The Scaling Report

Does the Future of Decentralized Finance Still Belong to Ethereum?

Cointelegraph Research

crypto research .report

Research Partners

arcana

brave

ANote Music

RADIX

fuse

CRYPTIX

CasperLabs

coinfinity

AMBIRE

bitpanda

CAKEDEFI

We thank our research partners for their support of this report.

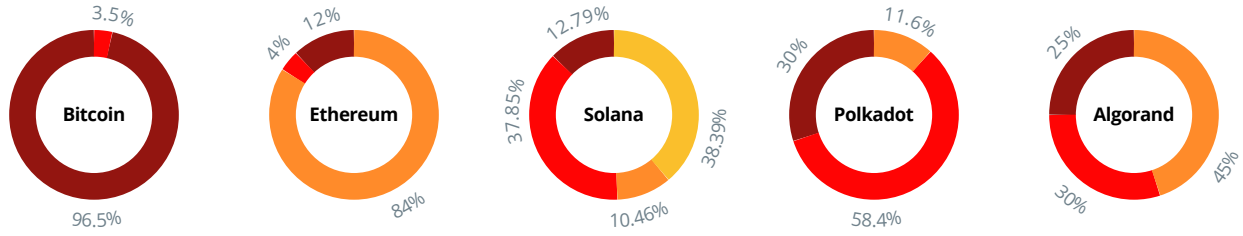
Key Takeaways

- Traditional Finance (TradFi) is starting to lose some ground to Decentralized Finance (DeFi). **DeFi has more than $250 billion in total value locked and is only increasing in size and popularity**.
- Bitcoin is the mother of all blockchain cryptocurrencies. Due to the limits of Bitcoin's code, it requires layer-two solutions to provide DeFi. This **opens the door for layer-one protocols, including Ethereum, Solana, Polkadot, and Algorand, to fight for the top spot in DeFi**.
- Ethereum is the market leader in non-fungible tokens, DeFi, and overall adoption rate. Some of **Ethereum's drawbacks include low transactions per second (TPS), high transaction costs, and delayed protocol updates. These issues allow other blockchains to potentially take away Ethereum's market dominance in the future**.
- Solana is a leading competitor to Ethereum. **High reported TPS speeds, low transaction costs, and expanding ecosystem** have helped Solana shoot up the ranks into a top-ten coin in 2021. The network has had a few issues in the past and is still considered in beta.
- Polkadot has the competitive advantage of being focused on interoperability and being a multi-chain ecosystem. This allows Polkadot to attract a large community which is helping to push growth. **Polkadot is still not live and functioning as a fully developed blockchain**, with its parachain auctions still well underway. By attracting developers, investment, community, and human capital, Polkadot is a project to keep an eye on.
- Algorand set out to answer the trilemma of security, decentralization, and scalability. Started by some of the leaders in cryptography, **Alogrand has low transaction costs, 1,000 TPS, and a growing rate of adoption**. Its growing ecosystem, connections with regulators, and long-term outlook make it a steady horse in the blockchain race.
- Radix is an up-and-coming layer-one purpose built for DeFi. Radix aims to challenge the status quo with a new asset-oriented paradigm that promises to make DeFi development safe and intuitive; and a **unique approach to consensus that scales linearly while preserving atomic composability** between shards.
- Ethereum has gone through many improvements in 2021, including EIP 1559, which changed its inflation rate. Ethereum's biggest change is proposed to be from ETH 1.0 to ETH 2.0, which has been pushed back to sometime in 2022. **If ETH 2.0 is delayed or has a problem deploying correctly, it could be the event that opens the door for blockchains in this report to rise even further in popularity**.
- DeFi, NFTs, and digital assets continue to increase in worldwide adoption. While Ethereum is currently still at the head of the pack when it comes to these categories, it is **important for investors to keep an eye on all risk factors and potential impacts in the short, medium, and long term**.

Table 1 Top Blockchains for Global Decentralized Finance Market

Cointelegraph Research

Metric	Bitcoin	Ethereum	Solana	Polkadot	Algorand
Market Cap	$1tn	$446bn	$68bn	$42bn	$10.2bn
Unique Active Addresses	950k active	520,000	1m	27,134	64,300
Total Value Locked in DeFi	$1.6bn (DFI)	$156bn	$11.2bn	$2.5bn	$100mln
Average Transaction Fee	$1	$28	$0.00025	$3.8	$0.0015
Actual TPS	2.5	13	2,300	166.6	1,200
Theoretical TPS	7	35	65,000	1,000,000	3,000
Time to Finality	30 min – 6 days	42–90 sec	21–46 sec	12–60 sec	4.4 sec
Protocol Revenue	$450m tx fees. $14bn mined (328k BTC)	$2.2bn tx fees $19bn block rewards	2.2m	7mln (annualized)	$498mln
P/S Ratio	70x when considering block rewards. 2,200x without.	22.2x w/block rewards 215x w/out	30,909x	4,715.76x	22.2x
Staking Returns	8% or less	5–7%	8.20%	14.60%	4–6%
NFT Sales Volume	N/A	$1.7bn (Oct 21)	$246bn (Oct 21)	N/A	N/A
NFT Transaction Volume	N/A	1.08m (Oct 21)	230m tx (Oct 21)	N/A	N/A
Initial Coin Distribution Breakdown (how much the team holds, early investors, public holders)	Estimates are that the creator(s) of Bitcoin mined 700k Bitcoin. This would be approximately 3.5% of the entire Bitcoin supply. None of the 700K Bitcoin have been transferred from their original wallet so far.	12% Team 4% Foundation and Grants 84% Community	12.79% Team 37.85% VC Sales 10.46% Foundation 38.39% Community	30% Team 58.4% VC sales 11.6% Community	25% Team 30% VC sales 45% Community



** Calculated on average of October 2021*

Authors

Raphael Spannochi

Raphael Spannocchi is a research analyst at Cointelegraph Research. He got into Bitcoin mining in 2013 and wrote white papers for Bitcoin Clean and Circle.one in 2017.

Alexander Valentin

After finishing his B.Sc. in Economics at the University of Mannheim, Alexander enrolled in the Ph.D. program in Economics at Goethe University in Frankfurt receiving his M.Sc. degree in 2018.

Demelza Hays, Ph.D.

Demelza Hays is the director of research at Cointelegraph, and formerly was a Forbes 30 Under 30, U.S. Department of State Fulbright Scholar, and fund manager of two regulated crypto funds.

Nikita Malkin

3+ years of working experience in crypto sphere and finance. Higher School of Economics graduate with diploma work related to digital asset market. Co-author of Security Token Report and research analyst at Cointelegraph Research.

Igor Kravchenko

Igor Kravchenko is a research analyst at Cointelegraph. He is currently pursuing a master's degree in quantitative finance at the Vienna University of Economics and Finance.

Vladimir Shapovalov

A Chemical Engineering graduate from the University of Cambridge with previous experiences in London brokerage services firm and British brain cancer treatment startup.

Ron Mendoza

Ron has worked in business development for several investment firms in Dubai and Abu Dhabi for more than six years. He has also covered cryptocurrency, blockchain, and fintech topics for several publications since 2019.

Michael Tabone

Michael Tabone is an economist at Cointelegraph Research. A Ph.D candidate, engineer, economist, and business strategist, he also provides strategic consulting to firms concentrating in the DeFi and blockchain space.

Helen Rosenberg

Helen Rosenberg is a research analyst at Cointelegraph, holds a bachelors' degree in economics and finance and has co-authored three reports at Cointelegraph Research.

Bryan O' Shea

Bryan O' Shea is a research writer at Cointelegraph. He holds a bachelor's degree in political science, and co-founded the Emerald Foundation, a free-market think tank in Ireland.

Dear Partners, Investors and Friends,

Bitcoin is the reason all other modern cryptocurrencies exist. Bitcoin utilizes decades of research in cryptography, computer technology, and information sciences. Bitcoin's evolutionary step was in 2009, and since then new generations of cryptocurrencies have spawned, looking to improve upon Bitcoin. Out of many that came after Bitcoin in the early days of crypto, one has stood the test of time and has risen to the number two cryptocurrency by market capitalization. That would be none other than Ethereum.

Ethereum went farther with its capabilities than Bitcoin, and the code was written in such a way that it made it easier to upgrade and change over time. Ethereum (ETH) allowed for the utilization of "smart contracts" or self-executing instructions based on computer code. This allowed Ethereum to create agreements between parties that did not have to form a bond of trust before interacting, because the code is impartial to either party. This allowed decentralized finance (DeFi) to explode.

DeFi allows individuals to trade digital assets quickly, efficiently, and in a way that is settled because of the actions of programmed code, not because of a centralized entity. This allows for borrowing, lending, trading, collateralization, and payments, none of which requires permission from an outside authority. This eventually culminated in the summer of 2020 and was called "DeFi Summer." There was a host of decentralized finance (DeFi) cryptocurrency projects which grew during that period, but none compared to the likes of Ethereum. Ethereum spawned into a vast ecosystem of asset management tools, decentralized exchanges (DEXs), asset tokenization, decentralized autonomous organizations (DAOs), stablecoins, insurance, and the list goes on.

Just like the evolution of Ethereum from Bitcoin, other chains have evolved as well. Ethereum, in its current state, has its drawbacks and opportunities for improvement. This is where other blockchains have stepped onto the stage. The likes of Solana, Polkadot, Algorand, and many others have begun to eat at the space Ethereum continues to carve out. Can Ethereum remain the "King of DeFi" in the coming years?

That is exactly the question this report seeks to answer. This report will explain why Bitcoin, while the mother of all cryptocurrencies, is not capable of DeFi at the levels of Ethereum. In addition, we will dive into some of the largest competitors in this space, such as Solana, Polkadot, and Algorand. By exploring each of these alternative Defi ecosystems in-depth, we can analyze each one's strengths, weaknesses, and how each one poses a potential threat to the throne of DeFi in the short, medium, and long term.

We hope you will enjoy the reading Cointelegraph and Crypto Research Report's analysis of how the blockchain technology is improving scalability and building the infrastructure required for the largest capital market in the world.

Cointelegraph Research helps blockchain companies communicate their cutting-edge research to the world by writing, designing, and publishing professional reports. We help companies gain wider audiences by developing educational materials in the form of in-depth reports. Our team of academics and seasoned blockchain technologists can cover a diverse range of topics, including tokenomics, macroeconomics, legal, tax, central bank digital currencies, decentralized finance, supply chain logistics, and venture capital.

To work with Cointelegraph Research's team on creating a one-of-a-kind report, contact us at research@cointelegraph.com.

Sincerely

Demelza Hays

Head of Research at Cointelegraph

Demelza Hays is the director of research at Cointelegraph, Forbes 30 Under 30, U.S. Department of State Fulbright Scholar, and former fund manager of two regulated crypto funds.

Content

Cointelegraph Research

Cointelegraph Research provides bespoke research reports and white-label content for organizations in the cryptocurrency industry. If your organization has a specific research question, our industry experts can find the solution. Our team's multidisciplinary knowledge of the blockchain technology and traditional finance world enable us to solve complex challenges. We leverage primary data sources to bring you actionable insights within the digital asset space.

We cover all the major sectors of the blockchain ecosystem, including layer-1 blockchains, Decentralized Finance (DeFi), mining, custody, non-fungible tokens (NFTs), private equity, and tokenomics.

Why Cointelegraph Research?

House of experts

Cointelegraph Research is led by industry veterans, technology analysts, and senior researchers that are up to date with the latest developments and analysis in the space.

Unparalleled approach

Cointelegraph Research's team strongly relies on a data-driven approach and trusted data sources. We uncover actionable opportunities for our clients by combining deep market structure analysis with years of consulting experience.

Tailor-made solutions

Cointelegraph Research's goal is to save you time. We will understand your unique business challenge and craft à la carte solutions to your questions.

Examples of Past Research Partners

coinfinity
bitpanda
Polkadex
Centrifuge
BITMAIN
BlockFi
bit.Country
ENJIN

Contact Us

research@cointelegraph.com

1 What Is Decentralized Finance?

One of the greatest applications of blockchain technology is in the realm of finance. As of this writing, the total value of all cryptocurrencies sits just below $2 trillion.[1] One of the reasons for the expanse in the market capitalization of cryptocurrencies is decentralized finance or DeFi.[2] DeFi continues to see a steady increase in users, and at the end of 2021, the total value locked (TVL) was more than $250 billion for all DeFi projects.[3] Capital is flowing into DeFi from not only retail but also institutional investors[4], and worldwide adoption of cryptocurrencies is only in its infancy.[5]

In the past, banks, investment services, insurance companies, and lenders would fall under the umbrella of finance for both the individual and businesses alike. Blockchain technology made it possible to provide the financial instruments which were offered by traditional finance (TradFi), which historically is characterized by centralized power, participation only by permission, high barriers to entry, and by "their rules."

Decentralized Finance (DeFi) turns TradFi on its head.

DeFi is permissionless — In Defi, there is no middle man that stands between two or more people to make an agreement. This gives power back to individuals over institutions holding the power. It does not require a credit score or personal information to be exchanged. Just participants in peer-to-peer (P2P) transactions, interacting over computer code in a "trustless" manner (meaning the code ensures the transaction occurs, not just trusting another person).

DeFi is a global phenomenon — decentralized exchanges (DEXs) operate 365 days a year, 24 hours a day. There is no institution that limits hours of operation, no government regulation, and no governance needed other than that of the participants themselves. There are no state borders in DeFi. This allows for people who would never have the chance to invest in a yield-bearing financial tool in the TradFi space the ability to better their lives.

DeFi has low barriers to entry — DeFi does not require users to have entire "coins" of a particular blockchain to participate. Each cryptocurrency coin can be broken into tiny fractions of a whole, up to eight or even more decimal places! This means that anyone can start acquiring and utilizing different DeFi tools to better their position.

DeFi gives power back to the individual, allowing them to control their funds 24 hours every day of the year. People can decide to store their funds in non-custodial wallets, meaning they alone hold the private keys to unlock the use of these funds.[6]

Investors should be looking to DeFi in two respects: utilizing the tools for better returns than in the TradFi space and for being invested in the underlying assets which make DeFi possible.

[1] Learn more about top-100 market capitalization coins here

[2] See "DeFi: A comprehensive guide to decentralized finance", *Cointelegraph*

[3] See "3 key metrics show DeFi's TVL on the verge of a new ATH", Jordan Finneseth, *Cointelegraph*, January 5, 2022

[4] See "Grayscale sets sights on institutional DeFi fund", Osato Avan-Nomayo, *Cointelegraph*, July 19, 2021

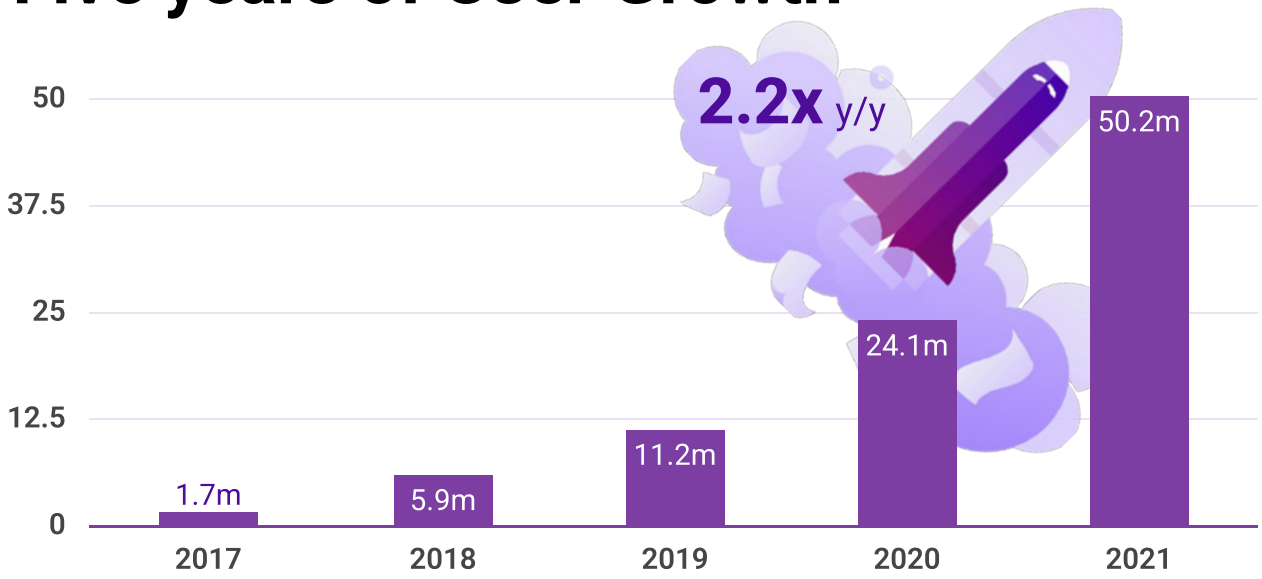
[5] See "The 2021 Global Crypto Adoption Index: Worldwide Adoption Jumps Over 880% With P2P Platforms Driving Cryptocurrency Usage in Emerging Markets", *Chainanalysis*, October 14, 2021

[6] See "How to store crypto in 2022, explained", Sarah Jensen, *Cointelegraph*, December 27, 2021

- 8M+ Brave Rewards users (BAT HODLers).
- BAT is the 11th most distributed token on-chain.
- BAT held cross-chain, with holders on Ethereum, BSC, Polygon, Solana, Gnosis Chain and Avalanche.
- BAT is supported in ETH and BSC DeFi, with cross-chain introduction into DeFi on Solana, Polygon, Avalanche and others coming in 2022.

Brave Browser monthly active users

Five years of User Growth



Brave Browser User Stats

16M
Daily active users

54.5M
Monthly active users

1.4M
Verified Brave Creators

2 Bitcoin

Key Takeaways

- Bitcoin is the mother of blockchains and still the largest crypto asset.
- Due to limited programmability, decentralized finance (DeFi) and nonfungible tokens (NFT) are only available on Bitcoin's layer-two solutions.
- DeFiChain and the Lightning Network show that Bitcoin may be able to capture part of the DeFi market.

Going back to Day 1, someone or a group of persons with the pseudonym "Satoshi Nakamoto" created Bitcoin. The network went live on the Jan. 3, 2009, implementing the seminal white paper "Bitcoin: A Peer-To-Peer Electronic Cash System[7]" that was published a few months earlier in 2008. **[Figure 1]**

Leaning on previous research from Hashcash and others, Nakamoto found a genius and novel way to set economic incentives in such a way that fraud always leads to more loss than gain. Central authorities become unnecessary, and participants can interact with the network without knowing about other participants. Bitcoin is called "trustless" for that reason.

The cryptocurrency sparked a revolution in thinking about financial transactions, economic incentives and collaboration that bloomed into a $2.5-trillion industry in just the next 12 years.

Completely open-source and maintained by a tiny group of core developers, who work on a pro-bono basis and are financed with donations, the Bitcoin blockchain has never suffered any global outage in its existence and now secures more than $1 trillion in assets. Its codebase, Bitcoin Core, has been cloned 105 times to create copycats and alternatives.[8] Bitcoin Cash and Bitcoin Satoshi's Vision are noteworthy; others were quick grabs for investor attention and pre-mined tokens — aka scams.

Figure 1 Satoshi Nakamoto released his genius white paper in 2008

Source: *https://bitcoin.org/en/bitcoin-paper*

[7] See "Bitcoin: A Peer-to-Peer Electronic Cash System", Satoshi Nakamoto, *Bitcoin.org*
[8] Learn more about Bitcoin Fork Count here

2.1 Real-World Use and Adoption of Bitcoin

Berlin once had a whole street where every cafe and falafel shop accepted Bitcoin payments, but slow transactions and high fees soon made hipsters change their minds and switch to contactless card payments.

Bitcoin's famous scalability problem[9] has not been solved yet, but the Lightning Network[10] has recently seen exponential growth in real-world transactions and widespread adoption in Latin America.

Bitcoin's price and market capitalization

One of the best investments in the last decade was buying Bitcoin early. Initially traded for cents per BTC, the price exploded to more than $68,800 in November 2021.

The Bitcoin community still celebrates its humble beginnings with the "Bitcoin pizza day" on May 22, the day that a young engineer named Laszlo Hanyecz paid a fellow user 10,000 BTC for two Papa John's pizzas. **[Figure 2]**

Bitcoin is a deflationary token, and only 21 million BTC will ever exist. New Bitcoin is created as a reward for miners finding a solution to computation-intensive cryptographical problems. The first to submit such a solution in the form of a fully formed Bitcoin block (a package of transaction data) receives a reward in the form of newly minted coins. On average, one block is discovered every 10 minutes and currently yields a 6.25-BTC reward.

Nakamoto laid out a plan to incentivize early adopters. From block 0 to block 210,000, every block received 50 BTC. The following 210,000 blocks got half of that, or 25 BTC, and so on until the most recent "Bitcoin halving" on May 11, 2020, which halved the block reward to 6.25 BTC. The next halving is in 2024, and each subsequent halving will happen every 210,000 blocks, or approximately every four years, until miners mine the last Bitcoin in 2140. Bitcoin is currently **inflationary** and will remain so for the next 123 years, albeit at decreasing inflation levels.

As of December 2021, 18.9 million BTC is in circulation[11], and 328,500 (~900 each day) is mined each year, an effective inflation rate of 1.7%.

Bitcoin's market capitalization has been above $1 trillion since February 2021, although it briefly dipped below that mark during the May 2021 downturn.

Unique Bitcoin addresses

Bitcoin addresses are created by calculating a public and private key pair that conforms to the protocol's specifications. The private key can then unlock the funds associated with its corresponding addresses, which is mathematically derived from the private key.

