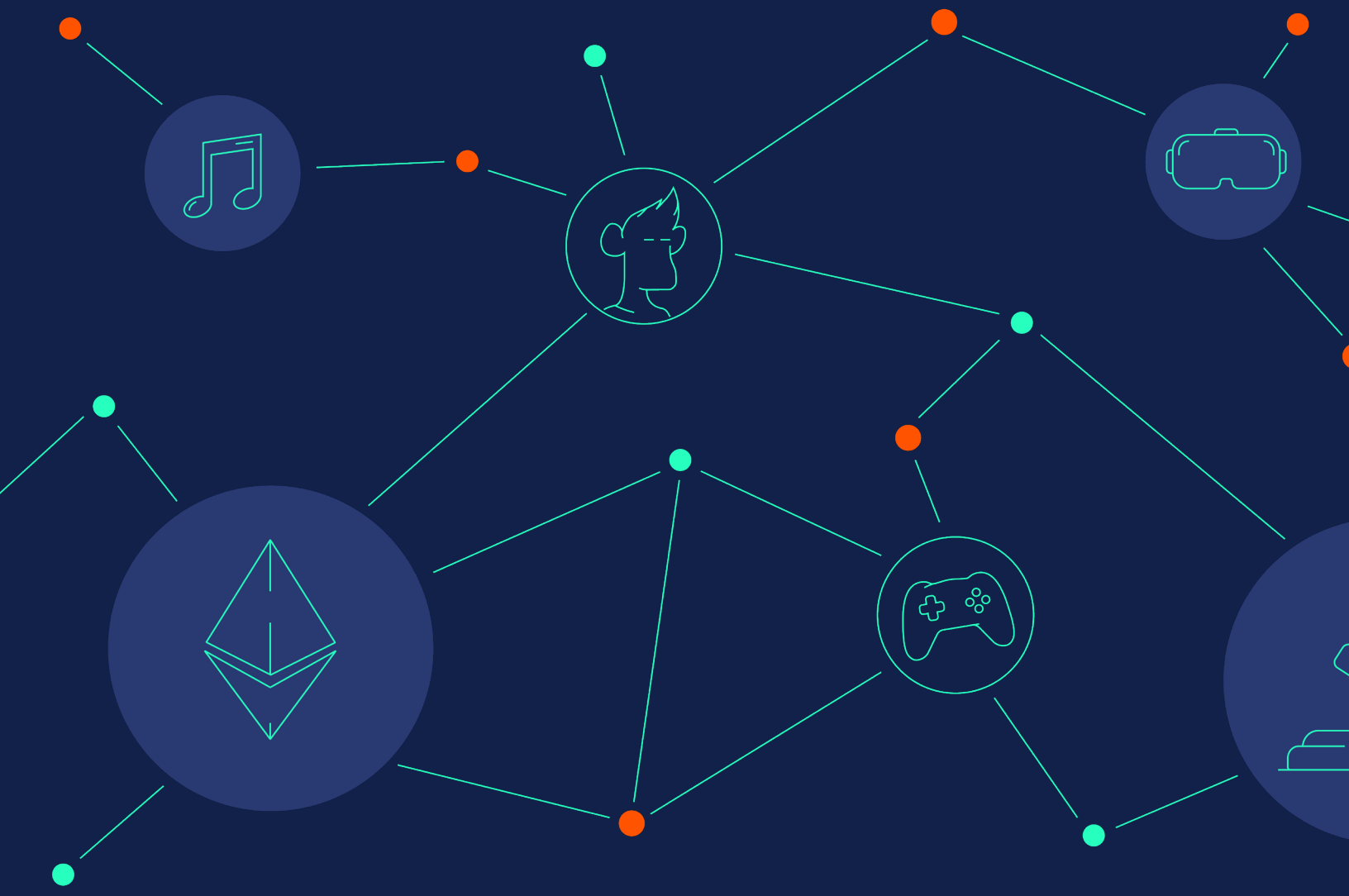
Chainalysis June 2022

The Chainalysis State of Web3 Report

Your guide to how blockchains are changing the internet



Web3 Is the Path for All Companies to Become Crypto Companies

In the '90s, many thought the idea that all companies would one day become internet companies was crazy. We see similar naysaying with cryptocurrency today — or, as many in our industry call it, "FUD," meaning Fear, Uncertainty, and Doubt. So, FUDders be damned, allow us to make a bold prediction:

One day in the near future, all companies will become crypto companies, complete with a "Connect wallet" button on their homepages. And web3 is how they'll get there.

This will happen for a few reasons. First and foremost, as more people enter the world of crypto, they'll need a seamless way to use their funds for everyday financial activity without converting back into fiat currency. Cryptocurrency is still niche in many ways, with an estimated 8% of Americans currently owning crypto assets. However, that number is growing every year — not just in the U.S., but around the world — and may soon reach a tipping point where adoption accelerates to mass levels.

As more people put a higher percentage of their net worth into cryptocurrency, they'll want the ability to use cryptocurrency for the full range of transactions they can currently carry out with fiat, such as lending and borrowing, trading assets, and payments. Web3 will enable them to do that with cryptocurrency faster and more easily than they can today. Let's use mortgage approvals as an example. Today, borrowers need to go through a cumbersome mortgage application process that relies heavily on human judgment — judgment that studies show often reflects human biases and unfairly punishes marginalized communities. In a web3 world, that process becomes faster and fairer. Borrowers would just connect their wallets, and an algorithm could instantly give them a yes or a no based solely on their financial profile and transaction history as represented on the blockchain.

Web3 won't just streamline existing financial activity though. It'll also unlock new use cases in finance that currently aren't possible due to the illiquidity of traditional assets. Imagine a world where you could sell fractional ownership of physical assets like real estate or vehicles. Sellers would be able to access capital they can't today, while buyers could invest in those assets more affordably via partial ownership. Web3 can make that happen.

Web3 can also eliminate middlemen and foster more direct relationships between sellers and customers. We see this most in art and entertainment, where artists and creators are already connecting directly with their fans through social media and content hosting platforms like Twitter, YouTube, and Substack, no longer having to rely on mass media platforms like newspapers and broadcasters. Still, these web2 platforms, and even more fundamental ones like payment processors and web hosters, can exert control over the artist-fan relationship through censorship, traffic throttling, and the like. Web3 can take middlemen out of the equation completely, and even opens up the possibility of fans purchasing full ownership of work from their favorite creators, rather than essentially renting it as they currently do from content providers like Netflix. NFTs are already enabling much of this, largely in static digital art, but the arrangement could easily be applied to music, film, and other mediums.

Finally, web3 can bring decentralization to the business world by enabling community ownership of companies rather than the current norm of top-down corporate control. We see this happening now with DAOs — decentralized autonomous organizations — in which anyone who buys in can help guide the direction of a company or project through an asynchronous voting process. DAOs already control some of the biggest protocols in DeFi, such as Uniswap and AAVE, and as web3 takes hold, we expect to see them make waves in other industries.

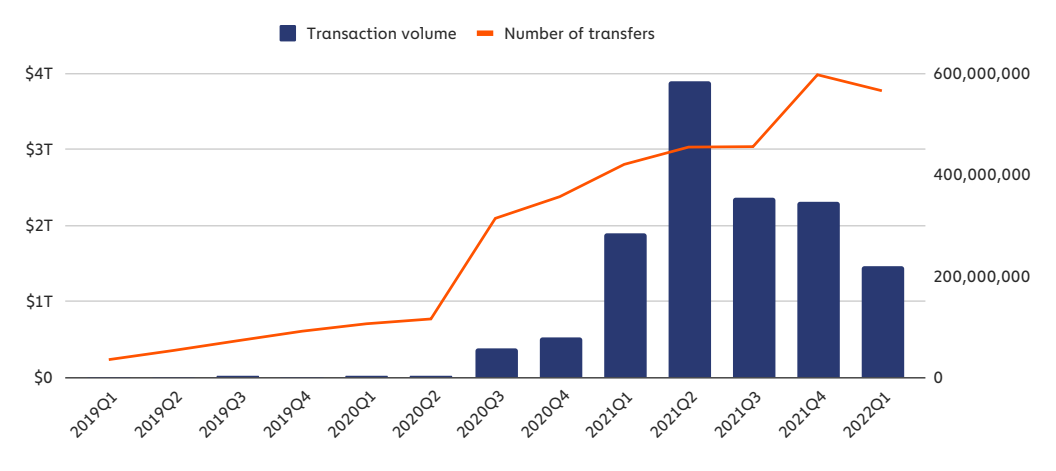
Where we are now and what happens next

The increasing transaction volume associated with DeFi protocols, which form the backbone of the web3 ecosystem, show that the web3 transformation is well underway.

DeFi activity exploded in 2021, peaking in Q2 at nearly $4 trillion in transaction volume. While growth has since leveled off, in part due to price

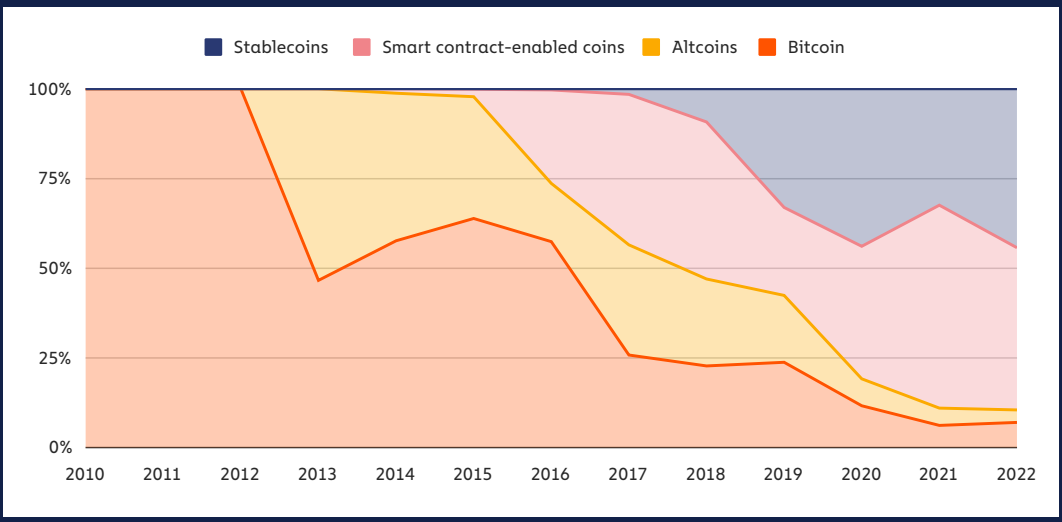
declines for Ethereum and other assets, the number of individual transfers has stayed level and even increased in some quarters, which suggests that more individual investors are still entering the ecosystem.

DeFi transaction volume and number of transfers by quarter, Q1 2020–Q1 2022



We also see DeFi's growth reflected in how the usage of different crypto assets has changed. Total transaction volume — once dominated by Bitcoin — now comprises a multitude of smart contract-enabled coins like Ethereum.

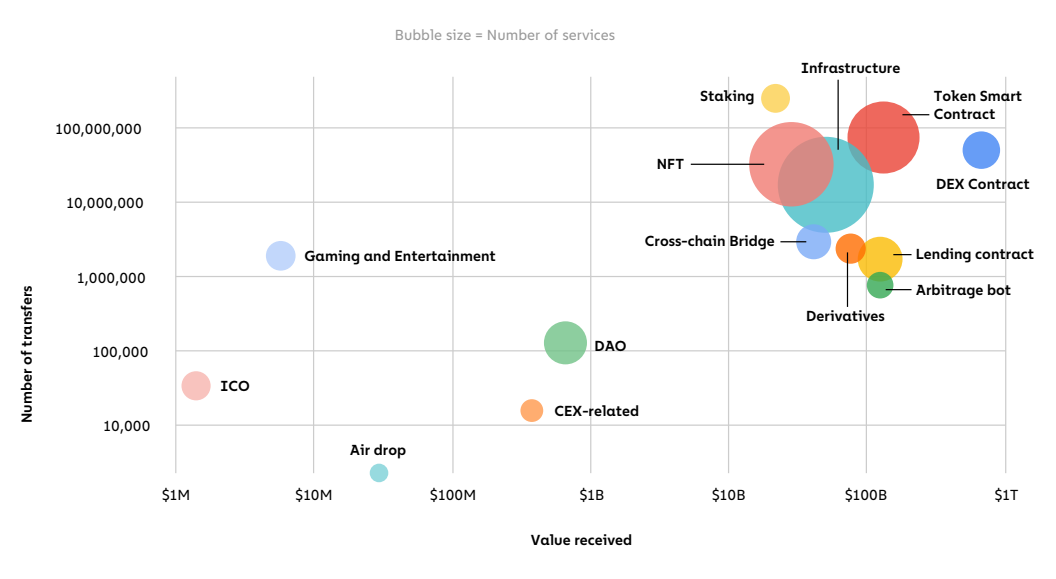
Share of total transaction volume by currency type, 2010–2022



Bitcoin accounted for the majority of crypto transaction volume as recently as 2016, but so far in 2022, represents just over 10%. Stablecoins account for

much of that, but cryptocurrencies with the smart contract functionality that powers DeFi and web3 now account for 45%.

Total value received, number of transfers, and number of services by DeFi service type



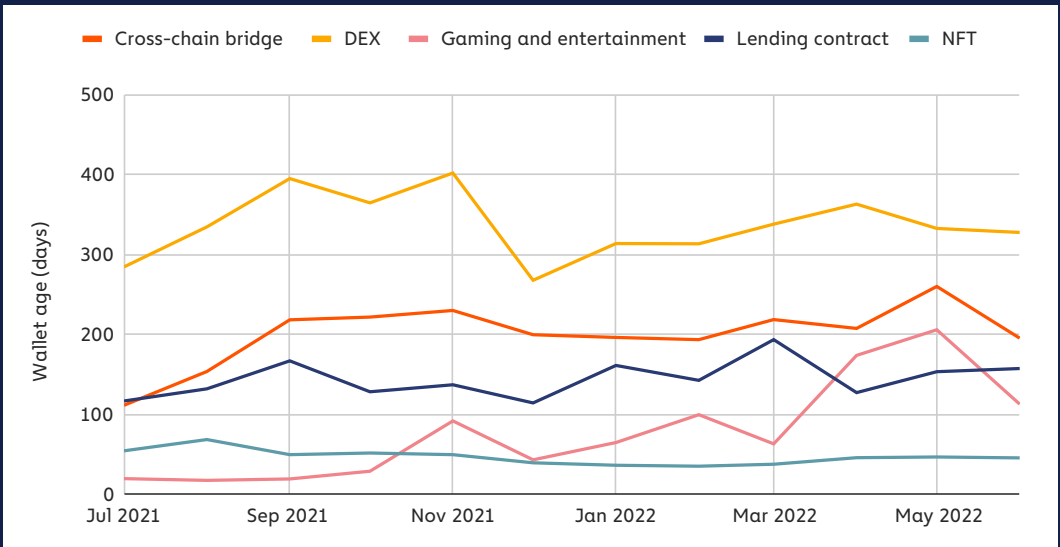
We've only begun to scratch the surface of all that web3 can enable, but already we see a variety of use cases generating significant economic activity:

- **Investing.** Users are trading and speculating on DEXs, and using staking and lending platforms to achieve stabler, more consistent returns
- **Borrowing and lending.** On the other side of those lending contracts are borrowers who put up their existing cryptocurrency as collateral to access capital
- **Art, entertainment, and culture.** NFT collectors have spent billions to own art they love, while in the more nascent web3 gaming space, users are monetizing their leisure time with play to earn
- **Infrastructure.** Protocols connecting disparate parts of the web3 ecosystem and setting the stage for future growth are raking in billions
- **DAOs.** Many of the protocols powering the use cases described above are governed by DAOs, which are themselves receiving billions in exchange for governance tokens, separate from funds received by the protocols themselves. As we explore later on, many DAOs today may

not be living up to their promise of decentralization due to concentration of governance tokens, and therefore decision-making power. But in the long term, as cryptocurrency adoption grows and more users participate in DAOs, the organizations competing in the web3 economy can become democratized.

That's a promising start, but right now, these use cases cater primarily to users who already hold cryptocurrency — while theoretically anyone could buy their first ever cryptocurrency and begin trading on DEXs or staking in liquidity pools, these protocols' interfaces can be difficult for new users to understand and feel comfortable with, and our data shows that DeFi adopters tend to be already established cryptocurrency users. An important exception to this is the use cases around art, entertainment, and culture, as these are widely popular industries that most people engage with already. And in fact, our data suggests that the rise of NFTs has attracted many users who hadn't previously engaged with the cryptocurrency ecosystem.

Average of wallet carrying out first DeFi transaction by DeFi protocol type, monthly, July 2021–June 2022



The graph on the previous page shows that wallets carrying out their first NFT transaction are generally younger than wallets transacting through other types of DeFi protocols, suggesting that first-time NFT users are more likely to be newer to cryptocurrency.

So, how can our industry capitalize on this momentum and build toward the ultimate vision of web3 — a world where all companies let you connect your wallet and you can take out a mortgage on the blockchain? We think it comes down to three things:

- **Onboard more new users into cryptocurrency generally.** This would increase the pool of people most likely to adopt web3 tools.
- **Better user experience for cryptocurrency and web3 tools.** Right now, the interfaces of many DeFi protocols are complex, intimidating, and difficult to use. Fixing this would make newbies more likely to onboard into web3.
- **Address use cases non-crypto natives care about.** NFTs grew because they attracted people who, while they may not have yet owned any cryptocurrency, cared about art and entertainment. Web3 operators should follow that example and build protocols that address broader market needs.

Meeting those three challenges is the key to ushering in the era of web3, and we're confident the cryptocurrency community is up to the challenge. In the meantime, keep reading for original data and research into where the web3 journey stands now.

Infrastructure

Layer 1 Blockchains

New Layer 1 Blockchains Are Expanding the DeFi Ecosystem But No Eth Killers Yet

Nearly all cryptocurrency tokens fall into one of two categories: Layer 1s and Layer 2s. Layer 1s are tokens with their own blockchains, while Layer 2s are built on top of Layer 1 blockchains, usually through smart contract technology. Layer 2s can be new tokens, or more complex projects known as decentralized apps, or dApps. However, there are also Layer 2 projects that don't utilize smart contracts, such as Bitcoin's Lightning Network, which is designed to facilitate faster and cheaper Bitcoin payments through transaction batching.

Different Layer 1 blockchains are designed and optimized for different goals. Bitcoin is designed to be a currency for simple, trustless transactions with enforced scarcity to preserve its value. However, its relatively simple structure limits what can be built on top of it. Ethereum was the first mainstream blockchain to incorporate smart contracts, and it hosted the first wave of dApps and tokens that ushered in DeFi and web3.

But, while Ethereum has become the most prominent blockchain for Layer 2 project development, its Proof of Work (PoW) mining system and high gas fees have proven an impediment to transaction speed and scalability within its DeFi ecosystem. Many, if not most, of the smart contract-enabled Layer 1 blockchains developed since were created to address those problems. Solana and Algorand, for instance, leverage a Proof of History (PoH) and Proof of Stake (PoS) consensus mechanism respectively, as well as other blockchain construction tactics, to provide lower fees and faster transaction times. Other Layer 1 blockchains, such as Avalanche, are built more for interoperability with other chains. We'll explore a few different Layer 1 chain's unique goals and characteristics in more detail later in the section.

Top 10 Layer 1 blockchains by market cap

Cryptocurrency	Market cap	Cryptocurrency, cont.	Market cap, cont.
1. Bitcoin	$385,184,629,479	**6. Polkadot**	$7,021,942,827
2. Ethereum	$134,597,034,431	**7. TRON**	$6,017,021,867
3. BNB	$36,086,988,333	**8. Avalanche**	$5,056,389,247
4. Cardano	$15,846,048,478	**9. Cosmos**	$2,110,450,042
5. Solana	$10,588,361,889	**10. Algorand**	$2,089,909,036

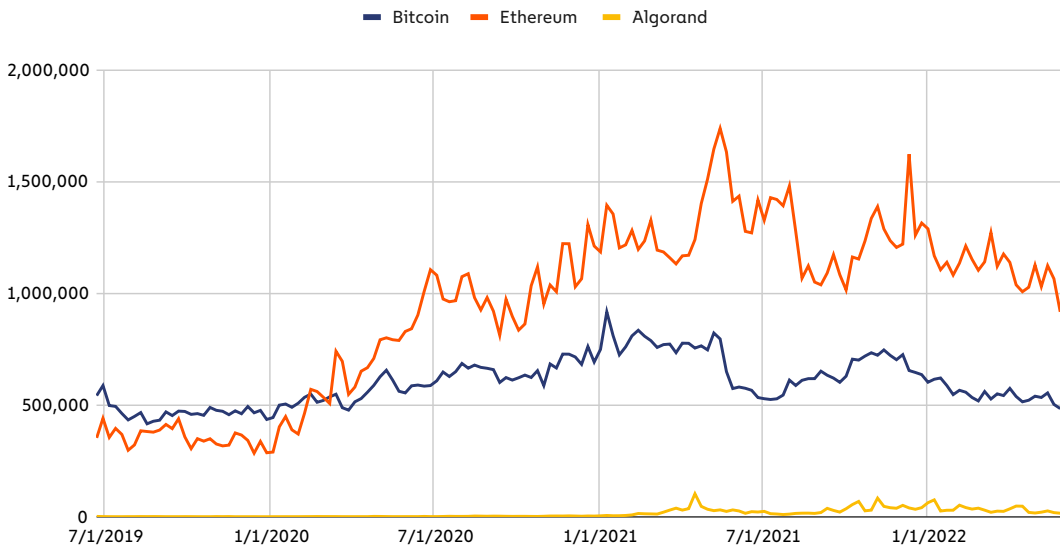
Source: CoinMarketCap. Data reflects market caps as of June 29, 2022.

Comparing Layer 1s: Bitcoin vs. Ethereum vs. Algorand

Using blockchain analysis, we can compare three prominent Layer 1 blockchains — Bitcoin, Ethereum, and Algorand — to see how their usage trends differ.

First, let's ask a basic question: Which blockchain has the most active users? We approximate this below by comparing the number of unique wallets sending each currency to services over time.

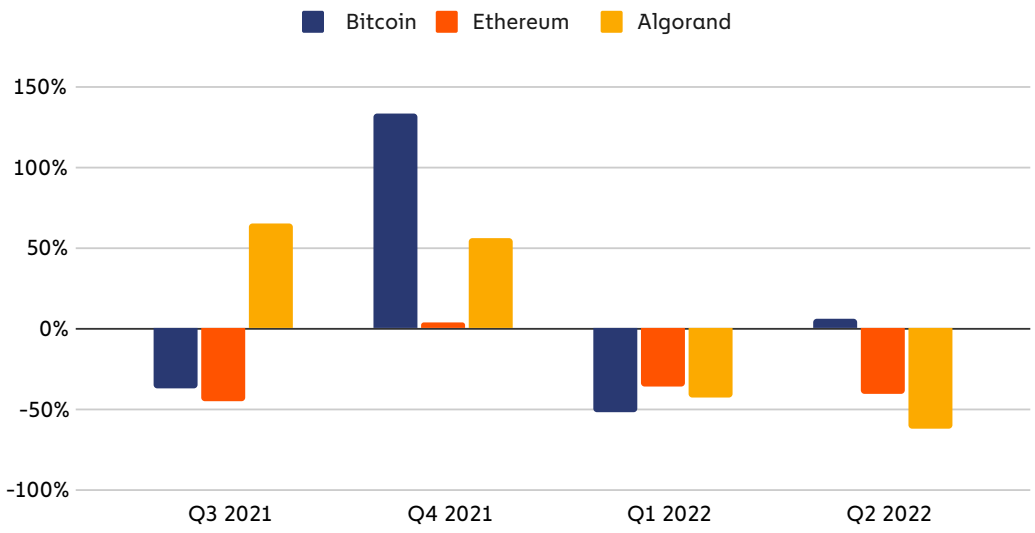
Number of unique wallets sending to services weekly, July 2019–June 2020, Bitcoin vs. Ethereum vs. Algorand



Bitcoin appears to have led in unique users until March 2020, at which point it was overtaken by Ethereum. This coincides roughly with DeFi growth, which makes sense, as the rise of DeFi fostered the creation of many services that accept Ethereum and other tokens built on its blockchain. Algorand, on the other hand, has yet to achieve comparable adoption, with a one-week high in active wallets of 103,000, compared to 1.7 million for Ethereum and 916,000 for Bitcoin.

As we can see on the previous page though, all three cryptocurrencies saw sometimes coinciding swings in active wallets throughout 2021 and 2022 to date. Overall though, each blockchain's growth in transaction volume wasn't correlated with the others for the most part.

Quarterly transaction volume growth by blockchain, Q3 2021–Q2 2022



Here, we see that during Q3 2021, Algorand saw its transaction volume grow 65%, while Bitcoin and Ethereum saw volumes drop 37% and 45% respectively. This may have reflected Algorand's growing hype — having launched in April 2019, Algorand was a relatively new blockchain, and reached an all-time price high in September 2021. Algorand and Bitcoin both grew transaction volumes significantly in Q4, during which time cryptocurrencies across the board were in a bull market, but curiously, Ethereum transaction volume grew very little. All three coins lost significant transaction volume in Q1 2022, but only Bitcoin grew in Q2, which saw steep declines possibly portending another crypto winter. That may reflect Bitcoin's perceived status as a relatively safe coin compared to Algorand, given that the latter is a newer asset.

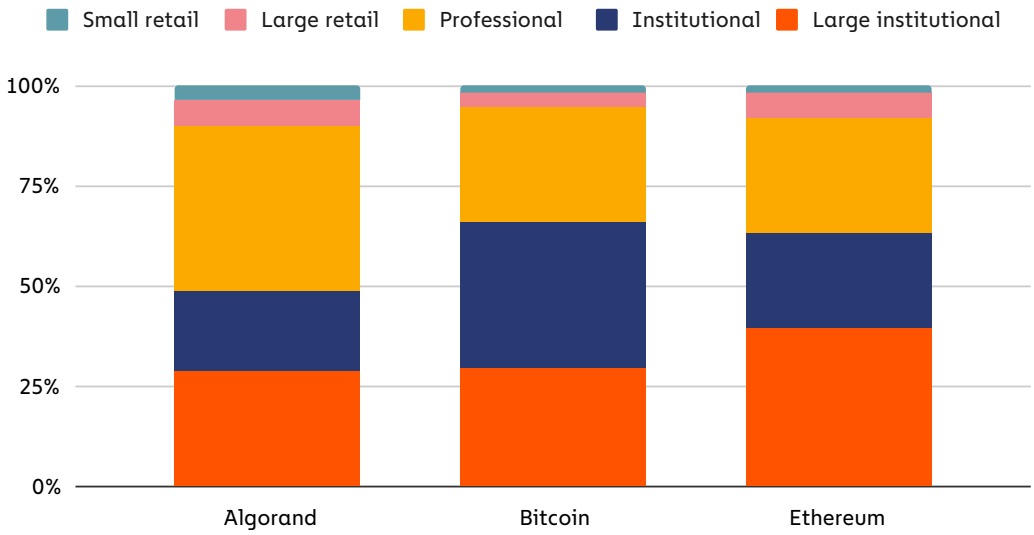
Investor profiles

We can approximate the types of investors who tend to use each of the three coins based on transaction sizes. We categorize transactions the following way:

- Small retail (<$1K)
- Large retail ($1K-$10K)
- Professional ($10K-$1M)
- Institutional ($1M-$10M)
- Large institutional (>$10M)

Below, we can see the share of total transaction volume by transaction size for the three currencies.

