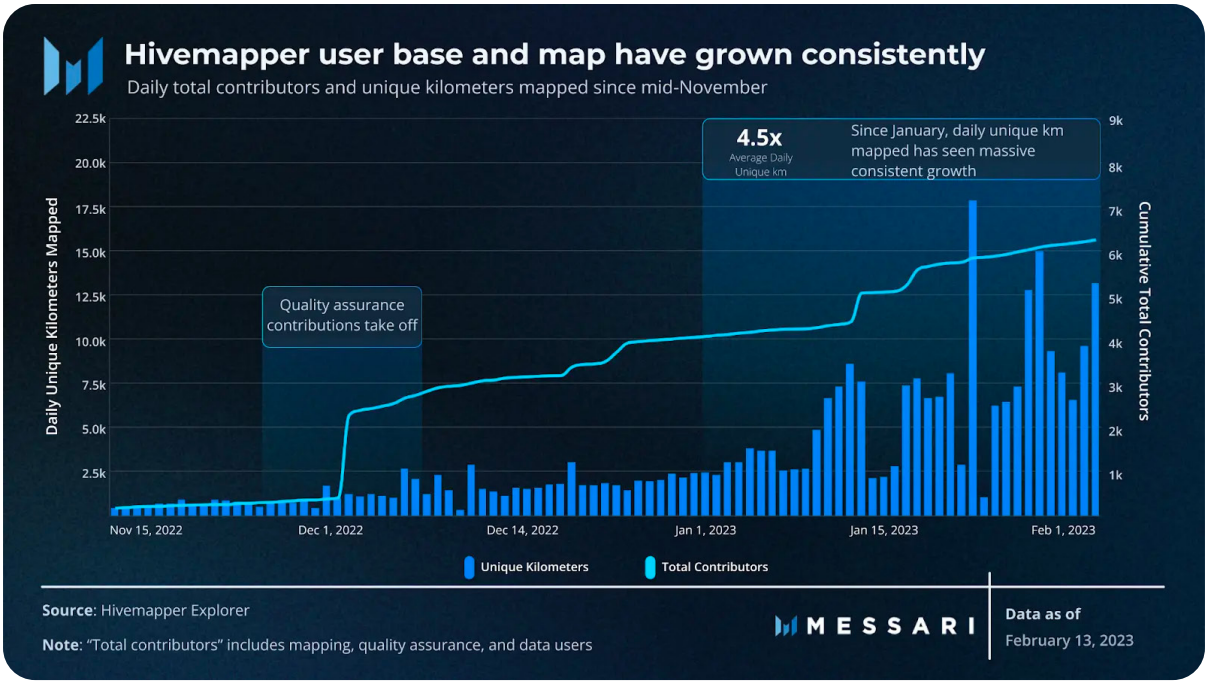
10.7 Decentralized Wireless Networks

Physical Resource Networks are having a moment. Helium Mobile, a carrier built on the Helium Network, introduced a $20 monthly phone plan this summer alongside T-Mobile, which offered unlimited text, talk, and data to new customers without the constraints of a wireless customer contract. Similar to the “hybrid cloud” model of decentralized storage networks, Helium Mobile created a “hybrid coverage” model, Dynamic Coverage, that leverages the reliability of an established network for high-quality roaming services that fill in the gaps for customers beyond Helium’s early bootstrapped coverage map.

At the same time, Helium Mobile customers have the opportunity to earn crypto through a program called Discovery Mapping, when they share their location data. This not only provides incentives to make the switch to Helium Mobile, but helps identify areas where additional radios might enhance network coverage and improve the quality of the service. Helium’s location and data transfer network can also benefit other DePIN networks like Hivemapper and Dimo which need to transmit their devices’ data which provides an additional revenue channel on top of traditional wireless monetization.



Critics will question the sustainability of Helium Mobile’s cost structure and the increasingly absurd regulatory constraints facing these sort of projects, but they would be betting against a team that has already installed functional hardware networks at scale in the past. I, for one, am in favor of any project that helps break the stranglehold of our data (Google and Apple) and wireless infrastructure (AT&T and Verizon) duopolies, and will be signing up to test it after I finish this monstrosity of a report. Fred Wilson already has it!