The address only becomes publicly visible when funds have been sent. Before, it only existed as a possibility. Theoretically, another user could generate the same private key but with infinitesimally slim chances. Bitcoin's pay-to-public-key hash address format can have a total of 1.4×10^{48} possible addresses.

Looking at active addresses is more relevant for this comparison. Around 800,000 active Bitcoin addresses exist as of December 2021. In the last six months, the number grew 25% but is still not back to the peak of 1 million active addresses registered in January 2021. **[Figure 3]**

The 100 richest Bitcoin addresses control around 15% of all BTC. Some of those haven't moved their coins in years. Hodl (Hold On to your coins for Dear Life) culture is a strong force behind the digital asset.

Bitcoin protocol revenue and price-to-sales ratio

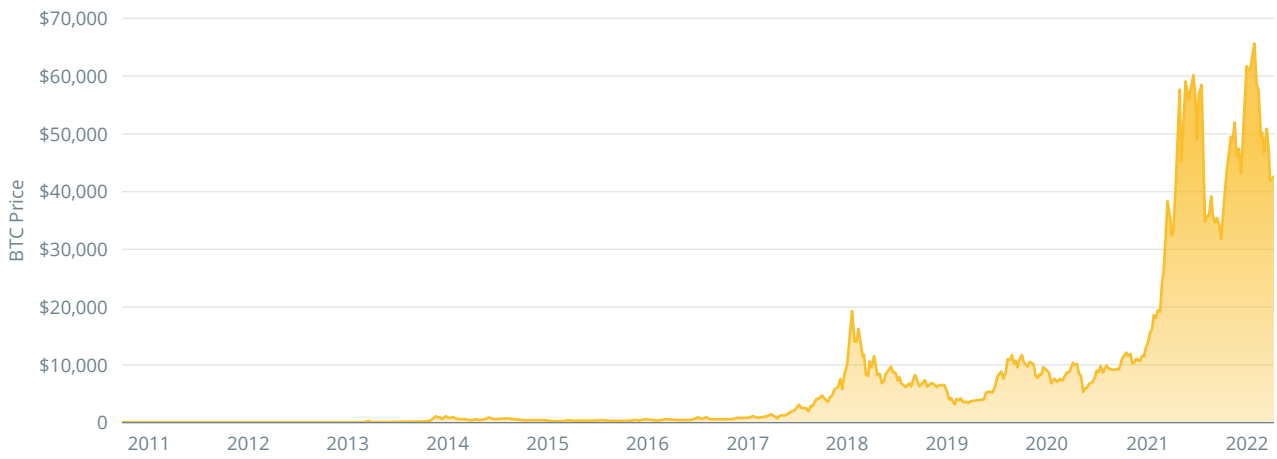
Miner revenue comes in the form of transaction fees and block rewards. Since Bitcoin's protocol can only process seven transactions per second, fee revenue is a fraction of block rewards. Except for short bursts of intense interest, transaction fees rarely cross the 3% threshold of miner profits. **[Figure 4]**

[9] See "Blockchain's Scaling Problem, Explained", Connor Blenkinsop, *Cointelegraph*, August 22, 2018

[10] Learn more about Lightning Network here

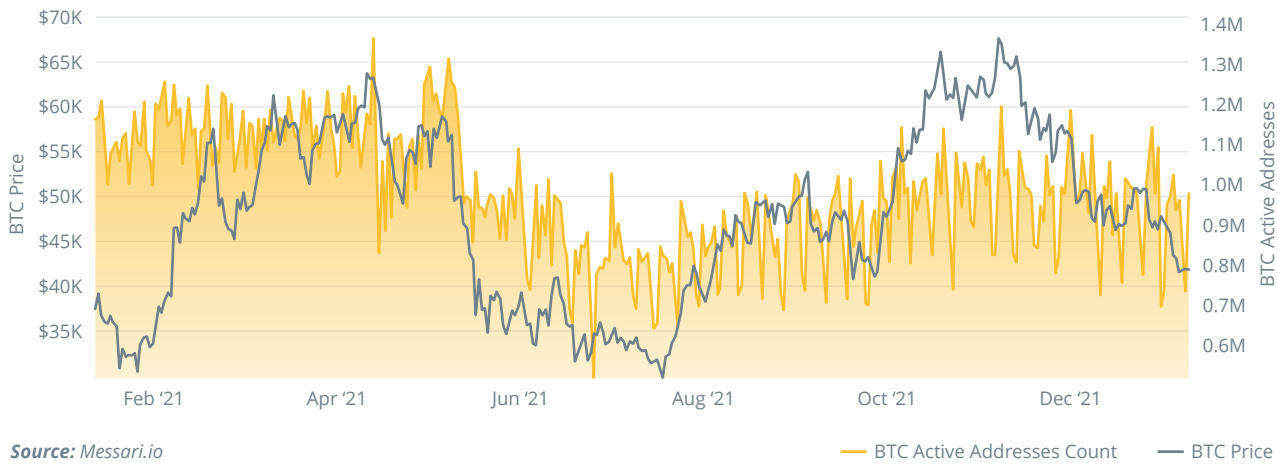
[11] See "How Many Bitcoins Are There Now in Circulation?", *Buy Bitcoin Worldwide*

Figure 2 BTC's price grew from $0.06 to $68,800 in 12 years



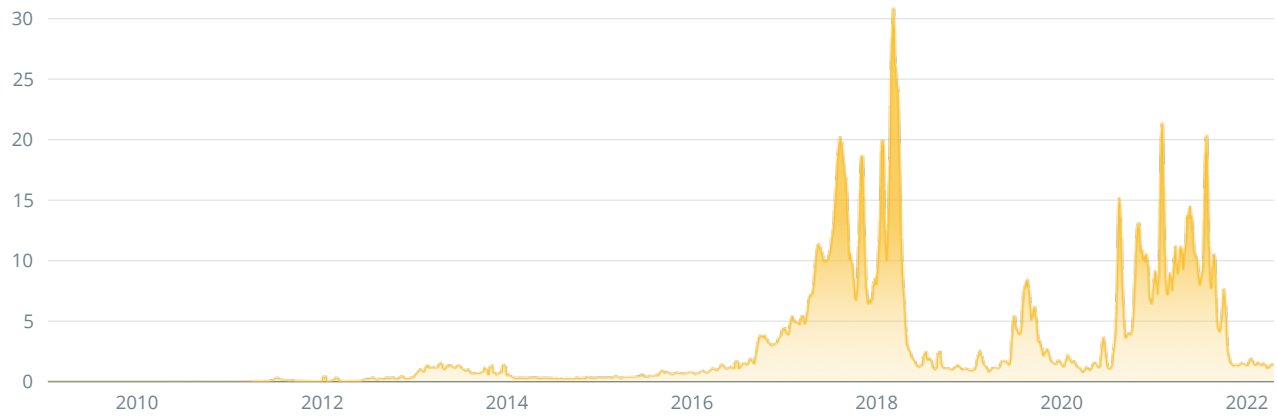
Source: *Messari*

Figure 3 Bitcoin active addresses fluctuate around 800,000



Source: *Messari.io*

Figure 4 Transaction fees as a percentage of block rewards. 40% spike in Jan 2018, 25% in May 2021



Source: *CoinMetrics*

In 2021, transaction fees were just short of $450 million. Bitcoin's market capitalization is 2,200 times more than transaction fees, but just 70 times more than block rewards and transaction fees combined, assuming an average price of $43,000 per BTC. Solana, for comparison, has a P/S multiple of 30,909x.

Staking and lending rates for BTC

Thanks to the wonders of decentralized finance, precious Bitcoin can be put to work. Flexible staking can yield up to 6% rewards on Celsius. Locking withdrawals for 90 days can increase yields to 7.5% on Binance Earn.

Bitcoin can be bridged to the Ethereum network, controlled by a smart contract called Wrapped Bitcoin (wBTC). This wBTC can, in turn, be lent to Aave, but it currently yields less than 0.25% interest due to immense liquidity and little demand — a bullish signal representing investor faith.

DeFiChain,[12] a DeFi application secured on the Bitcoin blockchain, offers up to 106% yield when providing liquidity to its exchange pools. Rewards are paid out in DFI, the project's native coin.

Bitcoin initial coin distribution breakdown

Bitcoin has never had any initial coin distribution. Satoshi Nakamoto set up a Bitcoin node on his computer and at least one other and started mining blocks as a background process.

While the competition to mine blocks escalated rapidly and soon led to the use of dedicated mining hardware,[13] the only "initial coin distribution" was the first-mover advantage that Nakamoto had. Research by the BitMEX[14] exchange attributes between 600,000 to 700,000 BTC to the mysterious founder entity. None of these coins have ever moved from their original addresses.

Only 2.8%–3.5% of all BTC belong to the founder, and they've never sold a single coin — a display of strength and purity of principle.

2.2 Scaling Bitcoin

Bitcoin's core developers have proven to be cautious with changes to the foundation laid out by Nakamoto. When transactions took six days to clear in December 2017, users demanded for relief in the form of greater block sizes to facilitate more transactions per second. This proposal did not meet developer support or miner acceptance. The situation became untenable for some, and Bitcoin Cash was born as a result of this confrontation. Bitcoin Cash increased the block size eightfold and can process up to 250 transactions per second (TPS).

How Bitcoin miners agree on transactions — The consensus mechanism

Bitcoin uses the proof-of-work (PoW) consensus, which was first implemented in Hashcash. PoW forces miners to try quintillions of different numbers (called nonces), which get appended to the data in a block, and are then hashed using the SHA256 cryptographic function. The resulting hash is 256 bit (32 characters) long and changes radically with even the slightest alteration of the underlying data. Hashing is a sound way to make data tamper-proof. The Bitcoin protocol only accepts hashes with a certain number of leading "0" characters. Since SHA256 is a unidirectional function, miners cannot work backwards from the desired hash to a fitting nonce but must try different numbers until one produces the desired result.

The number of leading 0s is set to such a length that all the miners in the world combined can only compute one block every 10 minutes on average. This is Bitcoin's block time.

Every block is linked to the block before, hence the moniker "blockchain." Other miners verify a submitted block to ensure the same coins are not sent twice, or

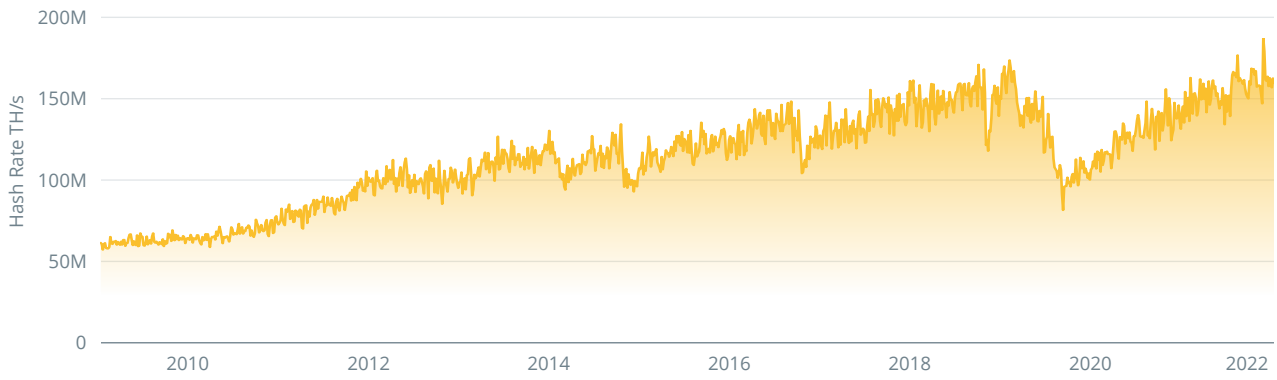
[12] More information about Decentralized Exchanges here
[13] Learn more about Antminer here
[14] Does Satoshi have a million bitcoin? | BitMEX Blog

from an address a user doesn't control. Only if they agree can a miner claim their rewards. Fraudulent activity means doing all the calculations in vain and wasted work.

Miners follow the longest possible chain of blocks. If an alternative version is proposed, it would need to recalculate all the blocks from the point of deviation onwards and overtake the main chain to write a different transaction history, known as a 51% attack, because the attacker would need the majority of the entire network's hashing power to succeed. Hackers could use such an attack to reroute payments and empty wallets without controlling their private keys.

Since the Bitcoin Core network currently has an astounding 185 quintillion hashes per second capacity, it is not economically possible to mount such an attack. **[Figure 5]**

Figure 5 The Bitcoin hash rate is a measure of network security — currently at 185 EH/s (185×10^{18})



Source: *blockchain.com*

The Bitcoin hash rate is a measure of network security — currently at 185 EH/s (185×10^{18})

Bitcoin's Script programming language

Satoshi Nakamoto foresaw the need for programs to efficiently interact with the Bitcoin blockchain and developed the "Script" programming language.

Script has limited functionality compared to Ethereum's Solidity or general-purpose languages, such as Rust, used by Solana. The main limitation is that Script prevents programs from looping. Loops are helpful for enumerations or working through datasets, but they can be used to empty wallets quickly in a series of smaller transactions.

Ethereum got to know what the vicious downsides of loops can entail when "The DAO heist" enabled a hacker to steal a large portion of all Ether (ETH) from a poorly designed smart contract.

This limitation makes Script "Turing Incomplete," a fancy name for not having as many instructions as a general-purpose language. Turing incompleteness makes Bitcoin much more secure because it limits the potential for nasty bugs; however, it hinders what can be developed. There will never be native NFTs or DeFi applications on the Bitcoin network. Clever developers have had to create more complex solutions built atop Bitcoin for security but process elsewhere, so-called layer-two solutions.

Bitcoin Core developers have not been sleeping in the meantime and updated Script to Tapscript with the Taproot upgrade, which allows more complex transactions.

The Taproot update to Bitcoin Core

The "Block wars" over Bitcoin's block size in 2017 left a deep and lasting wound on developers and stifled innovation. Bitcoin's Taproot update is as much a healing process as it is a big step forward for the network's technology.

Updates used to need a one-year announcement period during which miners could signify their approval. The "Speedy Trial" overlay in the Bitcoin Improvement Proposal (BIP) 8 reduced this timeframe to three months.

After the third try, 90% of miners signalled approval of BIP-340 and BIP-342, known as the Taproot update,

on June 12, 2021. The update was locked in on Nov. 14 and went live without a hitch. The corresponding software updates to nodes propagated through the network in the months afterwards.

Taproot features two significant upgrades:

- Schnorr signatures: Replacing ECDSA signatures, Schnorr's algorithm allows keys to sign transactions in aggregate. Bitcoin becomes more private this way because transactions signed by multiple parties are indistinguishable from single-signer transactions. They also enable Bitcoin scripts to sign transactions, expanding the possibilities of Bitcoin native programs.
- Tapscript: Expands the functionality of the Script programming language to facilitate more complex transaction conditions, helping the Lightning Network and other layer-two solutions become more private and efficient.

The most crucial aspect of all might be that Bitcoin developers left the path behind and found a renewed confidence in innovating with the full support of miners. This trust and confidence is the key to keeping Bitcoin relevant with meaningful innovation in the future.

Average fee per Bitcoin transaction

Being a peer-to-peer electronic cash system suggests that users should be able to pay with Bitcoin for mundane tasks such as buying a cup of coffee or a pizza. The chapters on transaction speed will explain why, but Bitcoin cannot facilitate these kinds of transactions.

Transaction fees and transaction times make it impossible to pay with BTC at the local deli.

Fees are auction-based. Miners include the most lucrative transactions in their version of the next block, so transaction senders need to include a large enough payment to have their transaction processed quickly — otherwise, they will have to wait. During price crashes, when everyone and their dog wants to sell BTC at once, prices are at a premium, and desperate sellers bid $100 or more for transaction fees. Recently, fees have oscillated between $1 and $3. **[Figure 6]**

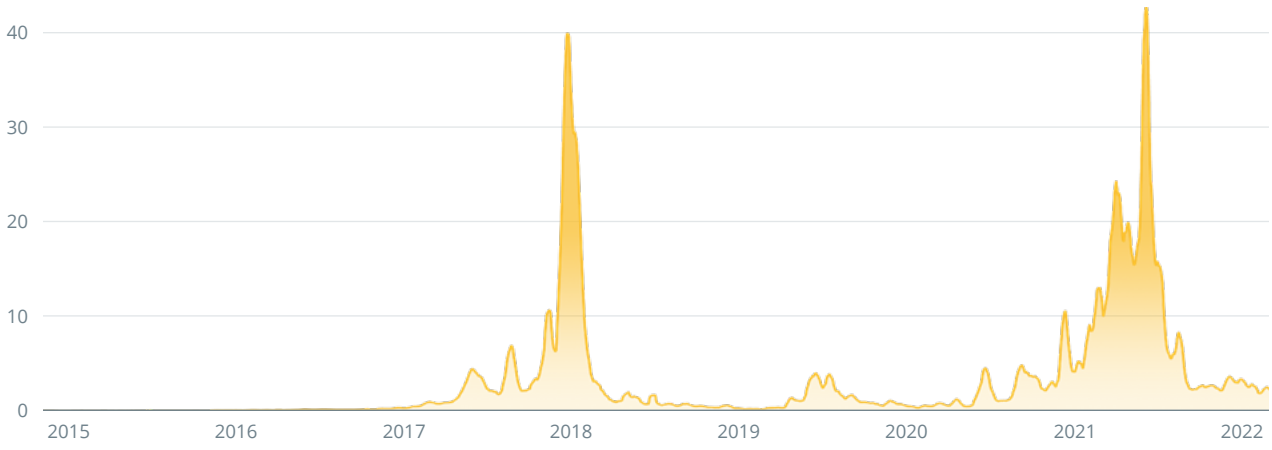
Bitcoin transactions are still much cheaper than Ethereum's, where simple transactions routinely cost more than $10, but the lower price is a sign of less demand, too. A $1 transaction fee is still too much for a coffee purchase.

Theoretical transactions per second (TPS) on the Bitcoin network

Bitcoin transactions consist of information about the senders, the recipients and the amount, plus some security information. Since a Bitcoin block cannot be larger than 1 megabyte in total, it can include a maximum of 3,500 average-sized transactions. This boils down to a maximum of 5.83 TPS, as a block is mined every 10 minutes.

Some blocks contain smaller transactions, and miners now process Segregated Witness transactions, which optimize space inside a block, making up to 7 TPS possible.

Figure 6 Bitcoin transaction fees rarely breached the $3 mark in Q4 2021



Source: *CoinMetrics*

Average transactions per second

Since Bitcoin transactions are slow, somewhat expensive, and faster blockchains exist, the number of actual transactions on Bitcoin rarely reaches the theoretical maximum. In October 2021, the protocol processed 3.18 TPS on average.

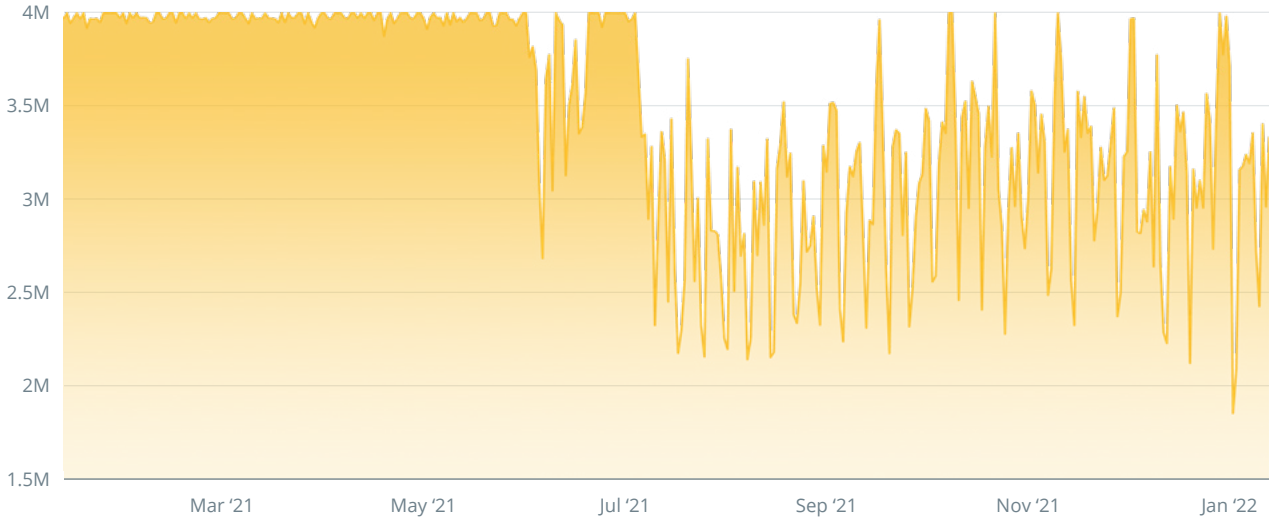
The Bitcoin protocol was a bit more active during most of 2020 with 3.85 TPS on average but saw a downturn in usage during the May 2021 crash, from which it has only partly recovered — a fact that is visible in the amount of blockspace used. Blocks are rarely more than half full in the second half of 2021. **[Figure 7]**

Time to finality for Bitcoin Core

Transactions are considered final after they are confirmed three to six times, depending on security requirements. The reasoning behind this is that alternatives could still overtake one block, but the effort needed to write a longer chain and catch up with more than three or six blocks is enormous.

Six confirmations mean a minimum of 60 minutes until finality. Just two confirmations mean between 10.1 and 20 minutes of waiting time before a merchant would be wise to accept a BTC payment. That's a long wait for a coffee.

Figure 7 Full capacity blocks until July 2021 and only half capacity later



Source: *BitInfoCharts*

2.3 Layer-two solutions to Bitcoin's scalability

Since Nakamoto wanted to design an electronic cash system, his successors had to think about possible solutions to Bitcoin's scalability problem. If BTC intends to be used for payments, multi-dollar transaction fees and hours-long wait times could not be tolerated.