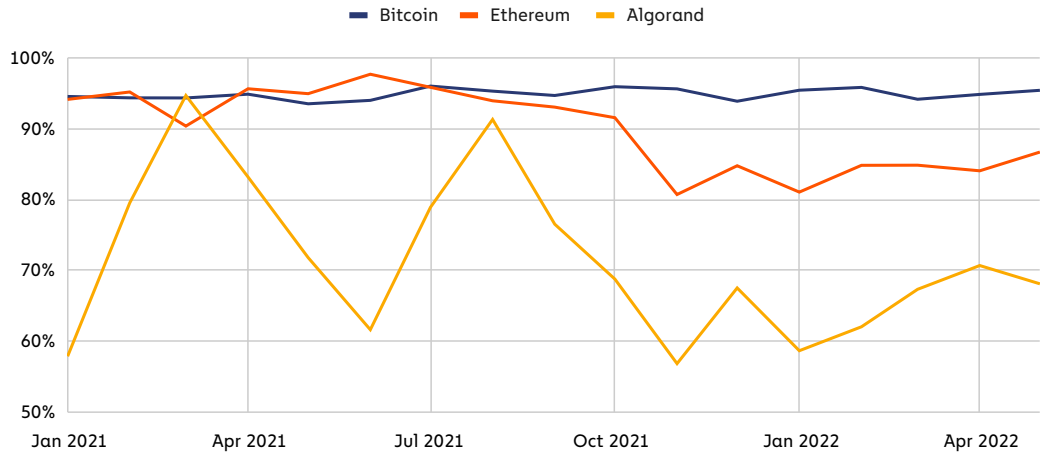
Transaction volume by transfer size category, June 2021–May 2022, Algorand vs. Bitcoin vs. Ethereum



Ethereum stands out as the cryptocurrency with the most institutional dominance. 40% of its total transaction volume comes from large institutional transactions, compared to just 30% for Bitcoin and 29% for Algorand. If we group institutional sized transactions in with large institutional, that figure becomes 66% for Ethereum and 64% for Bitcoin. Algorand, on the other hand, sees just 49% of transaction volume made up of institutional and large institutional transactions. On the other end of the spectrum, 10% of Algorand's transaction volume comes from retail or large retail transactions, compared

to 5% for Bitcoin and 8% for Ethereum. Again, this likely reflects Algorand's status as a relatively new blockchain. It may also signify that Algorand is succeeding in its goal of enabling a high volume of smaller transactions.

Share of total transaction volume above institutional size ($1M USD), January 2021–May 2022, Bitcoin vs. Ethereum vs. Algorand



Overall, the level of institutional interest in Bitcoin stays stable, but not so for Ethereum and Algorand. Ethereum saw a slight dip in institutional interest beginning in November 2021, which has yet to recover. Algorand, on the other hand, saw a much larger dip beginning in September, which has only seen a modest recovery. Still, the rise of DeFi 2021 appears to have sparked a huge increase in investor sentiment for Ethereum relative to Bitcoin.

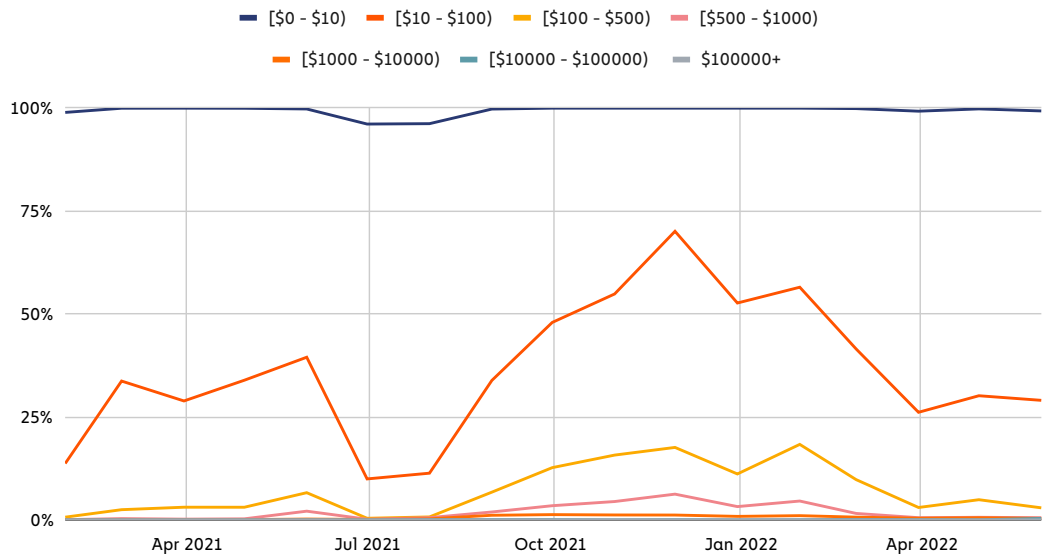
ETH-BTC price appreciation, January 2019–June 2022

Ethereum's price appreciation versus Bitcoin more than doubled over the course of the year, as total transaction volume skyrocketed to $4 trillion, compared to just $454 billion in 2020. That speaks to the power of web3: Smart contract functionality has created new use cases for Ethereum, leading to drastic increases in usage, and investors have taken notice.

The problem with Ethereum

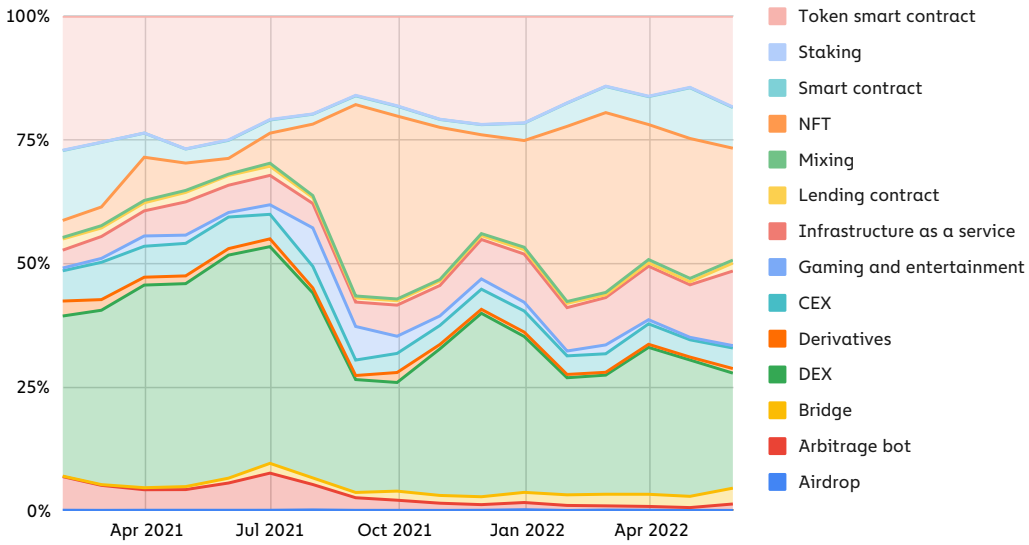
Ethereum, however, isn't perfect despite these successes. Due to its PoW consensus mechanism and current methodology for processing transactions, Ethereum can only handle roughly 15 transactions per second, compared to 1500 for non-cryptocurrency solutions such as the Visa network. Gas fees, which act as another source of compensation for miners and as a mechanism for preventing an overload of transactions, also harm Ethereum's scalability. This is especially true for smaller transactions.

Share of Ethereum transactions where fee is 20% or more of transaction value by transaction size, January 2021–May 2022



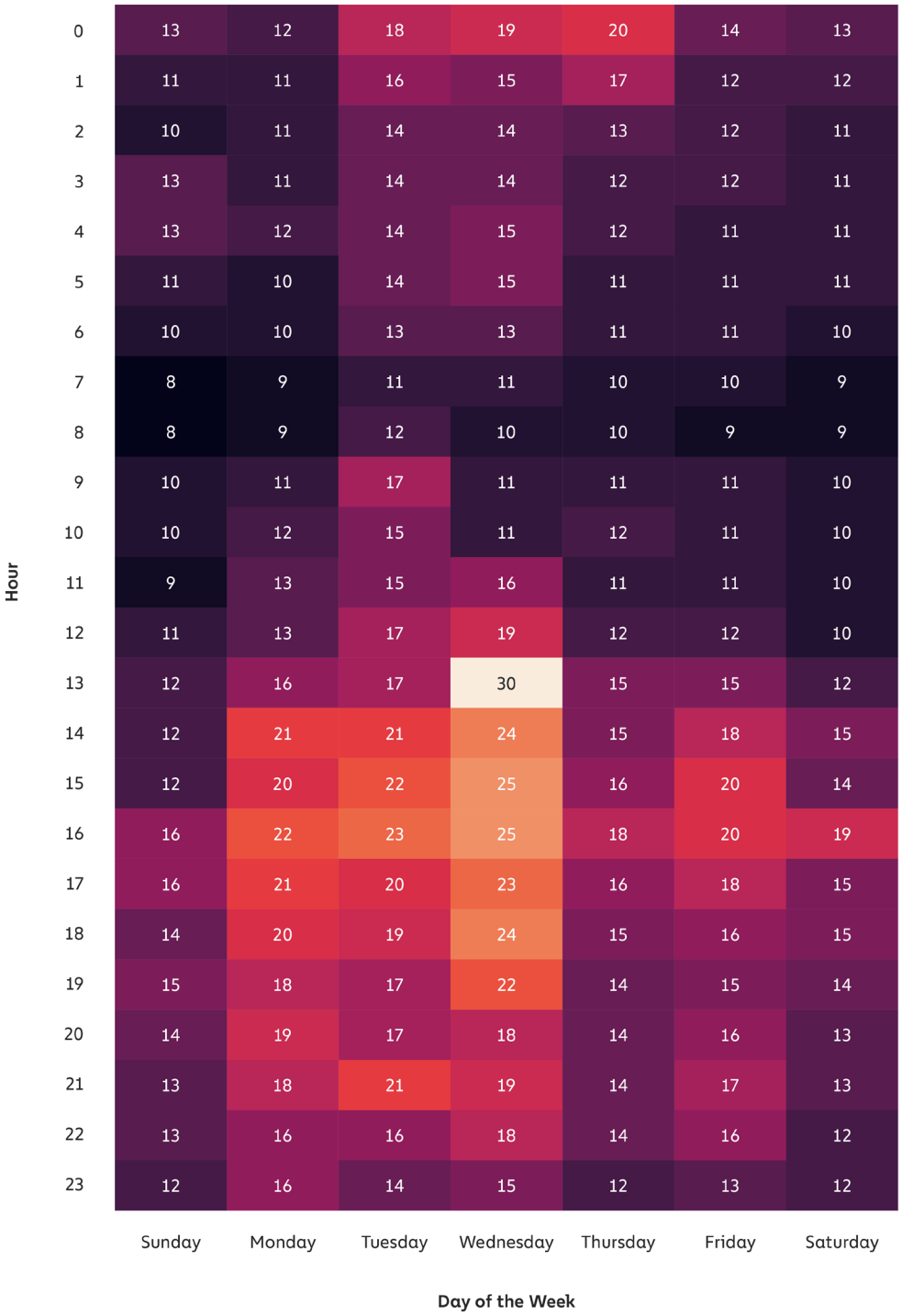
Gas fees are virtually always at least 20% or more of the actual transaction amount at values below $10, and frequently cross that threshold as well for transactions between $10 and $100. It isn't until transactions above $500 that Ethereum fees reach parity with the average credit card transaction, which typically carries a fee of 4% or lower. DEX and NFT users bear the brunt of these fees.

Ethereum fees by DeFi category, January 2021–May 2022



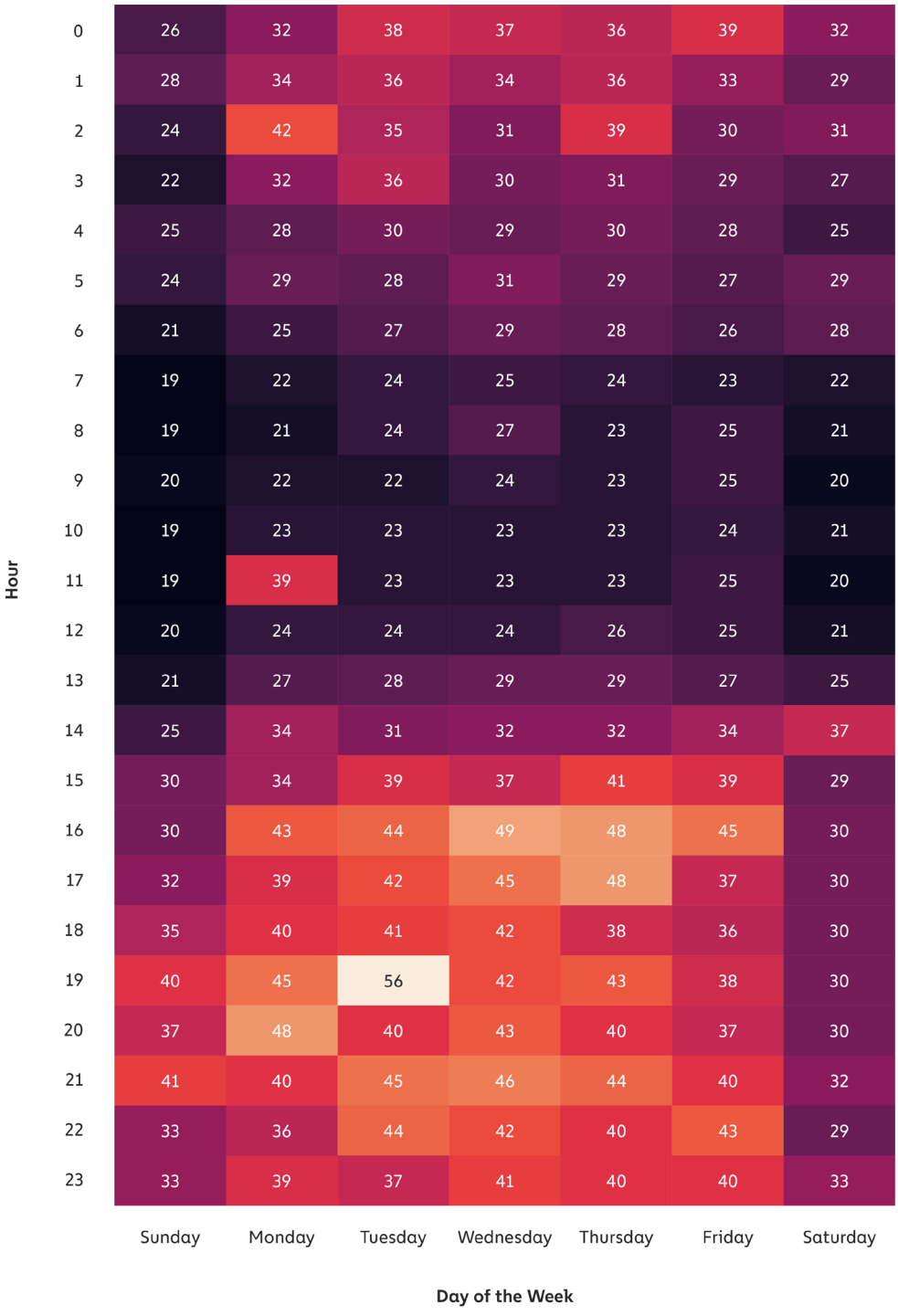
Not only that, but gas fees vary greatly hour-to-hour depending on how many people are transacting. In August 2021, Ethereum implemented a proposal called EIP-1559, also known as the London Hard Fork, that aimed to make gas fees more predictable. However, it doesn't appear to have been successful. The grid on the following page shows average gas fees as a percentage of transaction totals by hour and day of week for the six months prior to the London Hard Fork.

Average Ethereum gas fees by day of week and hour, six months before EIP-1559



Here's that same grid for the six months following the fork.

Average Ethereum gas fees by day of week and hour, six months after EIP-1559



We see no meaningful difference in predictability, and in fact, fees appear to have gotten higher overall since the implementation of EIP-1559, though it's possible that EIP-1559 or a variation of it eventually ends up mitigating the issue. For now though, high gas fees, and the negative effects they have on dApp scalability, are the primary reason many developers see opportunities in creating new smart contract-enabled blockchains. We'll look at a few of them below.

Layer 1 blockchain breakdowns: How other blockchains are building scalable solutions for web3

Solana

Solana was developed by computer scientist Anatoly Yakovenko and entrepreneur Raj Gokal starting in 2017, with the goal of addressing Ethereum's scalability problems. Solana does this with a unique consensus mechanism that combines PoS with Proof of History (PoH). PoH seeks to solve the issue of timestamping transactions that occur on a blockchain, which determines the order in which validators confirm those transactions. While other blockchains rely on outside infrastructure for time stamping, Solana's PoH mechanism allows timestamping to be built into the blockchain itself, which enables faster block validation and therefore faster transaction time.

Solana Foundation Communications Rep Chris Kraeuter told us that PoH enables Solana to achieve the following metrics:

- Transactions per second generally between 1,500 and 3,500, with a maximum of 65,000 depending on transaction complexity
- 400 millisecond block confirmation time
- $0.00025 in fees per transaction

These attributes have enabled Solana to become one of the biggest blockchains by total value locked (TVL) at $2.53 billion as of June 2022. While that figure fluctuates with market prices, Solana's TVL has continuously trended upwards when measured in its native currency, and sits at over 70 million SOL as of June 2022. That steady growth suggests that participation in the Solana

ecosystem is growing consistently regardless of price swings. In fact, Kraeuter shared that Solana's daily active users have grown more than 40% over the last 90 days.

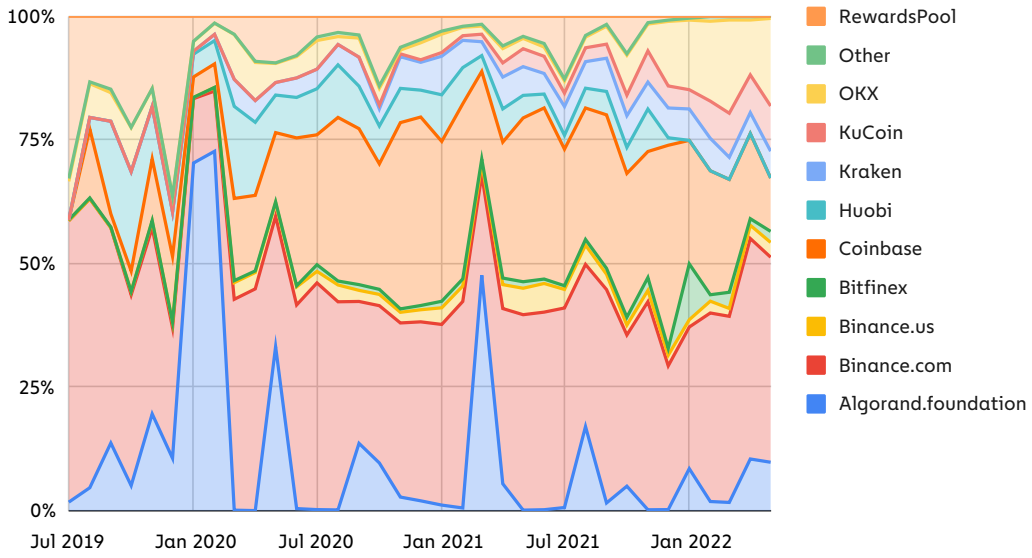
One area where Solana is growing rapidly is NFTs. Solana still trails Ethereum in overall NFT trade volume, though it has surpassed it in individual 24-hour periods. However, Solana's low-fee structure has made it much easier for creators to launch new projects. Nearly 15 million NFTs have been minted through Metaplex, the NFT standard on Solana, versus just over 1 million on Ethereum. It remains to be seen if the ease with which new NFTs can be created on Solana at such low costs will allow it to supplant Ethereum as the blockchain of choice for NFTs, given that the latter has a first mover advantage and more transaction volume.

Algorand

Launched in April 2019 by MIT Computer Scientist Silvio Micali, Algorand is intended to support high-frequency, payment-sized transactions. Currently, Algorand facilitates an estimated 1,000 transactions per second with five seconds for final confirmation on the blockchain. It achieves this in part with a unique, two-tiered blockchain structure. The base layer supports basic transactions, as well as smart contracts for new tokens and atomic swaps. The second layer, on the other hand, is reserved for more complex smart contracts, such as those powering dApps. This bifurcation of the Algorand blockchain enables Algorand to process transactions efficiently.

For its consensus mechanism, Algorand uses a variant of PoS called Pure Proof of Stake (PPoS), with much lower staking requirements than other PoS blockchains — 1 ALGO is all it takes to stake. This results in a more democratized blockchain, but the lower barrier to entry may disincentivize validators from acting in the best interest of the entire network at all times. However, with gas fees running high on Ethereum, many developers have chosen to build dApps on Algorand. We break down the biggest of those dApps by transaction volume on the following page.

Algorand's top services by transaction volume, July 2019–May 2022



Most transaction volume for Algorand is moving through big, centralized exchanges, but its staking rewards pool also sees significant activity.

BNB Chain

Originally known as Binance Smart Chain, BNB Chain is a blockchain launched by cryptocurrency exchange Binance, with BNB being its native token. BNB chain achieved high growth for a few reasons, a key one being its capability of supporting new tokens and dApps without the high fees of Ethereum. In fact, according to DappRadar, more Layer 2 projects have been built on BNB Chain than on any other blockchain.

BNB Chain is of course also able to draw on the enormous customer base of Binance, the largest cryptocurrency exchange in the world, capitalizing on resources like Binance's extensive language support to attract users around the globe. However, there are potential downsides to that as well. BNB Chain can't be said to be fully trustless – in the technical sense — as it's maintained by a centralized, legally incorporated business entity. We see one example of this in BNB Chain's tokenomics.

As we mentioned above, there's more being built on BNB Chain than anywhere else. But what exactly is being built? According to DappRadar, DeFi protocols make up a much bigger share of BNB Chain's Layer 2 protocols compared to similar blockchains like Ethereum. Meanwhile, platforms devoted to NFTs and other collectibles are much less prominent.

Avalanche

Avalanche touts itself on three key attributes:

- Customizability to build a variety of dApps and tokens.
- Scalability thanks to low fees.
- Interoperability to interact with other blockchains. For instance, Avalanche is compatible with the Ethereum Virtual Machine (EVM), meaning that dApps and tokens built on the Ethereum blockchain can be migrated to the Avalanche blockchain with minimal extra effort from developers.

With these three capabilities, Avalanche says it can be a "platform of platforms" and support significant Layer 2 development. Avalanche accomplishes this with a set of three blockchains, each serving different use cases:

- C-Chain executes transactions related to Ethereum-native dApps, and is currently the most-used of the three blockchains.
- X-Chain allows for the creation and exchange of new assets built on top of the Avalanche blockchain
- P-Chain coordinates the Avalanche blockchain's validators and the creation of subnets.

Subnets are sets of Avalanche validators responsible for a single blockchain built on top of Avalanche. Each layer 2 blockchain on top of Avalanche has one subnet, but individual subnets can validate many blockchains. The C-chain's compatibility with Ethereum has enabled Avalanche to integrate with several large Ethereum-based DeFi projects, including bZx and SushiSwap. Meanwhile, its PoS consensus mechanism has enabled low fees and a high throughput of 4,500 transactions per second. Unlike Ethereum, Avalanche burns all transaction fees in order to create deflationary pressure for its native AVAX token, rather than pay them out to validators, as is the case on the Ethereum blockchain.

DappRadar tracks a total of 297 dApps built on Avalanche, more than half of which are DeFi protocols, while another 8% of dApps are devoted to NFTs.

What's next for Layer 1s?

Several new Layer 1 blockchains have emerged to stake out their own place in the growing web3 ecosystem, largely driven by a demand to address Ethereum's problems with scalability, speed, and fees. While many of them have attracted substantial investment and user bases, questions remain.

For instance, will any of them surpass Ethereum in adoption? Many new Layer 1 blockchains perceived to solve Ethereum's problems have been billed as "eth killers" primed to replace the second-most popular cryptocurrency as the go-to for web3 and DeFi, but so far, none have been able to do it. Ethereum is still far ahead in transaction volume, especially in popular areas of web3 like NFTs, and the Ethereum Foundation is working with miners to implement changes to address its issues. The upcoming Ethereum 2.0 upgrade, which will see Ethereum switch to a PoS consensus mechanism and implement sharding to process a higher number of transactions in parallel, is expected to increase Ethereum's scalability and lower gas fees. If Ethereum's entrenched status as the number two blockchain behind Bitcoin is already allowing Ethereum to fend off competitors, it seems especially unlikely that another smart contract-enabled blockchain will challenge it should these changes prove successful.

That would raise another question: If new Layer 1 blockchains can't challenge Ethereum, will they survive as alternatives in the long term? So far, many new Layer 1 blockchains have attracted investment at least in part by convincing investors they can challenge Ethereum in the long term, and the bull market of 2021 allowed them to attract new investors as prices grew. With a possible crypto winter on the horizon along with improvements to Ethereum, it's possible that investment in alternative Layer 1s slows down, and that web3 becomes a winner-takes-all market, with Ethereum as the dominant player.

What do Layer1 blockchain builders think about? An interview with ParallelChain CEO Ian Huang

ParallelChain is a relatively new layer1 blockchain designed to support the building of enterprise-level layer 2 applications. The company has already built a number of such solutions itself, including:

- ParallelWallet, a crypto wallet software solution supporting biometric security
- eKYC-chain, a blockchain-based solution for digital identity verification
- PreventiveChain, a tool for organizations to prevent insider attacks and leaks of sensitive information

ParallelChain's mainnet launch is on the way, but in the meantime, the company has launched four testnets for developers to build and test dApps on its blockchain free of charge. We spoke with ParallelChain CEO Ian Huang about his work on ParallelChain, how it fits into the current DeFi ecosystem, and what he thinks about the future of web3 generally.

Chainalysis: What problems is ParallelChain trying to solve and how does it differentiate itself from other Layer1 blockchains?

Ian Huang: As blockchain use cases grow in scope, scale, and complexity, multiple blockchain systems have gained a foothold in the Layer1 market. This has opened up the space for technologies like Polkadot or Cosmos that facilitate cross-chain and multi-chain interactions. While we all want to see these systems gain mainstream adoption, we feel like that there are still problems not addressed by existing cross-chain systems. We're thinking about two problems in particular:

1. More interconnected systems and applications invariably mean more attack vectors that can (and will) be exploited by parties hostile to the ecosystem.

2. The seamless flow of data between public networks will make it more challenging for enterprise users to protect sensitive information and ensure legal compliance.

These are a big part of what's guiding ParallelChain's development. ParallelChain Mainnet and ParallelChain Private support multi-chain interaction models that we believe make our ecosystem more robust to the security, privacy and adoption challenges that are coming with the increased connectivity between platforms as well as applications.

What are the biggest obstacles standing in the way of mass adoption for your project?

It's always challenging to convince organizations to migrate from their long established IT infrastructure and adopt an entirely new tech stack. We would have to break into the market by focusing on niche use-cases first, solving problems that existing software couldn't while developing tools and solutions that are complementary to their existing systems.

From a user's perspective, what do you think are the most important factors that determine the use of one Layer1 over another?

Metrics such as speed, cost of transaction and security are basic qualities that should be expected of any platform nowadays. The ecosystem supporting the platform, both in terms of quantity and quality of apps, has been, and will always be, a priority for ParallelChain. You can have the best technology in the world but if nobody is engaging with it then it's pointless.

What are the most exciting things on your roadmap for the coming year?

2022 for ParallelChain is full of exciting plans and new horizons. We have four testnet releases spread over the coming months, before the Mainnet takes off in Q4. And of course, there's our flagship DeFi product ParallelWallet, a multi-biometric crypto wallet that will have a meaningful impact on how we perceive and manage identity in the decentralized digital space and metaverse.

What do you see as the connection between ParallelChain and web3? How about the connection between the broader Layer1 space and web3?

At the minimum, we see the connection between ParallelChain and web3 in the form of a bridge between real world and DeFi assets. We believe

these kinds of asset swaps will be necessary as more use cases develop. Inter-blockchain oracles, like the ones on Inter-ParallelChain Communication (IPC) in ParallelChain will play a significant role in connecting broader Layer1 space and web3 together.

How do you foresee all these different Layer1s interacting in the years to come? Will there be one chain to rule them all?

I believe Ethereum will still dominate as a general purpose smart contract platform and a settlement layer (where users cash out their funds), with more mission-specific DeFi applications like (e.g. exchanges, NFT marketplaces, games) moving towards other faster and cheaper platforms. There will always be some dominant platforms, but all will exist as pieces to a puzzle.

What are the biggest obstacles for broader crypto adoption as well as the coming of web3?

We need to educate the world on how decentralization makes the foundation for the new web and business models, and shift the public perception away from treating crypto merely as a type of investment, but as a vehicle that brings web3 into realization.

I also believe that more consumer-facing businesses integrating crypto and DeFi into their existing products and services would be a great channel to drive wider adoption.