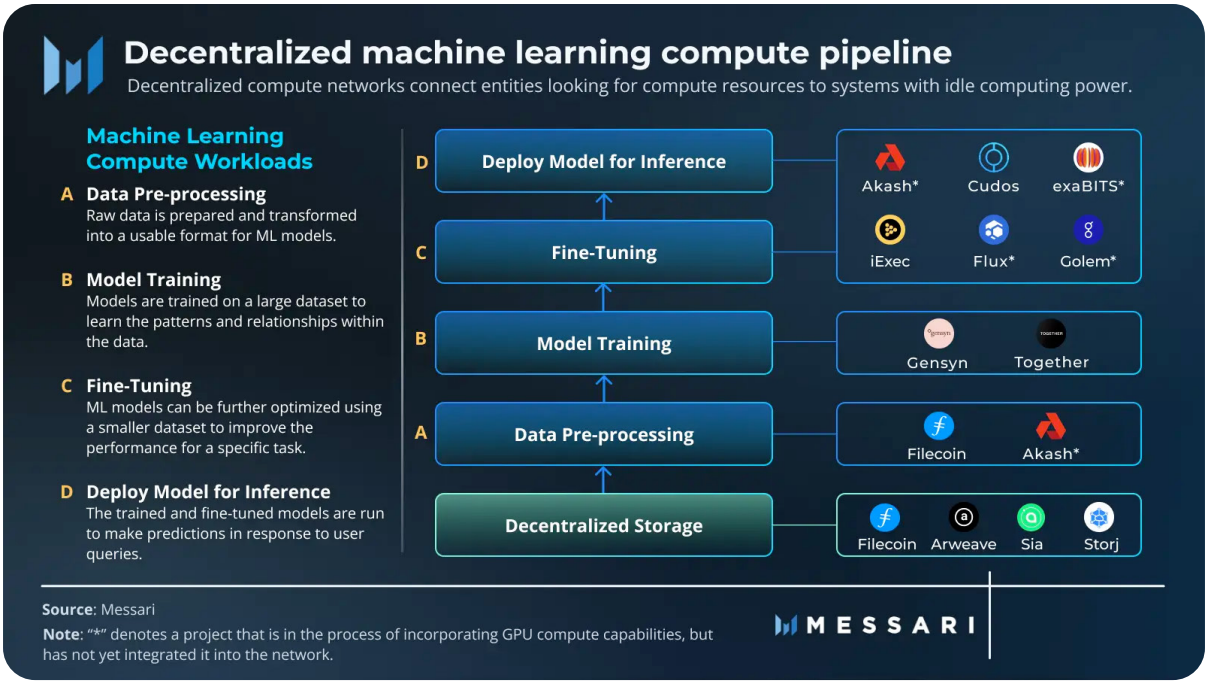


10.8 DePIN's AI Machines

The AI revolution is largely a revolution in hardware. Nvidia was the top performing Fortune 500 company of the year. (And hardware-driven Meta isn't far behind.) The failed coup against OpenAI founder Sam Altman appears to have been driven in part by his efforts to raise billions of dollars for a new specialized AI chip. And AI solutions in crypto will similarly be hardware centric.

The development of artificial intelligence is currently facing two critical challenges: the computing bottleneck, which is a sort of speed limit on development, and a lack of collaboration, with most AI research being conducted behind the secretive confines of big tech companies and AI labs. The dual trends create risks that AI will concentrate in the hands of a few centralized powers.