After Bitcoin miners rejected a proposal to increase Bitcoin's block size to 2 megabytes in May 2017, Bitcoin Cash was created as a hard fork of Bitcoin Core. In a hard fork, every holder of coins on the parent chain also holds coins of the offspring, but the blockchains diverge after that. Sometimes, most miners decide to ditch the older chain, and it fades into oblivion. But that was not the case with Bitcoin Cash, whose acceptance remains far below Bitcoin to this day. Bitcoin Cash can achieve 350 TPS, which is a welcomed improvement but still a far cry from real-world demands. The Visa network processes up to 56,000 TPS on busy shopping days.

Thankfully, a few clever developers found a solution and introduced the Lightning Network[15] in 2016, officially launching it in 2018.

[15] See "What is the Lightning Network in Bitcoin and how does it work?", *Cointelegraph*

The Lightning Network

The Lightning Network white paper was released on Jan. 14, 2016, and written by Joseph Poon and Thaddeus Dryja. Since then, Lightning Labs' team has made steady progress under CEO Elizabeth Stark.

Lightning specifies a peer-to-peer payment system on top of Bitcoin using payment channels. The mechanism is simple and elegant:

- Alice tops up her Lightning payment channel to Bob with BTC (first on-chain transaction).
- Alice sends Bob a transaction.
- Alice can send Bob as many other transactions as she wants until her funds are depleted.
- Alice and Bob agree on the total paid and close the payment channel (second on-chain transaction).

The fee for sending a Lightning transaction is zero if a direct connection exists between the parties. Lightning can also route a payment through many hops. The transaction propagates like, well, Lightning in the sky until it reaches its desired recipient. Hops charge minuscule fees, often fractions of 1 Satoshi, for their services in providing the necessary liquidity.

The Lightning Network is like a social network for payments. Since each hop can only facilitate less than what they topped up, network capacity can become an issue for large transactions. Mercifully, 2021 saw exponential network capacity growth, exceeding 3,000 BTC (~$150 million) in October 2021. **[Figure 8]**

In December 2021, there were more than 17,100 Lightning nodes worldwide, most of which in the United States and the European Union. These nodes have more than 77,000 open payment channels. Lightning wallets for iOS and Android have matured enough to be usable by regular users. And in Venezuela, savvy residents shop with BTC.

Buying a coffee with Bitcoin has never been easier.

DeFi on (top of) Bitcoin

In the section about Bitcoin's Script protocol language, we discussed that many applications are not possible on Bitcoin due to its limited instruction set.

That's why there will never be Bitcoin-native DeFi applications because the underlying smart contracts (a fancy name for tiny programs that self-execute and run natively on a blockchain) need a complete instruction set.

Figure 8 Visualisation of the Lightning Network

Source: *Acinq*

Script allows the creation of something called Atomic Swaps, however. You might have noticed that Bitcoin developers are almost as creative as Apple's marketing department in finding awe-inspiring names for their products. Avoiding undue technicality here, Atomic Swaps allow Bitcoin to be exchanged with coins of other blockchains such as Litecoin or Ethereum in one transaction and without intermediaries. The exact mechanism involves Hash Time Locked Contracts[16] and is beyond the scope of this research.

Only two projects offer decentralized financial services on top of Bitcoin — DeFiChain and Portal.finance.

DeFiChain

DeFiChain uses an intelligent way to secure transactions on its own chain by storing cryptographic representation to the Bitcoin blockchain every 30 minutes. DeFiChain's own network is fast and tailored to decentralized finance by expanding Bitcoin's Script language just enough to allow building, lending, staking and tokenizing functionality without becoming Turing complete and compromising on security.

DeFiChain went live in 2020 and introduced the ability to create digital tokens from stocks in November 2021. Users can currently get up to 400% APR when providing liquidity with Tesla, Google and other stocks in pairs with stablecoins.

The download of a proprietary wallet is necessary to participate. Thanks to rapid innovation and its clever security mechanics, DeFiChain has attracted more than $1.8 billion of assets[17] to its applications.

Total value locked in DeFi on Bitcoin

Portal.finance has not been released to the public yet. Investors can start a whitelisting process to participate in the creation, and Portal announced $650 million of funds pledged to its development.

DeFiChain is the only running layer-two decentralized exchange on Bitcoin, and the total value locked (TVL) on Bitcoin is the same — $1.8 billion. Watching out for Portal's start and traction is recommended for anyone interested in this unique space.

Summary

Bitcoin's design has unique features that make it impossible to do certain actions, and this has driven developers and users to search for greener pastures in the Ethereum ecosystem. However, the same drawbacks conversely make Bitcoin more secure and stable. Seen in a more poetic way, Bitcoin seems like the wise grandfather of modern cryptocurrencies. And while it may be considered old-fashioned, its stringent adherence to core values makes it inherently trustworthy and commands great authority.

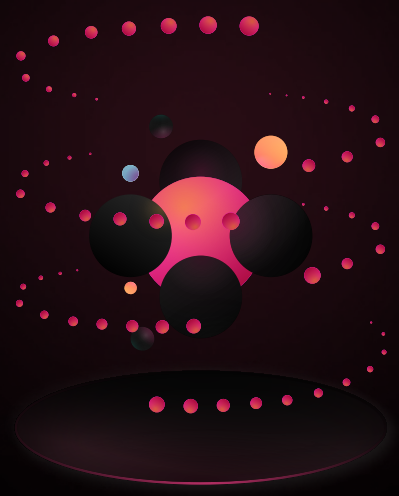
DeFi has arrived on top of Bitcoin. While Ethereum allows native financial decentralized applications (DApp), transaction fees for providing liquidity to exchange pools have frequently exceeded $100 and occasionally topped $1,000. Layer-two solutions on top of Ethereum are all the rave now, so there's no reason to think of layer-two DeFi as "less real" than layer one.

Bitcoin is still a valid synonym for crypto as a whole, and Taproot, Lightning Network, and layer-two DeFi mean it is more than just the first cryptocurrency, it is still a formidable competitor for the blockchain foundation of the global decentralized finance market.

[16] See "Researchers Say New Lightning Network Attack Could Create 'Chaos'", Felipe Erazo, *Cointelegraph*, June 29, 2020
[17] Learn more about DeFiChain here

arcana

Catalysing The Privacy Big Bang



Build privacy preserving apps with tools to:

- Authenticate Users
- Encrypt and Store Data
- Share and Manage Access

ARCANA POWERS THE NEXT GENERATION OF DAPPS

Private NFTs & Creator NFTs

Power creator platforms to Mint, Sell, Rent, and Buy content from creators seamlessly. Make content private to just the NFT owners.

Wallets

Add social auth to create wallets for users and reduce login friction, or make it passwordless email login with Magic links.

Social Media

Build truly decentralised platforms where users own their data/creations, without any of the UX overhead.

Identity

Manage identities with DID and create private/ public profile pages for users where they control what parts of their profile can be shared.

BACKED BY THE BEST IN THE BUSINESS

Republic Crypto

Woodstock Fund

Digital Currency Group

Fenbushi Capital

Balaji Srinivasan
Ex-CTO, Coinbase

Sahil Lavingia
Founder, SHL Capital

Santiago Santos
Ex-General Partner, Parafi Capital

Sandeep Nailwal
Co-Founder, Polygon

JD Kanani
Co-Founder, Polygon

and more...

www.arcana.network twitter.com/ArcanaNetwork t.me/ArcanaNetwork

3 Ethereum

Key Takeaways

- Ethereum's full instruction set allowed developers to dream big.
- The ICO craze, DeFi summer and the NFT boom brought crypto to the masses.
- Ethereum 2.0 can't come soon enough, as blocks were always full in 2021.

DeFi and Ethereum are almost synonymous. Ethereum smart contracts enable the trustless transactions that make up decentralized finance, and most projects developed on top of the "world computer."

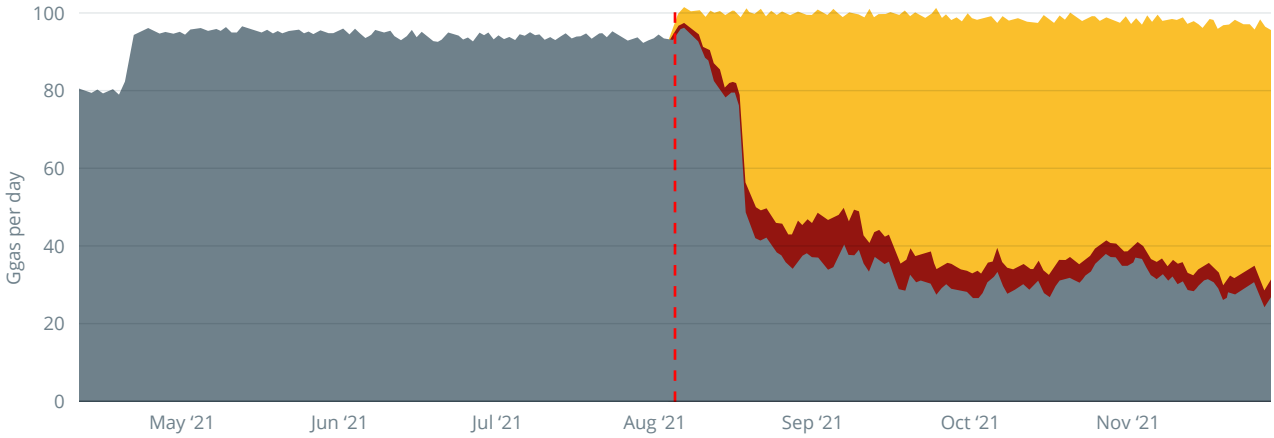
This research focuses on the fundamentals of real-world use and gives an overview of Ethereum's scalability — or lack thereof. Finally, we will explore Ethereum's astounding dominance in both NFT sales and value locked in DeFi.

Vitalik Buterin co-founded Ethereum in 2013. Due to legal challenges with Ethereum's initial crowd sale, it took almost two years to launch the network on July 30, 2015. Buterin wanted to expand Bitcoin's programmability radically. He saw blockchain-native programs as a powerful catalyst for usage and adoption. His ideas were met with intense pushback by the Bitcoin developer community, so he started to pour his efforts into a project of his own, which he called Ethereum. After receiving a $100,000 grant from the Peter Thiel Foundation in 2014, he began assembling a core team of contributors.

Some of today's most prominent figures in crypto were among early Ethereum developers, such as Charles Hoskinson, founder of Cardano; Gavin Wood, founder of Polkadot; Joseph Lubin, founder of ConsenSys; and Anthony Di Iorio from TMX. These heavy hitters embarked on a rocky journey, which saw them facing intense infighting among the team, massive delays caused by regulatory uncertainty and near bankruptcy.

Ethereum finally launched and proved that programmability was incredibly powerful and equally dangerous. The initial coin offering (ICO) hype of 2017, DeFi summer and the NFT boom in 2020 did more for crypto adoption than anything else, while the DAO heist[18] nearly ended Ethereum's existence in 2017. **[Figure 9]**

Figure 9 The Ethereum network has been at full capacity since May 2021



Source: *Twitter*

Legacy tx (types 0 and 1) | Legacy-equivalent tx (type 2) | EIP-1559 tx (type 2) | London hard fork

[18] See "The DAO: Chronology of a daring heist and its resolution", *Deloitte Blockchain Institute*, September, 2016

Ethereum hit the ceiling of its transaction capability this year. Most of the time, blocks are at capacity, but transaction fees have skyrocketed to peaks of $10,000 during coveted NFT launches.

The situation has become untenable and frequently priced out participants with lower net worth. Other blockchains picked up the slack, and Ethereum now faces innovative competition from Solana, Avalanche and Fantom.

Will Ethereum remain the predominant ecosystem and continue to be at the forefront of innovation and adoption? Or will it fall behind and get overtaken by blockchains with better performance and faster development?

3.1 Real-World Use and Adoption

Ether price and market capitalization

ETH, short for Ether, is the native token of Ethereum. There is no maximum amount of Ether, and currently, 118.9 million are in circulation. This amount grows as block rewards are paid to miners and are reduced by base transaction fees being burned after a recent upgrade to the protocol. In 2021, Ether had a 1.8% net yearly inflation.[19]

Ether's price has been above $3,000 since August 2021, and its average market capitalization was $440 billion in October 2021. Starting in July 2020, its market cap rose in tandem with the TVL. In December 2021 the ratio of market cap to TVL was around 2.9x which places Ethereum between Fantom with just 0.76x and Solana with 4.4x. This is a good measure for how valuable a chain is in relation to the assets locked. **[Figure 10]**

Ethereum daily active addresses

The number of active addresses represents the number of accounts with at least one transaction on a given day, which is a good measure for the overall liveness of a blockchain. Ethereum surpassed 500,000 daily active addresses in the second half of 2021 and peaked at 800,000 in November 2021. Growth has been hampered by high transaction fees and longer wait times lately, as can be seen by the plateau on the graph above, which started in May 2020. The amount of active addresses is likely to stay at current levels until major technical upgrades become available. **[Figure 11]**

Ethereum protocol revenue and price-to-sales ratio

The Ethereum network currently employs a PoW consensus mechanism. More on this later. Miners secure the blockchain in return for block rewards and transaction fees. Block rewards were 5 ETH per block until October 2017, when the Byzantium upgrade reduced the rewards to 3 ETH per block. The Constantinople upgrade in February 2019 went a step further, and now miners receive only 2 ETH per block or around 13,000 ETH per day for their services. **[Figure 12]**

Transaction fees are now split into base and priority fees ever since Ethereum Improvement Proposal 1559 was implemented, part of the famed August 2021 London[20] upgrade. Apart from different naming geography, it introduced a mechanism to burn the base transaction fees and only award miners the priority fee. The priority fee is like a tip that users add to their transactions to be processed quicker. Sometimes, substantial amounts are tipped during high transaction demand, like NFT launches. Burning the base fee will make Ether net deflationary when the network merges to its next iteration, Eth2, scheduled in 2022.

With Ether prices around $4,000, **block rewards are close to $19 billion** per year. Priority fees per day can peak up to 32,000 ETH. In the second half of 2021, they have evened out at an average of 1,500 ETH per day or **$2.19 billion per year**.

The price-to-sales ratio divides the market capitalization by the protocol revenue to make blockchains more comparable in the same way a price-to-earnings ratio does for stocks.

Ethereum has a 22.2x price-to-sales ratio, and a 214.9x ratio of price to transaction-fees. Both reflect a solid fundamental value of Ethereum when other blockchains such as Solana have a P/S of more than 30,000x.

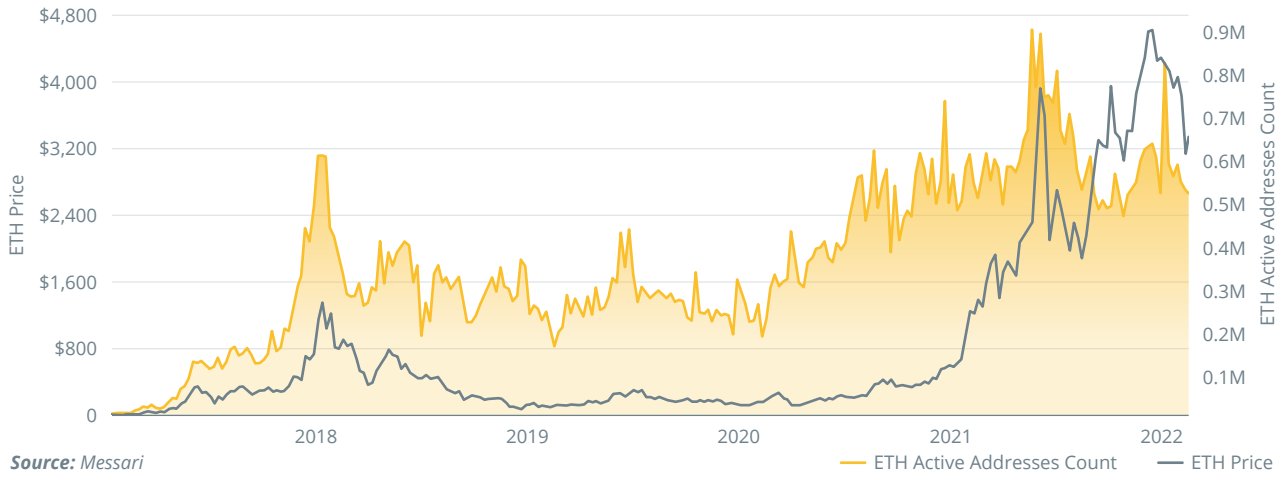
[19] More information about Ethereum's inflation here

[20] See "Ethereum's London hard fork sets ETH on a more deflationary path", Anirudh Tiwari, *Cointelegraph*, August 12, 2021

Figure 10 Ethereum's price near all-time-highs in December 2021

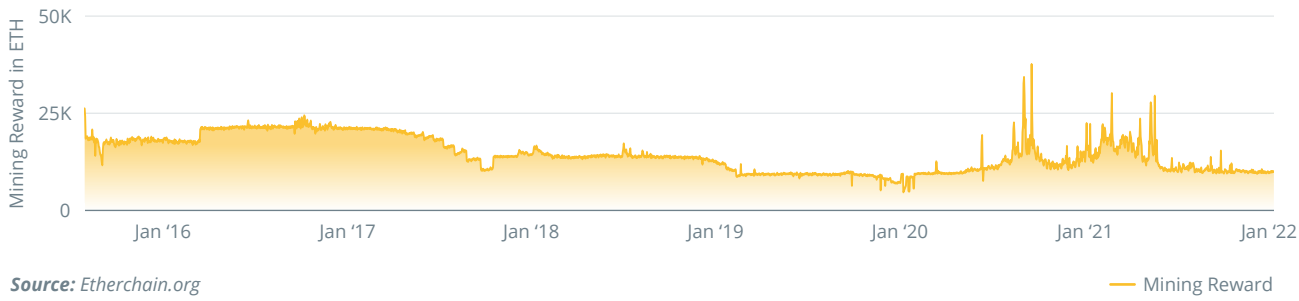
Source: *Messari*

Figure 11 Ethereum active addresses surpass 500,000 in the second half of 2021



Source: *Messari*

Figure 12 The total mining reward per day in ETH is the block rewards plus the transaction fees

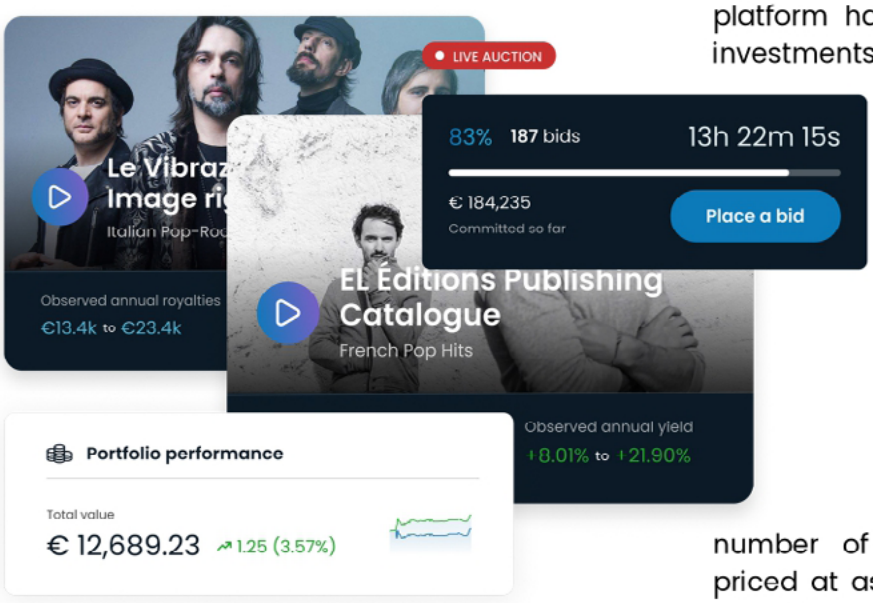


Source: *Etherchain.org*

ANote Music

Unlocking artist creativity with blockchain

Europe's **leading marketplace for investing in music royalties**, ANote Music bridges the gap between the music industry and the capital markets, enabling publishers, record labels, and artists to sell music rights, while offering music enthusiasts a new investment opportunity and the chance to **own shares in established music creator's catalogues**. Since launching in July 2020, the platform has provided investors access to a roster of tracks performed by the likes of Avicii, The Beach Boys, The Kinks and Drake.



ANote is integrated with the blockchain technology platform Algorand, which applies a proof-of-stake consensus algorithm to validate transactions. The partnership enables the allocation of tokenised music assets and NFTs listed on the exchange to investors, proving **the right to receive a share in future royalty streams**.

In addition, ANote works alongside regulated partners and entities to deliver a robust and trustworthy framework designed to maximise security of transactions and user experience.

ANote's adoption of Algorand's technology was a **landmark for music investment**. With this move, ANote positioned itself as one of the pioneering companies listing music assets to retail investors on the blockchain, allowing them to receive royalties payouts as a return on their investment. Algorand's 'logic-rather-than- transaction signatures' capabilities embedded in ANote's platform have supported the rapid growth in investments registered on the platform over the past year, with **year-on-year revenues rising by +550%** in 2021. ANote registered a repeat customer rate of 67%, accounting for a significant proportion of its more than **10,000-strong community** of registered investors.

The spectrum of listings on ANote's exchange spans a range of musical eras and genres; a product offering of 100 artists across a growing number of catalogues. With royalty shares priced at as little as 6 euros, ANote's business model ensures **a low barrier to entry** and supports its mission to drive **greater inclusion in the market**. Once the reserve of in-the-know music-industry heavyweights, music royalties are entering a new stage in their lifecycle with individual catalogues backed by a greater number and range of asset owners.