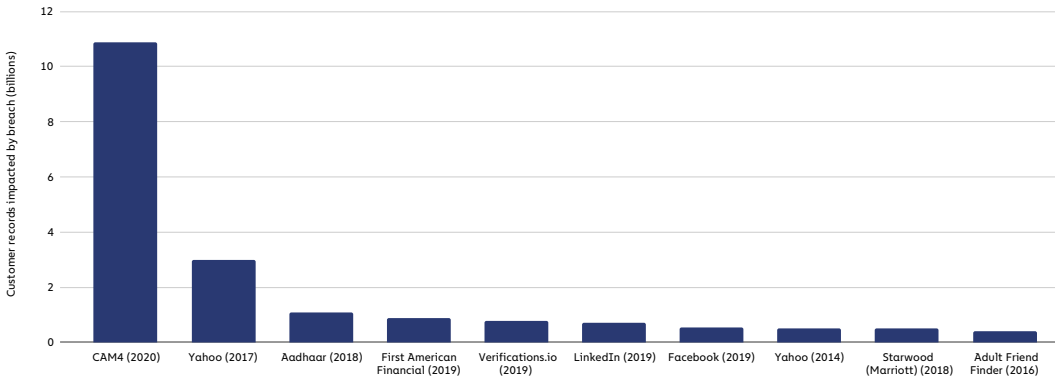
Ian Huang
CEO, ParallelChain

Infrastructure
Digital Identity

How Digital Identity Can Make Web3 Safe and Empower Users

One of the biggest shortcomings of web2 is the precarity of consumers' data security and privacy. According to data privacy startup, Mine, the average consumer's personal data is held by 350 different brands. Unsurprisingly, not all of these companies prove to be trustworthy custodians of user data. Millions of people around the world have had their personal information compromised in data breaches, resulting in losses of billions of personal data records.

Biggest corporate data breaches in history



Consumers affected by data breaches are at higher risk of cybercriminals obtaining their information and using it to target them for scams, including the highly prevalent blackmail scams we've analyzed in our reporting on cryptocurrency-based crime.

Web3 can help solve this problem by disentangling payments and customer-business relationships from real world identity except where absolutely necessary. Already, many web3 services and DeFi protocols allow users to sign up by simply connecting their cryptocurrency wallet, without providing an email address or any other information. While this may not be sufficient for all services — depending on where they're located, businesses enabling money

transmission likely need to request users' KYC information for compliance purposes — it should be adequate for many others.

That's not to say web3's wallet-based login system is perfect. We've seen several examples of phishing scams in which bad actors create apps and websites that mimic legitimate cryptocurrency projects, inviting users to connect their wallets, at which point the scammers steal the wallet's contents. But with more education on security best practices, such as creating a new address for each new service one connects to, and better policing of scammers by both law enforcement and the cryptocurrency community itself, wallet connection as a login mechanism can provide better data security for users than the current web2 paradigm of usernames, emails, and passwords.

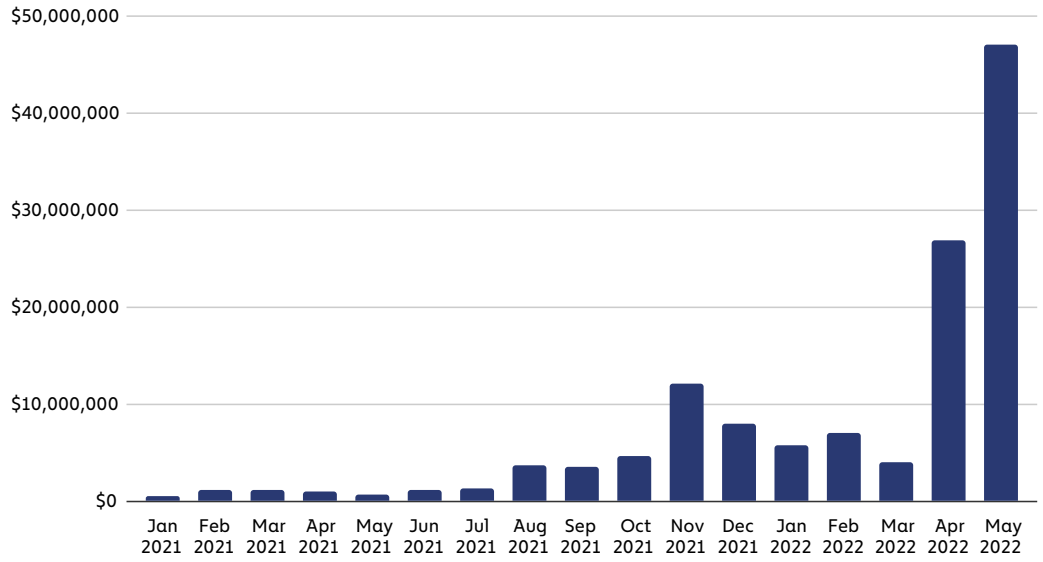
ENS is bringing online personas to cryptocurrency wallets

Of course, digital identity isn't just about how you log into websites. In an increasingly online world, where many find community and build their reputation on the internet, digital identity is just as much about self-representation, whether it's tied to one's real world name or a digital pseudonym. That's what the Ethereum Naming Service (ENS) aims to do for web3.

ENS is a service built on top of the Ethereum blockchain that, at its core, lets users tie an easily readable domain to an Ethereum address. By default, Ethereum addresses are long strings of letters and numbers, so right away, this makes it easier for users to send funds to ENS-linked addresses. Most ENS domains end with the suffix ".eth," similar to the better-known top level domain ".com," though others are available as well. ENS domains are issued as NFTs by the ENS Registrar, and require a small fee for registration and ongoing fees for renewal, similar to standard domains. Currently, ENS charges $5 per year for domain names of five characters or more, and $160 per year for domains of four characters or fewer.

As of now, the ENS foundation says that 1.1 million ENS domains have been purchased by more than 400,000 unique owners. We can use Chainalysis data to look at recent trends in ENS domain purchasing.

Monthly value received by ENS, Jan 2021–May 2022



After a huge month in November 2021, volume seems to have fallen off steeply, which may reflect a bigger downturn in cryptocurrency and DeFi transaction volume overall.

ENS has pursued integrations with other services to enable use cases beyond simply naming an Ethereum address. For instance, ENS is integrated with the ICANN registry, which acts as a database of conventional, web2 internet domains (such as, say, chainalysis.com) to ensure there are no conflicts and that each domain is only issued to one person or organization. ENS' integration with ICANN allows the owners of web2 websites to import their website names into the ENS ecosystem. That means that, if we wanted, chainalysis.com could act as both our company's website domain, and also as a name for an Ethereum wallet we could use to conduct web3 transactions. The ENS-ICANN integration could prove to be a crucial bridge from web2 to web3, and at the very least makes it easier for web2 businesses to accept cryptocurrency payments and expand their customer targeting to crypto natives.

ENS has also integrated with the InterPlanetary File System (IPFS), a peer-to-peer network for publishing data and content on the internet, similar to the HTTP system most websites use. The key difference is that as a peer-to-peer network, IPFS is decentralized, unlike HTTP. Rather than relying on a small group of centralized servers to host the files that make up the content appearing on the web, IPFS users can themselves host files, or

discrete parts of files, similarly to how distributed ledgers are saved across many users' computers in a blockchain ecosystem. Without a single point of failure, the content IPFS hosts is less likely to be lost, meaning fewer 404 errors. IPFS also says that its system decreases the possibility of censorship and surveillance online, and can also lead to better web performance, e.g. faster loading times.

By integrating with IPFS, ENS domains can represent these decentralized websites as well as Ethereum addresses. ENS domains linked to IPFS-powered websites can be accessed on any browser if an Ethereum wallet like Metamask is enabled, and if not, can be accessed by adding ".link" to the end of the domain following ".eth." Almonit.eth, which displays a directory of decentralized websites hosted through IPFS using ENS domains is a great example — you can browse it directly if you have an Ethereum wallet like Metamask enabled, or enter Almonit.eth.link to browse without a wallet. Several DeFi protocols and other cryptocurrency projects already have websites set up using this framework, as well as a number of personal websites and blogs. The combination of ENS and IPFS can go beyond addressing privacy and security concerns, and may represent the beginning of a more democratized, bottom-up internet, in which users and creators can interact free of middlemen, censors, and other third parties.

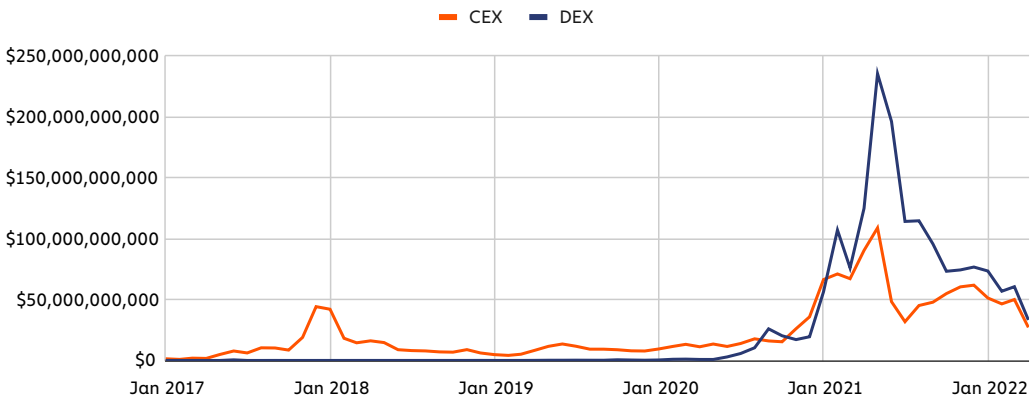
Defi

DEXs

DeFi-Driven Speculation Pushes Decentralized Exchanges' On-Chain Transaction Volumes Past Centralized Platforms

Over the past five years, decentralized exchanges (DEXs) have emerged as a self-custodial, programmatic way for cryptocurrency investors to trade. DEXs allow users to swap between hundreds of trading pairs without an intermediary. And fifteen months ago, these DEXs for the first time eclipsed centralized exchanges (CEXs) in on-chain transaction volume.

On-chain transaction volume on centralized vs. decentralized exchanges, January 2017–April 2022

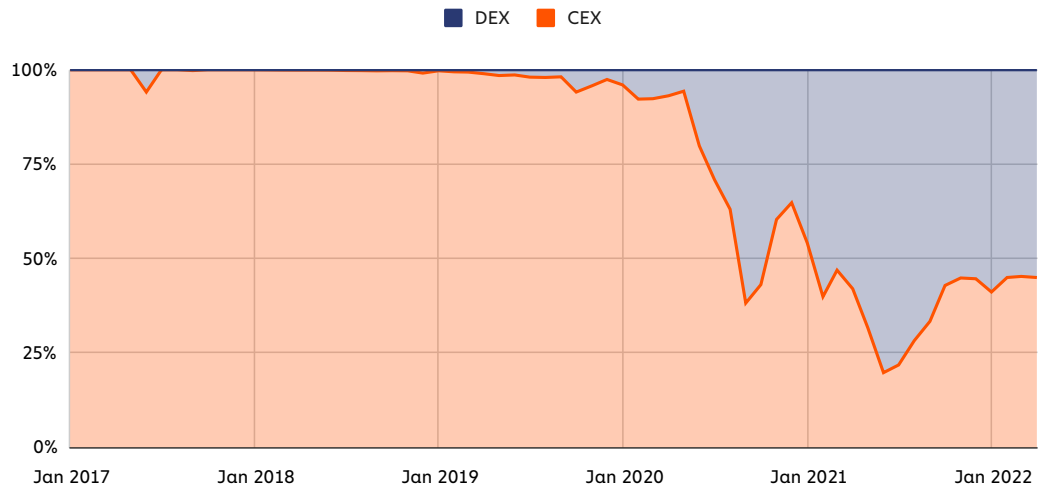


While most CEX transactions happen off-chain on centralized databases and captured on their order books to save on transaction fees, every DEX transaction occurs via smart contracts on-chain. For this reason, as well as the rapid growth of DeFi generally, DEXs now have a confident lead in on-chain transaction volume: from April 2021 to April 2022, $175 billion was sent on-chain to CEXs, well below the $224 billion sent to DEXs.

The transaction volumes at centralized and decentralized exchanges are closely correlated with market performance. For example, CEX transaction volume reached an all time high in late 2017 as Bitcoin climbed to its all-time high. Similarly, DEX and CEX transaction volumes alike skyrocketed in 2021 as cryptocurrency prices again multiplied. But with the recent market slump, the amount sent to both exchange types declined, with CEXs proving slightly more resilient than DEXs in current market conditions.

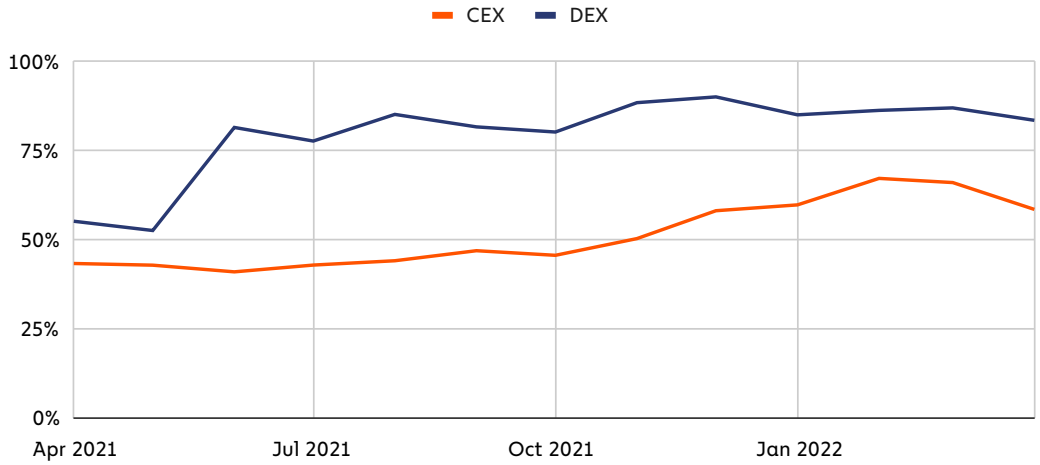
The balance first shifted away from centralized to decentralized exchanges in September 2020, when centralized exchanges supported below 50% of on-chain volume for the first time. DEX dominance then reached its peak in June of 2021; that month, DEXs facilitated more than 80% of on-chain transaction volume. Today, their share of on-chain volume is more evenly split, with 55% happening on DEXs and 45% on CEXs.

Percentage of on-chain transaction volume occurring on centralized vs. decentralized exchanges, January 2017–April 2022



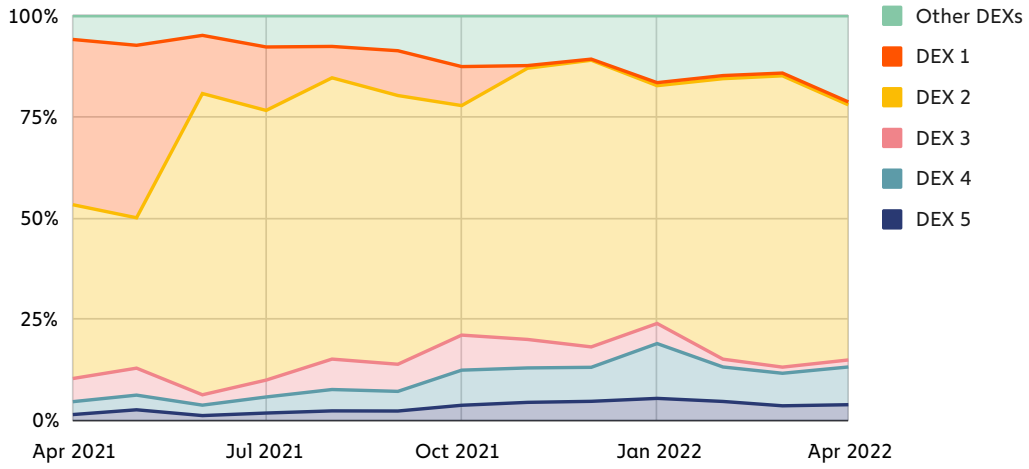
At the service level, the concentration of transaction volume at the top five DEXs is much higher than the concentration of volume at the top five CEXs.

Percentage of transaction volume concentrated in the top five services by exchange type, April 2021–April 2022



The top five decentralized services currently support roughly 85% of all DEX and aggregated DEX transaction volume during the time period studied.

Top DEXs by percentage of total on-chain DEX transaction volume, April 2021–April 2022

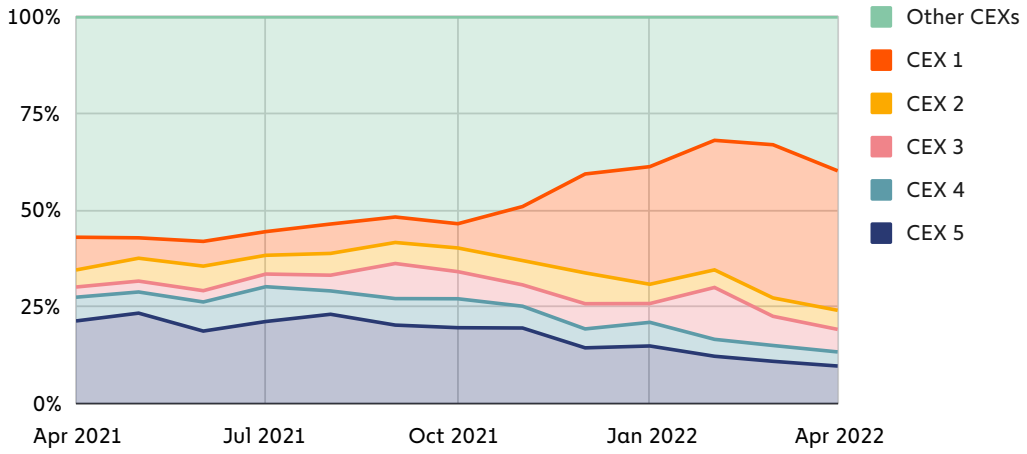


The high concentration of DEX transaction volume is likely a byproduct of DEXs' recent emergence. Without as much time on the market, fewer DEXs have been able to establish themselves and sustain an active user base. For example, even seemingly established DEXs — like DEX 1 — have seen their users abandon ship en masse during the recent decline in DeFi activity.

Another possible explanation is economies of scale, an important mechanism for DEXs. DEXs with higher liquidity may be able to provide more stabilized pricing for even the biggest market participants, but smaller pools may struggle to do the same without causing considerable price slippage — an unappealing proposition for both consumers and liquidity providers. A third explanation is simply that competition is intense

By contrast, the top five centralized exchange services supported roughly 50% of all on-chain CEX transaction volume during the time period studied. However, it is worth noting again that on-chain CEX volume represents only the flows into and out of CEXs, not the trading volume of their off-chain order books.

Top CEXs by percentage of total CEX transaction volume supported, April 2021–April 2022



Centralized exchanges' lower concentration may be due to greater competition among CEXs, greater focus on regulatory hurdles within and across jurisdictions, and/or greater variability in how much these services' users also use personal wallets.

How much do DEX users earn for providing liquidity?

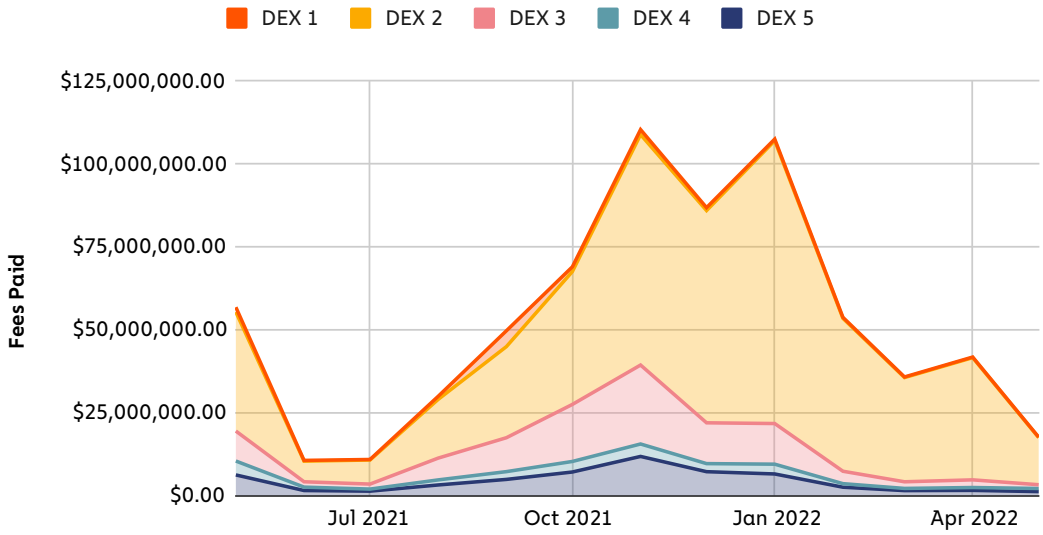
Many automated market maker (AMM)-style DEXs run on liquidity pools — cryptocurrencies stored in smart contracts that support trading pairs. These

pairs, such as ETH-USDC and USDT-DAI, allow users to swap between almost any cryptocurrency at a fair price and without an intermediary.

Users who fund these AMM-style DEX pools are known as liquidity providers or LPs. In exchange for filling these pools with cryptocurrencies, LPs collect transaction fees on any trades that use their liquidity.

How much do LPs earn? To find out, we measured the transaction fees collected by ERC-20 token liquidity providers on the top five DEXs.

Fees earned by ERC-20 liquidity providers on the top five DEXs, May 2021–May 2022



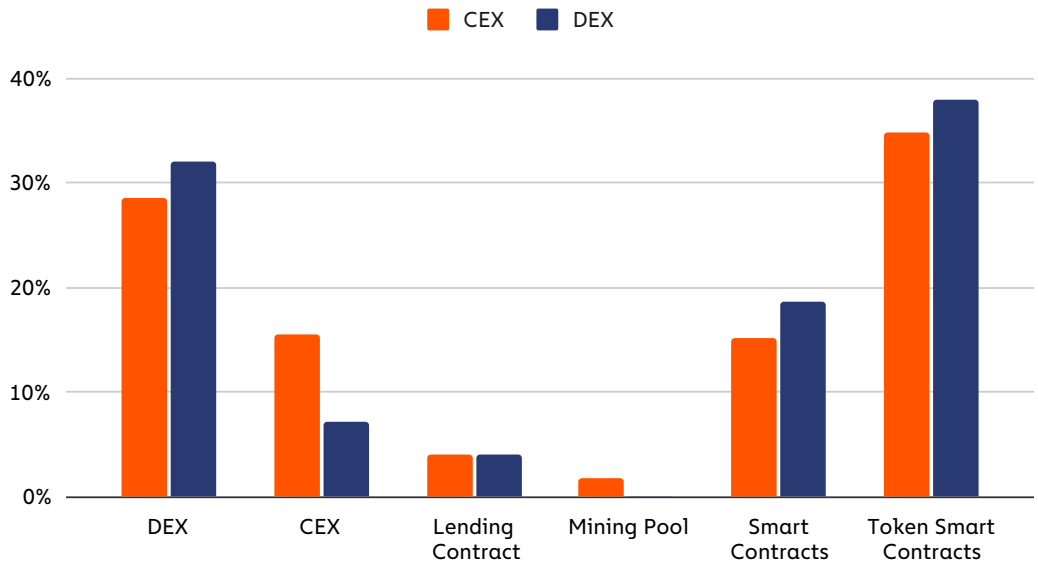
The fees earned by LPs are closely tied to DEX transaction volumes. On a monthly basis, fee earnings have fluctuated between $50 and $150 million, a small fraction (0.05% to 0.3%) of the $50 to $300 billion that has flowed through these exchanges during the same period. The recent downturn has impacted both of these elements equally, as fewer transactions means fewer opportunities to collect fees.

Some DEXs also issue governance tokens that may give their holders voting rights over different aspects of the protocol. In some cases, those governance tokens may be traceable on a secondary market.

How are DEX users different from CEX users?

There aren't any major behavioral differences between the top 10,000 ether (ETH) senders to centralized versus decentralized exchanges, but there are some minor ones.

Exposure profile of users sending ETH to CEXs vs. DEXs



The biggest difference between the two types of users is in what percentage of their ETH came from a centralized exchange. Just 7% of DEX users' funds came from a CEX, but 16% of CEX users' funds came from another CEX. This could reflect decentralized exchange users' preference for self-custody — both personally and when deciding with whom to transact — over third-party custody.

Will DEXs maintain the lead?

Whether DEXs will ultimately keep their lead in on-chain transaction volume may depend on a number of factors, including:

- whether they can offer lower fees and fairer pricing than their centralized counterparts;

- whether they face more regulatory scrutiny; and
- whether they can shift mainstream attitudes in favor of further automation, disintermediation and self-custody.

As DeFi competition intensifies, it will be interesting to see how CEXs and DEXs may continue to converge and differentiate.

Defi
Lending and Staking

Decentralized Staking and Lending Pools Can Provide Consistent Returns for DeFi Users, But Not Without Risks

DeFi isn't just providing decentralized options for active trading in the form of DEXs. There are also many protocols devoted to more passive forms of investment. The most prominent of these are staking and lending.[1]

At their core, staking and lending are very similar: In both cases, a user is sending their cryptocurrency to a DeFi protocol to hold, and in return they receive a consistent, relatively low-risk (but not risk-free!) return — typically a small percentage of the original investment, as opposed to the outsized returns users seek on more speculative platforms.

The difference between the two comes down to how the funds sent to the protocols are used. Staking occurs on blockchains that use a proof-of-stake consensus mechanism, in which validators are chosen to confirm new blocks and receive the associated rewards based on how much of the blockchain's tokens they've staked to the network. Stakers play the equivalent role of miners in a proof of work system, and similarly, often band together to form staking pools to improve their odds of winning new blocks in exchange for fees and a dispersal of rewards. Funds sent to lending pools, on the other hand, are loaned out to borrowers, who can use them to trade and invest, with lenders making money on the interest. We'll look more at staking and lending pools in-depth in the following pages.

1 One note of clarity: this section primarily focuses on decentralized staking and lending platforms, not centralized services like Celsius and BlockFi that provide interest. In our later section on risk in web3 and market contagion, we discuss the risks of both decentralized and centralized lending and yield generating services together.

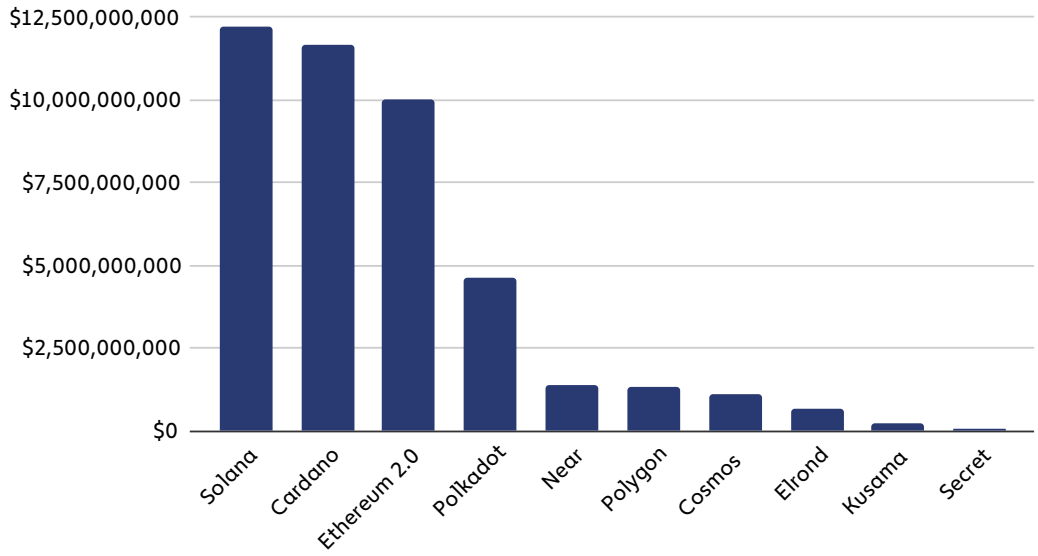
Staking provides rewards and powers proof of stake consensus mechanisms

Proof of stake (PoS) is an alternative consensus mechanism to proof of work (POW) that, among other things, seeks to address POW's energy consumption. Under POW, miners compete to validate new blocks by racing to solve mathematical puzzles requiring computing power. Energy is wasted because miners who expend computing power but lose receive nothing. Under PoS, validators are randomly selected to confirm new blocks and earn the associated rewards, and can increase their odds by staking more of the blockchain's tokens to the network. With nothing required from validators but staked holdings, POS uses much less computing power than POW, making it much more eco-friendly.