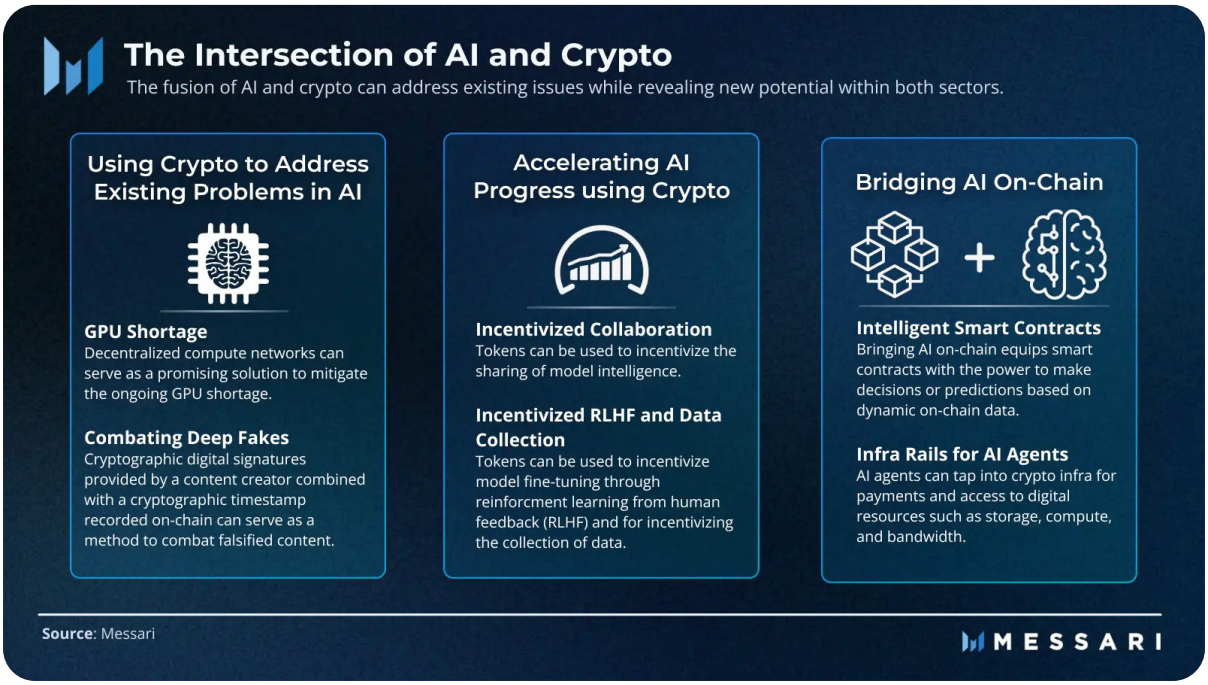
AI projects within crypto are addressing both issues. Decentralized GPU marketplaces like Gensyn offer a solution to the imbalance between the short supply and skyrocketing demand for the GPUs needed to train AI models, creating a sort of decentralized supercomputer. Bittensor is revolutionizing the way AI researchers work together by incentivizing the creation and sharing of machine intelligence. The Bittensor network enables individuals to contribute to open-source AI and monetize their work, regardless of the size or niche of their contributions. This is akin to how the internet made niche contributions economically viable and empowered individuals on content platforms like YouTube. In essence, Bittensor strives to commodify machine intelligence and become the internet for AI.



Additionally, the convergence of AI and crypto widens the design horizons of crypto in a few ways:

1. AI agents can utilize crypto infrastructure for payments and access to digital resources (storage, compute, bandwidth) autonomously.
2. Innovations such as "zkML" enable smart contracts to securely query AI models, thus broadening the capabilities inherent to blockchains.

3. Tokens provide a means to reward individuals for fine-tuning models and for collecting valuable real-world data, intersecting with DePIN.



[Required Reading: Growing Synergies in AI and Crypto, Decentralizing Machine Learning]

10.9 Select DAO Dysfunction

In the crypto-utopian vision of the future, DAOs would be benevolent, AI-driven protocol governors that operate with clear objectives and make excellent resource allocation decisions.

Here's how DAOs actually work:

1. A founder or small group of founders create a project. It could be a new protocol or an investment vehicle (for venture capital, research, public goods funding, etc.), or a combination of the two. Remember, DAOs are basically group chats with bank accounts.