10% CASHBACK BONUS

Scan the QR code to create an ANote Music account and we'll help you kickstart your music investment journey. Benefit from a **10% cashback bonus*** upon successful bids on auction deals and no upload fees when adding funds to your account for the **first 60-days after sign up**.

**capped at €1.000*

anotemusic

anotemusic.com

Ethereum staking and lending rates

The next iteration of Ethereum will be a proof-of-stake (PoS) network where validators need to have at least 32 ETH to vote on transactions. Parts of this network are already parallel to the main PoW blockchain, and investors can stake their Ether on the new network. This stake is locked until the migration is complete, and until now, it's unclear whether this will happen next year or even later. Staking Eth2 is a strong indicator of trust. So far, 7% of all ETH is staked on Eth2. Compared to Solana, which has 76% of its SOL staked, this might seem low, but some perspective is needed. If the transition never succeeds, which is a possibility, these funds are lost.

Users with less than 32 ETH need to delegate their coins to other validators to collect rewards. Centralized exchanges such as Kraken have made that very comfortable and offer **5%–7% APY on staked Ether**. Decentralized protocol Rocket Pool allows users to stake and unstake Eth2 at will with 4.3% APY. Plus, there's a token. **[Figure 13]**

Lending platform YouHodler pays 5.5% APY, with CoinLoan and BlockFi offering more than 4.5% each.

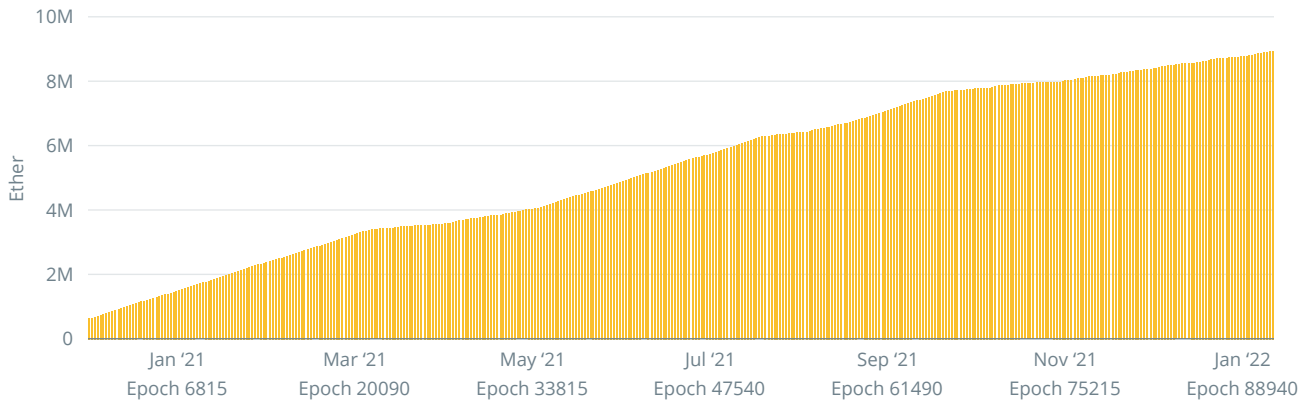
Juicier gains are realized when providing liquidity to decentralized exchanges (DEX) such as SushiSwap, where pairing ETH with stablecoin TerraUSD (UST) yields 46% APY this December.

Initial coin distribution of Ether

Buterin and his early team often get a lot of flak for Ethereum's alleged centralization. The truth is that the core team did get around 10% of all ETH in circulation. Even then, the exact distribution was a contested issue and led to some bad blood. After this initial distribution, the team had a crowd sale — arguably the first ICO ever — where investors could purchase Ether for Bitcoin. Thousands of individuals bought 60 million ETH, about half of the supply in 2021. This share represents Ethereum's early community, which got well rewarded for their faith in a project headed by a scrawny 20-year-old. **[Figure 14]**

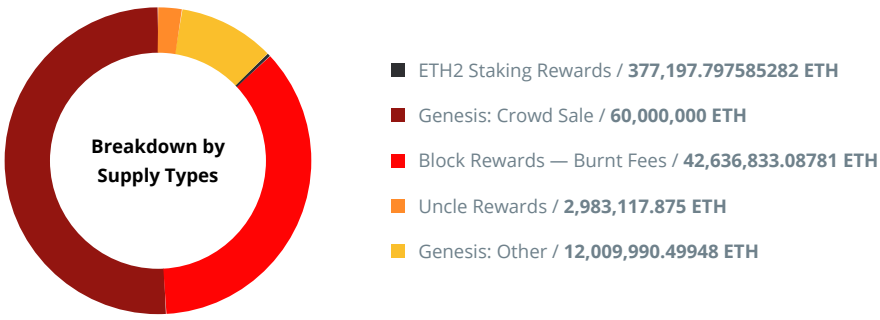
Compared to Solana and many other blockchains, Ethereum has little centralization. Conversely, the setup is not as squeaky clean as Bitcoin's, where nothing was pre-mined.

Figure 13 Amount of ETH staked



Source: *Beaconcha.in*

Figure 14 Breakdown of Ethereum's Initial Coin Distribution



Source: *Etherscan.io*

3.2 Scalability

Ethereum was designed in 2013, with its final implementation launching in 2015. Performance was not the first objective then, so the protocol was designed for robustness and made it easy for enthusiasts to run nodes. With more than $160 billion in locked value and thousands of projects running, the need for radically improved performance has become pressing.

Enter Ethereum 2.0

The next generation of the Ethereum protocol will introduce three significant changes:

- A move from PoW to PoS.
- Introduce a sharded blockchain, basically multiple synchronized chains in parallel.
- Replacing the Ethereum Virtual Machine with eWASM.

The move to **proof-of-stake** will be a quantum leap toward making Ethereum more energy efficient and carbon neutral. PoS means that validating nodes vote on transactions and get rewards for successfully submitting blocks to the blockchain. The network's energy use will come from the computers running nodes, mostly standard desktop machines. Miners consumed 45 terawatt-hours of energy[21] in 2021 as millions of high-end graphics cards churn away to compute the necessary calculations securing the network.

Sharding is a widely used process in database management where tables with high demand are spread out among multiple servers to make access more performant. Ethereum sharding will split its blockchain into multiple chains running in parallel and synchronizing to the so-called Beacon Chain. Sharding will improve Ethereum's performance from a maximum of 35 transactions per second (TPS) to a theoretical maximum of 100,000.

Last but not least, the switch from the Ethereum Virtual Machine (EVM) to **eWASM**, which stands for Ethereum Web Assembly, will mean that smart contracts can be written in most general programming languages, such as Rust, C++, Python and others — a big boost for developer access and productivity.

Ethereum 2.0 — The timeline to launch

Upgrading Ethereum is like open-heart surgery. There are thousands of projects and millions of active users, and hundreds of billions of value operate on the network, but any significant mishap would spell an irreparable loss of trust in the blockchain. Accordingly, Ethereum developers are cautious and test and retest every upgrade before rolling it out to the mainnet.

No fixed date for the launch of the next steps toward Ethereum's future is set, much to the community's chagrin, however. Nevertheless, the Eth2 Beacon Chain was successfully deployed in December 2020, and a successful merge of Ethereum to PoS Eth2 was demonstrated on a testnet in October 2021, representing an important milestone.

The **merge** of Ethereum's v1 mainnet to v2 is expected for **May–June 2022**. Miners will no longer be able to produce blocks after that. The shift from a single-threaded blockchain to **sharding** is expected a year after the merge, sometime in **2023**. Eth2 stakers are in for a long ride: Unstaking requires a minor update after the sharding upgrade.

Consensus mechanism

Like Bitcoin, Ethereum also uses a proof-of-work consensus mechanism. Miners collect transactions for a block, aggregate them cryptographically, and then have to try quintillions of different numbers, called nonces, until the resulting hash has a certain number of leading zeroes. While Bitcoin uses the industry-standard SHA256 algorithm, Ether miners compute "Ethash," a slightly altered version of the SHA3-256 and SHA3-512 algorithms. It is much harder to build application-specific chips (ASIC) for Ethash, so the ASIC arms race never happened on Ethereum. Instead, miners use high-end graphics cards (GPU) like the Nvidia RTX 3090. Miners' insatiable demand led to Nvidia implementing a throttling switch when cards detect mining workloads, so gamers could afford GPUs.

[21] See "Ethereum transaction energy use equals 2.5 miles in a Tesla Model 3: Report", Cointelegraph Research, *Cointelegraph*, December 9, 2021

Figure 15 MSI Nvidia RTX3090 graphics card, typically used for Ethereum mining

Source: msi.com

Solidity — Ethereum's programming language

Vitalik Buterin wanted to allow developers the freedom to run everything they could dream of on top of the blockchain and create a massively distributed system. He called Ethereum the "world computer" because miners worldwide would execute programs.

Bitcoin has a programming language called Script that has limited functionality. Ethereum's language needed a complete instruction set to give developers more freedom.

Gavin Wood, who later founded Polkadot, was the first to implement a working version of Ethereum and developed Solidity as Ethereum's language. Later, another language called Vyper was introduced. (Smart contracts can be written in both.)

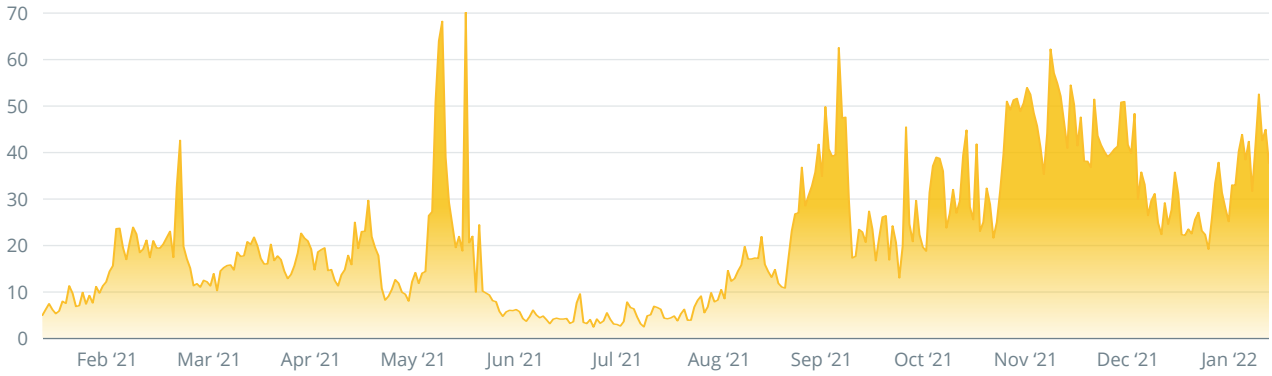
Since miners run different hardware, Solidity compiles to so-called bytecode, executed by the Ethereum Virtual Machine (EVM), abstracting the hardware layer. This way, a developer doesn't have to worry about what machine a miner will run. The EVM takes care of that.

Solidity is easy to read and is quite similar to JavaScript in the way the code looks, although it has several fundamental differences — e.g., more stringent variable data types.

Average transaction fee on Ethereum

Transaction fees are auction-based; users paying the highest fees get their transactions processed first, leading to bidding wars. Since the Ethereum network is at 100% capacity, transaction fees have been painfully high. In October 2021, average transaction fees were $28. Sending funds costs about $9, and more complex transactions such as swaps or adding liquidity on decentralized exchanges often cost more than $100 in the last quarter. Ethereum earned itself the critique of being a "rich boys club" because smaller investors simply cannot participate anymore.

Figure 16 Ethereum transaction fees were $28 on average in October 2021, and peaks were $70



Source: *Blockchair*

Average and theoretical TPS and time-to-finality

One Ethereum block is mined every 13.8 seconds on average, but this number fluctuates with mining capacity. Since only a limited number of transactions can be included in a given block until its storage capacity is filled, the theoretical maximum of Ethereum transactions is **35 per second**, assuming that all transactions are small. Ethereum de facto processed 1.2 million transactions per day in October or **13.8 TPS**. Transactions for staking, minting and swapping use more data and fill a block faster.

Since a consensus of other miners could still overwrite the most recent block, most applications demand three to six blocks to pass before they deem a transaction to be final. Time-to-finality is 42–90 seconds, accordingly. Users have to wait for finality until they can move on in their trades, and 90 seconds is a long time for the internet age.

Ethereum 2.0 will drastically change that and offer up to 100,000 TPS, and time-to-finality could be as low as six seconds, depending on the final implementation.

Current throughput and speed mark Ethereum as a member of the "old guard," but strong network effects remain relevant. The big question is whether the upgrade to a sharded, performant Ethereum 2.0 will come soon, or whether other chains will take a piece of Ethereum's pie.

Insider Insight

How can cryptocurrency investors avoid being front-run?

Ivo Georgiev, CEO of Ambire

There are a few definitions of front-running when it comes to cryptocurrency investing. For one, when buying altcoins, it's possible that there are early investors in that altcoin that you don't know about. They bought at a much lower price before the coin was publicly traded so they are incentivized to sell and bag in a profit. To avoid this, cryptocurrency investors need to do deep due diligence and analyze the whole circulating supply of a specific coin/token before investing.

Second, when you buy/sell tokens on a DEX, you may get front-run or sandwiched, allowing bots to benefit from your allowed slippage. Slippage in DEXes is the difference between estimated execution price before the trade and the execution price when the trade actually happens (when the transaction is mined), and sandwiching is inserting transactions right before/after your trade to manipulate the spot price, so that your trade is executed at the worst allowed price for you. It's still a form of front-running because the bot benefits from knowing your trade before it happens, and it's the most widespread form. To prevent this, you can use a technology like Flashbots, which is a way of directly negotiating mining of your transactions with a miner, without

broadcasting them publicly. The easiest way to do that is to use a wallet that has Flashbots built-in, like Ambire Wallet.

Is secure storage of Layer 1 cryptocurrencies like Ethereum different from secure storage of Layer 2 cryptocurrencies like Polygon (Matic)?

Secure storage of cryptocurrencies is the same regardless of whether it's a L2 or L1 — it's all about key management, and the industry standard for secure key management is to use a hardware wallet like Trezor/Ledger.

There is one caveat to that — bridged assets that exist on Ethereum but not natively on Polygon, but are bridged to Polygon, carry the extra bridge risk — for example, if the bridge gets hacked, the Polygon wrappers of those assets may suffer. As such, it's better to keep those on their native chain (Ethereum).

What are the best blockchains for earning yields in DeFi and what yields per annum can investors make potentially?

This varies by the day but UST on Terra is pretty popular these days, allowing over 30% yields on their native stablecoin. Of course, as a less proven chain, this is probably riskier than lending USDT/USDC on Ethereum for something like 3–5%. A middleground in terms of risk/reward is earning yield on stablecoins on Polygon, with a couple of solid options: Aave and Tesseract (Yearn alternative on Polygon), both allowing yields between 5–10%. Whatever the case may be, all these yields are at least ten times better than what banks can offer you, especially in this low-interest economic climate.

What are the risks with DeFi and how can investors mitigate those risks?

The biggest risk in DeFi is the so-called rug pull, which can be generalized to any action by the project team that is unexpected and harmful to investors, but often immensely profitable to the project team.

To some extent DeFi allows more opportunities for such actions, because the space is new, quick-moving, and investors are hungry for new opportunities and projects to invest in. This is why they often skip doing detailed due diligence. Furthermore, due to the complex nature of smart contracts and DeFi composability, it's often possible for a big risk to be hiding in plain sight, and unless you're experienced in reading Solidity and actually put in the time to do due diligence, you won't spot it.

For example, when Sushiswap vampire-attacked Uniswap, they had a so-called migrator contract as part of the design. The contract owner could set this migrator contract to a malicious address and withdraw all LP tokens. While this didn't happen in Sushiswap, many of it's forks exploited this to steal all the liquidity staked, even if a migration was never on their roadmap.

One way to protect yourself from such risks is to check if a project has been audited by a reputable security firm, but a significantly better way is to be able to read the code and understand the contracts yourself, as this will allow you to understand "intended behavior" that would pass an audit but allows the project team to "rug pull", such as the one given in the example. If you're unable to, just trusting your intuition in terms of whether something seems shady or too good to be true goes a long way.

Over time, DeFi will actually become more resistant to this — because of its open nature, anyone being able to read code can actually feel safer putting their funds in a DeFi project rather than a centralized exchange or platform. As the industry matures and more people learn how to analyze these projects, DeFi's strength of being fully transparent and auditable will shine.

3.3 Decentralized finance on Ethereum

DeFi directory Defiprime lists **214 Ethereum DeFi projects**. DappRadar lists 2,990 decentralized applications (DApp). No other blockchain has inspired more developers, and Ethereum's stack has become the de facto standard for many other blockchains. Even strong competitors such as Avalanche, Moonbeam or Fantom feature EVM compatibility to allow teams easy portability of projects from Ethereum. Names such as Uniswap, Curve, dYdX and Instadapp have all deployed on Ethereum first and moved on to become household names in the crypto community. Ethereum is where DeFi was invented, and it is the protocol with the most exciting innovations, such as dYdX or OlympusDAO, and the largest and wealthiest user base. **[Figure 17]**

Total value locked (TVL) on Ethereum DeFi

It is no surprise that the most value in decentralized finance is locked on Ethereum. DeFi applications on this blockchain control more than $150 billion. **[Figure 18]**

Figure 17 Ethereum ecosystem map of main DeFi building blocks

Source: The Defiant

Figure 18 TVL on Ethereum is $157.6 billion, 11% of which is locked on Curve

Source: *Defi Llama*

The three most significant projects — Curve, Convex Finance and MakerDAO — account for 36% of all TVL on Ethereum. Counting locked value has some crucial challenges, however. Staked coins can be used in farms whose liquidity provider tokens can again be further deployed and so on. The double- and triple-counting of an uncertain percentage of all assets is unavoidable. TVL numbers should be viewed as a general indicator of growth and activity and not be taken at face value.

Top DApps on Ethereum

The No. 1 DApp on Ethereum is the NFT marketplace OpenSea. OpenSea outpaced its competition in 2020 and is now the go-to place to trade and collect NFTs. With more than $10 billion in total sales, it is a true juggernaut, solely responsible for 135,000 ETH (~$450 million) in burned transaction fees since the London upgrade in August 2021.

No. 2 is the DEX poster child Uniswap, which brought Bancor's Automated Market Maker model to the mainstream and is the go-to for coin swaps. Following these two monsters are SushiSwap, an erstwhile Uniswap clone that now lives on more blockchain platforms than any other DEX, and OlympusDAO and Curve Finance, two DeFi powerhouses.

NFT sales volume and transaction volume

Ethereum NFT sales amounted to $2.2 billion in September and $1.7 billion in October 2021, according to research by Messari, more than eight times the volume of the next competitor, Solana. Most of that volume comes from big-ticket sales such as CryptoPunks or BoredApes, where a single deal can be worth millions.

However, looking at just the dollar-denominated volume doesn't paint a complete picture. Ethereum saw 132,879 unique buyers in October, compared to 68,235 on Solana. The average amount a collector spent on Ethereum was $12,878 in October 2021. While Solana's dollar-denominated value was only an eighth of Ethereum's, its activity was half. Ethereum certainly faces strong competition in the NFT market, and sky-high fees hurt its position because they price out new entrants. **[Figure 19]**

Figure 19 Daily NFT sales on Ethereum

Source: *NonFungible.com*

NFT transaction volume declined sharply, from 1.08 million sales in October to 360,000 in December 2021. While these numbers are alarming, top projects such as CryptoPunks and BoredApes sell for record prices, and traditional companies such as Adidas or Nike launched NFT collections. It's safe to assume that this technology has not run its course yet.

Insider Insight

What is DeFi currently lacking and how can we overcome it?

Bernhard Koch, Founder and CEO Cryptix

As a venture builder in the fintech sector, we build bridges between innovation and effective everyday usability. Thus, it is a given that we closely follow the developments in the DeFi space and the increased use of DAOs. What we recognize, however, is that DAOs intentionally lack substance when it comes to financial regulation:

DAOs are unregulated and legally unaccountable — not the right approach we deem suitable to serve the masses. The widely used "dot-org-constructions" based on non-profit-foundations are mainly used to avoid taxes.

At Cryptix, we have chosen to go the extra mile with a long-term regulated approach. While the main character of a DAO meets our requirements for decentralization and community engagement, it lacks the legal safety and conformity for the masses. Consequently, we have tried to think out of the box, and have successfully created a superior solution: We call it DGO — decentrally governed organization.

Unlike a DAO, a DGO makes use of a legal body: The Societas Cooperativa Europaea (SCE). While an SCE is not a new concept, we've discovered that very few are aware of this cooperative form, despite its great number of benefits:

- Legal clarity and compliance by using a real legal entity.
- Responsibility and commitment as the SCE is legally liable.
- DGOs can have a for-profit motive, thereby creating more sustainable and engaging incentive structures for its members, which are ultimately more supportive and loyal to a project.
- An SCE can change residence within EU countries with low hurdles to operate from a jurisdiction where the environment favors innovative approaches of such DGO and its members.
- Voting on governance and strategic decisions can be made accessible and incentivized in a user-friendly mobile app, with absolute transparency and no manipulation due to real on-chain voting. While members, due to its simplicity, won't even notice they've just voted on-chain.

These benefits come with a more complex, time-intensive, pioneering and expensive path. Nevertheless, we are committed to going down this path and thereby creating a never-before-seen and promising concept, born from the connection between SCE and blockchain technology. In our opinion, this is the next logical step towards enabling a non-crypto community to experience the benefits of decentralized finance, and include them in a powerful, transparent and direct way of decision-making in important projects.