Ethereum is set to switch to a PoS consensus mechanism when it upgrades to ETH 2.0. And in fact, the ETH 2.0 blockchain currently exists as a beacon chain, which will be merged with the ETH 1.0 chain once the upgrade is complete, but already provides a great example of how staking works. Validators on the ETH 2.0 blockchain stake Ethereum to participate, and will receive Ethereum in return when the upgrade is complete and the two chains merge — current estimated rewards stand at 4.6% of Ethereum staked per year. Until the upgrade, those rewards are inaccessible, though as we'll explore later, one Ethereum staking pool has gotten around this short-term lack of liquidity.

While Ethereum has the biggest market capitalization of any PoS blockchain, ETH 2.0 is the third blockchain overall by amount staked, behind Solana and Cardano.

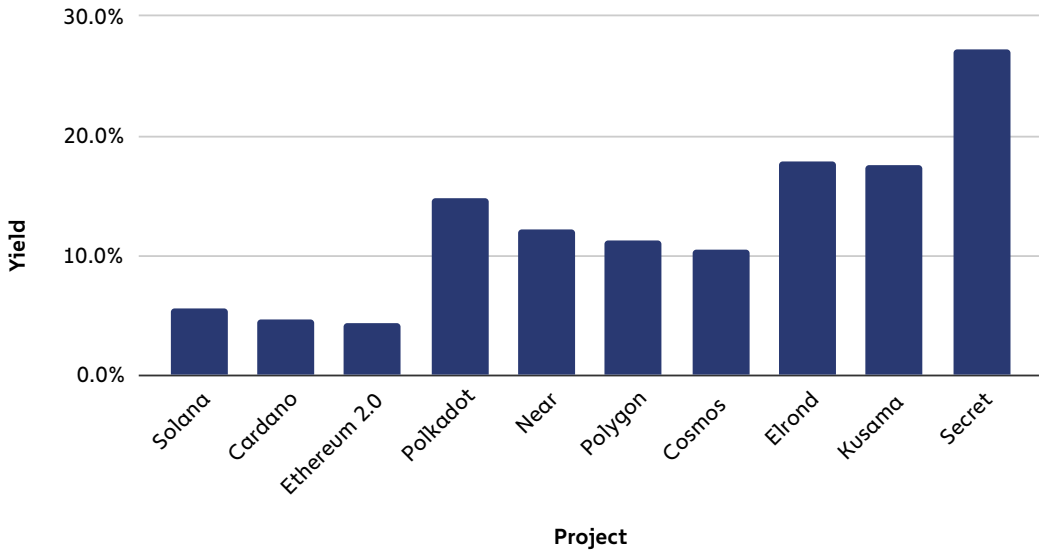
Total value staked by blockchain



Data source: Chainalysis, Staked, and Kaiko

As we see below, PoS blockchains vary widely in rewards yield and percent of market capitalization that is currently staked.

Staking yield by blockchain



Data source: Staked

ETH 2.0 offers the lowest staking yields at 4.6%, while other currencies like Secret offer yields as high as 27.2%. Of course, with a bigger market capital-

ization and a more proven track record, investors likely feel safer staking with Ethereum in the long term.

Just as miners create mining pools to combine their computing power and maximize their chances of mining new blocks, stakers can also gather into staking pools to do the same thing. Staking pools make it easy for any holder of the relevant blockchain's assets to participate in validation and earn rewards — all they need to do is send their tokens to the pool's address, and the pool operator does the rest. In return, stakers receive tokens from the pool representing their staked tokens and rewards, which can be redeemed for the real token. By pooling assets, staking pools can validate more blocks, and therefore give participants more consistent rewards than if they tried to stake alone. But that doesn't mean staking pools are risk-free. Staking pools pay out rewards in their own native tokens, so if something happens to the pool, such as a hack or general decline in popularity, those tokens can lose their value.

Lido provides a great example of how staking pools work. Lido is the biggest Ethereum staking pool operating now, and promises stakers 3.8% annual yield on their staked Ethereum after fees. Users who stake Ethereum with Lido get stETH, a token created by Lido, equal to what they stake, and also receive rewards in stETH. Holders can trade stETH tokens as they would Ethereum or any other crypto – whoever holds them is getting the staking rewards. This is an important value add that Lido provides, because by default, Ethereum staking rewards are inaccessible to validators and essentially "frozen" until the ETH 2.0 upgrade is complete and its chain merges with the ETH 1.0 blockchain. Lido's stETH is essentially a way of making currently illiquid Ethereum staking rewards liquid right away.

However, stETH isn't without its risks. Lido users can deposit their stETH at lending protocols (which we describe in greater detail below) in order to increase their rewards through lending yield or as collateral to take out loans themselves. Recent reporting from Coindesk examines how users who repeatedly engage in this activity in so-called "revolving loans" greatly increase potential risk and reward, which can be especially dangerous in the event of a market downturn like the one happening now. In other words, the ability to invest stETH with any service, no matter how risky, turns what by design is a relatively low-risk asset into a high-risk one.

Decentralized lending protocols automate borrowing for crypto and provide steady yields

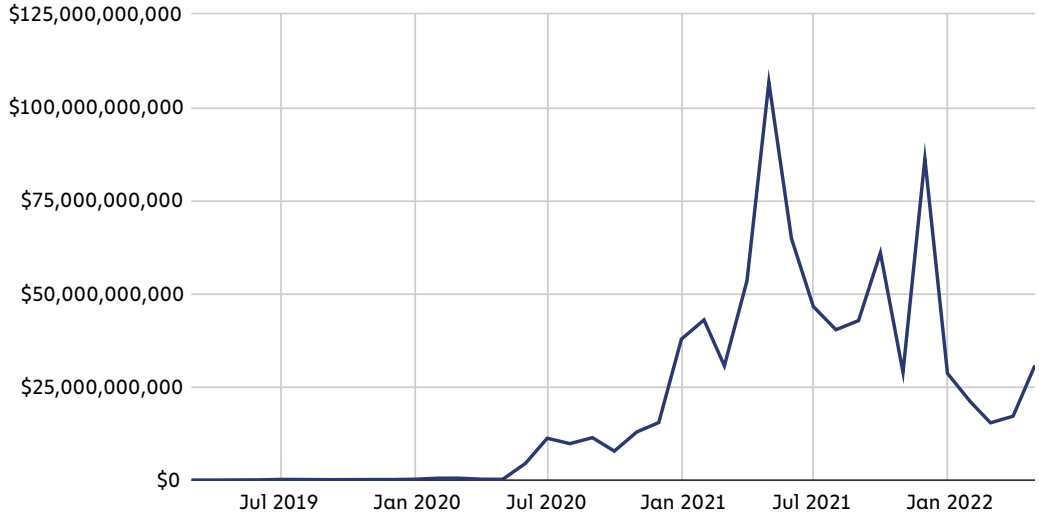
Lending protocols are another way for investors to put their cryptocurrency to work and earn steady returns. Users send cryptocurrency to the protocol's pool, and similar to staking, receive tokens minted by the pool of equivalent value to what they put in, as well as rewards generated by their deposit. The difference is that the rewards come from interest as the funds in the pool are loaned to other users, rather than from rewards for validating new blocks.

Compound is an example of a popular lending pool. Users can lend ETH to Compound's pool, and in return they receive cETH (Compound ETH), which can be traded like any other coin and redeemed for equivalent ETH from the pool. Other examples of popular lending pools include Make and AAVE.

Some consider lending pools to be a more reliable source of returns than staking pools, as staking rewards can change based on the number of people in the pool and the pool's success rate at validating new blocks. Lending pools, on the other hand, typically set their own interest rates, and while those rates can be changed or the pool could become less popular, there's less immediate variability outside the pool operators' control than with staking.

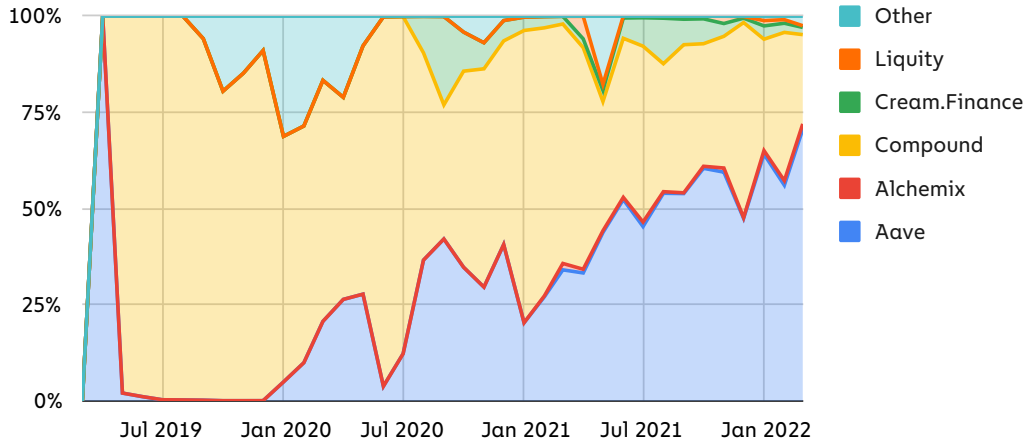
However, the growth of lending pools has been less consistent than that of staking pools.

Monthly value sent to lending protocols, March 2019–May 2022



After huge spikes during the summer of 2021, when DeFi usage was extremely high, the value received by lending protocols has declined so far in 2022. Through the end of May, users have sent $113 billion worth of cryptocurrency to lending protocols. At the same time in 2021, that figure was just under $272 billion.

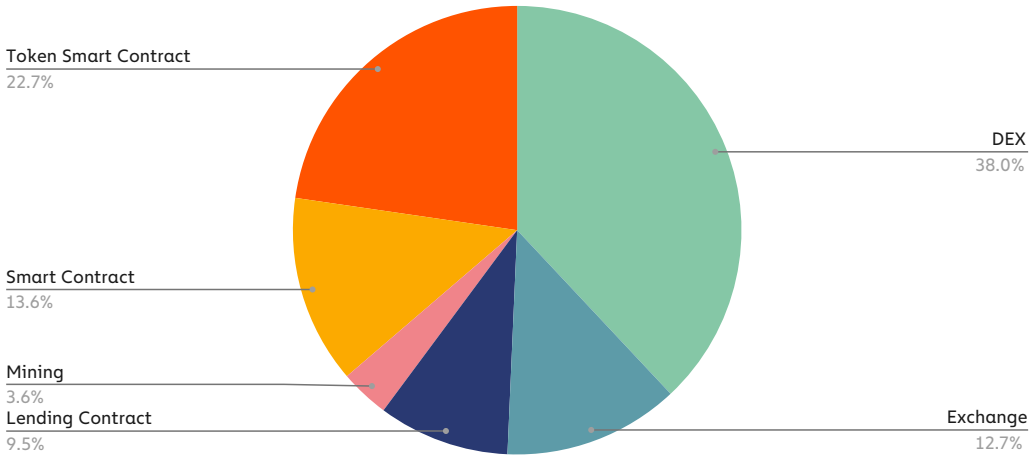
Share of total value sent to lending protocols by protocol, March 2019–June 2022



AAVE has become the go-to lending pool, accounting for between 55% and 85% of all funds received by lending pools each month so far in 2022.

What exactly do borrowers do with the funds they received from pools?

Destination of funds borrowed from lending protocols by service category



Overall, 84% of funds borrowed from lending protocols go to other DeFi protocols — primarily DEXes, but also protocols associated with new tokens and DeFi-based services. While this can be positive in terms of growing the overall DeFi ecosystem, it can also be dangerous in the event of market downturns like the one that began recently. If users invest borrowed funds in another risky, high-yield DeFi protocol, and that protocol fails, those users may be unable to pay back their loans — if that happens to too many users at once, the original lending protocol can become insolvent. We explore this concept of cascading risk in DeFi in greater detail later on in our section on risk in web3.

DAOs

Dissecting the DAO: Web3 Ownership is Surprisingly Concentrated

Decentralized autonomous organizations (DAOs) are a staple of web3. Internet-native and blockchain-based, DAOs are intended to provide a new, democratized management structure for businesses, projects, and communities, in which any member can vote on organizational decisions just by buying into the project.

At a high level, this is how DAOs work:

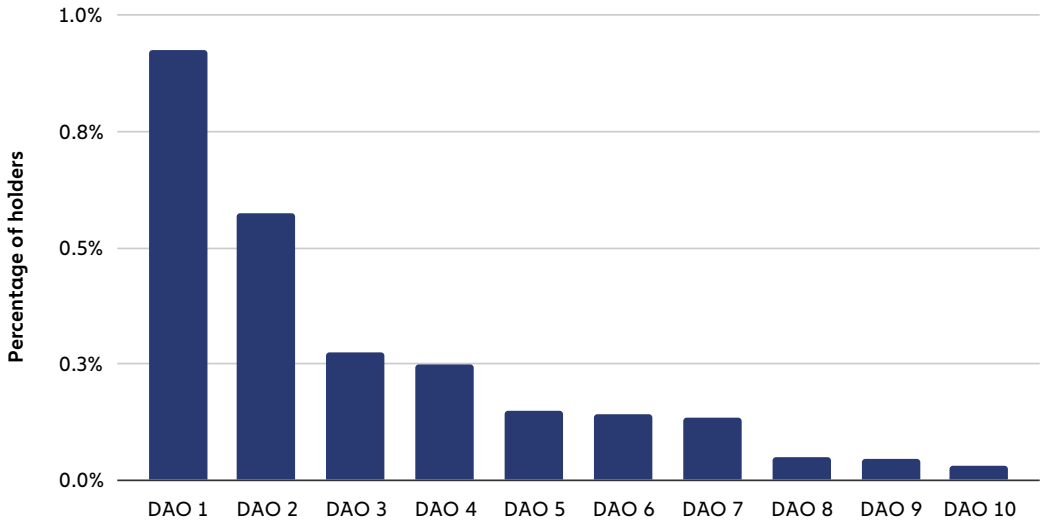
1. DAO founders create a new cryptocurrency, known as a governance token;
2. They distribute these tokens to users, backers, and other stakeholders;
3. Each token corresponds to a set amount of voting power within the organization. Each token also corresponds to a price on the secondary market, where it can be bought and sold at will.

While this process is often described as a way to decentralize power, governance token data suggests that DAO ownership is highly concentrated.

The concentration of governance token holdings

By analyzing the distribution of ten major DAOs' governance tokens, we find that, across several major DAOs, less than 1% of all holders have 90% of voting power.

Share of users holding 90% of all governance tokens by DAO



This has meaningful implications for DAO governance. For example, if just a small portion of the top 1% of holders worked together, they could theoretically outvote the remaining 99% on any decision. This has obvious practical implications and, in terms of investor sentiment, likely affects whether small holders feel that they can meaningfully contribute to the proposal process.

The impact of high concentration on DAO governance

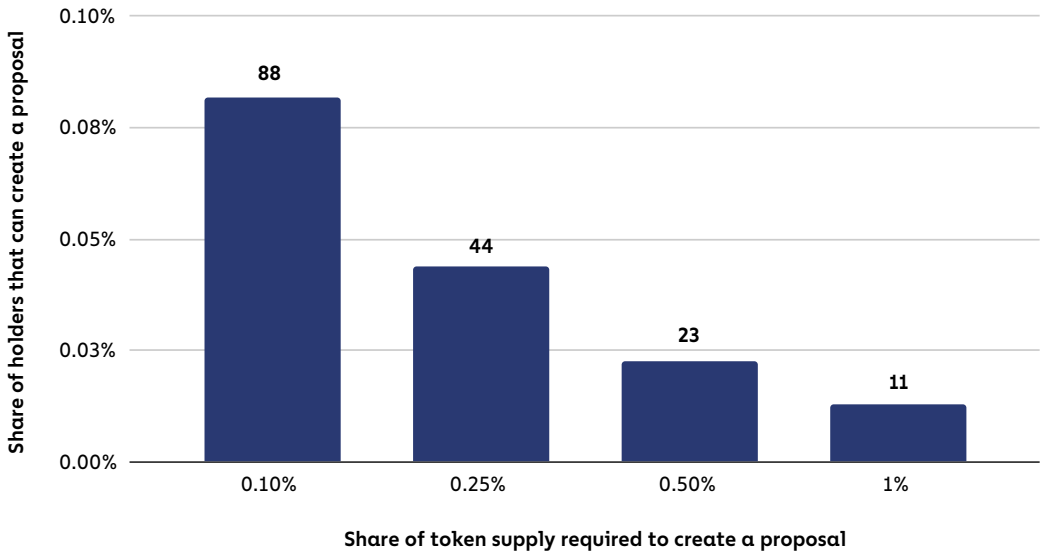
For a governance token holder, there are three key governance actions. Voting is simple — any holder can do it. But what about creating a proposal? And what about passing it?

Per these ten DAOs proposal requirements, we find that:

1. A user must hold between 0.1% and 1% of the outstanding token supply to create a proposal.
2. A user must hold between 1% and 4% to pass it.

Using these ranges as lower and upper bounds, we find that between 1 in 1,000 and 1 in 10,000 of these ten DAOs' holders have enough tokens to create a proposal.

Share and number of holders that can create a proposal



There are several tradeoffs at play here. If too many holders can create a proposal, the average proposal's quality may fall, and the DAO may be riddled with governance spam. But if too few can, the community may come to feel that "decentralized governance" rings false.

When it comes to single-handedly passing a proposal, between 1 in 10,000 and 1 in 30,000 holders have enough tokens to do so.

Overly concentrated voting power in DAOs can result in decision-making that seemingly contradicts the tenets of decentralization on which web3 is built. For instance, in June 2022, the DAO governing the Solana-based lending protocol Solend faced a problem: Solana's price was dropping, and if it fell much further, the protocol's biggest whale user would face a margin call that could render Solend insolvent and send roughly $20 million worth of Solana onto the market, potentially tanking the asset's price and upending the entire Solana ecosystem. The DAO called a vote to take control of the whale's account and liquidate its position through OTC desks, rather than the open market.

The proposal passed easily, with over 1.1 million "yes" votes to 30,000 "no" votes. However, more than 1 million of those votes came from a single user with enormous governance token holdings. Without their vote, the motion wouldn't have passed the 1% participation rate necessary for quorum.

Source: Solend on Twitter

The decision triggered a backlash from the cryptocurrency community, with many questioning how a platform could claim to be decentralized and then take control of a user's funds against their will. Following this, the Solend DAO voted again to invalidate the proposal, and the whale user eventually began to unwind their position. While the crisis was averted in this case, it raises questions about the ability of a DAO to act in the best interest of all participants when some voters control such an outsized share of governance tokens.

How do DAOs govern, exactly?

Actual governance processes vary enough from DAO to DAO that this question is best answered with examples. Let's start with the biggest one: Uniswap.

Example: Uniswap Governance

Uniswap is a decentralized exchange (DEX), and, like many DeFi protocols, it is governed by a DAO.

Anyone who holds Uniswap's governance token, UNI, is a member of this DAO. They can participate in governance by delegating their voting rights to their own or another's address, by publicizing their opinions, or by submitting their own proposal. The contents of these proposals vary widely: holders have recently voted on whether to finance a grant program, whether to integrate a new blockchain, and whether to reduce the governance proposal submission threshold.

But before someone can submit a proper proposal, their idea must pass the first two phases: temperature checks and consensus checks.

1. The temperature check determines whether there is sufficient community will to change the status quo. At the end of the two days, a majority vote with a 25,000 UNI yes-vote threshold wins.
2. The consensus check establishes formal discussion around a potential proposal. At the end of five days, a majority vote with a 50,000 UNI yes-vote threshold wins.

If both checks pass, an official governance proposal can be put to a vote. Then, there's a seven-day deliberation period to discuss the merits of this proposal occurs on governance forums. If at the end of this period there are at least 40 million yes-votes with no-votes as a minority, the proposal has passed, and will be enacted after a two-day timelock.

Example: Dream DAO Governance

Not all DAOs function like Uniswap, but most at least run on similar infrastructure, using voting systems like Snapshot and chat servers like Discord. Dream DAO is no exception, though its mission and therefore its governance process is necessarily unique.

Dream DAO is an impact-oriented DAO created by 501(c)(3) charity Civics Unplugged and designed to provide diverse Gen Zers globally with the training, funding, and community they need to use web3 to improve humanity. Their governance process is run by holders of SkywalkerZ — NFTs

that function as both governance tokens and fundraising incentives for anyone interested in donating to the program. For every SkywalkerZ NFT purchased by a donor, a new SkywalkerZ is reserved for a future Gen Zer to join as a voting member, thereby receiving power in the DAO without needing to pay. The purchaser of the NFT can apply to join the DAO and become a voting member as well, or they can leave it to the Gen Z student they've sponsored — either way, the NFT is theirs to keep.

By removing financial barriers from the process of participating in DAO governance, Dream DAO empowers its target audience – future Gen Z leaders – to influence decision-making, immerse themselves in web3, and leverage blockchain technologies positively.

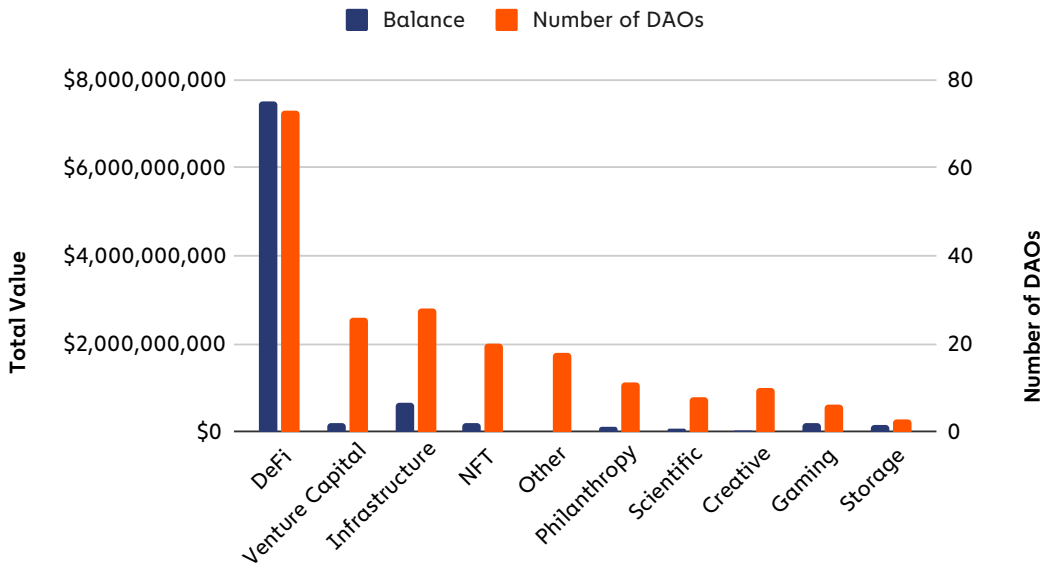
Where are DAOs most common and well-funded?

DAOs span the entire length of web3. They govern:

- DeFi protocols like Uniswap ($UNI) and Sushi ($SUSHI).
- Social clubs like Friends With Benefits ($FWB) and Bored Ape Yacht Club ($APE).
- Grant-makers like Gitcoin ($GTC) and Seed Club ($CLUB).
- Play-to-earn gaming guilds like Good Games Guild ($GGG) and Yield Guild Games ($YGG).
- NFT generators like Nouns (1 NFT = 1 vote).
- Venture funds like MetaCartel and Orange DAO.
- Charities like Big Green DAO and DreamDAO (1 SkywalkerZ = 1 vote).
- Virtual worlds like Decentraland ($MANA) and Sandbox ($SAND).
- And more.

In terms of the number of DAOs and their treasury sizes, however, DeFi-related DAOs have a giant lead. The DeFi category accounts for 83% of all DAO treasury value held and 33% of all of the DAOs by count.

Total assets held and number of DAOs by web3 category



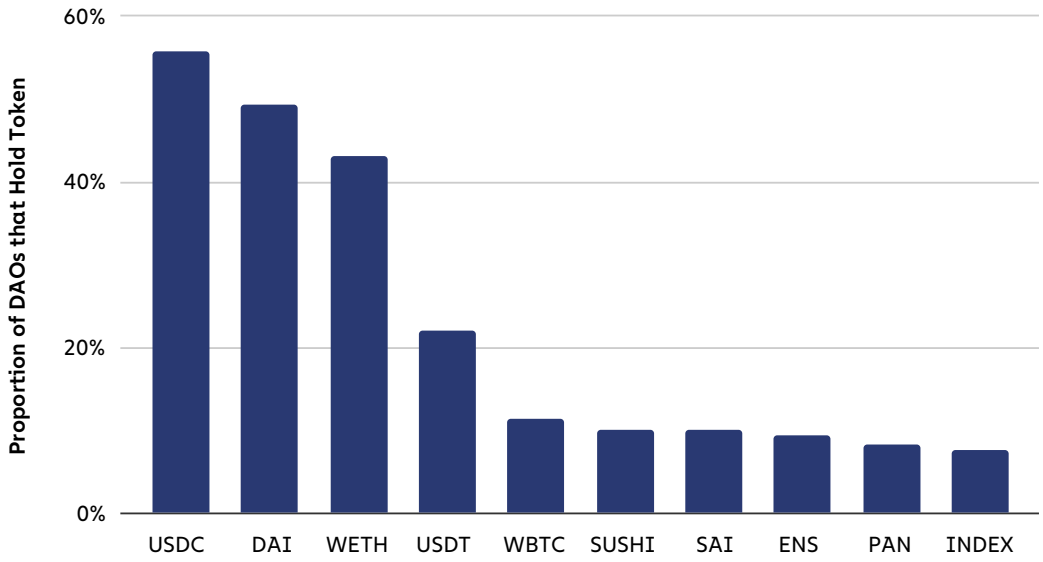
There are also a large number of DAOs focused on venture capital, infrastructure, and NFTs, suggesting that DAOs are appealing to investors, developers, and artists. Their on-chain treasuries, however, are relatively tiny.

To be fair, the lines between these categories are blurry. Gaming DAOs often engage with NFTs, venture DAOs often provide funding to DeFi, and infrastructure DAOs support all of the above categories.

Treasury management: What assets do DAOs hold?

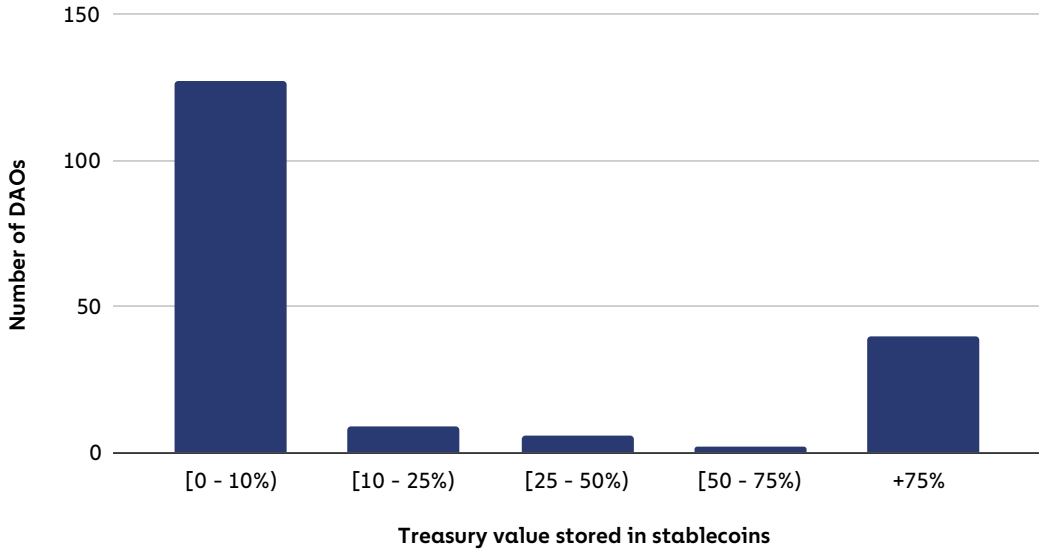
Even though DAOs vary in type and size, most of their on-chain treasuries hold similar cryptocurrencies. The most commonly held cryptocurrency is the stablecoin USD Coin (USDC), with over half of the 197 DAOs we analyzed holding a balance of USDC.