2. The founding group launches a token that confers some governance rights over the project's assets (IP and funds), and potentially economic rights (fees on the protocol or upside in the investments made). They make the initial decisions on how that token will be distributed (private token sale, airdrops, incentive farming, contributor tokens with vesting, bonding curves, etc.), and who will manage the distribution (a "Labs" company, a foundation, a token-governed DAO, or a combination of the three).

3. All three types of entities at the core of token projects are largely unaccountable. Labs entities tend to have major conflicts that implicitly or explicitly encourage them to double dip on their work in ways that misalign their shareholders and project token holders. Many of today's foundations are black boxes run by unaccountable bureaucrats. And DAOs themselves have been deemed "unincorporated associations" by the U.S. courts, which open up their contributors to uncapped personal liabilities.

4. Protocol governance is an emerging field with no set standards, and legal and regulatory clouds frequently create disincentives to improve governance. Transparency is used against projects, by agencies like the SEC, and the delegates that tend to fill governance gaps at major projects are a sliver of market participants who are willing to take on outsized legal risks (or are unaware of them) post Ooki. The courts have essentially made it functionally impossible to move towards representative democracy.

5. These dynamics create graft (nepotistic rewards between related counterparties and the equivalent of no-bid contracts), security issues (there are few well-incentivized watchmen paying attention to day-to-day operations, with slow reaction times in the event of crises), and underperformance due to mob rule (as George Carlin explains, Democracy means that 50% of the voters governing you are dumber than average).

When you lay it out like this, it is miraculous so many crypto projects survive at all, and it brings credence to the idea that projects that survive and thrive with today's community governance norms truly are run by zealots "in it for the code" and will probably get more antifragile over time. Early crypto governance is like a mash-up of early American Federalism and Silicon Valley boardroom hijinks. It's a shitshow, and it's glorious.

In the absence of well-compensated professional managers and legal structures that actually work, most DAOs will likely operate under the crypto equivalent of the "Mandate

of Heaven," with founders operating in public and enjoying a great deal of deference, with cursory checks provided by off-chain signaling tools such as Snapshot to ensure things stay on the right path directionally. Often, these checks will be mere "ratifications," not true "proposals" subject to token holder vetoes.

We'll eventually see a fork between two different types of DAOs: true Decentralized Autonomous Organizations, which are run by intelligent AI agents and actually run autonomously (exciting and terrifying possibilities), and "Delegated Authority" Organizations, which more closely reflect today's communities, but with the benefit of legal entity wrappers.

To that end, the most meaningful developments for DAO governance over the next few years might take place in legislative chambers and amongst crypto lawyers, not onchain. As outlined in Chapter 5, don't hold your breath on U.S. federal legislation. Instead, keep an eye on smaller countries and U.S. states. The path to success will be at the state level - similar to the LLC's journey to mainstream acceptance back in the 70s. So far we have seen some form of DAO legislation in four (soon to be five?) states: Wyoming, Vermont and Tennessee had early legislation that contemplated DAOs as legal constructs, Utah joined the fray this year. And a DAO bill passed the Texas House this spring, and awaits consideration by the state Senate.

Mind-numbing, but important work that will dictate whether onchain governance becomes a legal possibility or gray market pipe dream.

These aren't mere thought experiments. Poor governance is expensive, and non-trivial, to solve. DeFi protocols face three core challenges to decentralizing governance power: Sybil attacks, low token claim rates for airdrops, and abysmal retention rates.

10.10 DAOs Are Worth the Headache

There's a criticism that DAO governance essentially boils down to this: we're simply re-learning all of the mistakes of the past in corporate governance, and building the equivalent corporate norms onchain after expensive trials and errors.

There's some truth to that, but I think we don't give enough credit to the few things that DAOs are *really* good at.

1. **They are lightning fast and cheap** to create from scratch. You can spin them up for virtually nothing, fund them, manage them, exit them, and functionally destroy them (by liquidating their onchain assets) within minutes. U.S. lawyers might scoff at this, but in countries with a weak rule-of-law, or for small or anonymous groups operating in gray market industries, these benefits will far outweigh any potential risks.