Cryptix is already employing the described DGO model and legal construction within one of its projects, a layer-1-blockchain with its own native cryptocurrency, products and complementary services in layer-2. These Layer 2 services will be run by a DGO and involve their users at the enterprise level in a very simple and highly transparent way as never before.

We are excited about this journey and are already receiving stunning feedback for this concept. We will keep a close eye on user participation and learnings to grow and adapt together for the benefit of the community, its members and our society.

Summary

Ethereum helped crypto to get to where it is today. Without NFTs, without DeFi, and without the ability to launch tokens in less than 30 minutes, many projects simply would not exist, and the world would be poorer for it.

Ethereum is here to stay. Massive network effects, a large pool of development talent, and a mature tech stack mean it is easier and more sensible to launch on Ethereum than any other blockchain.

The onus is now on Ethereum's developers to manage a timely upgrade to a more scalable and renewable future without compromising security and uptime — a genuinely colossal feat. The last upgrades to the mainnet have gone off without a hitch and have inspired well-earned confidence in the skills and thoroughness of the contributors.

2022 will be a make-or-break year for Ethereum. Its open, self-reflective culture and the surprisingly far-sighted thought leadership of Vitalik Buterin inspire confidence that it will be its best year yet.

fuse

Launch community-centric payment systems and token economies on an Ethereum-compatible blockchain.

fuse.io
t.me/fuseio
blog.fuse.io
Fuse_network

VISION

Provide an open-source infrastructure for the global financial system by making crypto-powered payments and DeFi available to the greatest number of people globally, primarily through enabling mobile-first applications.

FUSE NETWORK BLOCKCHAIN

Fuse Network is a layer 1, Ethereum-compatible blockchain that focuses on building market-leading business and mobile-ready infrastructure to expedite and ease the development of real-world applications.

The project emphasises scalability and interoperability with the wider blockchain technology landscape, as well providing middleware technology to remove the complexities involved in building dApps designed for mainstream use.

Fuse's core focus is DeFi and payments but the platform also supports wide-ranging applications including NFTs, gaming, supply chain, trade finance and more.

Consensus: Delegated Proof of Stake (dPOS) + AuRa algorithm

Blocktime: 5 Seconds

KEY INFRASTRUCTURE & INTEGRATIONS

Fuse's key partnerships and integrations include The Graph for smart contract data querying, Pocket Network for maintaining a robust network of full nodes, Ramp Network for fiat-to-crypto on-ramps, Elk Finance and ChainPort for interoperability, Request Network for compliant payment processing, and Sushi and Ola Finance for developing innovative DeFi products on the platform.

the graph · POKT · Ramp · Elk Finance · ola · ChainPort · Request · SushiSwap · Beefy.finance

DeFi ON FUSE

Fuse features a rapidly expanding DeFi ecosystem with mainstream adoption-centric, Voltage Finance, playing a leading role.

Voltage offers a DEX, lending, yield farming, and a mobile gateway designed for easy use in the form of the Fuse Cash wallet.

Other major 3rd party DeFi protocols are also deployed on the platform.

Voltage · fuse.cash

TECH STACK

The Fuse platform is comprised of a 3 layer tech stack:

1.) EVM-compatible chain that is permissionless and governed by network validators and their delegated stakers. Launched in 2019.

2.) Enterprise middleware and infrastructure designed to fast track businesses and other organizations wishing to build and launch innovative, community-centric payment systems and tokens economies amongst other applications.

3.) Mobile wallet infrastrucutre and busineess APIs designed for mainstream adoption through gamification and removing friction such as fees, minimum deposit amounts and alphanumeric addresses.

FUSE TOKEN

Fuse token is the primary currency of the network and the decentralized applications that it supports.

Transactions fees: 100% of fees are paid to network validators.
Security & consensus: Delegated proof-of-stake with an additional inflation model.
Governance: Proportional, stake-based voting.
DeFi: Token-backed stable-coin issuance. Lending and borrowing.
Genesis Token Supply: 300M
Inflation: 5%
Staking participation: 50%+

REAL WORLD APPLICATIONS

GoodDollar: Leverages yield-earning DeFi products and a digital coin to deliver Digital Basic Income on a global scale. A top five dApp globally - by the number of daily users according to DappRadar.

Peepl: Sustainable local economy project backed by the UK government via a $1M grant. Building a decentralized version of Deliveroo including an alternative currency.

Mystic Valley: Events organizer in Thailand that exclusively uses Fuse's technology stack for payments including a customized version of the wallet. Over $1.3M transacted at the last event.

Kolektivo Labs: Regenerative economy project in Curaçao headed up by leading DAO experts from the Ethereum ecosystem. Leverages Fuse for high-speed, low-fee sending and receiving of the island's digital currency, CuraDAI.

Comunitaria: For-profit technology and services company that helps charities efficiently target aid to those in need whilst promoting economic recoveries in local neighbouhoods.

Flambu: A sharing economy platform on Fuse. Mobile app plus crypto wallet and a two-token system for rewards and payments

GoodDollar · bitazza · Comunitaria · peepl. · Kolektivo · flambu

FUSE CORE TEAM

Mark Smargon
Founder & CEO

Robert Miller
PR & Communications

Isaac Rodgin
Strategy

Carl Anthony
Business Development

Mikhail Nekrasov
CPO

Leon Prouger
Lead Tech

Daniil Gorbatenko
Partnerships & Content

4 Solana

Key Takeaways

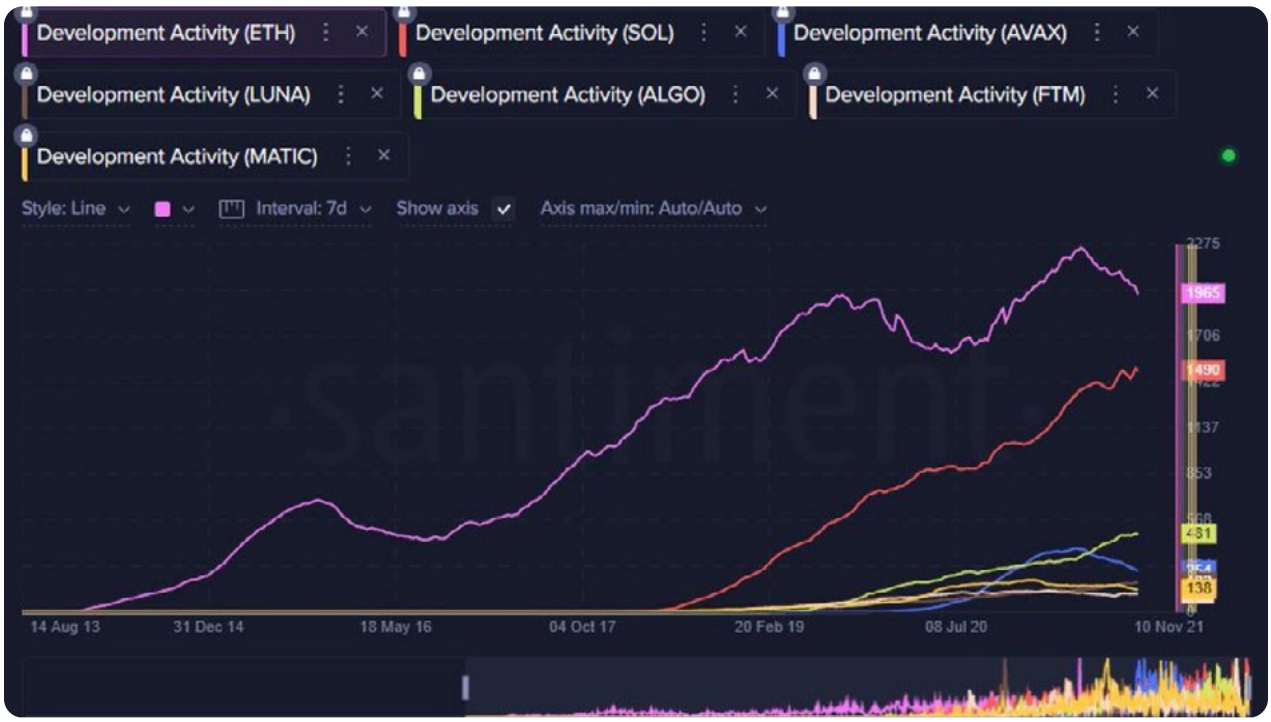
- Solana wants to offer Nasdaq performance on a blockchain.
- Backed by Sam Bankman-Fried and a16z, SOL was one of the highest ROI assets in 2021.
- Large holdings by VCs and the team mean the rug could get pulled from under smaller investors.

Named after a famous beach near San Diego, California, Solana is the brainchild of former Dropbox engineer Anatoly Yakovenko. Development started in 2017, and in April 2018, he and his co-founder, Greg Fitzgerald, secured their first backing from Abstract Ventures and 500 Startups. Solana had its big break in 2020 when Sam Bankman-Fried backed the project. He successfully deployed FTX's decentralized exchange protocol, Serum, on Solana. In 2021, Polychain Capital and a16z injected $314 million into the blockchain venture with a private token sale.

Driven by DeFi activity and NFT sales, Solana rose to prominence the fall of 2021. Constantly pushing the envelope, its team now wants to onboard "one billion users" in the following years.

Solana's beta mainnet saw the light of day in March 2020 and quickly attracted developer attention. According to recent research, it is on a path to overtake Ethereum when comparing developer activity in the form of GitHub commits, pull requests and forks.

Figure 20 Solana developer activity exhibits substantial growth



Source: *Twitter*

4.1 Real-World Use and Adoption

This chapter will focus on metrics that reflect the real-world usage of Solana. Looking at the meteoric price growth is a good indicator of investor confidence. To gain a deeper understanding, we'll look at unique addresses, lending and staking rates, and protocol revenue plus the price-to-sales ratio.

As a marker of centralization risk, we'll finally look into how many tokens are held by the team and VC backers.

SOL token price and market capitalization

Solana's (SOL) price was on an absolute tear starting in August 2021, called "Solana Summer." The token's value rose from $35.15 to a high of $258.65 between Aug. 1 and Nov. 6, 2021. A boom in NFT sales, perpetual futures volume and a tight-knit community propelled Solana's market capitalization to more than $73 billion and made the token No. 4 on the CoinMarketCap list of coins sorted by market cap at times.

Seen from a November 2021 perspective, Solana is up more than 130x from a year ago and outperformed all other top 100 tokens except Axie Infinity (AXS), Kadena (KDA) and Fantom (FTM). **[Figure 21, 22]**

Solana unique addresses

Solana's implementation is fundamentally different from Ethereum's. On the latter, programs can hold state; on the former, they cannot. A program's state is the data it uses. For example, one piece of data could be an incremental counter that assigns a number to NFTs as they are minted. This incremental counter would be stored in a program's state on Ethereum, which Solana cannot do.

Instead, Solana uses accounts to store and access data. Accounts can also store multiple addresses to send and receive tokens. Like Ethereum with its ERC-20 standard, Solana also supports tokens built atop it. Unlike Ethereum, every token needs an address of its own, which is then part of an account. It is a bit similar to Bitcoin's HD wallets[22] in practice, but with a different implementation and functionality.

To make a long story short, we will look at active accounts instead of unique addresses. Though this number is difficult to pinpoint accurately, research from CoinDesk and Solana Beach[23] arrives at a substantiated estimate of 1.2 million active accounts.

Solana protocol revenue and price-to-sales ratio

One of Solana's most vital selling points is its low transaction fees. Currently, a transaction costs $0.00025. Transactions on Solana are a bargain compared to Ethereum, where a Uniswap trade frequently costs over $100. Conversely, these low fees lead to lower protocol revenues.

The Graph reports earnings of just $3.2 million for Solana, while Ethereum miners gained $1.5 billion in the 30 days leading up to Nov. 16, 2021.

Looking at the price-to-sales ratio, Solana lands on a multiple of 30,909x earnings, while storage protocol Filecoin has a multiple of "only" 514x.

Solana is in a difficult position from a price-to-sales perspective. On the one hand, it needs low fees to remain attractive for traders and financial applications. On the other hand, SOL's price is hard to justify at this point. **[Figure 23]**

Staking and lending rates for SOL

SOL holders enjoy a variety of options for putting their tokens to work. Non-custodial staking is available in the Exodus wallet or with the native Solana-CLI command-line tool.[24] Staking rewards are around 7%–7.5% APY at the time of writing.

Custodial staking is possible on Binance Earn, Kraken and FTX and, typically, offers fewer earnings. Binance Earn offered 6.5% APY this November 2021.

Then there's lending on platforms such as Solend or Tulip Finance. Even staked SOL can be lent on Tulip, albeit for a meager 1.79% yearly yield, while Solend offers 3.87% for supplied SOL.

Lending becomes more exciting when providing stablecoins. Solend offers 24% on USD Coin (USDC), and Tulip grants 15% APY on USDC-USDT pairs via Raydium.

[22] See "10 Steps to a Better Bitcoin Wallet", Evander Smart, Cointelegraph, July 18, 2015
[23] More information about Solana supply here
[24] Learn more about Solana staking here

Figure 21 Solana Summer: SOL price rose more than sixfold in autumn 2021

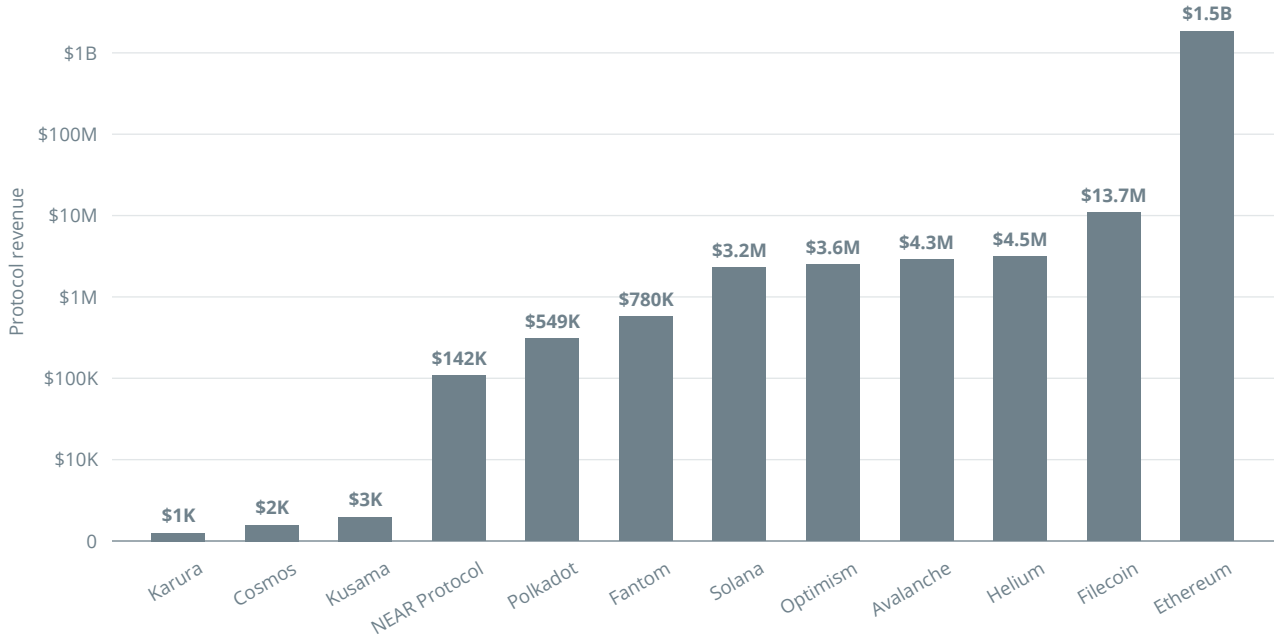
Source: *Messari*

Figure 22 YTD gains on Nov. 15, 2021

Name	Axie Infinity AXS	Kadena KDA	Fantom FTM	Solana SOL	Polygon MATIC
Price	$144.42	$22.15	$2.6	$242.88	$1.76
YTD%	▲ 24,269.3%	▲ 15,204.62%	▲ 14,968.17%	▲ 13,106.92%	▲ 9,777.48%

Source: *CoinMarketCap*

Figure 23 Solana 30-day protocol revenue is just $3.2 million vs. Ethereum's $1.5 billion



Source: *Token Terminal (Y-axis has a log scale.)*

Solana initial coin distribution breakdown

The degree to which Solana is decentralized was the subject of heated controversy on Crypto Twitter this autumn. The pièce de résistance is the number of tokens held by the team and by VC backers. Solana has an initial token supply of 500 million SOL with a yearly inflation rate of 1.5%.

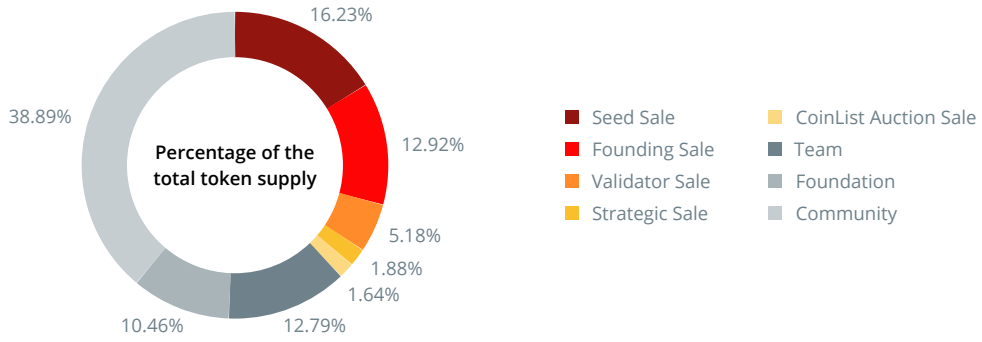
Binance Research found out that the team holds 12.79%, and VCs bought 29.15% of all tokens during the seed and funding sale, a total of 41.94%. **[Figure 24]**

The pie chart doesn't include the $314.15-million token sale[25] that Polychain Capital and a16z completed in June 2021, and the exact amount of tokens involved was not published. The exchange price for SOL was $30–$40 in the months ahead, though it's probably fair to assume that a steep discount was applied, given the scale of the purchase. Presupposing a $20 token price, 15.7 million SOL or 3.14% of the initial supply would have changed hands.

Staking validators have to pay transaction fees on voting and syncing transactions but earn staking rewards as well as block rewards. Running a viable validator requires a stake that produces rewards in excess of transaction costs. In September 2021, the minimum stake required had surpassed $1 million[26] — a significant barrier to entry for new validators.

Despite that, almost 1,200 validators are operational at the time of this writing. The top 19 validators control 33% of all SOL staked and could theoretically halt the network if they colluded.

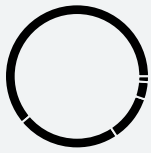
Figure 24 Solana initial token supply distribution



Source: *Binance Research*

Figure 25 Number of validators and staking APY

Validators	Weighted Skip Rate	Nominal Staking APY	Node Versions
1,199	**8.0%**	**7.03%**	**1.7.14** (61.1%)
Superminority: **19**	Non-weighted: **9.2%**		1.8.2 (23.2%) 1.7.15 (10.5%) 1.8.1 (3.9%) others (1.3%)



Source: *Solana Beach*

[25] See "Solana Labs Completes a $314.15M Private Token Sale Led by Andreessen Horowitz and Polychain Capital", Austin Federa, *Solana*, June 9, 2021

[26] Learn more about Solana's controversy here

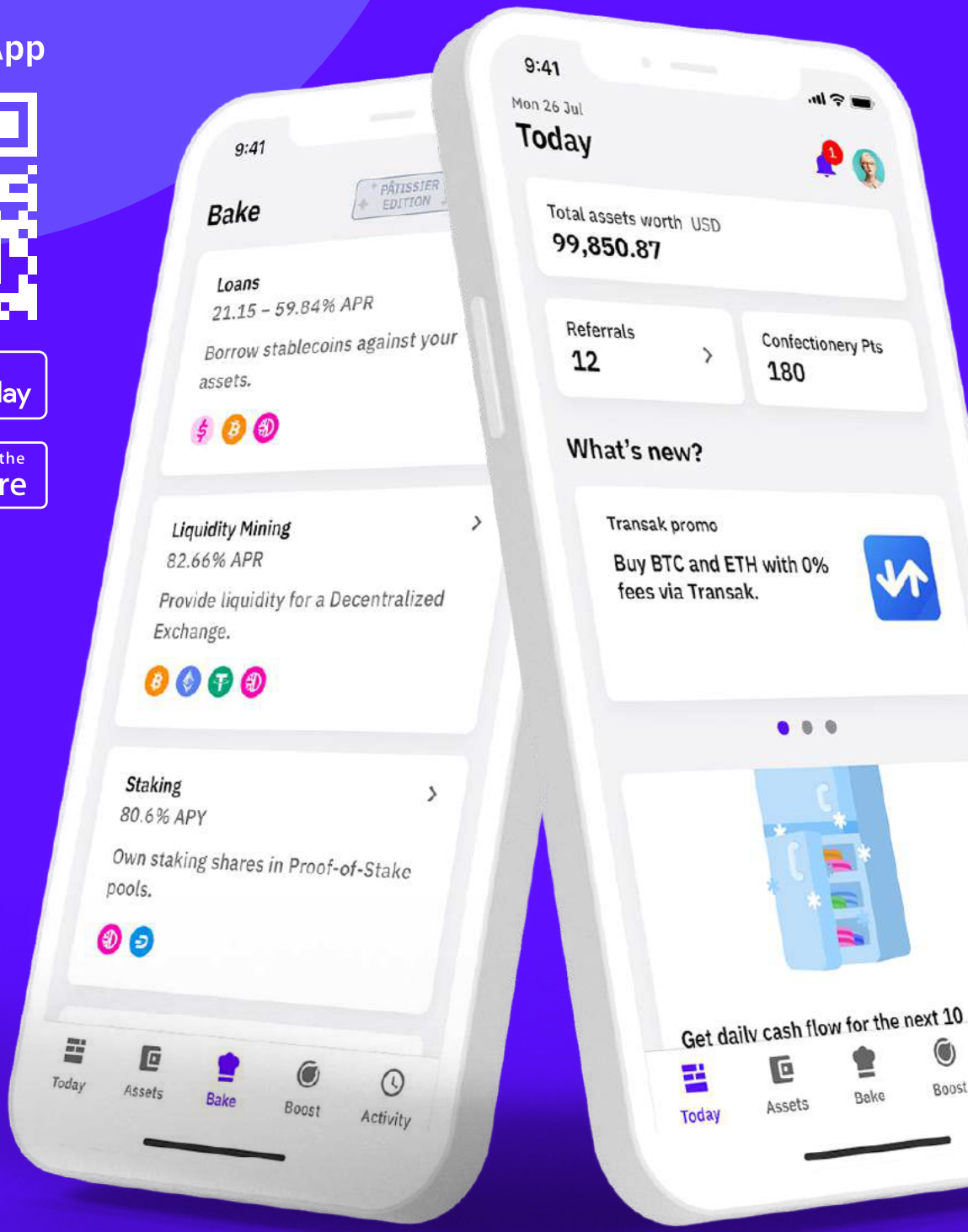
CAKEDEFI

The most transparent way to put your crypto to work

Download App

GET IT ON Google Play

Download on the App Store



4.2 Scalability

This chapter will look at Solana's scalability prowess. How do validators reach a consensus on transactions? What is the network's transaction speed in theory and practice? And what are the advantages and disadvantages of the design choices involved?