Cryptocurrencies held by the most DAOs



However, stablecoins seldom account for a majority of an on-chain treasury's value. On average, 85% of DAOs' on-chain treasuries are stored in a single asset, and that asset is a stablecoin in only 23% of the DAOs we studied.

Percentage of DAO treasury allocated to stablecoins

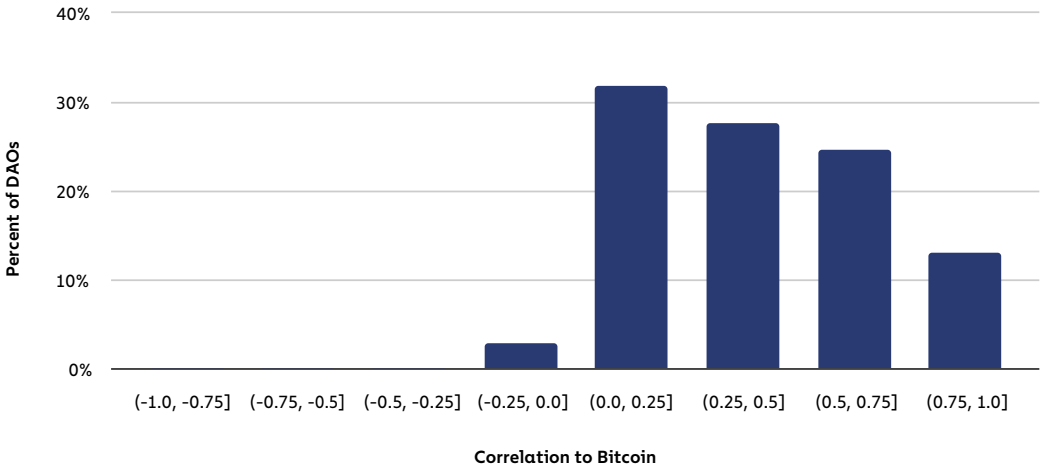


These on-chain treasuries are roughly as volatile as Bitcoin. By assuming DAOs' current holdings are their historical portfolios over the last year, we find that:

- The average DAO with assets over $1 million has an annualized volatility of 82%, versus 69% for Bitcoin.
- The average DAO with assets over $1 million suffered a maximum drawdown of 51% over the past year, compared to Bitcoin's drawdown of 72%.

DAO treasury values are also fairly correlated with Bitcoin price movements. 38% of on-chain DAO treasuries have correlations with Bitcoin that are between 0.5 and 1.00.

How strongly DAO treasury values correlate with Bitcoin price movements



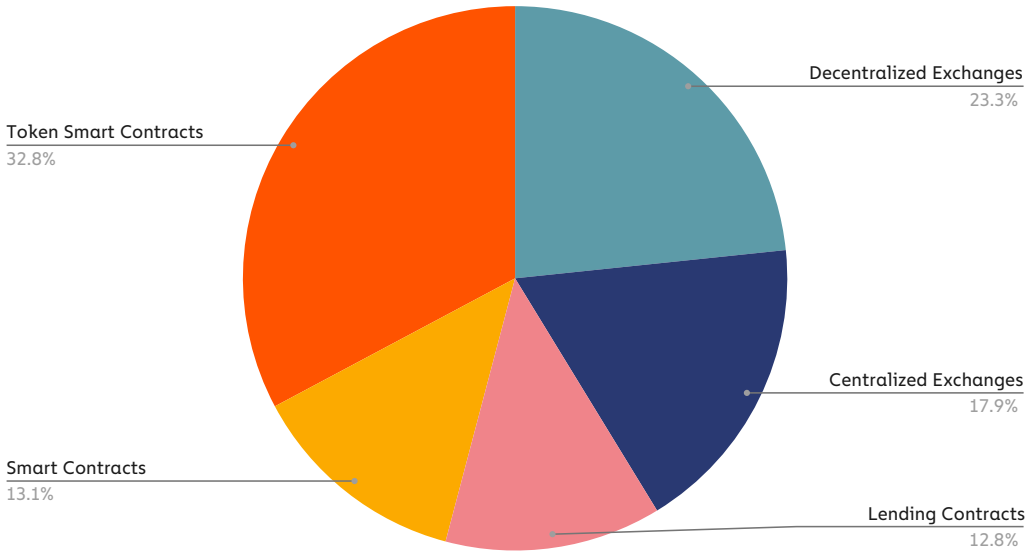
One of the most interesting areas of DAO treasury management that has yet to take off is in mergers and acquisitions (M&A). M&A makes sense for DAOs because it allows them to get into adjacent areas without having to develop internal tooling. As the DAO model matures, we suspect M&A will become more commonplace.

DAOs thus far have also been fairly limited in terms of the types of instruments they use and hold. For example, few DAOs to date have used loans or credit, perhaps due to their uncertain legal status. As DAOs mature, we are likely to see more standardized regulations, management strategies, and reporting practices.

Who contributes to DAOs?

While we don't collect demographic data about DAO participants, we can learn some things about DAO contributors using blockchain data.

Where DAO contributions come from



Token smart contract = a project-specific ERC-20 or Layer 1 token contract

As one might expect, DAO participants are advanced users of cryptocurrency services. Only 17.9% of DAO treasury funds came from centralized services, while the remaining 82.1% originated at decentralized services. This suggests that most DAO contributors also engage with DeFi platforms and likely self-host their cryptocurrency.

The future of DAOs

As DAOs gain momentum, a cottage industry of tooling services and advocacy groups have emerged to help them grow and govern. Superdao streamlines DAO creation; Snapshot simplifies governance; and Coin Center advocates for the industry on Capitol Hill. As they continue to expand, it will be interesting to see what they can accomplish, what they will become, and to what extent they will achieve their goal to decentralize the ownership of the internet. With the proliferation of DAOs today, we'll have plenty of chances to see.

NFTs

NFT Transaction Activity Stabilizing in 2022 After Explosive Growth in 2021

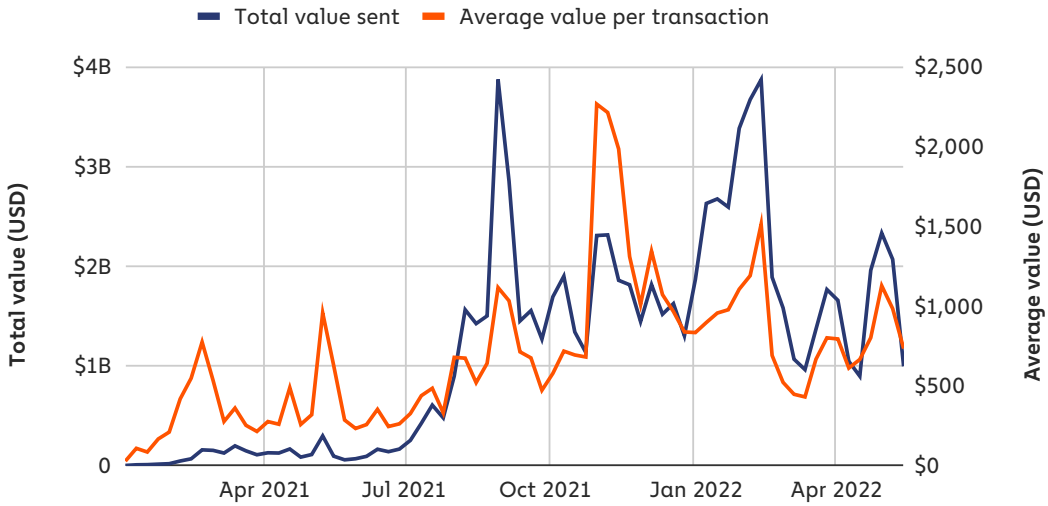
Non-fungible tokens (NFTs) have been one of the most dynamic and prominent parts of Web3 over the last two years. NFTs are blockchain-based digital items whose units are designed to be unique, unlike traditional crypto-currencies whose units are meant to be interchangeable. NFTs store data on blockchains — with most NFT projects built on the Ethereum blockchain — and that data can be associated with files containing media such as images, videos, and audio, or even in some cases physical objects. NFTs typically give the holder ownership over the data, media, or object the token is associated with, and are commonly bought and sold on specialized marketplaces.

NFTs saw explosive growth in 2021, but this growth hasn't been consistent and has leveled off so far in 2022. Below, we'll explore how the NFT market has grown and contracted since the beginning of 2021.

NFT activity growing since 2021, but not consistently

Since the beginning of 2021, NFT transaction volume has grown significantly, but this growth fluctuates. NFT activity ebbs and flows month to month — in 2022 thus far, the value sent to NFT marketplaces continued its 2021 growth in January, entered a downturn in February, and then began to recover in mid-April.

Weekly total cryptocurrency value and average value per transaction sent to NFT platforms, January 2021–May 2022

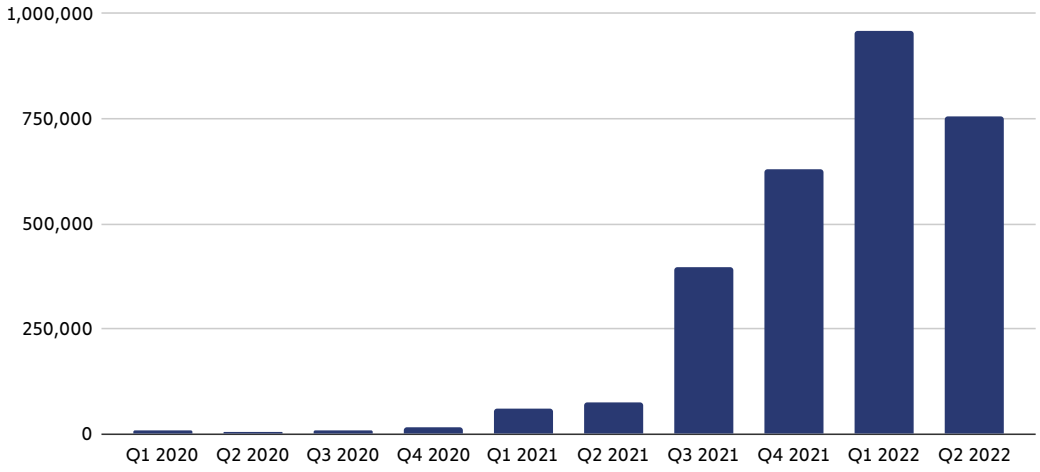


Overall, collectors have sent over $37 billion to NFT marketplaces in 2022 as of May 1, putting them on pace to beat the total of $40 billion sent in 2021. However, since late summer 2021, NFT transaction growth has come in fits and starts, with activity largely remaining flat except for two big spikes: One in late August, which was likely driven by the release of the Mutant Ape Yacht Club collection, and one stretching from late January to early February of 2022, which was likely driven by the launch of the LooksRare NFT marketplace.

After that spike though, NFT transaction activity declined significantly beginning in mid-February, dropping from $3.9 billion the week of February 13 to $964 million the week of March 13 — the lowest weekly level since the week of August 1, 2021. The NFT market began to recover in mid-April, however, and is now approaching the weekly volumes it hit earlier in the year, likely due to the recent launch of Bored Ape Yacht Club's metaverse project.

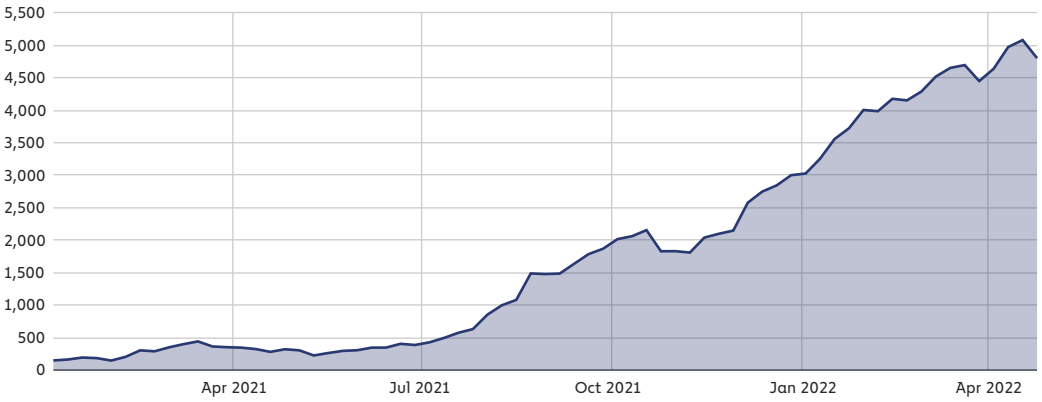
Despite these fluctuations in transaction volume, the number of active NFT buyers and sellers continues to grow.

Number of active NFT buyers and sellers, Q1 2020–Q2 2022



In Q1 2022, 950,000 unique addresses bought or sold an NFT, up from 627,000 in Q4 2021. Overall, the number of active NFT buyers and sellers increased every quarter from Q2 2020 onwards, until finally dipping in Q2 2022.

Weekly number of active NFT collections on OpenSea, January 4, 2021–April 25, 2022

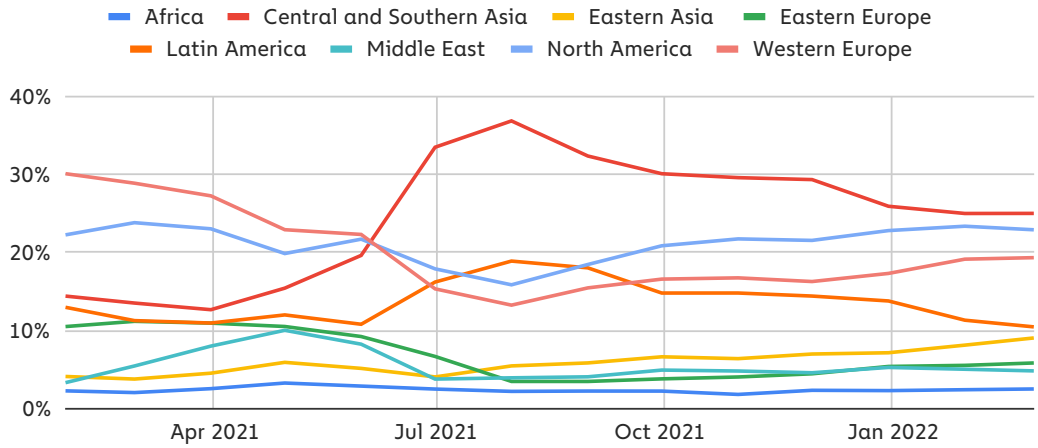


The number of active NFT collections on OpenSea — meaning those with any transaction activity in a given week — has also grown consistently since March 2021, and above 4,000 as of late April.

Who uses NFTs?

Analysis of web traffic to popular NFT platforms reveals that the asset class attracts users from all over the globe.

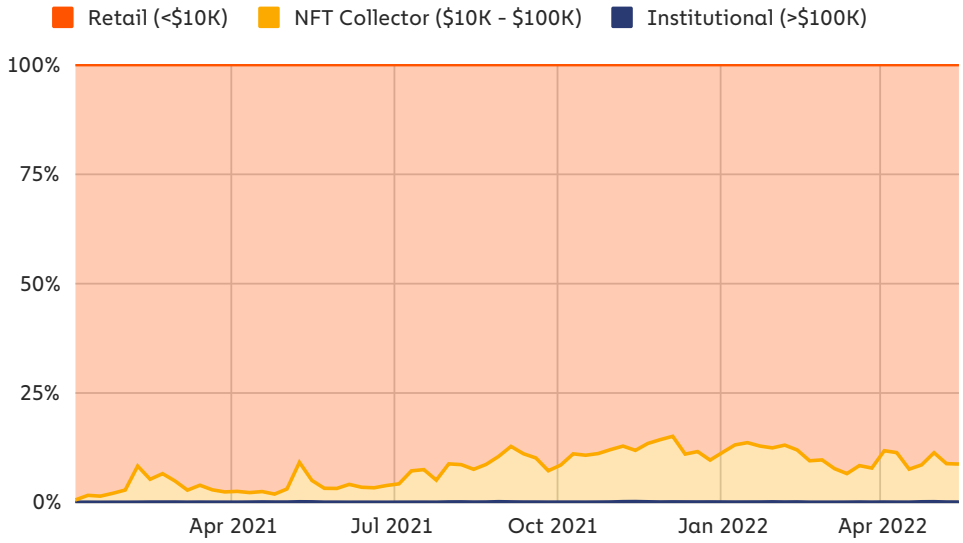
Monthly share of web traffic to NFT marketplaces by region, 2021–2022 YTD



Central and Southern Asia leads the way, followed by North America and Western Europe. While some regions certainly lag, the fact that no region has made up more than 40% of all web traffic since the beginning of 2021 suggests that, like cryptocurrency as a whole, NFTs have captured a global audience.

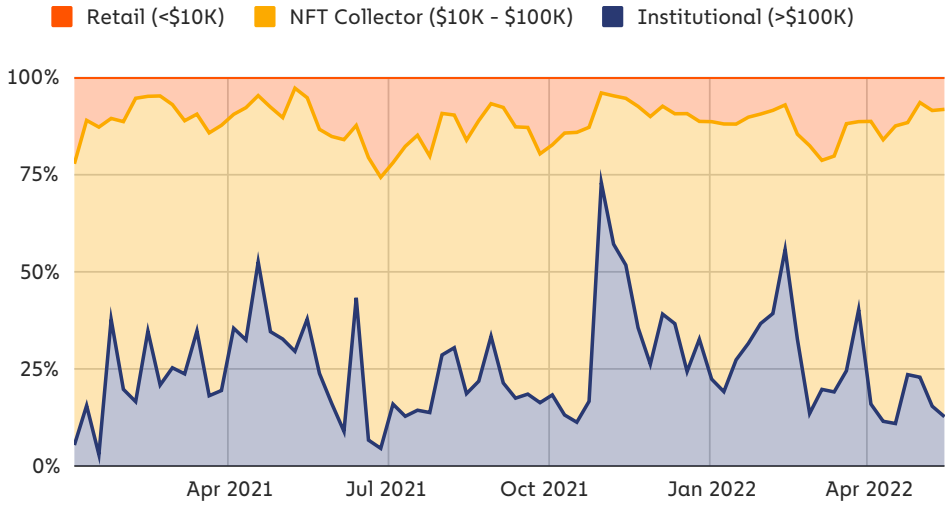
Analysis of NFT transaction sizes can also tell us a great deal about who's investing and collecting.

Weekly share of NFT transactions by transfer size, Jan 2021–May 2022



The vast majority of NFT transactions are at the retail size, meaning below $10,000 worth of cryptocurrency. NFT collector-sized transactions (between $10K and $100K) grew significantly as a share of all transfers between January and September of 2021, but since then have stayed flat. This suggests that, for the time being, the addition of new retail NFT investors is keeping pace with the addition of bigger NFT investors.

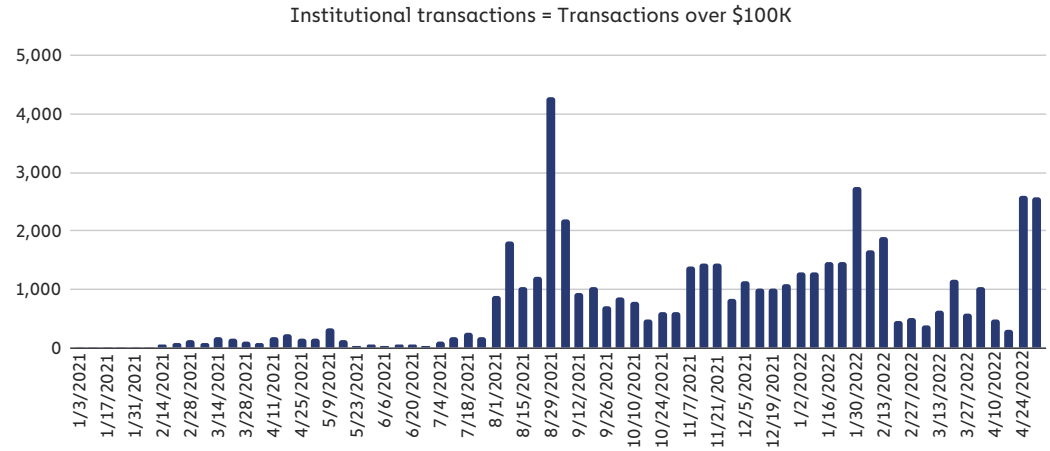
Weekly share of NFT transaction volume by transfer size, Jan 2021–May 2022



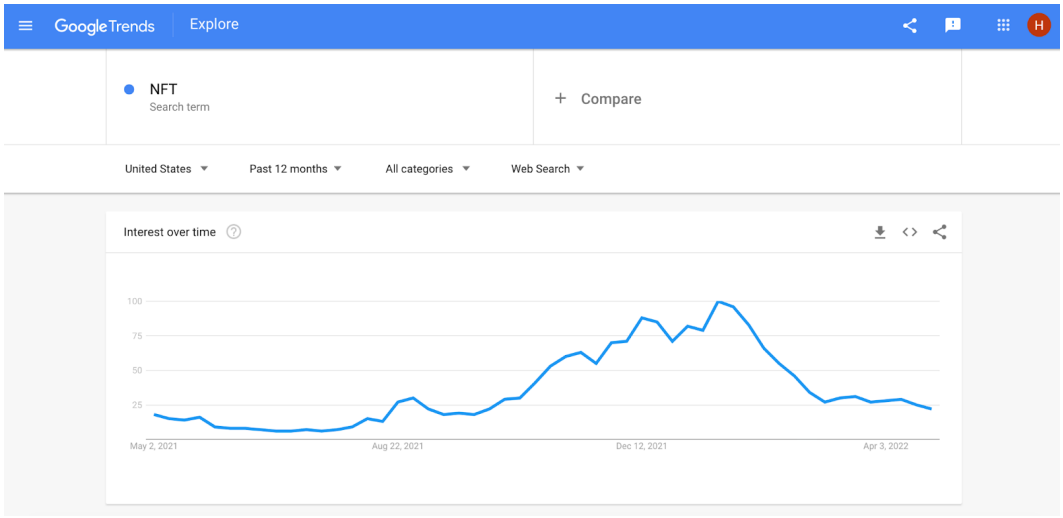
However, if we think in terms of transaction value rather than number of transfers, we see that NFT collectors make up a majority of activity. Institutional investors are nipping at their heels, and even make up the majority of activity in certain weeks when extremely large purchases have been made. For instance, during the week of October 31, 2021, institutional transfers made up 73% of all activity, largely due to the purchase of several NFTs in the Mutant Ape Yacht Club collection. More institutional-sized transfers followed in subsequent weeks, and since then, institutional transfers make up 33% of all activity.

However, as is the case with the NFT market as a whole, the growth of institutional-sized NFT transactions hasn't been consistently sustained.

Number of institutional-sized NFT transactions per week, January 2021–April 2022



Between late November and mid-February, institutional NFT purchasing grew each week, reaching 1,889 transactions the week of February 13, after having spiked to 2,739 two weeks prior. Institutional NFT activity fell abruptly after that, dropping to just 473 transactions during the week of February 20. As of April 17, 2022, institutional NFT activity has yet to reach the levels it did in the winter of 2021. This period of reduced institutional activity also roughly coincides with what appears to be an overall decline in interest in NFTs generally.



Credit: Google Trends

We make no claims as to the statistical relationship between Google searches for NFTs and NFT transaction activity, at the institutional level or any other. However, it'll be interesting to observe whether NFTs can recapture the broad public interest they achieved in late 2021, and whether this leads to increased transaction activity or rising prices for popular NFT collections.

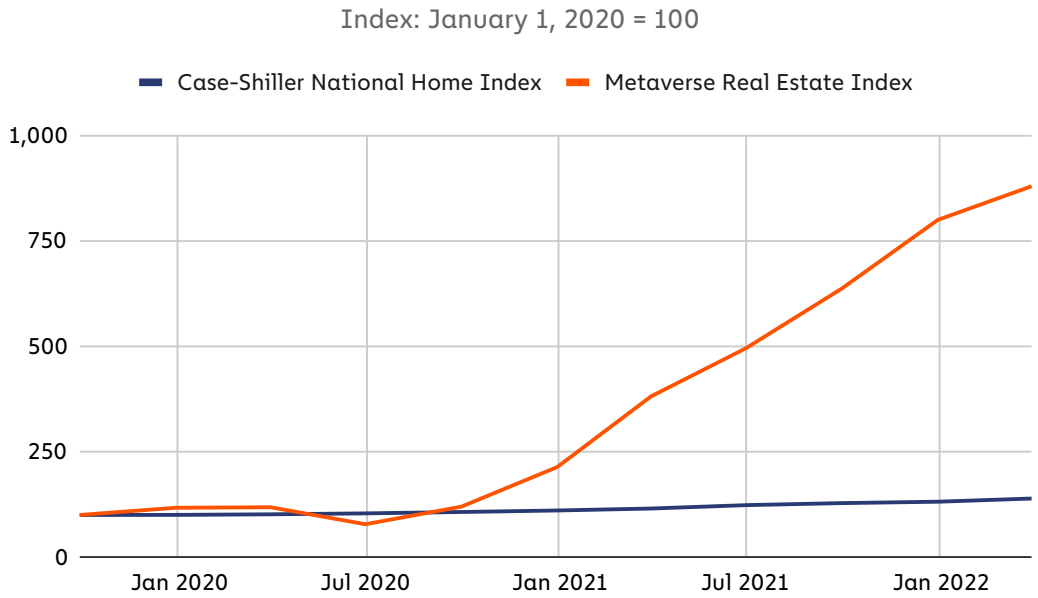
Metaverse and Gaming

Real Estate and Gaming Are on the Rise in the Metaverse. VR and NFT Integrations Could Boost Them Further

For artists, brands, and gamers, the metaverse is a living reality. Travis Scott's Fortnite concert was attended by 27 million; JP Morgan just signed a yearlong virtual property lease; the Vatican is opening a non-fungible art gallery.

This swift adoption is a testament to the metaverse's current and future utility – and it's reflected in virtual real estate pricing. From September 2019 to March 2022, blockchain-based virtual real estate prices grew by 879%. *Real* estate prices, meanwhile, grew by 39%.

Price growth in real versus digital property, January 2020–March 2022



The comparison isn't apples-to-apples – the Case-Shiller index tracks actual housing, while the Metaverse index tracks virtual parcels – but it's nonetheless surprising that the growth of virtual real estate prices has outpaced that of physical real estate by 532%.

Why might that be? Let's dive in.

What's the utility of metaverse property?

Blockchain-based virtual real estate (VRE) offers both present-day and prospective benefits to the people who own it. Let's take a look at both types of amenities.

Present-day utilities

- Embedded videos, images, NFTs, and interactive objects
- In-game single-player and multiplayer activities
- Play-and-earn integrations
- Screen-sharing and town hall functionalities
- Access to private events and NFT-gated communities

This last feature – access to private events and exclusive communities – has been a big driver of NFT demand to date, and it looks to be translating into sales of virtual real estate. Bored Ape Yacht Club, for example, has always bundled its NFTs with entertainment, socialization and digital community. and they've since parlayed that appeal into a $310 million metaverse land sale.

Prospective utilities

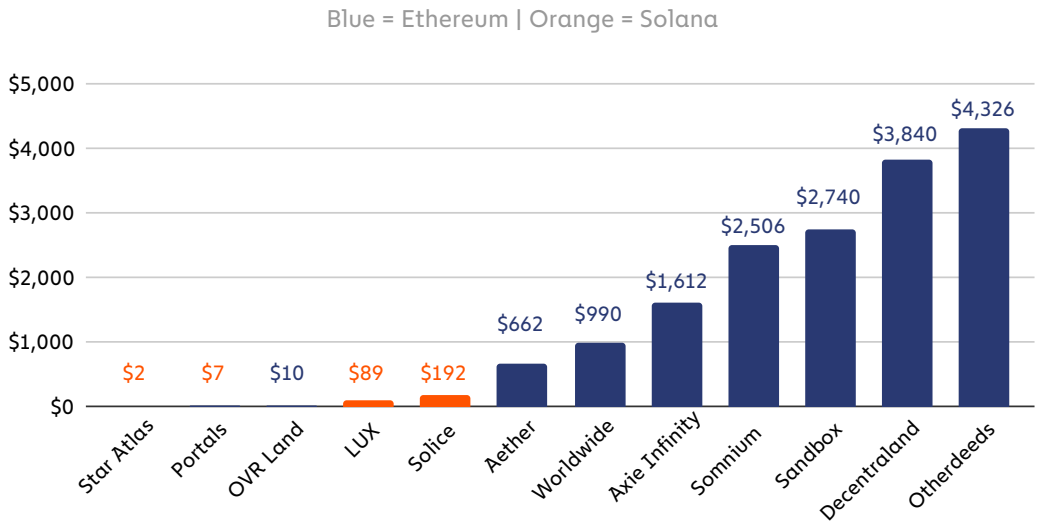
- Renting and leasing
- Free airdrops of future VRE NFTs
- Future AR/VR integrations and functionalities

Not all metaverse projects have all of these utilities, but most of them have a combination of many.