2. **Code crosses borders (and can reach friendlier jurisdictions) faster than legal process can react.** Which means that the legal "nexus" of a DAO is fluid, and

liability is more difficult to enforce *at* scale. Although a U.S. judge ruled that "Ooki DAO" should have registered as a CFTC-regulated commodities trading platform, it's unclear who will actually pay that court-ordered fine, or how that penalty can and will be enforced. No individual DAO members were found liable, and there is no corporate entity. That sort of jurisdictional arbitrage is an advantage to DAOs in practice, even if authorities throw the book at some of the more egregious DAO "representatives" in a scattershot approach. It resembles the SEC's selective enforcement actions against various token projects during the ICO boom. There are simply too many DAOs to pursue, and not enough government resources. (The bigger risk is on the civil liabilities side, as there will never be a shortage of plaintiffs' attorneys, who now have the upper hand in commercial litigation following the Ooki precedent.)

3. **There is unlimited potential for creative new corporate actions.** The frontier of new types of transactions, IP deals, and new management models are limitless. Imagine a hostile takeover via a flash loan: rather than conduct a malicious oracle attack, a buyer could "take private" or merge a protocol by amassing majority control of a protocol in a matter of seconds. We're already seeing plenty of experimentation in the user-generated experience genre. Shorting a DAO's potential based on short-term headwinds betrays a lack of imagination or sense of crypto history.

That said, there is nothing I would rather waste my time or limited lifeforce on than precedential onchain M&A or proxy battles.

Yes, there is potential for project consolidation, synergies of various projects and their treasuries, etc., but it all sounds nightmarish to me. Consider Aragon's years-long battle for its $200 million treasury, which may yet end with a wind down of the project. Fei protocol's ill-fated merger with Rari and ultimate dissolution of the project. Arbitrum's pre-spent "spending authorization" bill.

DAO governance limitations remind me a bit of our historical exchange compliance limitations: the most qualified people to serve as DAO representatives and proxy voters are also the most attuned to the risks of "serving" in such a precarious capacity. The courts are going after some of the higher profile DAO leaders who have participated in good-faith onchain protocol governance in the past. I think it's a travesty to punish good faith efforts at crypto governance, and that DAOs are worth fighting for.

But I'm sure I'm not alone in shying away from today's unlimited liability status quo. This is a dilemma I personally want to help solve in 2024.

We can and should set better governance standards, and browbeat regulators into working with us on safe harbors in whatever jurisdictions we can.

[Required Reading: A16z's DAO Canon, Machiavelli Series - Part 1 and Part 2]

BONUS

RE-READ

As I did last year, I'll share some final thoughts for anyone interested in how the horrible monkey inside my mind works and processes the world - inside and outside of crypto.

1. Why You Must Write

I've been asked how I can write this annual report and still run a company. As I said in the introduction, this is a good marketing asset for attracting enterprise customers, partners, and recruits; it should drive good conversion to our Pro product (ahem), and it doubles as my annual crypto deep dive and product ideation session. "What did I miss, and where are we headed?"

I'd flip the question back to you: how can you survive the remote-first, globally-distributed, hyper-growth, crypto chaos without writing well? Reading helps me identify blind spots, but it's writing that helps me focus and streamline my thoughts.

Whether it's code or prose, you must get better at writing.

And when you write, be concise and write music. Last year, I wrote: *"good code elegantly communicates your ideas to computers, and spits out products that delight users. Good prose elegantly communicates your ideas to other humans, incepting new ideas into their heads (through memes), and if you're doing it right, converting missionaries to your cause."* With the advent of AI, the two are going to merge.

Get busy writing (or as the cool kids call it, "prompt engineering") or get ready to become obsolete. We are entering a brave new era of the internet.

2. No Idols

Never become the main character on Twitter.

If you want a case study in the perils of a high profile, just look at the number of "crypto billionaires" who are now on the lam, penniless, or in prison after overextending themselves and believing too many of their own press clippings.

Stay hungry and humble. Stay disciplined. Stay hard. Merry f*cking Christmas.