Consensus mechanism

Solana has a unique consensus mechanism called TowerBFT and proof-of-history (PoH). Co-founder Anatoly Yakovenko, with a background in distributed systems design, thought hard about blockchain scalability problems in 2017 after Bitcoin transactions took days when demand surged.

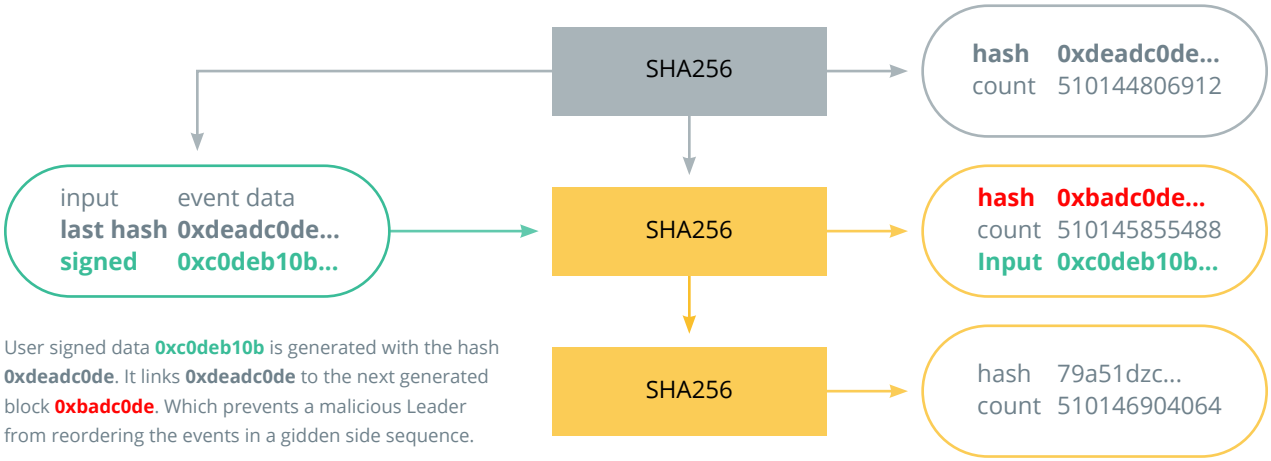
According to an interview with Acquired,[27] he discovered that most consensus issues vanish when the systems involved agree on a common timeline. Take the dreaded double-spend issue, for instance. In a synchronized system, you can assume that the first transaction is valid and the second is thus fraudulent.

Solana implements a surprisingly straightforward method of synchronizing nodes. It uses a sequential hash that runs over itself continuously, creating a rhythm that all nodes follow.

Proof-of-history uses recursive calculations where the previous output is used as the next input. Only with the output of the current function "X" will a validator be able to calculate the output of the next function "Y." All validators need to solve the same function "X" and then be able to derive the output for the next function "Y" around the same time. Like this, Solana creates synchronization across its network. **[Figure 26]**

Besides PoH, Solana uses its version of the practical Byzantine fault tolerance (PBFT) consensus mechanism called Tower. PBFT is an industry standard.

Figure 26 The proof-of-history flow of control



Source: *Binance Research*

[27] See "Special: Solana (with CEO Anatoly Yakovenko)", *Acquired*, July 18, 2021

[28] See "pBFT— Understanding the Consensus Algorithm", Sheffield Nolan, *Coinmonks*, November 19, 2018

Programming language

Solana uses Rust, a recent, functional programming language for programs that run on top of its blockchain and base layer.

Rust has seen a remarkable rise in popularity for blockchain applications thanks to its performance advantages. From a purely technical point of view, it seems like a clear winner compared to Ethereum's Solidity. However, the lack of tooling, libraries and knowledgeable developers means that many wheels need reinventing to get DApps off the ground. The advent of the Anchor framework has ameliorated that somewhat by reducing the amount of work necessary just to get started by 80%.

Average Transaction Fee

Low fees are one of the existential selling points for Solana. As with Ethereum, the actual fee is a function of supply and demand. When demand for block space rises, the price to include a given transaction in a block appreciates accordingly.

Solana features a much higher transaction capacity than Ethereum. We'll cover just how much in the chapter on theoretical transactions per second.

A look at network explorer Solana Beach reveals transactions cost between 5,000 and 10,000 lamports. One lamport equals one-billionth SOL. In dollar terms, the average Solana transaction has cost $0.00025.

Actual transactions per second (TPS)

Between 2,000 and 3,000 TPS are conducted on the Solana network at the time of this report. This number dwarves Ethereum's 35 TPS by almost two orders of magnitude. **[Figure 27]**

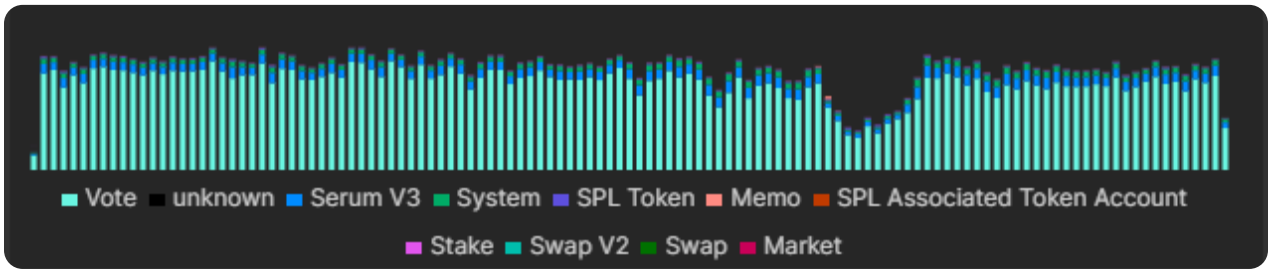
On Solana, 80%–90% of all transactions are used for voting and synchronization, so this number is misleading on its own. Other blockchain projects have ridiculed Solana for its inflated numbers in the past.

Source: Twitter

Avalanche CEO Sirer weighs in on Solana's transaction numbers

Before comparing apples to apples, voting has to be factored out of transaction counts since Ethereum nodes don't vote. Assuming the upper bound of 90% votes, Solana would still process 200–300 TPS or 10x Ethereum at a fraction of the cost.

Figure 27 Solana transaction breakdown



Source: Solana Beach

Theoretical TPS

The first slide in Solana's seed round deck reads: "Solana is blockchain at NASDAQ speed." Solana block times are measured below 400 milliseconds, which demands considerable network speed and node processing capacity. As a result, Solana node requirements[29] are steep. A prospective node needs a 12 core CPU, 128GB RAM (256GB for an RPC node) and a blazingly fast 500GB SSD.

As a proof of concept, Solana's testnet has demonstrated 400,000 TPS on a single machine without any networking, which is almost at Nasdaq speed, where the trading servers handle up to 500,000 TPS.

Out in the wild, Solana's testnet has reached bursts of 59,400 TPS, making it "faster than Visa." In lab environments, 50 nodes were able to conduct 111,609 TPS on their mainnet. Real-world speed in a distributed system with nodes spread across the globe is, of course, affected by available network speeds. **[Table 2]**

Solana's white paper claims that the theoretical limit to its capacity is even higher than 400,000 TPS and will continue to increase as network speeds and node processing capacity rise and network latency shrinks.

Solana's performance is achieved without sharding, which is the approach that Ethereum will implement in its next iteration. With sharding, a blockchain is split up into multiple pieces that work in parallel. Still, it introduces complex problems for DeFi when assets processed on different shards are composed.

Time to finality

Transactions per second are not the best metric to gauge users' felt experience. Crypto influencer Packy McCormick stated that using Solana felt like "using the internet" in his analysis for Not Boring. But what does that mean?

Transactions are only deemed final after three to 12 validators have confirmed them, depending on the desired security level. The time it takes for these three to 12 confirmations is called the **time to finality**. Solana takes five seconds on average, with outliers at 12 seconds — a long time for internet standards.

Research by email client Superhuman revealed that users experience delays of more than 100 milliseconds as noticeable friction. Rival layer-one blockchain Avalanche boasts only 1.3–1.6 seconds to finality.

Table 2 Solana TPS in a lab environment

Node Count	Avg TPS	Max TPS	Avg Confirmation	Max Confirmation
5	35,340	108,302	3.9	22.3
10	35,229	87,586	3.7	11.2
25	32,599	101,845	6.4	23.3
50	31,894	111,609	8.1	39.1

Source: *Solana.blog*

[29] Learn more about Solana Validator requirements here

CRYPTIX

We're hiring:

Problem Solvers

First Movers

Python Whisperers

(Self) Developers

Marketing Magicians

Cryptoholics

Start value building with us today

Join us on our vision to create "The People's Financial Marketplace" in Switzerland, Austria, Slovenia, Estonia, Liechtenstein, Lithuania or remote.

cryptix.ag/career

4.3 DeFi

Thanks to the incredible speed Solana offers, and due to the timing of Solana's market entry coinciding with "DeFi summer," DeFi applications have always been a mainstay for this cryptocurrency. 116 DeFi projects are listed on the enterprise's website as of November 2021. **[Figure 29]**

DeFi is an integral part of any blockchain ecosystem because of the possible earnings generated. While Ethereum miners get paid handsomely via transaction fees, Solana's business is more service-oriented. Cumulative DeFi revenue across all blockchains is set to surpass $3 billion soon, and Solana is well-positioned to grab its share of this emerging market. **[Figure 28]**

Total value locked (TVL) in DeFi on Solana

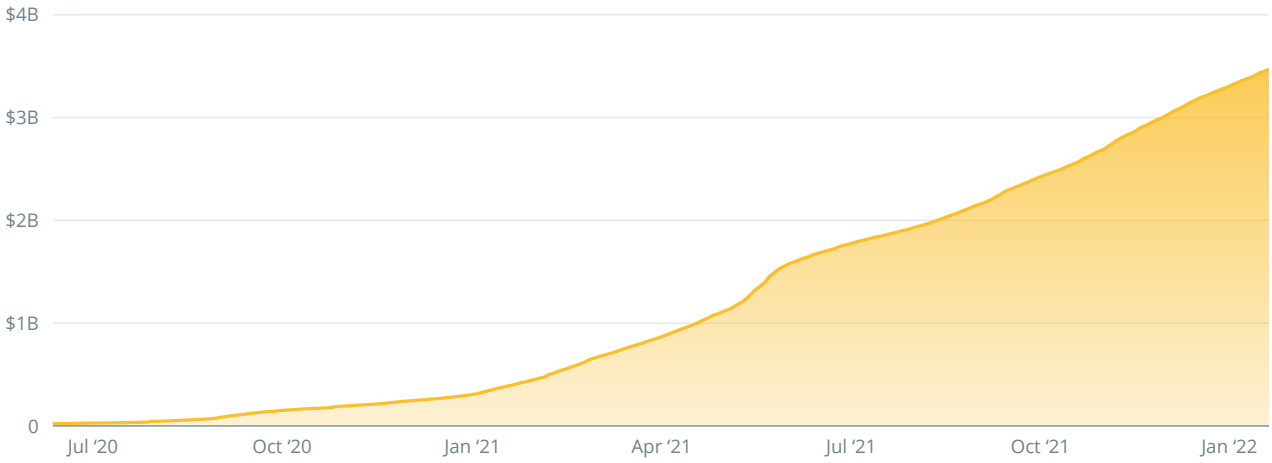
TVL is the total amount locked in a currency's DeFi DApps. The best way to compare TVL is by denominating amounts in native tokens. SOL's price has appreciated 20x since April 2021, and the dollar-denominated TVL would have increased by the same amount without additional SOL locked. **[Figure 30]**

A look at Defi Llama's chart reveals healthy growth until mid-October, followed by a slump. 11 million SOL was locked at the beginning of April 2021 and 81 million SOL in October. $257.6 million of locked value grew to $14.8 billion during the same period. Research by Messari found extraordinary growth of perpetual future trading on Solana. Notably, SOL perpetuals on Solana DeFi grew 60x compared to 13% for Bitcoin perpetuals, showing a tight focus of the ecosystem on itself. **[Figure 31]**

Raydium and Marinade Finance are the two projects with the most value locked, while Mango Markets is the number one futures market. Serum, a DEX and a trading protocol developed by FTX exchange, is another important player.

DeFi is not the only driver of Solana adoption. Digital artists have also embraced the platform's low fees and created some smash hits in the process.

Figure 28 Solana's cumulative DeFi revenue



Source: *The Block Research, Ethereum ETL, The Graph*

Figure 29

Solana ecosystem map

SOLANA

AMM
- Raydium
- Orca
- Saros
- Saber
- Penguin
- Mercurial Finance
- Invariant
- Sencha
- Hydraswap
- Sentre
- MORA
- Atrix
- Cyclos

Wallet Extension
- Coin 98
- Phantom
- Sollet.io
- Slope
- Math Wallet
- Solong
- Solflare

Decentralized Stablecoin
- Terra
- UXD
- Cashio.app
- Mixture
- Soteria
- Epsilon
- UPFI Network
- Sol Invictus

Lending
- Parrot
- Solend
- Apricot finance
- Larix
- Port
- Acumen
- Jet
- Oxegen
- Everlend
- Soda
- Zero Interest
- Solaris

Derivative
- Mango markets
- 0 1
- LIQ Protocol
- Drift
- Symmetry
- Synthetify
- Spin
- Fabric
- Hedgehog
- Incept

Launch Pad
- Solanium
- Raydium
- Dexlab
- Delta Protocol
- Boca Chica
- Solstarter
- Solpad
- Solster
- Solrazr

Others
- Bonfida
- DeFi Land
- Tribeca
- Hxro
- Ratio
- Sonar
- Crate
- Ancient 8
- Stream Flow Finance
- Staking.io
- MeanFi
- BetDex
- Diabolo
- Arrow
- Aver

Options
- PSY Options
- Zeta
- Unk Finance

Staking
- Marinade
- Socean
- J Pool
- Parrot
- Stafi
- Lido
- MonkeDAO

CLOB Dex
- Serum
- Dexlab
- Solape
- Raydium
- Aldrin

Asset Management
- Tulip
- Solrise Finance
- Friktion
- Step
- Jupiter
- Solfire
- almond
- Francium
- Cropper finance
- Sunny
- Dappio
- Plutos Network
- Sypool
- Laguna
- Chest
- Tap finance
- A sol
- Solyard
- Investin
- Prism
- Lifinity
- Bunny Ducky

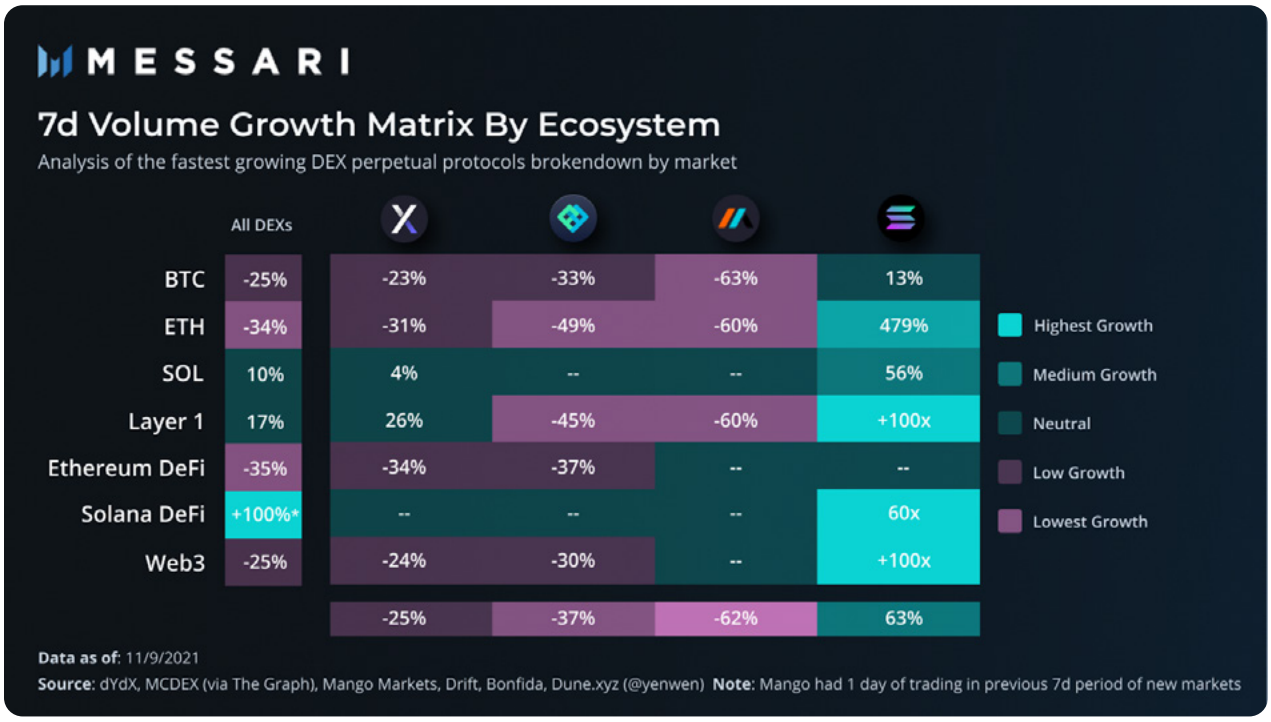
Yield Farming
- Raydium
- Orca
- Saber
- Quarry
- Atrix
- Katana
- Delta Protocol

Source: *Cointelegraph Research*

Figure 30 TVL locked in DeFi on Solana, denominated in SOL

Source: *Defi Llama*

Figure 31 Perpetual future trading volume seven-day growth



	All DEXs				
BTC	-25%	-23%	-33%	-63%	13%
ETH	-34%	-31%	-49%	-60%	479%
SOL	10%	4%	--	--	56%
Layer 1	17%	26%	-45%	-60%	+100x
Ethereum DeFi	-35%	-34%	-37%	--	--
Solana DeFi	+100%*	--	--	--	60x
Web3	-25%	-24%	-30%	--	+100x
		-25%	-37%	-62%	63%

Source: *Messari*

Solana NFT sales and transaction volume

The two top NFT projects on Solana are "Degenerate Ape Academy,"[30] which hit the ball out of the park in August 2021 and sold out in minutes, and rival "Solana Monkey Business,"[31] whose secondary sales have continued growing in the last months.

Total NFT sales reached $247 million in September 2021 and $246 million in October. At the same time, Ethereum NFT sales amounted to $2.2 billion and $1.7 billion, respectively. Most of that volume comes from big-ticket sales such as "CryptoPunks" or "Bored Ape Yacht Club," where a single deal can be worth millions of dollars.