Where's the most affordable metaverse housing?

The biggest differences in metaverse land pricing seems to be *between* blockchains, not within them. Relative to metaverse land on Ethereum, metaverse land on Solana has much lower entry-level pricing.

Floor prices of virtual real estate (VRE) on Ethereum vs. Solana



Source: MagicEden / OpenSea

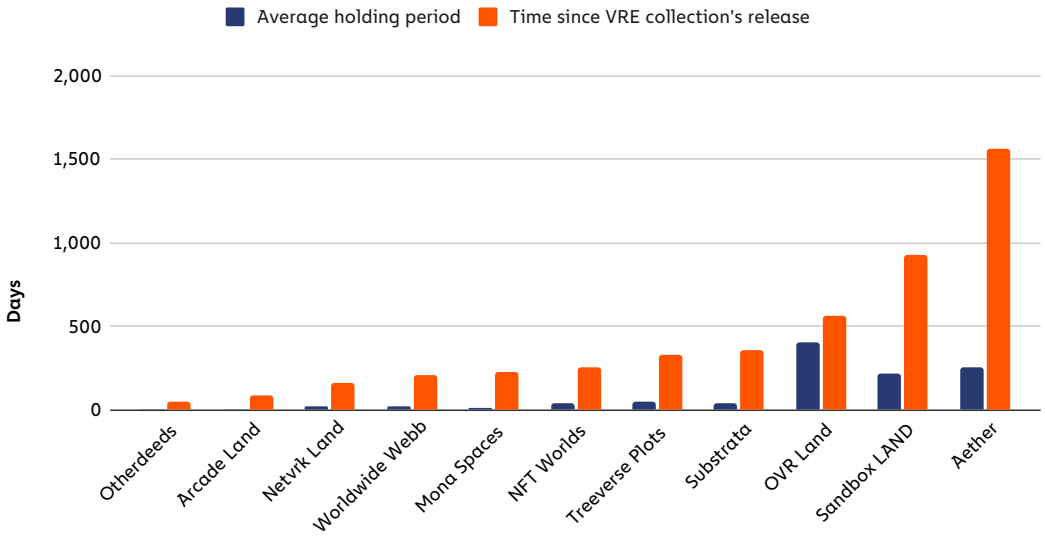
Solana gas fees average $0.00025, a fraction of Ethereum's $5 to $50. This may make "affordable metaverse housing" more practical for holders and developers on Solana.

That being said, almost every Ethereum-based metaverse listed above has recently integrated with Polygon, an Ethereum sidechain that competes with Solana on cost and speed. So while this gap may be explained in part by transaction fees, it could soon (or already) be explained by differences in popularity or monetization strategies.

How long are users holding their virtual real estate?

The average duration of users' land holdings varies widely. Across the 11 Ethereum-based metaverses for which we have data about holdings, most signs point to speculative activity.

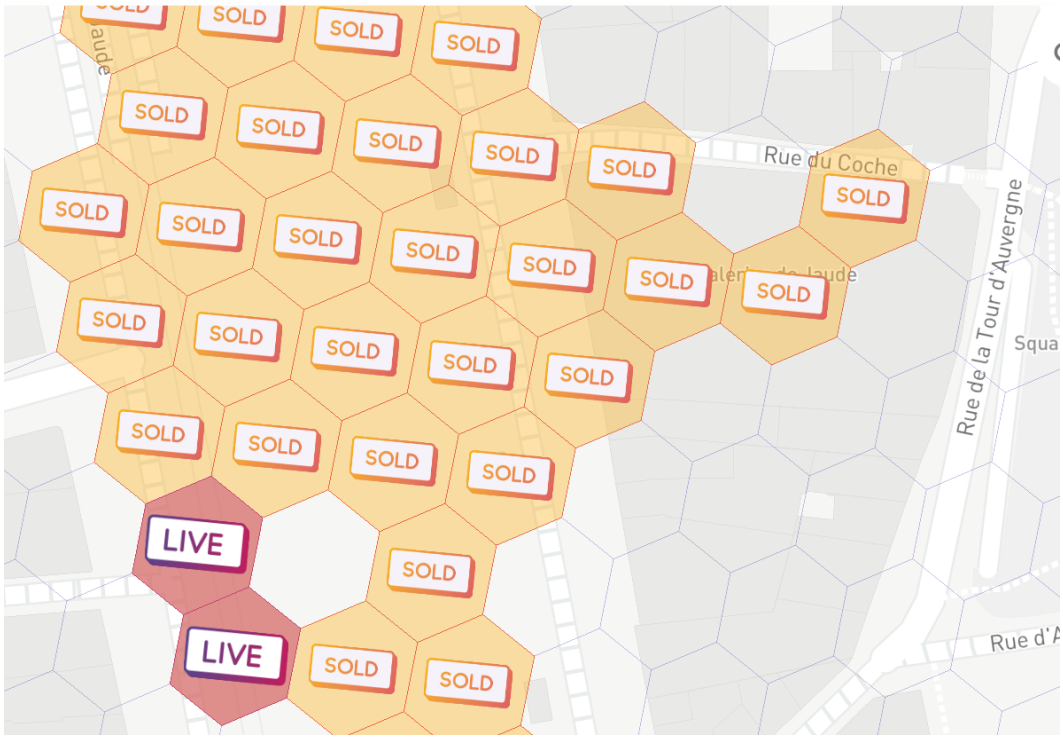
Average VRE holding period and number of days since metaverse project's NFT release



In 10 out of 11 of the projects we studied, users have held their VRE NFTs for less than 25% of the time the NFT collection has been live. In 6 out of 11, they've held it for less than 15%. In other words, VRE purchases in most of the above projects would be best characterized as "flipping."

The biggest exception is OVR Land. OVR Land has the longest holders for three likely reasons: the land is abundant, cheap, and takes time to develop. There are more than 1.6 trillion OVR lands, each one costs just $10 to $50, and when you buy one, what you're actually buying is the opportunity to overlay augmented reality (AR) experiences on top of real-world geography.

For example, here are two parcels of OVR land listed for sale in France.



Source: OVR Marketplace

But building an AR experience is neither fast nor easy – especially for a solo software developer. This may partially explain why most users are buying and holding, but not often selling. Another possible explanation is that AR feels closer to being realized than VR, which is what most VRE collections have pitched themselves as eventually supporting. In this way, the payoff of holding OVR land may seem to users like it will come sooner than holding land from other projects.

What external factors will determine the long-term value of virtual real estate?

Because the metaverse is such a nascent space, the long-term value of block-chain-based VRE depends on a number of external factors. While most of these factors are hard to foresee, we believe that a couple of them may be:

- Whether AR/VR systems are more interoperable or proprietary
- The pace of adoption of new computing technology

Interoperable vs. proprietary technology

It's easy to imagine a world where the R&D budgets of companies like Meta (current developer of the Oculus Rift) and Niantic (creator of Pokemon Go, the augmented reality hit) give way to a massive technological lead. The question, then, is whether the fruits of this labor will be broadly shared. In other words: to what extent will these companies' technologies be open-sourced and accessible to build upon? And will they allow other metaverse companies to connect their projects, or will they create a walled garden within which only they can develop?

Meta had this to say about the subject in May:

> "The metaverse will be an interconnected system that transcends national borders, so there will need to be a web of public and private standards, norms and rules for it to operate across jurisdictions. There won't be a Meta-run metaverse, just as there isn't a 'Microsoft internet' or 'Google internet' today."

In June, big-name tech companies like Meta, Microsoft, and Epic Games formed the Metaverse Standards Forum (MSF). This group is meant to create open standards for all things metaverse, including AR, VR, and 3D technology. Other big names include Nvidia, Unity, Sony, and the World Wide Web Consortium (W3).

It remains to be seen whether these companies will build out their metaverse(s) in a fashion that is interoperable with current metaverse projects and blockchain technology. However, there is at least one early indication of a more blockchain-compatible future: Epic Games' acceptance of crypto games in its game store. While this has limited import to *metaverse projects* today, it's extremely important to blockchain gaming – an industry with very similar commitments and aims. We cover these in more detail in the coming pages.

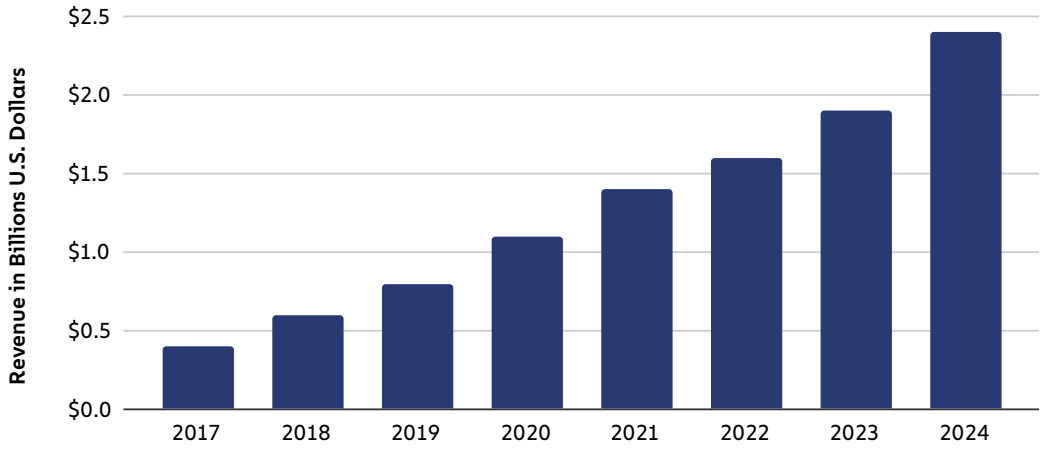
The pace of adoption of new computing technologies

Assuming some degree of interoperability, blockchain-based metaverse

projects stand to benefit immensely from the adoption of VR technology. The more immersive and life-like the virtual experience, the more likely it is for NFT-based ownership to feel tangible to users. So the faster VR technology grows, the better it is likely to be for metaverse land offerings.

Fortunately, the revenue generated from VR-based gaming is growing rapidly. From 2017 to 2021, VR gaming revenue had a compound annual growth rate of 28.5%.

Virtual reality (VR) gaming revenue worldwide, 2017–2024 (est)



Source: Statista

Also, analysts suspect that the VR boom will get only bigger – thanks in part to blockchain technology. Citi estimated in a March 2022 report that by 2030, the metaverse economy could be an 8 to 13 trillion dollar total addressable market. In its report, Citi listed VR and blockchain technology as two of the five key metaverse building blocks:

1. Operating systems connecting people and content
2. Blockchains that decentralize economic systems and digital asset ownership
3. Natural user interfaces e.g., voice control and gestures for greater user immersion
4. Extended reality (XR) headsets
5. Cloud networking infrastructure.

Blockchains and gaming

Blockchain games, while seldom linked to metaverse projects today, have many of the same ambitions:

- To build more open-ended economies
- To connect individuals and communities
- To push the boundaries of digital ownership
- To decentralize and share the value they create
- To make the virtual world as immersive as reality

They've also, like metaverse projects, exploded in popularity and funding. DappRadar recently reported that blockchain-based gaming activity has increased 2,000% over the last year. Furthermore, blockchain-based game companies fundraised $2.5 billion last quarter, up 150% from the quarter before.

But what about traditional games and game companies? What would happen if already-popular games adopted NFTs and cryptocurrency? Let's take a look and see (with a healthy suspension of disbelief).

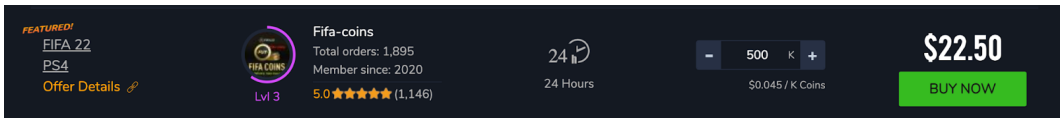
A blockchain gaming thought experiment: EA Sports on the blockchain

In fiscal year 2021, Electronic Arts (EA) generated $1.62 billion from its FIFA, Madden, and NHL Ultimate Team offerings.

In Ultimate Team (UT), players assemble, trade, and compete against one another with a squad of athletes, each of which are represented by a trading card. Players can buy packs of 12 to 30 of these trading cards with either points, which can be purchased with real money, or coins, which can be collected for free by playing. Players can then sell the cards they've drawn to other players in exchange for coins – but they can never convert these coins into points or real money.

At least in theory. In practice, despite EA's best efforts, there's a gray market for these coins that undercuts EAs pricing. For example, to buy an Ultimate Pack – EA's highest-tier and most expensive pack – players must spend either

2,500 points or 125,000 coins. Bought from EA, the pack costs $23; bought from the gray market, it costs $6.50.



Source: PlayerAuctions

In other words, this gray market both threatens EA's main revenue stream and makes "good citizen" players worse off. When third parties sell these coins for real currency, EA gets nothing – but players get three times the value for money.

But what if, instead of maintaining a closed-loop economy and forgoing this revenue leakage, EA minted their trading cards as NFTs, which could then be sold between players on a secondary market? How would this alter their revenue – and create new ways for players to make money?

For one thing, it would introduce a new revenue stream for EA. Usually, when an item is minted as an NFT, a portion of every sale is passed back to its creator as a royalty. UT already features a 5% transaction fee on its player-to-player market – so this is hardly unprecedented– but today it's not an actual revenue stream. Instead, it's a "gold sink" – a way to prevent coins from hyperinflating.

For another, it would heighten the concept of rarity. While no cards in today's UT economy have a predefined supply, this is the de facto standard for NFTs – and a key reason why they can fetch such high prices.

Lastly, it would give UT players the ability to make money. This is a win-win: if players can sell their cards for cryptocurrency, they can earn back some or all or even multiples of their original spending; if EA enables these trades, they can collect a small slice of every sale price.

Modeling Ultimate Team with NFTs

We now construct a simple financial model for both EA's revenue and Ultimate Team players' earnings in a game mode reimagined with NFTs.

Assumptions:

- 25 million active players. Ballpark estimate based on EA statements.
- $65 annual player spend. Ultimate Team revenue ($1.62 billion) divided by active players.
- 5% resale royalties. A common rate for NFTs.
- NFT primary sale price = secondary sale price. Some cards will surely rise in value following their primary sale while others will fall, so for simplicity's sake, our model assumes that in aggregate, all cards' secondary sale prices will equal primary sale prices.

Variables:

Annual resales: Our model projects NFT sales revenue for both EA Sports and its UT players at three different possible levels of annual NFT resale volume: 100%, 300%, and 500%. 100% resale volume would mean that for every $1 of annual player spend on primary NFT sales, there is $1 of secondary market sales. 300% would assume $3 of secondary market sales, while 500% would assume $5.

EA revenue: UT x NFTs	Annual resale volume		
	100%	300%	500%
Annual EA Sports revenue assuming $65 per player spend on primary card sales	$1,706,250,000	$1,868,750,000	$2,031,250,000

Interpretation: Introducing NFT player cards could generate significant additional revenue for EA Sports. Under our lowest resale volume model (100%), in which players spend $65 on NFTs and engage in $65 worth of secondary market activity, EA generates $1.7 billion in annual revenue – $81 million more than they do today. At 300% resale volume, EA generates $1.87 billion – $244 million in additional revenue. And at 500% resale volume, EA generates over $2 billion in annual revenue – $406 million more than today.

But how do the players fare?

Player earnings: UT x NFTs	Annual resale volume		
	100%	300%	500%
Annual player revenue assuming $65 per player spend on primary card sales	$1,543,750,000	$1,381,250,000	$1,218,750,000

Interpretation: Introducing NFTs could create a first-of-its-kind market for players to profit. Under our lowest resale volume model, players collectively realize $1.54 billion in annual earnings – none of which they realize today. At 300% resale volume, players' earnings fall to $1.38 billion. And at 500% resale volume, players' earnings rest at roughly $1.22 billion. In this model, players' total earnings fall as resale volume rises, because more resales means more fees, and our model assumes no increase in card value upon resale on average — again, some cards will rise in value, while some will fall. However, total player earnings could increase if the average card price rose over time, as is the case with many NFT collections generally.

Discussion

It's worth noting that in this model, primary sales would still be EA's main revenue driver. But the secondary sales, while accounting for only a fraction of EA's $1.87 billion in revenue, would benefit players immensely. Even if we relax the assumption that the NFTs hold their original value, players of Ultimate Team could still walk away with hundreds of millions in earnings collectively – a far cry from the $0 they earn as "good citizens" today.

Furthermore, because in this model players recognize that they have a chance to resell their cards for a profit, it may attract an even higher annual player spend than our original $65 assumption.

The metaverse is fast approaching

All trends point to the metaverse. Virtual real estate now offers real-world utility; VR technologies are coming closer to reality; and blockchains are imbuing digital ownership with meaning.

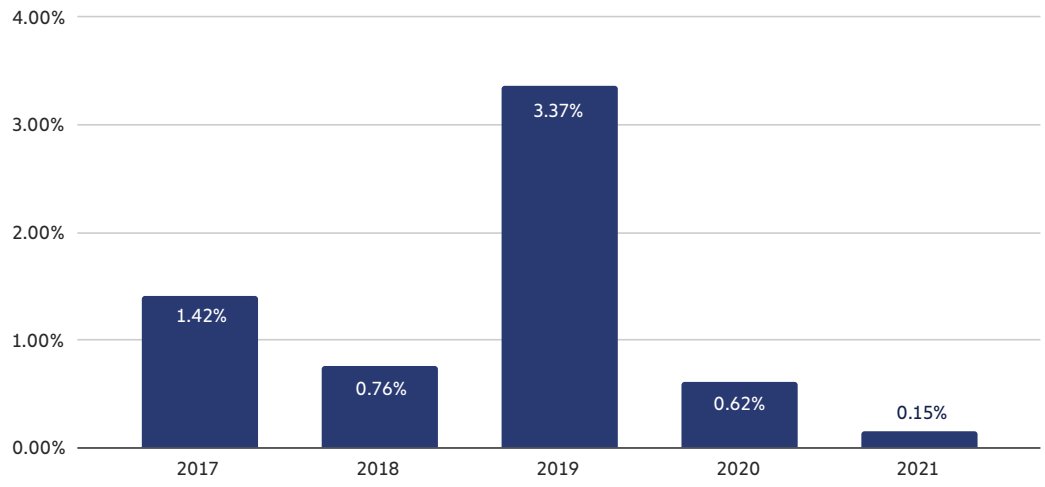
We're thrilled to be working with companies at the intersection of these three trends to build trust in blockchains, metaverses, and gaming. When these trends finally collide, it'll be a fascinating time to be extremely online.

Safety and Compliance

Theft, Money Laundering, and NFT Market Manipulation Underline Importance of Safety and Compliance in Web3

Any new technology that can offer benefits to the world at large likely also has the potential to be abused by bad actors for their own personal gain. Operators in the industry associated with that technology need to work to stamp out that abuse — sometimes with the help of the public sector — so that new users can feel safe adopting the technology and the industry continues to grow. If they do this successfully, we'd expect to see illicit usage of the new technology make up a smaller and smaller share of total usage over time. That positive progress is exactly what we've seen with cryptocurrency.

Illicit share of all cryptocurrency transaction volume, 2017 - 2021

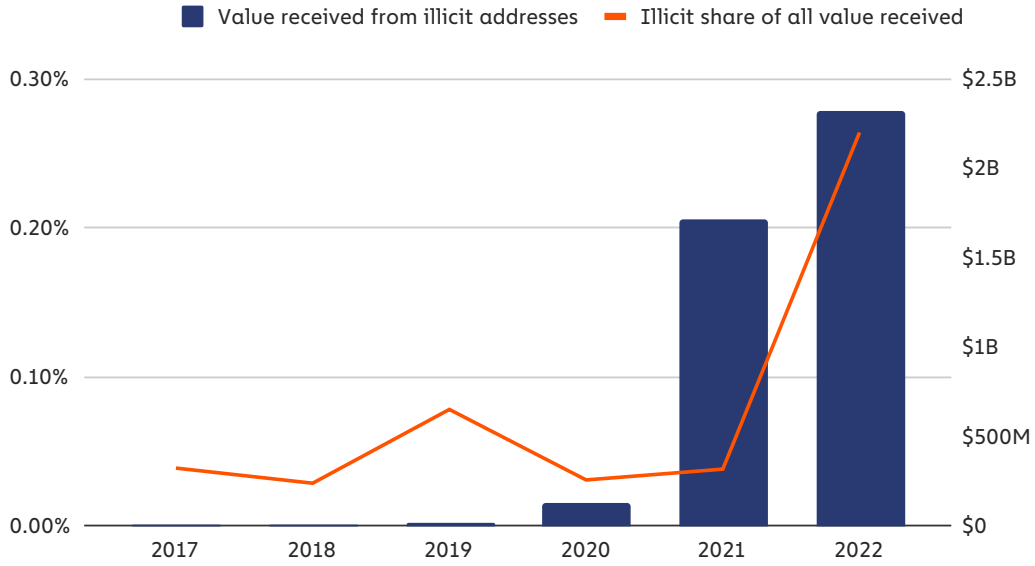


Note: 2019 has an unusually high share of illicit activity largely due to the PlusToken Ponzi scheme

While cryptocurrency-based crime remains an important problem to solve, especially given that rising overall transaction volumes mean the raw value of illicit transactions is still growing, illicit activity has become a less prominent part of the overall cryptocurrency ecosystem over the last three years.

However, DeFi specifically appears to be going through the same growing pains that cryptocurrency as a whole was previously, with illicit activity rising over the last two years.

Total value received by DeFi from illicit addresses vs. illicit share of all value received by DeFi

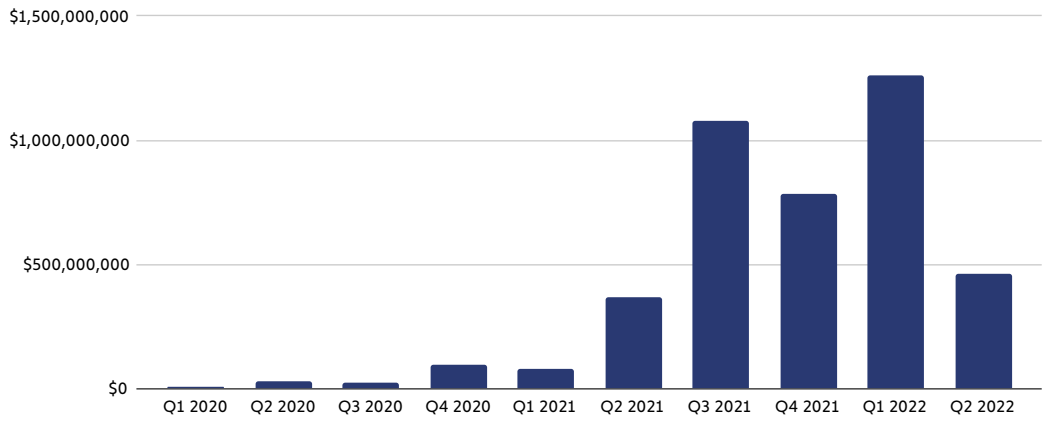


Illicit DeFi transactions have risen steadily over the last three years, in terms of both raw value and also as a share of all transaction value. We see this primarily in two areas: Theft of funds through hacking, and abuse of DeFi protocols for money laundering. Let's look at both in more detail below.

DeFi protocols are the go-to hacking target

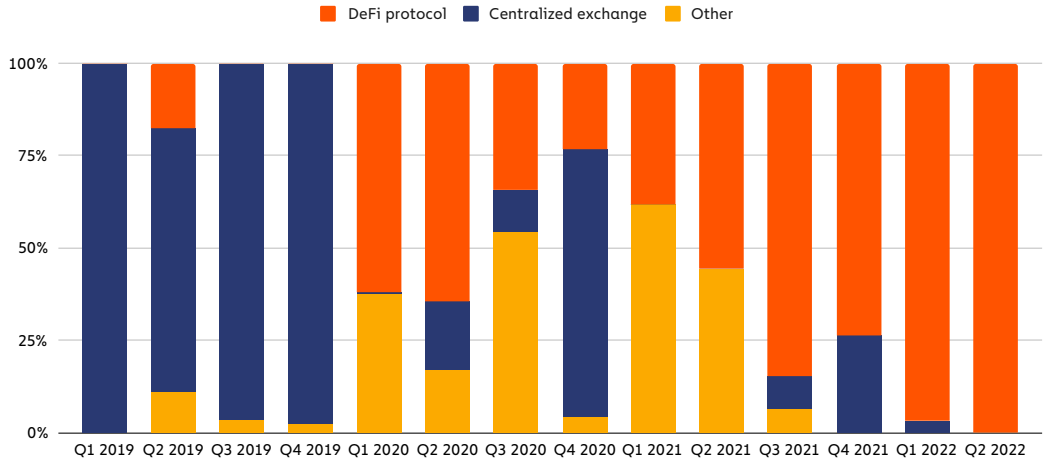
The value stolen from DeFi protocols has been trending up since the beginning of 2021, reaching its highest ever levels in Q1 2022, driven by hacks of the Ronin Bridge and Wormhole Network.

Quarterly cryptocurrency value stolen from DeFi protocols, Q1 2020–Q2 2022



In fact, over the course of 2021, DeFi protocols became the go-to target for hackers looking to steal cryptocurrency.

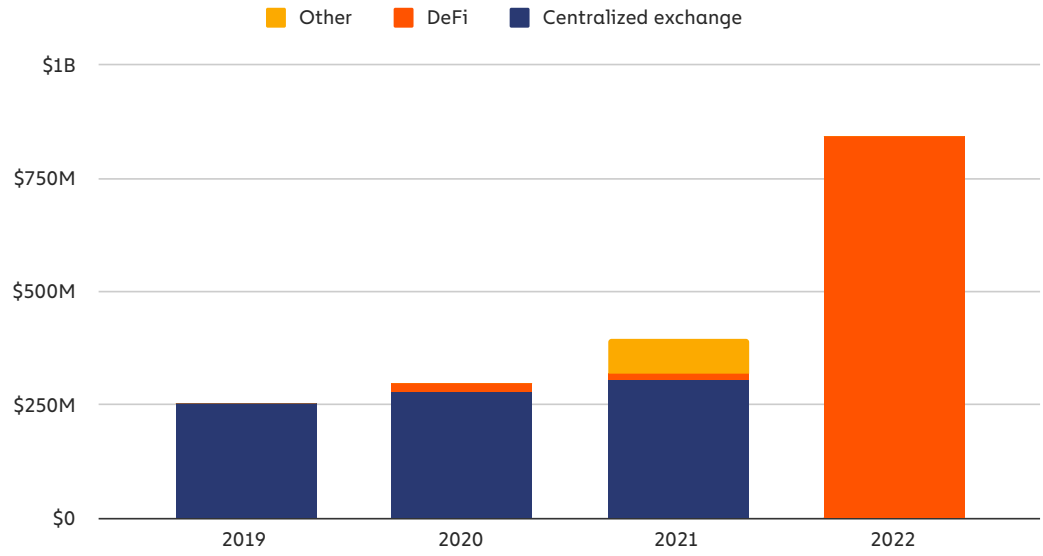
Cryptocurrency value stolen by victim platform type, Q1 2019–Q2 2022



DeFi protocols have accounted for an ever-growing share of all funds stolen from cryptocurrency platforms since the beginning of 2020, and lost the vast majority of stolen funds in 2021. As of May 1, DeFi protocols account for 97% of the $1.68 billion worth of cryptocurrency stolen in 2022.