3. Must Read

High Output Management, Principles, Crypto, The Federalist Papers, and although he was no fan of bitcoin, Charlie Munger's Poor Charlie's Almanac. Learn the Cadence of a SaaS startup, lessons from vertical software investing, and how to work backwards. Subscribe to *On the Brink*, the top crypto pod. Turn off Twitter notifications.

"Don't follow your passion. Seriously. Don't follow your passion. Your passion is likely more dumb and useless than anything else. Your passion should be your hobby, not your work. Do it in your spare time. Instead, at work, seek to contribute. Find the hottest, most vibrant part of the economy you can and figure out how you can contribute best and most. Make yourself of value to people around you, to customers and coworkers, and try to increase that value every day."

4. Tips & Productivity Tricks

The most important productivity hack I recommend at work is surrounding yourself with good people who are insanely mission-driven, relentless, organized, communicative, and poised. I'm lucky to have found good, hard-working people who share my vision for the future, and help bring it into sharper focus each day, while allowing for the fact that there are some things I will simply never get better at, regardless of my best efforts.

That is to say, thank you to the Messari team (especially the leadership team) for running a tight ship that helps me disappear for a month to write this damn thing. Here are a few of my other habits, for better and for worse.

Communication: I live by Gmail's snooze button and multiple inbox setup, which serves a similar purpose as software like Superhuman. I also use pinned Twitter lists, keep open DMs, maniacally filter, unsubscribe, and report negative messages on Twitter and email. I've significantly limited my time on Telegram and Discord this year, and I'm happier for it. Slack for the team, email for business, Twitter for play. That's it.

Meetings: I try to limit internal meetings to 20% of my time per week, which is not bad when you add up product syncs, bi-weekly all hands, 1:1's, monthly functional team meetings across eight different groups, quarterly skip-level meetings, and other miscellaneous strategy, product, and HR syncs that arise in the normal course of scaling.

Mind, Body, Soul: I have had Headspace installed on my home screen for ~~five~~ six years and have used it ~~12~~ ~13 times. (Once since last year! Again!) I have also learned that I get a really good night's sleep when I read books before bed and turn off my phone without ending my day doomscrolling Twitter. I have even done this successfully three or four times, and I have completed the first chapter or two of dozens of books. I have gotten so out of shape sprinting to finish this report, so I'm going to go hit things now. (Thanks, Fightcamp.) I'm also starting to get into longevity, as that's what crypto people do when they realize that money doesn't buy health.

5. Life Advice

I'll end the same way I did last year and the year before: I don't know what I'm doing and neither do you.

But if you are fortunate enough to do so: get married, have kids, and move to the burbs. (Eventually). You will survive the winters and gain some valuable perspective when your day ends with a seven-year-old laughing about one of his farts, a five-year-old telling you a story via a three minute run on sentence, a half-naked three-year-old tackling you at the knees during your final Zoom call of the day, and a newborn who's starting to giggle. (Four is enough by the way, I'll be taking a long weekend for March Madness or the Masters this year.)

If you're reading this, you are (hopefully) a time billionaire. That does not change the fact that you are at The Tail End of many of your relationships (I read this post once per year), and that it is always Day 1 and everything is in your control.

2023 is in the books. Good. Onward.

6. End. My Lawyers Made Me Do It - AKA Disclaimers

We know this is obvious, but the Theses is neither financial nor investment advice. You should conduct your own research, and consult an independent financial, tax, or legal advisor before making any investment decisions. Nothing contained in this report is a recommendation or suggestion, directly or indirectly, to buy, sell, make, or hold any investment, loan, commodity, or security, or to undertake any investment or trading strategy with respect to any investment, loan, commodity, security, or any issuer. This Theses should not be construed as an offer to sell or the solicitation of an offer to buy any security or commodity. Messari does not guarantee the sequence, accuracy, completeness, or timeliness of any information provided in this Theses. Author(s) may hold cryptocurrencies or other assets named in the Theses, and each author is subject to Messari's Employee Holdings Policy and Disclosures. Additional disclaimers apply - check out our Terms of Service for more information.

messari.io