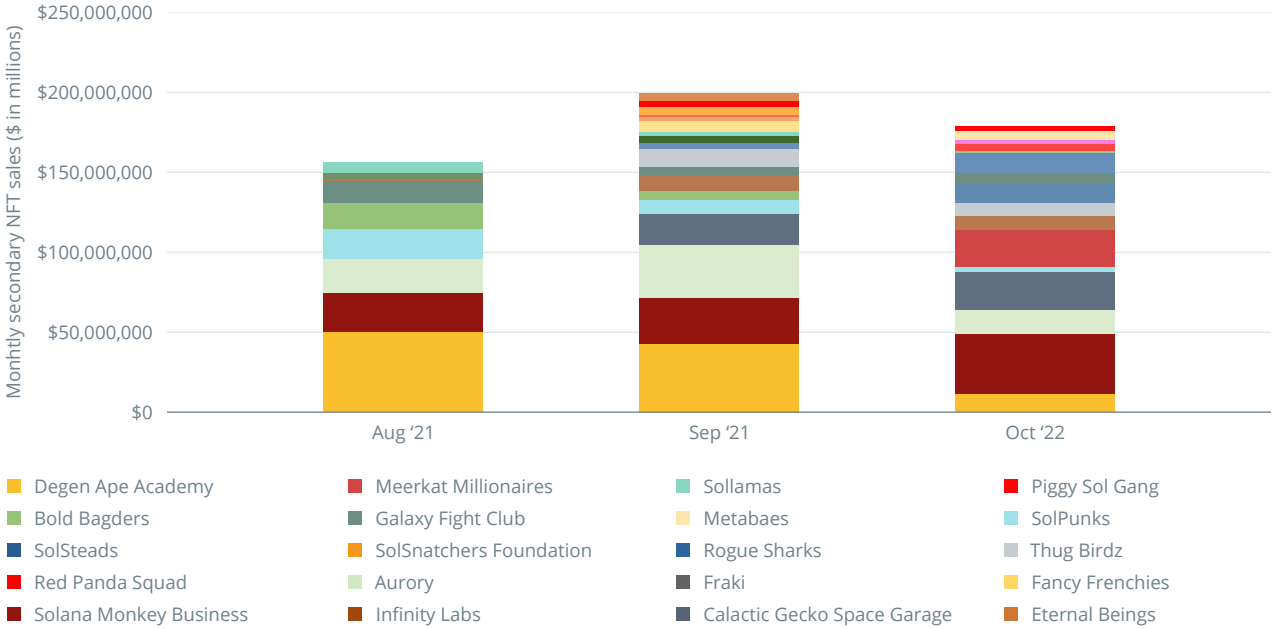
Looking at just the dollar-denominated volume doesn't paint a complete picture, however. Ethereum saw 132,879 and Solana 68,235 unique buyers in October, according to Messari.[32] The average amount paid for an NFT on Solana was $1,097 in October 2021, signifying 224,000 purchases.

From a liquidity standpoint, selling NFTs on Solana might be even more attractive to artists than Ethereum because competition is less intense, and the number of transactions is still half. **[Figure 32]**

Summary

Solana is backed by the high and mighty in crypto, and the project showcases promising technological innovation. Centralization risk is a caveat, but large token holders are unlikely to dump significant amounts of SOL any time soon — not while there is money to be made in DeFi, futures and NFTs. Solana is here to stay. However, Buterin's "world computer" is a force of nature and still the main driver of innovation and value in crypto.

Figure 32 Secondary sales for Solana's top NFT projects from August to October 2021



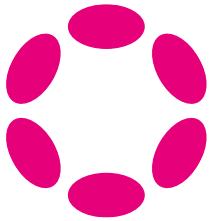
Source: *Messari*

[30] Learn more about Degenape Academy here

[31] Learn more about Solana Monkey NFT collections here

[32] See "Layer-1 of The Rising Sun: Solana NFTs", Mason Nystrom, Messari, November 2, 2021

5 Polkadot



Key Takeaways

- Polkadot is a multichain ecosystem designed for mass adoption using interoperable blockchains.
- Polkadot does not compromise on the blockchain trilemma: decentralization, scalability and security.
- Developed and backed by some of the brightest minds in Web3, Polkadot will arguably emerge as the top competitor to Ethereum.

Ethereum and Polkadot are attempting to accomplish similar goals but through different avenues. Both platforms are infrastructure to replace the internet as we know it, with secure community-owned and -operated networks. Ethereum aims to implement a globally decentralized, un-ownable, digital computer for executing peer-to-peer contracts (smart contracts). In contrast, Polkadot aims to provide a framework for building your own blockchain and an ability to connect different blockchains with one another. Put simply, Ethereum is a world computer, while Polkadot is a blockchain of blockchains.Ethereum's key strength is its large and established ecosystem of developers, users and businesses, including its rich set of developer tools, tutorials, etc. It already enjoys significant network effects from this ecosystem, making it the de facto smart contract platform. Ethereum standards, in many cases, become industry standards, such as ERC-20.

The value of the Ethereum network is similarly significant, providing a high degree of economic security based on the value of the underlying Ether token. The DeFi space, which is one of the areas in the crypto space with the most developer traction, is largely built on Ethereum and leverages the composability among different Ethereum smart contracts that can call one another in the single Ethereum Virtual Machine that powers Ethereum 1.0.

The key challenge facing Ethereum is scalability. The success of the CryptoKitties application demonstrated some of the scalability limits that affect Ethereum 1.0. One popular application was able to significantly degrade the performance and throughput of transactions on the network.

Another challenge is the gas cost required to run smart contracts on the platform. Gas fees are required for the security of the system overall and to protect it from being stalled by runaway programs. But as the value of Ether has risen, gas fees for running smart contracts has also risen and has made certain use cases prohibitively expensive. These costs tie back to scalability because if there were more capacity, the fees for each transaction could be lowered.

Polkadot's genesis

Gavin Wood is a gifted programmer credited with inventing the Solidity language, and consequently, smart contracts. As Ethereum's first chief technology officer, Wood sought to build a decentralized internet capable of hosting uncensorable applications and public good utilities. Despite achieving some of the stepping stones to his vision along the way, he became frustrated by the Ethereum Foundation's slow pace in building Ethereum 2.0. After all, multichain Ethereum 2.0 was always his vision (Ethereum 1.0 — the current proof-of-work version — was supposed to be very temporary).

In 2016, he left Ethereum and founded the Web3 Foundation and Parity Technologies, both of which were tasked with researching and developing the project that evolved into Polkadot — a project bearing close similarities to his vision of Ethereum 2.0. Conceptually, Polkadot intends to form the protocol layer of a new Web3 internet that's fully decentralized, interoperable, secure, private and scalable to billions of people globally.

Figure 33

Polkadot ecosystem map

Polkadot

Canary Network
- Kusama
- Altair
- Basilisk
- Calamari Network
- Crust Shadow
- Darwinia Crab
- Khala Network
- Kpron Network
- Mars
- Polkasmith
- Sakura
- Moonriver
- Genshiro
- Shiden Network
- Karura
- Sherpax

Bridge
- ChainX
- Darwinia
- InterlayX
- pLibra
- Abmatrix
- Snowfork
- Ren
- Pontem Network
- Polka BTC

DApp
- Chads. VC
- DemodyFI
- DTrade
- Local Coin Swap
- Paid network
- Web3 Analytics
- Xaya
- Poolz Finance
- Bridge Mutual
- Patrastore
- Polkasocial
- TrustFI Network
- Kwikswap protocol
- Plethori
- Polkalaunch
- Polkafoundry
- Open emoji battler

Smart Contracts
- Edgeware
- Cap 9
- Patract Labs
- Moonbeam
- Kulupu
- MathChain
- Clover Finance
- Trustbase
- Parastate
- Astar Network

DeFi
- Acala Network
- Bifrost Finance
- Stafi
- Laminar
- Mantra DAO
- Polkaswap
- Bandot
- OAX Foundation
- Rio Chain
- Sora
- Keysians Network
- Equilibrium
- Reef Finance
- Polkadex
- Conversation Protocol
- Zenlink
- Summa Natwork
- Mangata Finance
- RAI Finance
- Polkastarter
- Tidal Finance
- Centrifuge
- Polkacover
- Swing
- Hydra DX
- Polkabridge
- Definsur
- Shadows Network
- Nsure Network
- Polka x
- Bitgreen
- Compound Gateway
- ETHA Lend
- Linear Finance
- Parallel
- Cycan network
- Skyrim Finance
- Nuts finance
- X Predict market
- Crafting finance
- Polkatrain
- Composable finance
- Bholdus
- Polkadog

Data
- Ocean Protocol
- Kilt Protocol
- Dock
- Gunclear
- DatDot
- DataHighway
- Litentry
- Crust Network
- IPSE
- Zentachain
- Subspace

Infrastructure
- HOPR
- Ontology
- Saito Network
- t3rn
- Polkasource
- Avado
- Apron network
- Nutbox
- Ankr
- NDNLink
- Map Protocol
- Polkadomain
- Bluezelle
- OnFinality
- Idavoll Network
- Polkaregistry
- Mask Network
- Polkaname
- Zero.io
- OriginTrail
- Aleph.im
- The Graph
- SEOR

NFT
- DEGO Finance
- Unique Network
- KodaDOT NFT
- RareLink
- Enjin JumpNet
- Bit.Country
- Ternoa
- Anmol Network
- Galital
- Polkacast
- Punk Network
- Uniarts Network
- Treasureland
- Kanaria
- Vera Protocol
- Banksy Finance

Privacy
- Phala Network
- LayerX
- SCS
- Caelum Labs
- Advanka
- Zeropool
- Manta Network
- zCloak Network
- Raze Network
- Automata Network
- Neatcoin
- Evanesco
- Ruby Protocol

Other
- Energy Web Foundation
- Totem
- Asure Network
- Mailchain
- Dipole
- Wiv
- Shift
- TransX
- SubSocial
- Radicle
- MediLedger
- DMScript
- Evercity
- Plain Finance
- Polimec
- Bondly
- Bestay
- Deeper Network
- DIA
- Konomi
- Listen
- Standard Protocol
- StoneDeFi
- SubGame
- Jambo Network
- Rococo
- ELP
- Nuchain
- Plutos Network
- Valiu Liquidity Network
- Zenchain Protocol
- Basin Logix
- OxyDev
- Parami
- Sunrise Protocol
- DOTMog
- Loom Network
- Celer Network
- EverLife.AI

DAO
- GameDAO
- Encointer
- Joystream
- OpenSquare Network
- SubDAO
- SpiderDAO
- Dora Factory

Oracle
- ChainLink
- Kylin Network
- PolkaOracle
- ZK Oracle
- Zeitgeist
- Ares Protocol
- Paralink
- OptionRoom
- Hazel
- ORAO Network

Wallet
- Polkadot-JS
- ZondaX
- imToken
- Enzyme
- Ledger
- Ellipal
- Stylo
- Polkawallet
- Hashkey Hub
- Cobo Wallet
- Mixin Messenger
- Trust Wallet
- Polkavault
- Math Wallet
- Bepal Wallet
- A Token
- Fract App
- Wallet Connet
- Lichen
- yiToken
- Parity Signer
- Lunie
- Airgap
- Safepal
- TokenPocket
- Moonstake wallet
- Fireblocks MPC Wallet
- Speckle OS
- Fearless wallet
- Qbao network
- Hyperpay wallet
- ONTO wallet
- Ao Link
- NGRAVE
- Hashkey ME
- Jadepool custody
- Coin 98 wallet
- Bitkeep wallet

Explorer
- Polkascan
- Polka Analytics
- Polkadash
- Subscan
- Polkapulse
- YieldScan
- Protos
- Polkaview
- Polkastats
- DoTreasury
- Polkacube
- Polkaindex

IOT
- Robonomics
- MXC
- Nodle Lot

Source: *Cointelegraph Research*

Architecture

Both platforms include smart contract functionality, based on Solidity for Ethereum and Ink for Polkadot. If we look at Ethereum 2.0, both platforms are pursuing a scaling strategy based on parallelized execution. Each thread of execution is called a shard in Ethereum 2.0, and a parachain or parathread in Polkadot. One of the biggest differences is design goals. Ethereum aims to be a platform for distributed finance and smart contract execution, whereas Polkadot has a vision of helping people build entire blockchains and integrating these blockchains with one another.

Ethereum 2.0's main chain is called the Beacon Chain. The primary load on the Beacon Chain is attestations, which are votes on the availability of shard data and Beacon Chain validity. Each shard in Ethereum 2.0 is simply a blockchain with the Ethereum WebAssembly (eWASM) interface. Ethereum 2.0 launched Phase 0 of a multi-phase rollout in December 2020, operating in parallel to the legacy Ethereum 1.0 chain. Phase 0 provisioned the Beacon Chain, accepting deposits from validators and implementing proof-of-stake consensus, eventually among many shards. Phase 1 will launch 64 shards as simple chains to test the Beacon Chain's finality. Each shard submits "crosslinks" to the Beacon Chain, which contains the information to finalize shard data. Phase 1.5 integrates Ethereum 1.0 as a shard to finalize the proof-of-work chain's blocks. Phase 2 implements the eWASM interface, phasing out proof-of-work and finally making the system usable to end-users. After the launch of the Beacon Chain in Phase 0, the roadmap was altered to prioritize the transition of Ethereum 1.0's chain from PoW to Ethereum 2.0's PoS consensus, preceding the rollout of shards on the network. The network will also have "side chains" to interact with chains that are not under the finality protocol of Ethereum 2.0.

Like Ethereum 2.0, Polkadot also has a main chain, called the Relay Chain, with several shards, called parachains. Parachains are not restricted to a single interface like eWASM. Instead, they can define their own logic and interface as long as they provide their state transition function to the Relay Chain validators so that they can execute it.

Table 3

	Ethereum 1.0	Ethereum 2.0	Polkadot
Architecture	Single chain	Multiple chains (shards)	Multiple chains (parachains, parathreads)
Backend development	Solidity (JavaScript-like), Vyper (Python-like)	Solidity (JavaScript-like), Vyper (Python-like)	Rust, Substrate Framework
Execution environment	Single VM	Multiple homogenous shards	Multiple heterogeneous parachains
Governance	Off chain	Off chain	On chain (e.g. Democracy, Council, Treasury modules)
Coinsensus mechanism	Ethash Proof of Work	Casper Proof of Stake	BABE/GRANDPA Proof of Stake
Program execution fees	Per-call gas/metering-based	Per-call gas/metering-based	Market cost for parachain slot with unlimited usage or per-call parathread fee

Source: *Cointelegraph Research*

Polkadot, now live as the Relay Chain, only plans to launch the ability to validate up to 20 shards per block, gradually scaling up to 100 shards per block. Besides parachains, which are scheduled for execution every block, Polkadot also has parathreads, which are scheduled on a dynamic basis. This allows chains to share the sharded slots, much like multiple small airlines might share a gate at an airport. In order to interact with chains that want to use their own finalization process — e.g., Bitcoin — Polkadot has bridge parachains that offer two-way compatibility.

Relay Chain: At Polkadot's core is the relay chain, a simple blockchain responsible for coordinating the Polkadot ecosystem of connected parachains. The Relay Chain doesn't support smart contracts to keep its functionality generalized and geared toward governance matters. The Relay Chain is Polkadot's hub and is the site of parachain auctions, governance votes and validation

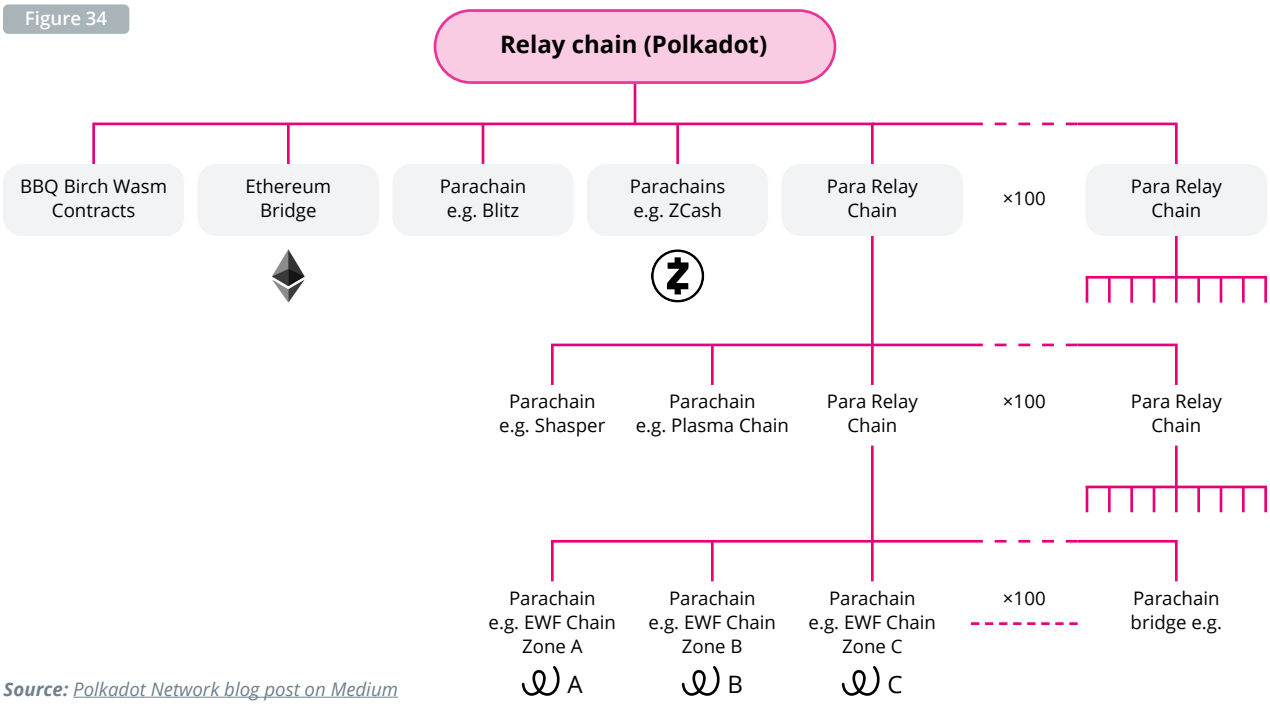
Parachains and parathreads: Whereas the Relay Chain is the hub, parachains are Polkadot's

spokes. Each parachain is a blockchain capable of independently running its consensus algorithm, utilities, tokens and so on.

Because the relay chain doesn't support smart contracts or other specific features, those responsibilities pass onto parachains. However, parachains are not bound to any rules apart from the requirement that they are trustlessly validated. Polkadot limits the number of parachains to 100 — a hard limit creating competition among projects vying to connect to Polkadot. To connect, potential parachains must win a parachain slot auction by outbidding other projects. Once a parachain wins a slot, it bonds Polkadot's DOT tokens to pay for its slot lease (parachain slots are never sold, only leased). If these auctions sound complicated, it's because parachain slots are scarce and Polkadot prioritizes serious, high-quality projects.

Instead of winning a parachain slot auction, a project can connect as a parathread instead. Parathreads are not standalone blockchains; they're meant for DApps wanting Polkadot's scalability, throughput and security without the expense and development associated with building parachains.

Figure 34



Source: *Polkadot Network blog post on Medium*

Consensus mechanism

Ethereum 1.0 uses a single blockchain to process all transactions, run all apps, and validate the network with mining. It does all this while using a slow PoW consensus algorithm that seriously restricts throughput. That's why network congestion is so frequent during high-traffic days. Polkadot eschews the single-chain design for a fully interoperable multichain ecosystem. Instead of using one chain to do everything, the Polkadot philosophy lets different chains specialize and share resources

Both Ethereum 2.0 and Polkadot use hybrid consensus models where block production and finality each have their own protocol. The finality protocols of Ethereum 2.0 and Polkadot both finalize batches of blocks in one round. For block production, both protocols use slot-based protocols that randomly assign validators to a slot and provide a fork choice rule for unfinalized blocks. There are two main differences between Ethereum 2.0 and Polkadot consensus algorithms:

- Ethereum 2.0 finalizes batches of blocks according to periods of time called "epochs." The current plan is to have 32 blocks per epoch and finalize them all in one round. With a predicted block time of 12 seconds, this means the expected time to finality is six minutes (12 minutes maximum). Polkadot's finality protocol finalizes batches of blocks based on availability and validity checks that happen as

the proposed chain grows. The time to finality varies with the number of checks that need to be performed (and invalidity reports cause the protocol to require extra checks). The expected time to finality is 12–60 seconds.

- Ethereum 2.0 requires a large number of validators per shard to provide strong validity guarantees. Polkadot can provide stronger guarantees with fewer validators per shard. Polkadot achieves this by making validators distribute an erasure coding to all validators in the system so that anyone — not only the shard's validators — can reconstruct a parachain's block and test its validity. The random parachain–validator assignments and secondary checks performed by randomly selected validators make it impossible for the small set of validators on each parachain to collude.

The DOT token

Polkadot's native utility token, DOT, is used for multiple purposes, including bonding, governance and staking.

Bonding: To earn a parachain slot, projects must raise and bond DOT tokens. While some projects will have private venture capital funds to acquire DOT tokens, others will source them publicly via crowdloans. Polkadot crowdloans are a crowdfunding model for borrowing DOT tokens from the public. In exchange for bonding your DOT tokens during a crowdloan, the project in question gives an amount of its native token. An interesting aspect of DOT bonding is that your tokens are always yours. When you lease them to projects raising DOT for parachain auctions, the tokens never actually leave your wallet. Instead, they're delegated from your wallet and are unlocked at the end of the lease.

Governance: DOT tokens are used for voting in governance matters called referenda. Voting on Polkadot referenda is always a yes or no binary — there is no in-between — keeping votes simple. This being Polkadot, there's a twist on governance that gives you more or less voting power. Using voluntary locking, you can lock your DOT tokens to increase voting power the longer the lock duration

Staking: Polkadot is a proof-of-stake network secured by validators staking DOT tokens on the Relay Chain. Staked DOT tokens act as collateral ensuring validators act honestly. If they don't, their DOT tokens are slashed. About 58.9% of the DOT liquid supply is staked, with the average staking reward rate currently standing at ~12% on exchanges, such as Kraken and in the Polkadot.js wallet.

With a current price of $38 and a circulating supply of just under 1 billion, DOT has a market capitalization of ~$38 billion, putting it in the No. 8 spot among the top 10 cryptocurrencies ranked by market cap. P/S Ratio, calculated by dividing the fully diluted market cap by the annualized protocol revenue is 4,729.70x. The cumulative protocol revenue (share of fees that goes to the protocol's treasury or directly to its token holders through e.g. a burn mechanism) for Polkadot is $81,930 (seven-day) or $719,020 (30-day), while the annualized revenue totals $7 million. The burn mechanism is similar to a stock buyback because it decreases the amount of tokens in circulation. There are a total of 808,000 addresses that hold DOT, with 27,130 addresses being active.