Even worse, much of the cryptocurrency stolen from DeFi protocols has gone to hacking groups associated with the North Korean government, especially in 2022.

Cryptocurrency value stolen by North Korea-affiliated hackers by victim platform type, 2019–2022 YTD

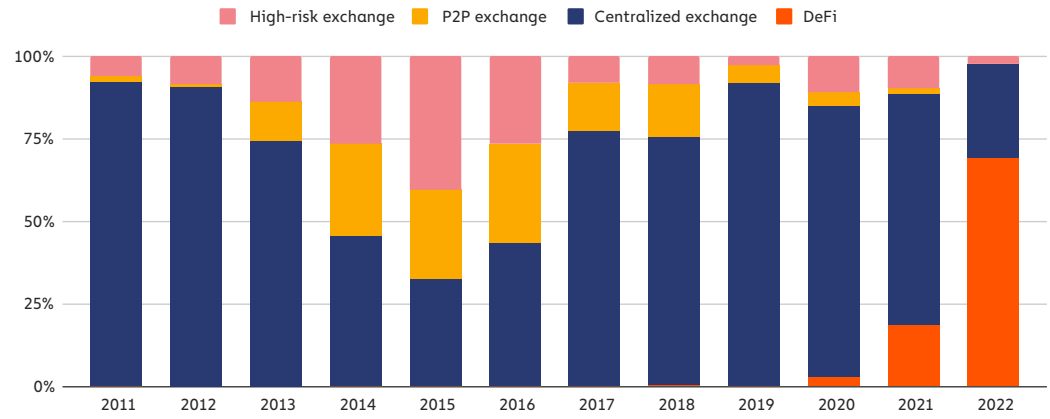


Already in 2022, North Korean hackers have had their biggest year yet for cryptocurrency theft at over $840 million, based entirely on hacks of DeFi protocols (it's possible that North Korean hackers are responsible for other hacks, both of DeFi protocols and centralized services, that have yet to be attributed to them definitively). The data goes to show that shoring up DeFi protocols' defenses against hackers isn't just a matter of building trust with users so that DeFi can continue to grow. It's also a matter of international security given that cryptocurrency stolen by North Korean hacking groups is used to support the country's development of weapons of mass destruction. The U.S. government is taking action, and most recently sanctioned a mixer for the first time given its role in laundering funds for DPRK-linked attackers.

DeFi-based money laundering on the rise too

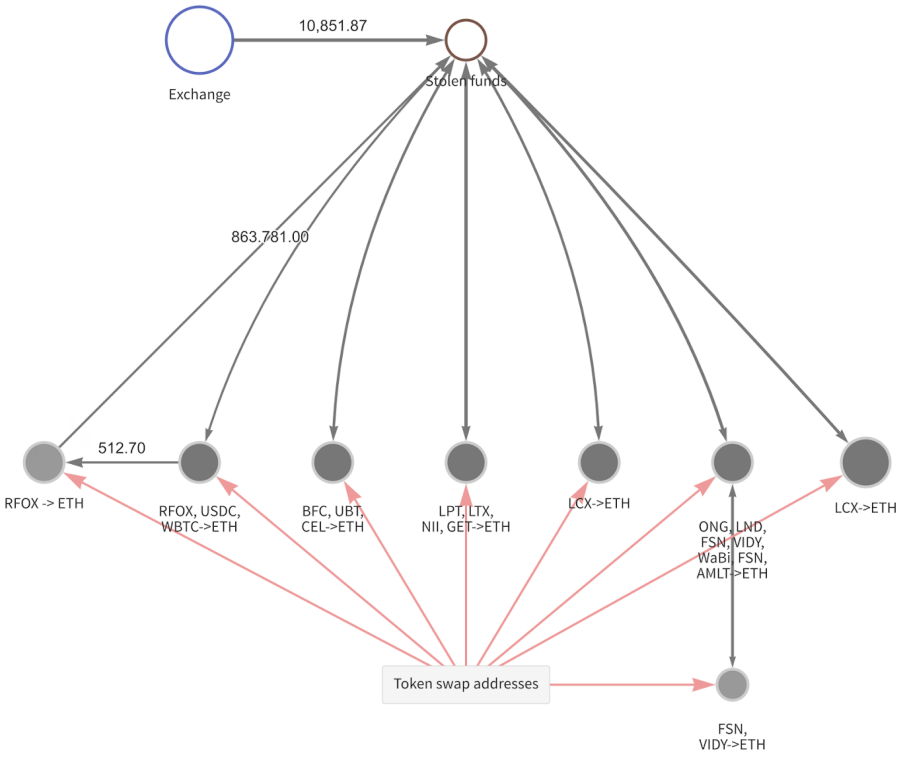
Money laundering is another serious issue, as DeFi protocols represent a bigger and bigger share of all funds sent from illicit addresses to services over the last two years.

Cryptocurrency service types by share of all illicit funds received, 2011–2022 YTD



So far in 2022, DeFi protocols have become the biggest recipient of illicit funds, taking in 69% of all funds sent from addresses associated with criminal activity, compared to 19% in 2021. One reason for this is that DeFi protocols allow users to trade one type of cryptocurrency for another, which can make it more complicated to track the movement of funds — but unlike centralized services, many DeFi protocols provide this ability without taking KYC information from users, making them more attractive to criminals. Chainalysis recently added cross-chain investigations features to Reactor to address the added complexities of DeFi-enabled chain-hopping.

DeFi-based money laundering is another area where North Korean hackers are leading the way. We saw an example of this in 2021, when the infamous Lazarus Group used several DeFi protocols to launder funds after stealing more than $91 million worth of cryptocurrency from a centralized exchange.



The hackers initially stole a variety of ERC-20 tokens, then used various DeFi protocols to swap those tokens for Ethereum. The hackers went on to send that Ethereum to a mixer and swap it again using DeFi protocols, this time for Bitcoin, before moving that Bitcoin to several centralized exchanges to liquidate it and receive cash. This is just one example of how hackers can abuse DeFi protocols for money laundering.

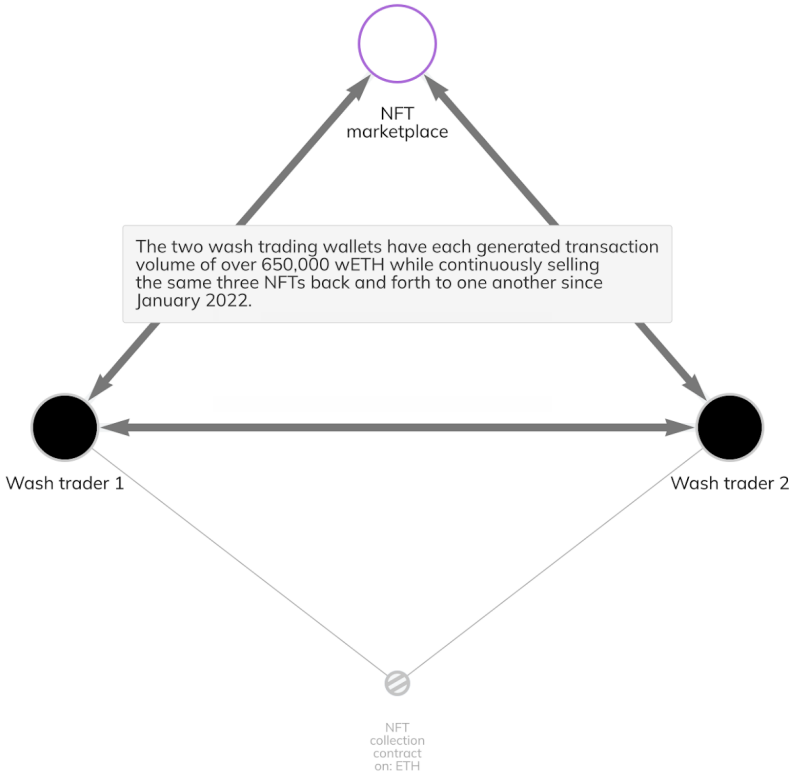
NFT wash trading lets users game the reward token system

In our 2022 Crypto Crime Report, we looked at examples of wash trading in the NFT market, and found that while most wash traders ended up losing money due to gas fees, the most successful ones turned large profits by artificially inflating their NFTs' values and offloading them to unsuspecting users. Now, we're going to look at another NFT wash trading scheme whose goals differ from conventional wash trading in one key way: Rather than inflating the value

of any particular NFT, the goal of this scheme seems to be collecting reward tokens given out by the NFT marketplace used by the wash traders.

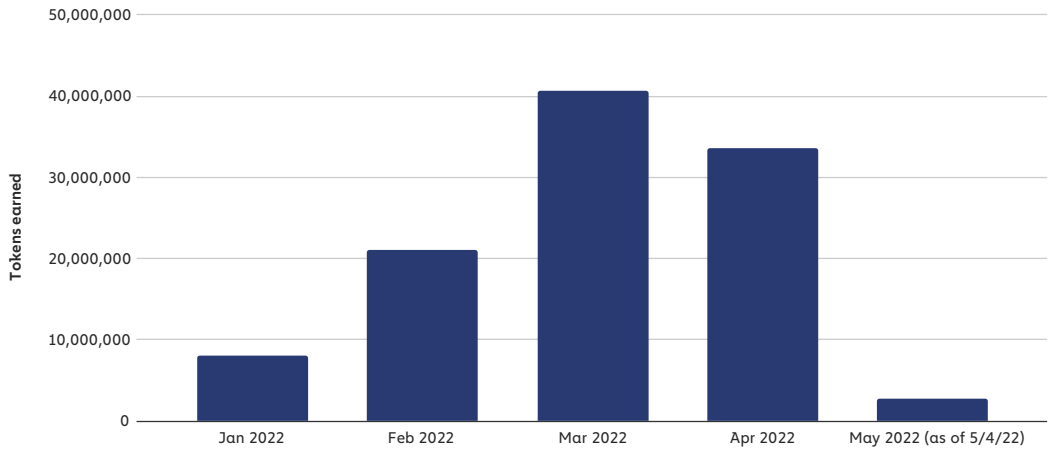
But before we dive in, we'll give a quick primer on wash trading. Wash trading is a form of market manipulation in which a seller is on both sides of a trade — in other words, selling an asset to themselves — in order to create a misleading perception of that asset's value or liquidity. Wash trading is relatively easy to do with NFTs, as some NFT trading platforms allow users to trade by simply connecting their wallet to the platform, with no need to identify themselves. One user could easily control multiple wallets and trade NFTs between them, and no one could know unless they took the time to analyze the wallets' transaction histories.

Now, on to our example. Below, we see two wallets, which we've labeled Wash Trader 1 and Wash Trader 2, that have generated over 650,000 wETH in transaction volume each while selling the same three NFTs back and forth to one another.



All of this activity has taken place on the same NFT marketplace. At no point has either wallet sold any of the NFTs to an outside party, so for the time being, it doesn't appear their goal is to rip off another NFT collector by selling them an artificially inflated asset. However, this particular marketplace offers incentive rewards in the form of its own native token to users whenever they buy, sell, or trade NFTs on the platform. The two wash trader wallets have generated huge amounts of the marketplace's rewards token through wash trading. Not only that, but the wallets have upped their earnings even more by staking their rewards tokens.

NFT marketplace rewards tokens earned by Wash Traders 1 and 2, Jan 2022–May 2022



All in all, between direct earnings from platform usage and staking, the two wash trading wallets have made over 106 million rewards tokens, currently worth over $185.5 million. Gas fees on the wash trades total just $114.6 million in gas fees, giving the wash trader(s) a profit of nearly $71 million. The wallets started with initial funding of 705.6 ETH, worth $2.4 million at the time of the first transfer, making this wash trading scheme a huge success.

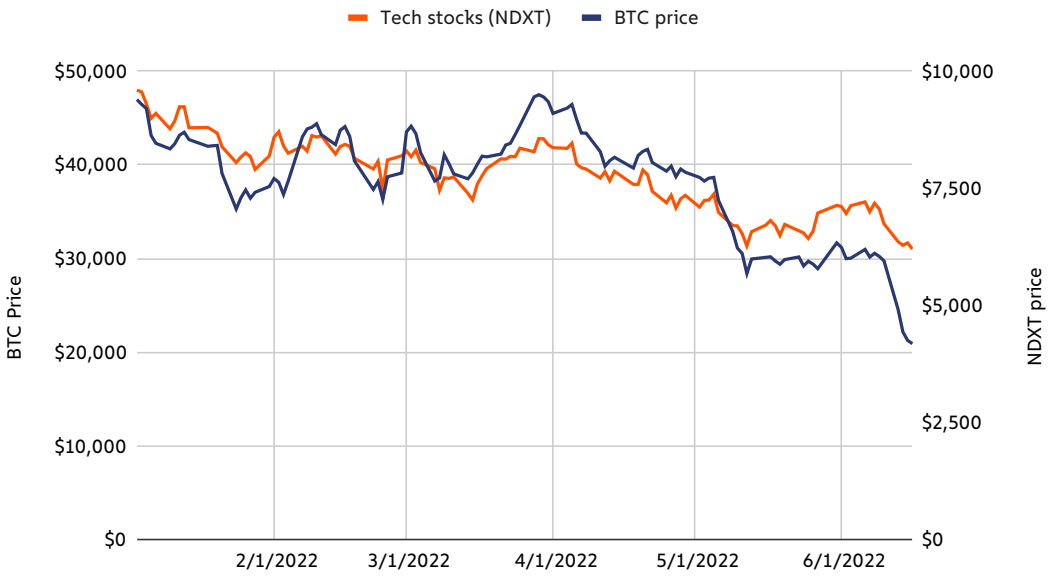
This type of wash trading scheme isn't victimless. For one, the NFT marketplace is being tricked into paying out rewards for phony activity. NFT collectors throughout the market are also potentially being tricked into thinking that this NFT marketplace has more transaction activity than it really does, and the same goes for the NFT collection the wash traders are using for their transactions.

Mitigating Financial Risk

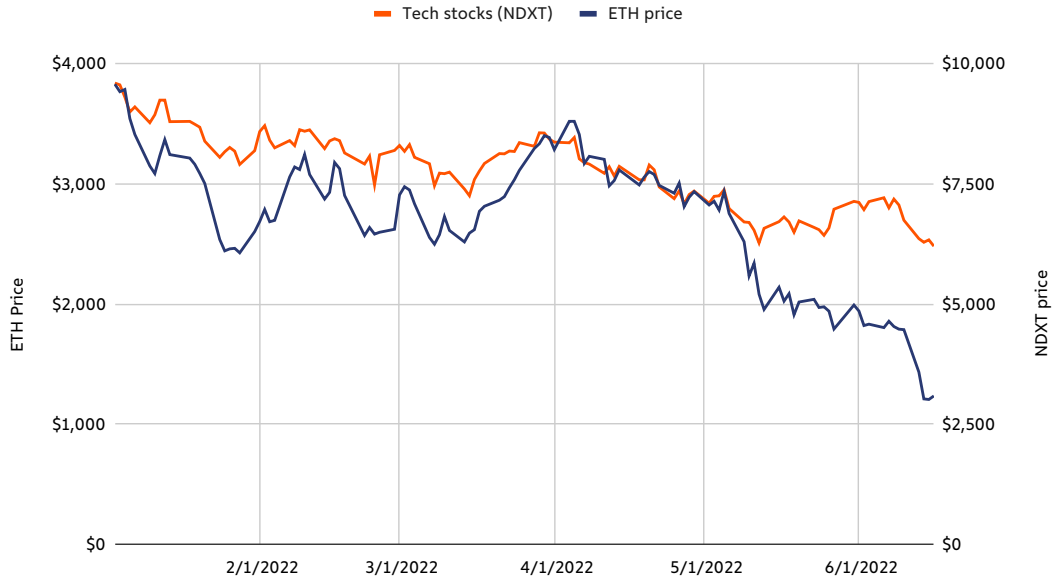
Risk in Web3: How the Crypto Industry Can Leverage Blockchains' Transparency to Understand and Prevent Market Contagion

As of June 2022, we're in a bear market across financial assets, and cryptocurrencies — especially Bitcoin, the most established cryptocurrency — are now more correlated to tech stocks than they were in the past. When the broader financial markets slump, crypto does too.

Bitcoin price vs. Tech stock prices, 2022 YTD



Ethereum price vs. Tech stock prices, 2022 YTD



This correlation reflects crypto's maturity as an asset class: there are a growing number of institutional players involved, new types of financial products are being offered, regulatory oversight is developing, and the market is more efficiently pricing in new information.

But there's one important difference between crypto and traditional finance: transparency. The market downturn has catalyzed mass liquidations of leveraged positions across both the traditional and crypto markets resulting in exacerbated price declines. In crypto, we are seeing this play out in real-time.

This is an opportunity for the industry to leverage blockchains' transparency to analyze systemic risk, build better systems, and design better rules for the next bull market. In this report, we'll break down what happened from a macro perspective as well as opportunities for regulators, lawmakers, and the industry overall to ensure the ecosystem can continue to grow safely and responsibly.

What happened: The bird's eye view

This isn't the first market crash in crypto. Here are a few of the greatest hits:

Daily Bitcoin price, February 2011–June 2022

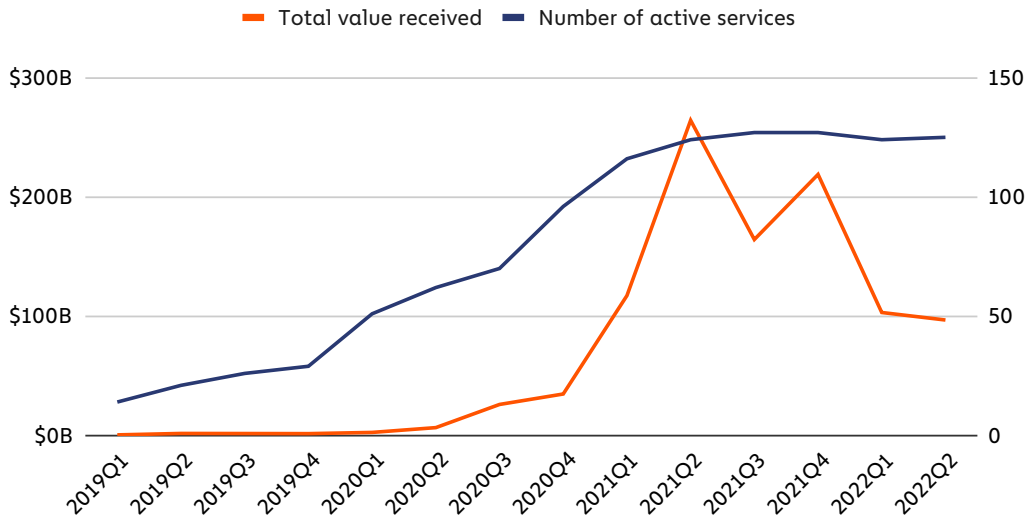
Only more recently have these downturns correlated with the broader markets. So why is the crypto market price crash more extreme than in the equity markets right now?

One major factor is that DeFi has gotten more competitive, driving some entities to execute on riskier investment strategies that can have ripple effects across the ecosystem.

How did we get here?

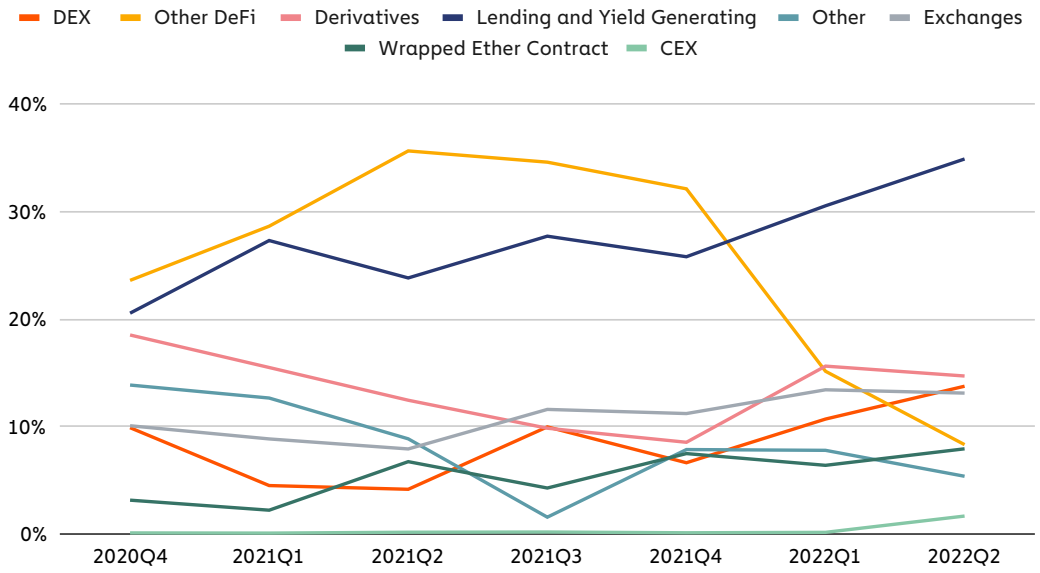
After the crypto crash of 2018, DeFi experienced explosive growth. As that growth slowed, the number of active DeFi services continued to accelerate, even as the value invested in DeFi started to drop.

Number of lending and yield generating services and total value recieved, Q1 2019–Q2 2022



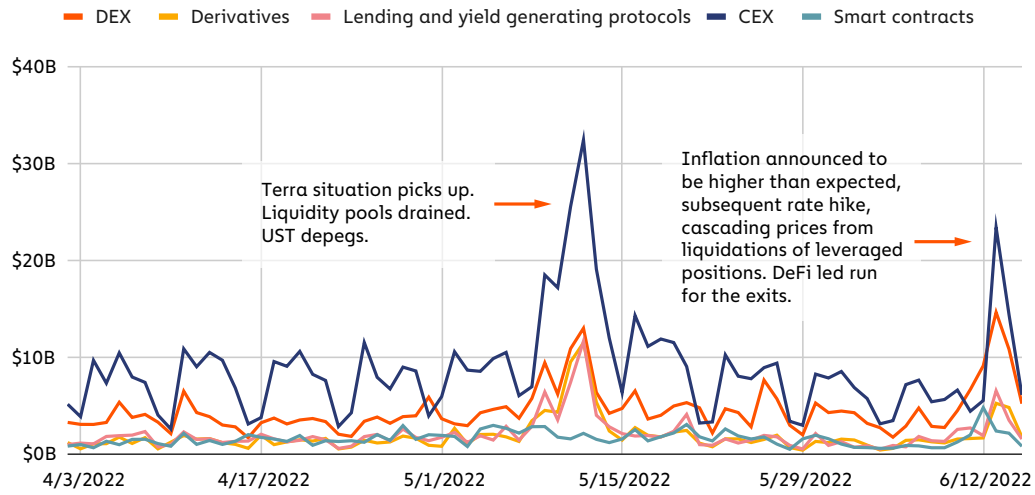
It appears that with more competitors chasing fewer investor dollars, lending platforms — which act as centralized entities — had to promise higher and higher yields to continue their growth. This led them to actively put user funds into riskier investments. For instance, as we see below, lending protocols' biggest source of funds became other lending and yield-generating protocols in Q1 2022. So, when asset prices began to drop, the effects cascaded throughout the DeFi ecosystem.

Receiving exposure of lending contracts, Q4 2020–Q2 2022



Given the broader bear market and other events including the UST collapse, net inflows to services have recently shifted. Most DeFi and exchange services suddenly saw huge inflows of cryptocurrency as people cashed out their funds or needed to pay back loans or avoid liquidations.

Daily cryptocurrency inflows to services, April 2022–June 2022



Our data shows that large institutions — identified as addresses that have received more than $1 million so far this month — are primarily behind these deposits, which is consistent with normal activity over time.

Opportunities for a safer ecosystem: Understanding systemic risks

Crypto's inherent transparency — especially during the current down market — is bringing some of the inherent risks of DeFi into the spotlight. Some projects that were hastily built or services that didn't properly manage risk will fail, and that's a natural process for any new technology or industry.

This is crypto's advantage. Due to the open nature of DeFi protocols, the market can often see where large, well-known players placed their bets and if those positions are facing liquidation. Furthermore, market participants can use this transparency to assess the stability of the core protocols that power the DeFi ecosystem.

However, this transparency has not stopped large, centralized companies from making bets on the price of various cryptocurrencies, both using open DeFi protocols and by lending funds to one another. This creates potential contagion risk, as various centralized market participants are financially exposed to one another. While DeFi protocols continue to function as designed at a technical level, some highly leveraged businesses have

struggled to unwind complex financial positions in a hostile macroeconomic environment.

Recent events demonstrate that it is important for regulators and the industry more broadly to understand both the decentralized and centralized parts of the cryptocurrency market and how they may impact each other. For example, centralized players investing in decentralized finance may find themselves over-leveraged if they have not appropriately calculated the risks, in particular in a bear market. The decentralized projects in which centralized entities have invested may also fall victim to code exploits or hacks and lose their value precipitously; this nearly played out earlier this year with the Wormhole exploit. Being able to adequately oversee centralized players will require understanding the entire ecosystem.

Mitigating Financial Risk

Case Study: Terra’s Collaspe

The Trades That Triggered UST's Collapse

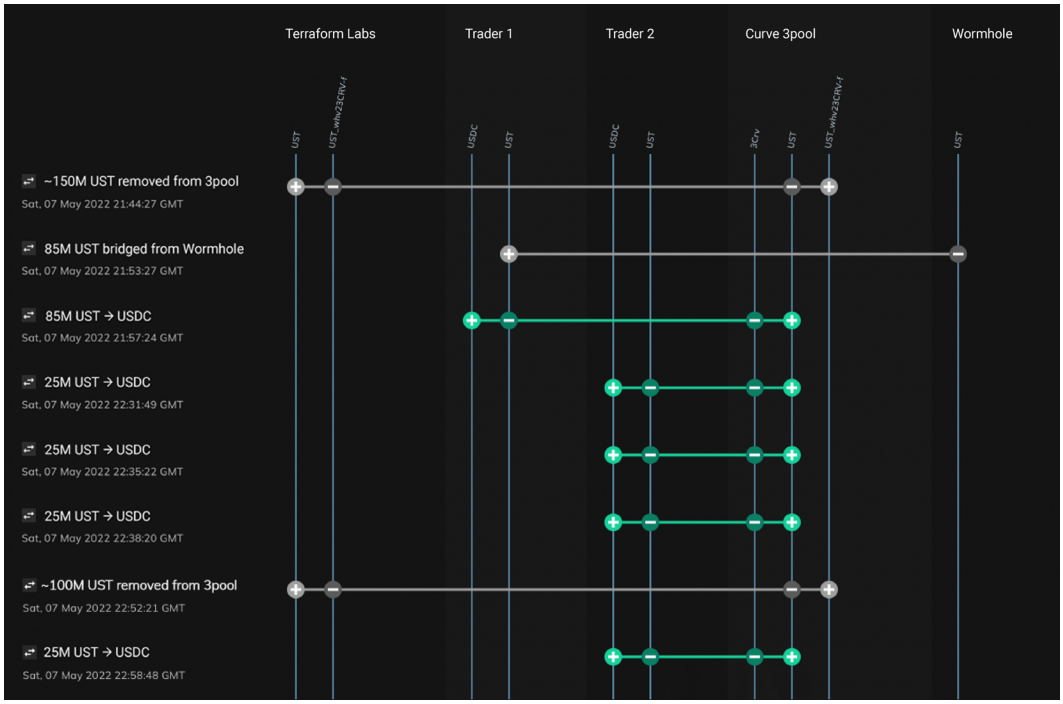
The 2022 crypto market downturn began with the collapse of the Terra-Luna ecosystem and its associated stablecoin, TerraUSD (UST). This single event is estimated to have erased as much as $60 billion in market value overnight.

In this section, we use blockchain analysis to explain how five trades from just two traders:

1. broke the stablecoin's peg,
2. drained its creator's reserves, and
3. led to the collapse of two tokens: LUNA and UST.

The three stages of UST's collapse

1. Two traders break UST's peg



The peg-breaking trades (green) visualized in Chainalysis Storyline, our new, web3-native blockchain analysis tool.

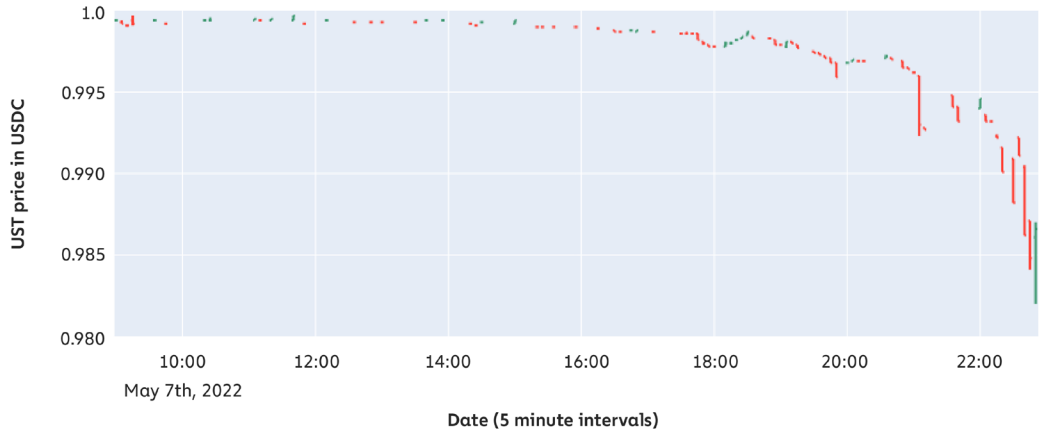
On the night of May 7th, Terraform Labs withdrew 150 million UST from 3pool, a decentralized stablecoin exchange, as part of a planned, public effort to move these funds to another pool. This made the pool more "shallow," i.e. prone to volatility.

Thirteen minutes later, one trader – perhaps taking advantage of this vulnerability – swapped 85 million UST for USDC. Over the next hour, another trader then swapped a total of 100 million UST for USDC in increments of 25 million.

In response, Terraform Labs withdrew another 100 million UST from 3pool. This was intended to "rebalance" the ratio of UST to other stablecoins.

But by this time, these large trades – and the many smaller ones that followed – had broken UST's peg.

UST-USDC prices on May 7th, 9:00 AM–10:50 PM UTC



Source: TradingView

Investors panicked, the sell-off began, and many holders with UST deposited in Anchor started to withdraw their funds.

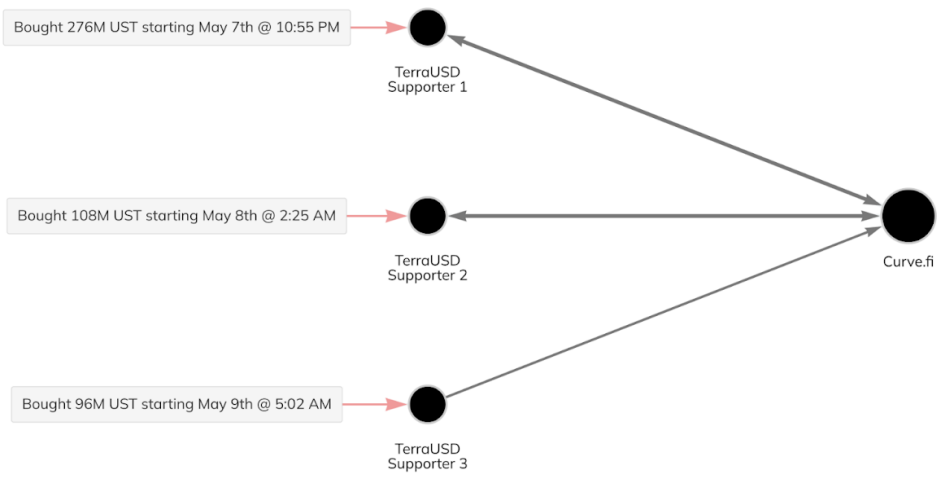
A note on Anchor

Anchor is a DeFi protocol operated by Terraform Labs, the creators of UST. For most of its existence it has paid 19.5% APY on any quantity of deposited UST. It has then lended these deposits at APRs that typically vary from 2% to 15%. Only about one half to one sixth of the deposited UST has been lent out to borrowers at any given time.

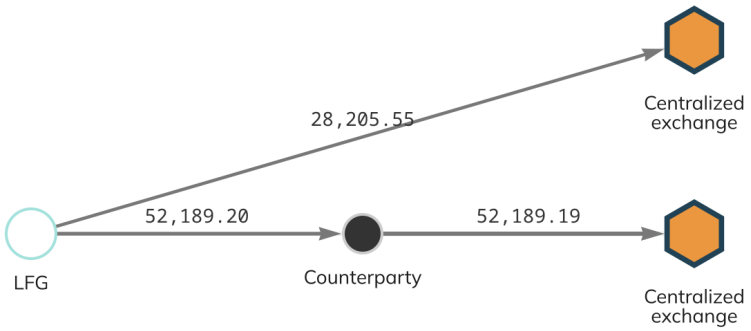
On March 13th, Bybit estimated that "at the current yield reserve of $24.7M UST and current ratio of deposits and borrowings … [Anchor has] a runway of about ~13 days before yield reserves have completely depleted." In mid-April, Decrypt reported that more than 72% of all UST was deposited in Anchor – indicating that a significant reason for holding UST may have been to earn Anchor's yields.

2. Repairs of the peg are successful but short-lived

To repair the peg and rebalance 3pool, three unidentified UST supporters swapped a combined $480 million Tether (USDT) for UST on May 7th, 8th, and 9th.

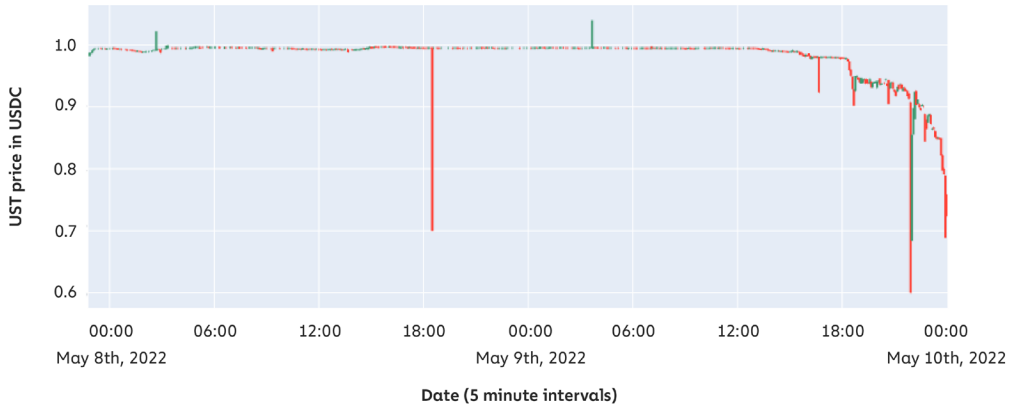


Then, on May 9th, the Luna Foundation Guard (LFG) sold billions worth of Bitcoin from its reserves to swap for UST.



But by May 10th, LFG's reserves were depleted and UST had again lost its peg – this time for good.

UST-USDC prices on May 7th, 10:50 PM–May 10th, 00:00 AM UTC



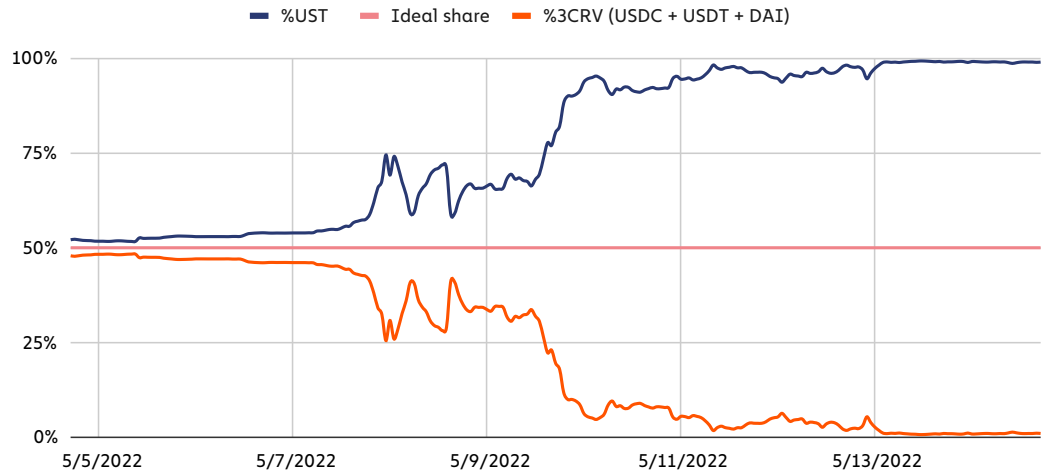
Source: TradingView

In a last ditch effort to stop the sell-off, multiple exchanges suspended withdrawals.

3. The mass minting of LUNA leads to hyperinflation and crash

Meanwhile, UST's largest liquidity pool was drying up. 3pool's balance of UST to 3CRV – a "basket" of stablecoins that includes USDC, USDT, and DAI – was fast approaching 95% to 5%, far from the 50% to 50% ideal.

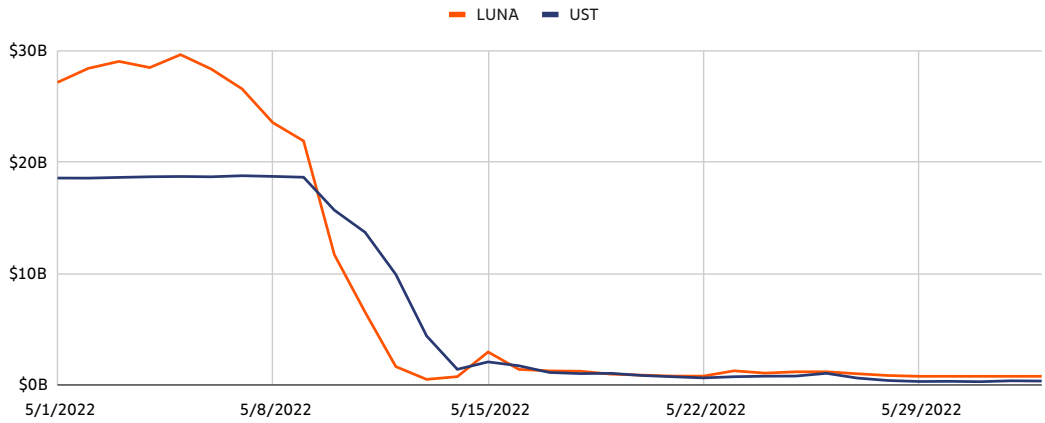
UST-3pool balance, 5/4/2022–5/14/2022



Only a single value-preserving exit remained. Per the stablecoin's algorithm, a UST holder could always "burn" one UST to "mint" one dollar worth of LUNA, no matter the price of LUNA.

And so holders burned their UST en masse, hyperinflating LUNA. Its supply entered the trillions; its price fell to fractions of a cent. When LUNA's market cap dipped below UST's, it became clear that not everyone could burn UST wfor equal value.

UST vs. LUNA market cap, 5/1/2022–6/2/2022



The remaining holders sold at lower and lower prices until UST was worth little more than a penny. The algorithmic stablecoin had collapsed.

UST-USDC prices on May 10th, 00:00 AM–June 2nd UTC

Source: TradingView

Undercollateralized, overcollateralized, and fiat-backed stablecoins

Unlike most stablecoins, UST was algorithmic and undercollateralized. Rather than maintaining its peg by holding assets in reserves, Terraform Labs used a sister token, LUNA, to "absorb the price volatility of UST."

Other stablecoins are crypto-backed and overcollateralized, like DAI. Borrowers must deposit $1.50 worth of ETH for every DAI they wish to borrow. Still others are fiat-backed and collateralized one-to-one, like USDC. Its reserves are held in cash and short-dated government treasuries.

Stablecoins vary in their utility as well. Both the algorithmic UST and the crypto-backed DAI serve DeFi, but fiat-backed stablecoins have other use-cases. They can help exchanges settle trades, migrants send remittances, and citizens of high-inflation countries store value. Tether recently launched a peso-backed stablecoin to facilitate remittances to and from Mexico, for example, and stablecoins are quite popular among inflation-weary Argentines.

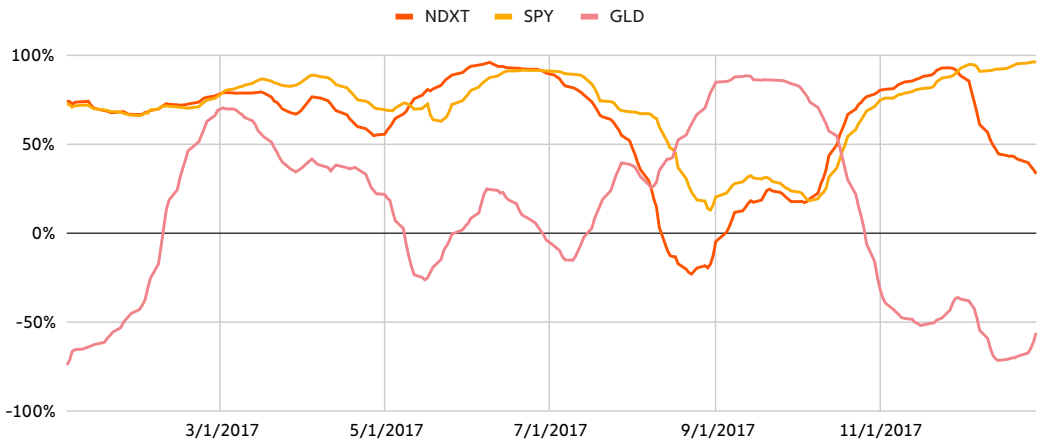
What were the macroeconomic impacts of the collapse?

UST and LUNA's collapse didn't happen in a vacuum. At the same time, several other crypto assets, including Bitcoin, also declined in what some have said may be the beginning of a third crypto winter.

But was the UST's collapse to blame for that decline? While it was definitely a factor, we find that because Bitcoin's decline was so closely aligned with the downturn of non-crypto assets — especially tech stocks — its price action may have been more connected to the tech slump than UST's crash.

Bitcoin's correlation with tech stocks is a relatively new development. The graph below shows the correlation between Bitcoin's price and that of several other asset classes in 2017.

Bitcoin correlations with NDXT, SPY and GLD in 2017

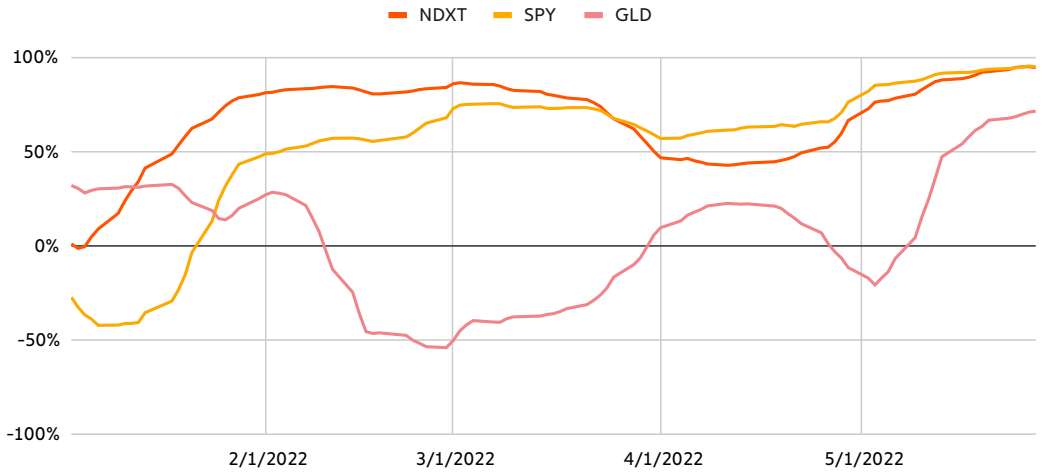


NDXT: NASDAQ-100 Technology Sector
SPY: SPDR S&P 500 ETF Trust
GLD: SPDR Gold Shares

While there were "waves" of correlation, that is typical of assets with no significant relationship. This pattern bolstered the narrative that Bitcoin was uncorrelated and therefore a safe haven during market declines.

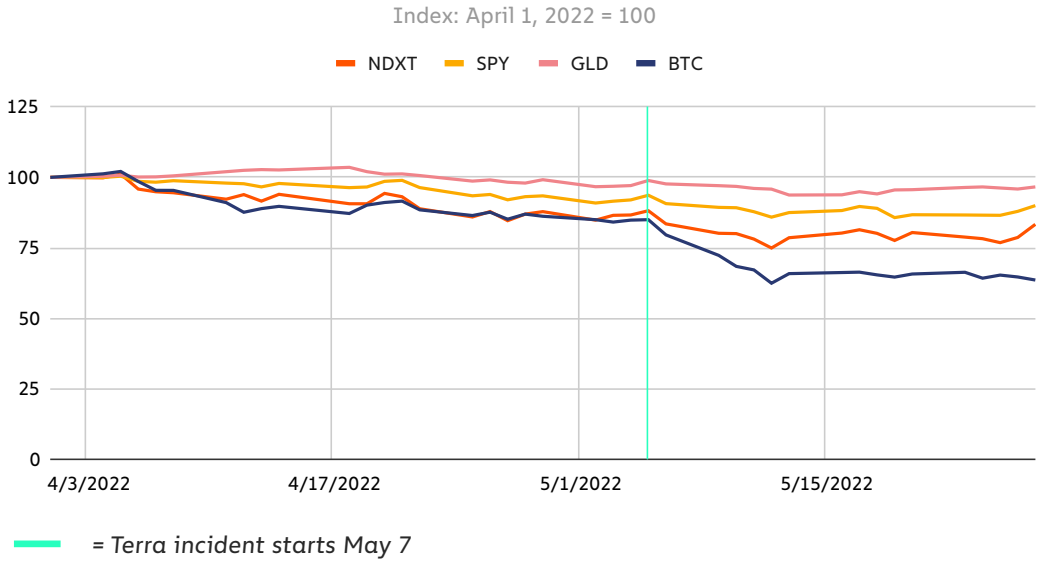
That narrative has become less tenable in 2022. Today, Bitcoin appears to move in concert with those assets.

Bitcoin correlations with NDXT, SPY and GLD in 2022



Bitcoin has maintained significant price correlations with NDXT and SPY this year while remaining entirely uncorrelated with GLD. So, when NDXT and SPY began to fall, Bitcoin followed suit.

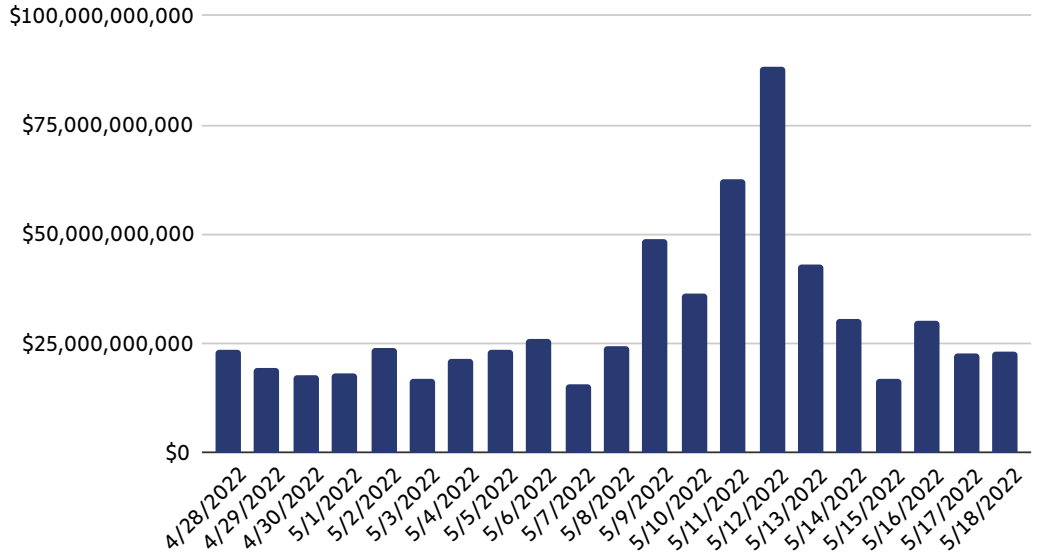
Indexed price growth of Bitcoin and select stocks, 4/1/22–5/27/22



For a few days, however, the collapse of UST may have accelerated Bitcoin's decline. This was expected — LFG sold billions worth of Bitcoin to repair the peg — but also short-lived. The accelerated decline ended around May 13 at roughly the close of UST's collapse, at which point Bitcoin's price action fell back in line with non-crypto tech assets.

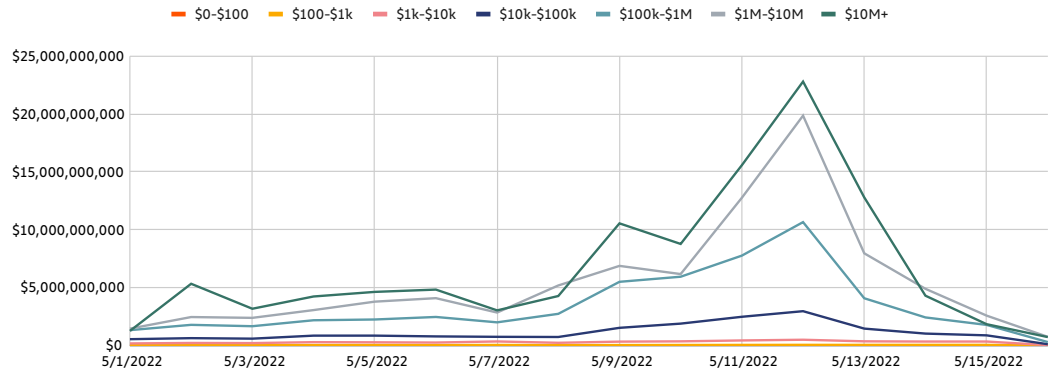
We also observed a spike in stablecoin sales during UST's collapse. From May 9th to 12th, hundreds of billions more stablecoins than usual were sold for cash.

Daily stablecoin volume on services, 4/28/2022–5/18/2022



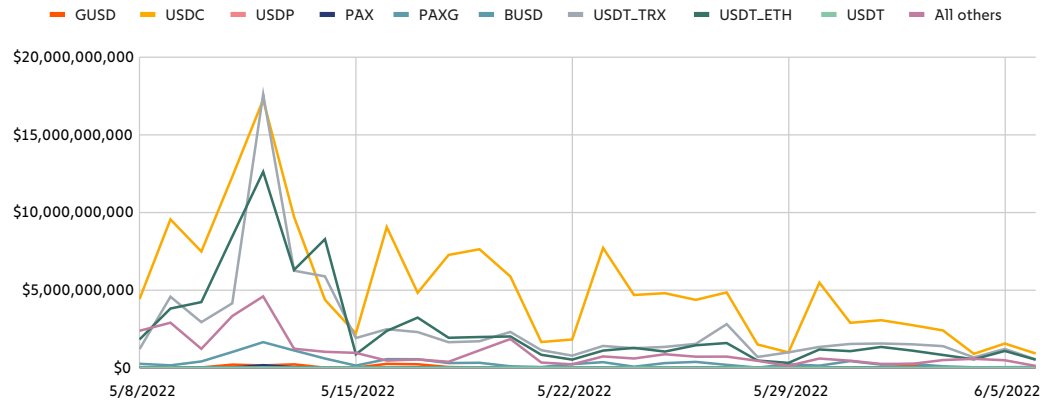
All kinds of investors sold their stablecoins during the crash, from big, institutional players to retail investors.

Daily stablecoin value transferred to services by transaction size, 5/1/22–5/16/22



Redemptions peaked across all stablecoins — algorithmic and asset-backed. This suggests that the collapse scared many investors away from stablecoins altogether, not just those of a certain class.

Daily stablecoin value transferred to services by stablecoin type, 5/8/22–6/6/22



Nonetheless, major stablecoins weathered the storm. Though Tether briefly fell by 3¢ on May 12, it quickly rebounded and was able to process over $13 billion in USDT redemptions over a week-long stretch.

Conclusion

UST's collapse may pose a threat to consumer confidence in the short term and serve as a legislative catalyst in the long term, but it's unlikely to stop the growth of responsible innovation in the industry. Fortunately, thanks to blockchains' transparency, we can learn from these incidents, educate others, and continue to build trust in cryptocurrency.

Chainalysis

Thanks for reading the State of Web3 Report

Chainalysis Authors

Kim Grauer
Director of Research

Will Kueshner
Content Marketer

Ethan McMahon
Economist

Henry Updegrave
Senior Content Marketing Manager

Chainalysis

Complete visibility into cryptocurrency

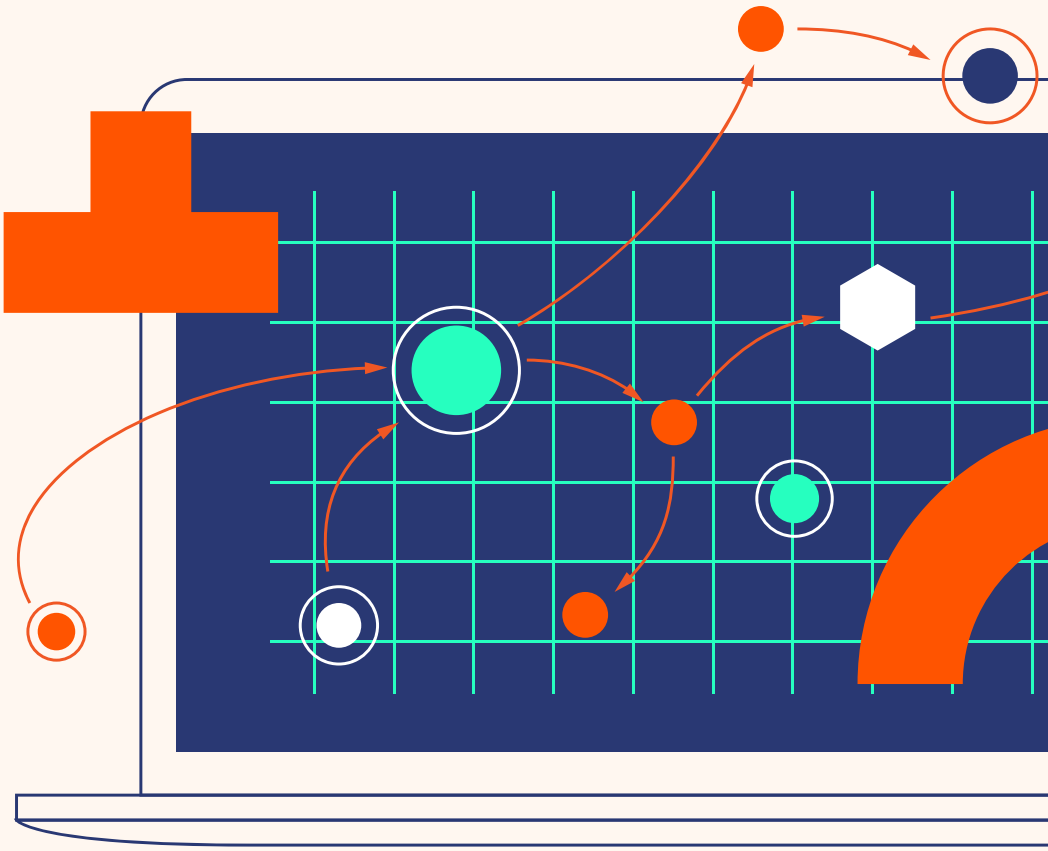
Compliance
Ensure you meet evolving local and global regulations

Investigations
Detect and investigate crypto crime

Defi
Safely participate in the DeFi revolutions

NFTs
Ensure safe access and controls for NFTs

Learn more about our solutions at www.chainalysis.com



Chainalysis

Building trust in blockchains

About Chainalysis

Chainalysis is the blockchain analysis company providing data and analysis to government agencies, exchanges, and financial institutions across 40 countries. Our investigation and compliance tools, education, and support create transparency across blockchains so our customers can engage confidently with cryptocurrency. Backed by Accel, Benchmark, and other leading names in venture capital, Chainalysis builds trust in blockchains. For more information, visit www.chainalysis.com.

GET IN TOUCH
info@chainalysis.com

FOR MORE CONTENT
blog.chainalysis.com

FOLLOW US ON TWITTER
@chainalysis

FOLLOW US ON LINKED IN
linkedin.com/company/chainalysis