Figure 35 **Polkadot** (DOT)

DOT Price
$38,22

24 hours	−5.81%	7 days	
30 days	−8.32%	180 days	
ATH $54,9		ATL $2,70	

Circulating market cap $41.31b	Total revenue 30 days $719.02k (+236.97%)
Annvalized total revenue $8.75m	P/S ratio 4,729.70x (−44.44%)
Annvalized transaction vol $353.,27b	
Fully diluted market cap –	Protocol revenue 30 days $575.21k (+236.97%)
Annvalized protocol revenue $6.99m	P/S ratio 5,912.12x (−44.44%)
Total value locked –	

Source: *Token Terminal*

Initial coin distribution breakdown

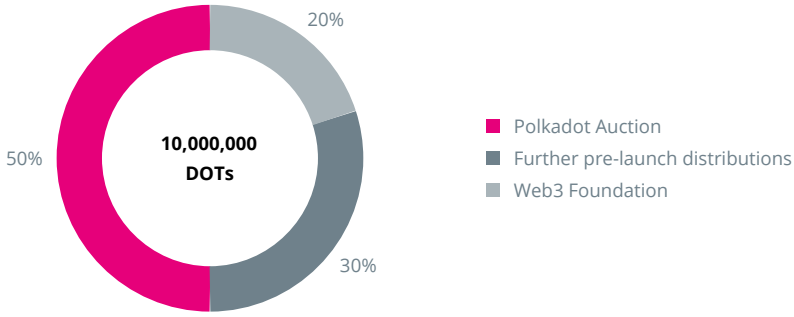
To date, Polkadot has raised roughly $200 million from investors from two sales of its DOT cryptocurrency, making it one of the most well-funded blockchain projects in history.

In October 2017, Polkadot raised a staggering $144 million in its token sale, which was one of the largest on record at the time. But Polkadot also had the misfortune of being one of the many victims of a hacking incident that was using Ethereum wallets at the time, resulting in some of Polkadot's funds being inaccessible — an issue The Foundation fortunately managed to resolve.

The total token supply of Polkadot was 10 million, which is far smaller than other digital currencies (Bitcoin has a rather small supply of 21 million tokens in total). Polkadot had its first crowdsale from Oct. 14 to Oct. 27, 2017, during which it sold 50% (5 million DOT) of the total supply through what was called a Spend-All Second-Price Dutch Auction.

Polkadot was redenominated on Aug. 21, 2020, after the Polkadot community approved a redenomination proposal. The redenomination did not affect the actual supply of DOT but changed the number of Plancks (the smallest unit of DOT, analogous to Satoshis in BTC) that constitute 1 DOT. Before the change, 1 DOT was 1^12 (1,000,000,000,000) Plancks, while it is now 1^10 (10,000,000,000) Plancks after the change.

Figure 36 Polkadot initial token supply distribution



Source: *Polkadot Network*

The average transaction fee currently on the Polkadot networks is 0.1 DOT or $3.8. Polkadot uses a weight-based fee model as opposed to a gas-metering model. As such, fees are charged prior to transaction execution; once the fee is paid, nodes will execute the transaction. Fees on the Polkadot Relay Chain are calculated based on three parameters:

- A per-byte fee (also known as the "length fee").
- A weight fee.
- A tip (optional).

The length fee is the product of a constant per-byte fee and the size of the transaction in bytes. Weights are a fixed number designed to manage the time it takes to validate a block. Each transaction has a base weight that accounts for the overhead of inclusion — e.g., signature verification — as well as a dispatch weight that accounts for the time to execute the transaction. The total weight is multiplied by a per-weight fee to calculate the transaction's weight fee. Tips are an optional transaction fee that users can add to give a transaction higher priority.

Together, these three fees constitute the inclusion fee. This fee is deducted from the sender's account prior to transaction execution. A portion of the fee will go to the block producer, and the remainder will go to the Treasury. At Polkadot's genesis, this was set to 20% and 80%, respectively.

The Polkadot advantage

Shared security: Polkadot explains its security model by describing it as pooled security. In other words, each parachain brings additional security to the network, increasing security as it grows. The way Polkadot's shared security works is by allocating the task of validating to the Relay Chain. This makes it nearly impossible for malicious actors to attack a

parachain because its protected by the economic security of the large Relay Chain. As activity and economic incentives on Polkadot grows, the number of validators increases, resulting in more DOT tokens staked thereby increasing the security for the ecosystem.

Forkless Upgrades: One of the most contentious aspects of blockchains is the question of how to upgrade them. Ethereum is community-centric in the extreme, so upgrades are accomplished by forking and creating an entirely new chain. Polkadot's Relay Chain features onchain governance that votes on upgrades. If an upgrade is voted on and passed, it's immediately deployed to the Relay Chain without contentious forking. This way, Polkadot is anything the community wants it to be without resorting to epic hash power fights.

Speed: Ethereum 2.0 is a proof-of-stake network that requires 32 ETH to stake for each validator instance. Validators run a primary Beacon Chain node and multiple validator clients — one for each 32 ETH. These validators get assigned to "committees," which are randomly selected groups to validate shards in the network. Ethereum 2.0 relies on having a large validator set to provide availability and validity guarantees. They need at least 111 validators per shard to run the network and 256 validators per shard to finalize all shards within one epoch. With 64 shards, that's 16,384 validators (given 256 validators per shard).

Polkadot can provide strong finality and availability guarantees with much fewer validators. Polkadot uses nominated proof-of-stake to select validators from a smaller set, letting smaller holders nominate validators to run infrastructure while still claiming the rewards of the system without running a node of their own. Polkadot plans to have 1,000 validators by the end of its first year of operation and needs about 10 validators for each parachain in the network.

Polkadot's greatest strength is Substrate. Substrate is a development framework for creating Polkadot-compatible blockchains, offering different levels of abstraction depending on developer needs. Polkadot was built with Substrate. It dramatically reduces the time, energy and money required to create a new blockchain.

Substrate provides a much larger canvas for developers to experiment on, as compared to smart contract platforms like Ethereum. It allows for full control of the underlying storage, consensus, economics and state transition rules of the blockchain — things you generally cannot modify on a standard smart contract platform.

The design of Polkadot, which allows for shared security within its network, is another strength. Shared security has two key benefits.

First, it reduces the burden on parachain builders by providing security-as-a-service from the Relay Chain. This shared security simplification lowers friction for builders and simplifies the process of launching a new parachain.

Second, shared security provides a framework for parachains to communicate with one another, which ultimately allows parachains to specialize.

Ethereum has a dominant position and the largest developer community of any developer-oriented platform. Furthermore, there are a lot of new platforms coming to market that are looking to compete with Ethereum and gain developer mindshare. At present, there are only so many developers to go around. We are in a situation where there are more developer platforms than there are developers to support and build on them. The real challenge for Polkadot is getting enough traction and building enough of an ecosystem and developer community for the network effects of its architecture to start to kick in.

Summary

It took Wood over three years to carefully design and develop the Polkadot ecosystem without compromising the blockchain trilemma. While in theory, Polkadot checks most boxes to emerge as the No. 1 competitor to Ethereum, but the technology is still new and unproven. However, the wheels have been set in motion, and with such strong fundamentals, the developer community has been flocking to the ecosystem. GitHub shows Polkadot having the second-most average daily development activity in the past 30 days. It is now a matter of when not if Polkadot will emerge as the top three blockchain ecosystems.

bitpanda pro

The secure European exchange for crypto-to-fiat markets.

Fully EU-regulated

Bitpanda Pro has a PSD2 licence issued by the Austrian FMA and is AML5 compliant. By staying on top of the latest cryptocurrency regulations, we have built a strong foundation for safe and reliable trading.

State-of-the-art API

REST and Websocket API connections allow traders to easily integrate with the platform, utilise trading bots and get real-time access to all relevant market data to help them achieve all their investing goals.

Advanced order types & low fees

Alongside Market and Limit orders, Bitpanda Pro allows for advanced order types including GtC, GtT, IoC and FoK. We also offer some of the lowest trading fees compared to similar exchanges.

Popular European fiat markets

We give you access to high liquidity for the most popular European crypto-to-fiat pairs including BTC/EUR, BTC/CHF, ETH/EUR and many more. Our list of supported fiat markets will soon include GBP and TRY.

Visit us on www.bitpanda.com/pro

6 Algorand

Key Takeaways

- Algorand uses an adapted version of PoS, which is called pure proof-of-stake for validating blocks into its chain, believing it as a solution to the blockchain trilemma.
- Algorand uses a unique staking process where no delegation is required.
- The network experienced considerable growth and adoption in 2021, and its future looks bright.

Algorand was founded in late 2017 as the brainchild of the renowned Italian Massachusetts Institute of Technology professor Silvio Micali. The 2012 Turing Award winner, celebrated for his contributions to cryptography through instituting zero-knowledge proofs, contrived the idea behind the network in hopes of addressing the blockchain trilemma of security, decentralization and scalability proposed by Ethereum co-founder Vitalik Buterin. Although the network's mainnet had launched in June 2019, the inventive protocol didn't pick up steam until 2020, which featured the network's major upgrade, Algorand 2.0. The network's uphaul unlocked vital capabilities needed to underpin the creation of sophisticated use cases, such as DeFi services, consistent with the thriving ecosystems on comparable smart contract-based blockchains.

Algorand is administered by the nonprofit Singapore-based Algorand Foundation, which concurrently commissions the for-profit Boston-based software company Algorand Inc. to nourish the development of the network. Algorand's native token, ALGO, has been lagging behind the rest of the large-cap crypto assets over the current extended bull market due to its disputable tokenomics and its what-was-once-restrained base layer — two aspects that were addressed over the course of 2021.

How Algorand works

Algorand's ability in offering high transaction throughput (1,000 TPS) combined with almost-instant transaction finality (~4.2 seconds) is bolstered by two network designs that help achieve this reality.

The first is the blockchain's unique dual-tier architecture that separates the computationally demanding processes by locating it on the network's off-chain layer (layer two) while designating the on-chain layer (layer one) to host relatively simpler smart contracts-based transactions. The network's two-layer architecture serves to forestall any bottlenecks from materializing. The second is the scalable and randomness-predicated iteration on the PoS consensus mechanism known as pure proof-of-stake.

Architecture

Algorand enables a two-layer architecture. Algorand's on-chain layer one is where the core activity takes place. Baked into the base layer is a set of features that equip the blockchain with the qualities necessary for fortifying its very own DeFi ecosystem and intricate real-world use cases. Among some of these components are Algorand Standard Assets (ASA), Algorand's Virtual Machine (AVM), Rekeying functionality and atomic transfers

ASA is the network's solution to bringing about the creation of four different types of standardized tokens that benefit from the ease, compatibility and shared security of the underlying network, as they are embedded into the blockchain layer itself, rather than being presented through add-on smart contracts. The proposed system is seen as Ethereum's ERC match, designed to normalize the token creation process, allowing the creation of: Fungible in-game points, system credits, loyalty points; nonfungible identity, in-game items; restricted fungible securities, government issued fiat currency; restricted nonfungible tokens

(real estate, regulatory certifications). To create one these, developers are only expected to fill out a form supplying its basic details, including asset and unit name and its total supply for it to be deployed, rather than compiling code. This approach enables fending off certain poor token designs that could jeopardize the asset's security as witnessed by the billions lost in 2021 due to exploitative hacks in Ethereum's DeFi ecosystem.

In addition to homogenizing the tokenization process, ASAs correspondingly capacitate transacting individuals with asset spam protections (ASP) while empowering token issuers with what's known as role-based asset control (RBAC). ASP protects users from receiving assets burdened with reputational or legal risk unless explicit consent to accepting the token is provided by users — an ensuing reality in places such as the United States where citizens are excluded from participating in airdrops due to the U.S. Securities and Exchange Commission's interpretation that they might be violating securities laws. On the other hand, RBAC entrusts token managers with the ability to quarantine certain accounts under investigation or introduce a whitelisting model where only a discrete group of users are warranted to transact, closely resembling schemes to that of the controlled financial environments ubiquitous in traditional finance.

Prior to the release of the AVM, Algorand was initially limited to supporting the creation of stateless smart contracts (ASC1) through its non-Turing complete language transaction execution approval language (TEAL), which restricted introducing complex logic into the applications, as TEAL programs were primarily focused on running basic operations like returning true and false while being used to approve and analyze transactions. Following its upgrade, Algorand's operating system is now capable of hosting DApps built with higher-level languages, such as Python, Reach (simplified JavaScript-like), Clarity and GO, facilitating the implementation of more sophisticated use cases and simplifying the ecosystem's maturity

Atomic transfers strongly position Algorand's main layer as a reliable financial ledger because they enable the frictionless exchange of assets between untrusting parties, almost instantaneously. Due to Algorand's almost-instant finality, transactions are combined together and get either fully executed altogether or rejected with funds reverting to their original users. This functionality opens the door for facilitating expeditious interlacing multi-party and multi-asset transactions that can extend beyond the realm of Algorand's ecosystem.

Rekeying functionality is Algorand's final attempt at fortifying the blockchain as a user-oriented network tailored for seamless use. The feature preserves a public address while interchanging the private key without imposing any structural changes to the account overseeing them both, which in return means that reassigning a contract's ownership is now as seamless as sending a transaction.

Even though computation and settlement can be run on both layers, as evidenced by the feature-packed layer-one smart contract capabilities, computationally intensive DApps are discharged to Algorand's off-chain layer (layer two) to prevent bottlenecks from materializing. Contracts that handle private stock placement, for instance, and need to refer to external databases of certified investors are better kept off-chain, as it is costly to hold sizable data on-chain. Other contracts employing privacy-oriented libraries, such as zk-SNARK, which requires considerable computing power, are also redirected toward the off-chain layer. The mechanism by which Algorand ties the off-chain layer to the main network's security is through randomly selecting a committee of nodes already partaking in block validation and calling on them when the time comes to execute more complex contracts. That way, scalability would be subsumed into the blockchain's core functionality.

Pure Proof of Stake and Block Production

Algorand's democratized variation on PoS, dubbed pure proof-of-stake, is essentially the secret recipe by which the network claims it achieves its holy grail of scalability, decentralization and security. Three properties actualize this reality. First, it democratizes access to network participation by requiring only 1 ALGO as the minimum stake to serve as either a relay or a participation node. Relay nodes are responsible for communicating across the network and ensuring messages are propagated properly, while participation nodes run and engage in the consensus algorithm. Second, it distributes validator rewards to all token holders as opposed to only validators present in the ETH model, amassing them ~4%–6% APY. Third, the aspect of randomness that guarantees a fair

opportunity of participation for all eligible nodes in respect to their stake.

In that regard, Algorand's process to block production, executable over three stages and reliant on on-chain randomness, includes a proposal, soft vote and certify phases. Proposals begin with all eligible nodes looping through the sub accounts they oversee while running a cryptographic primitive, known as a verifiable random function (VRF), to determine which ones are nominated to propose a block in the next stage of consensus based on their hashed proofs.

VRFs, in short, are pseudo-random cryptographic functions capable of providing proof that their outputs were correctly calculated by their submitter, as it is mapped to their public key. They perform similar to a weighted lottery system in that the total number of staked ALGO increases the probability of being chosen as every token acts like it is its own lottery ticket for its owner's address

Selected accounts then transmit their next proposed block linked up with the associated VRF output that substantiates their validity as a proposer. The next stage proceeds with the aim of reducing all block proposals to one. The VRF gets reexecuted to form the soft vote committee where participants are randomly selected to vote for the proposal with the lowest hash value, repeatedly, until a quorum is reached. Finally, the certify vote stage arrives with the formulation of a new committee to testify that the proposed block is absent of any double- or over-spending issues. The committee then votes to certify the block if a quorum is present in an analogous manner to the previous stage.

Algorand's key component in achieving scalability without compromising on either security or decentralization is the element of randomness abstracted in the pure proof-of-stake algorithm and its reciprocal cryptographic sortition mechanism relating to the VRF.

Randomness bolsters security as the proposing or committee accounts are chosen randomly and secretly without any peer-to-peer messaging overhead. Nodes only loop through their accounts and run a personal lottery to validate if they were chosen, meaning that block-producing nodes' identities are concealed, further protecting them against any distributed denial-of-service attacks. Even if they were identified, nodes and committees are replaced intermittently with a randomly selected group in every round of consensus; so, targeting them that late would be fruitless.

Not only does this reduce the chances for a network attack, but it also inhibits the network with its unforkable state. To put in context, miners in PoW-based systems are susceptible to solving the cryptographic puzzle at the same block height, which results in a soft fork of the chain, where the one belonging to the lower-activity chain will be eventually discarded. Within Algorand's consensus, only one block can be confirmed as accounts are randomly chosen to propose the block and form the committee to fill this expectation at once and then replaced by its next random-weighted round of selected accounts.

Every participating node will be eligible to propose and approve a block, relatively proportional to its stake, as it is periodically and randomly chosen per round. There will never be a rigid set of validators controlling the block production process since nodes are randomly rotating, no matter how deep their pockets might be. Finally, randomness ensures scalability is maintained in that a 1,000-member committee along with a single-block proposer will always periodically and randomly rotate to lead new rounds of consensus, at 100M, 1B, and 10B users network scale.

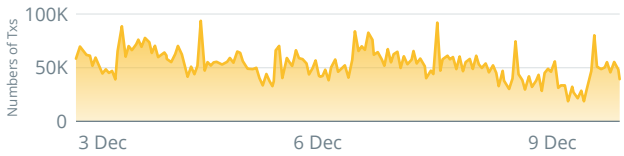
Tokenomics

The ALGO token is the network's native currency and the bedrock for any activity on top of the Algorand blockchain. ALGO is capped at 10 billion tokens that were minted during the token generation event, with only 25 million sold during the first public ICO on CoinList at a price of $2.4 in June 2019. The wide discrepancy between what private investors bought at versus the public price created an initial huge selling pressure, prompting the foundation to offer two buy-back programs in August 2019 and June 2020 for all retail investors who were affected by the chaotic launch, where almost all of the retail investors opted in for redemption, as it was significantly higher than ALGO's current market price.

Figure 37 **Algorand** (ALGO)

ALGO Price	Block speed	TPS
$1.5709	4.4 sec	10.87
	TX cost	Accounts
	$0.00157	16,717,348

Transaction history (one week)



Source: *https://algoexplorer.io/*

When it comes to its utility, ALGO is used as a medium of exchange to pay for storing data and processing transactions. The token is also used as an instrument to participate in the network's consensus by allowing any individual with at least 1 staked ALGO to become a validating node, contribute to the block production process, and secure the network. Finally, ALGO will be also used to participate in the newly rolled out community governance, while locking the token for a predefined period enables holders to vote on the root governance matters, in addition to yielding further rewards of ~17% per quarter as a result of governance participation.

Algorand's initial tokenomics projected that the entire supply of 10 billion should be reached by 2024, with 2.5 billion allocated for communal ALGO sales, 1.9 billion for ecosystem support, 3.1 billion for incentivizing an early relay node runners program, 500 million for the Algorand Foundation, and 2 billion will be dedicated to the software company Algorand Inc. Listening to the community's criticism nevertheless, the token distribution has been updated with a focus on rewarding participants that can prove their commitment to the long-term growth of the projects through staking for a lengthy period — to be extended until 2030 with the revised distributions below as well as the protracted token release schedule.

Algorand Ecosystem

The carbon-neutral blockchain did not really pick up steam until last year. Early 2020 saw the Algorand 2.0 network upgrade introducing some of the layer-one capabilities that make up the present foundation of the blockchain's core functionality, such as stateless smart contracts, atomic transfers and the ASA protocol. However, it was the debut of stateful smart contracts in August 2020 that set the ball rolling for Algorand to garner attention as it became capable of servicing the exciting new wave of DeFi projects currently being developed on top of the network. **[Figure 38]**

Few players understood Algorand's potential early in the journey as initial rounds of adoption saw Algorand ink partnership with the Marshall Islands to underpin the issuance of their central bank digital currency while integrating conventional stablecoins such as USDC and USDT onto the network to cater to DeFi's rudimentary substratum. Algorand also collaborated with SIAE, the largest Italian copywriting agency, to issue 4 million NFTs representing over 95,000 creators as ASAs. This complemented another coalition with planetwatch, an environmental monitoring service designed for capturing data to operate air-quality sensors in hopes of maintaining a global air quality ledger on Algorand's blockchain.

Figure 38 / part 1

Algorand ecosystem map

Algorand

Accelerator/ Incubator
- Neomoon
- WAGMIswap.io
- QMG.finance

AMM
- Ferrum Network
- Glitter Finance
- Tinyman
- Hipo Protocol
- VerdeX Finance
- Bitsoko
- Humble DeFi
- Anirand
- ELEMENT
- Pact
- WAGMIswap.io

Analytics
- WhereDefi
- Tinychart
- Tinybar
- Flipside crypto
- Hallar
- Blockrank
- Algocharts
- Algogator.finance
- Algogems
- Pact

Block Explorer
- Hallar
- AlgoScout

DEX
- VerdeX Finance
- Humble Defi
- AlgoDex
- Pact
- WAGMIswap.io

Oracle
- Verida
- Glitter Finance
- CarbonStack
- @Pay
- ORIGINO
- Algoracle

Art
- X Finite
- Data History Museum
- Crazy Goose Flock
- DRINKITS
- Board
- Captain Squishy PFP
- Kaafila
- Octorand
- Alkemint
- Algo Curator
- Nekoin
- Svansy coin
- Loot Box ASA
- Masu
- Lil Slashers
- Anirand
- Algogems
- Algosprites
- Karen coin
- MAGMA
- Mandalore
- CodeX
- Seedbomb

Developer Tooling
- bountyblock
- Headline Inc
- Tinychart
- Verida
- Opulous
- Visual Studio Algorand Extensions
- TEAL#
- dacade
- STOI
- Irulan
- Data History Museum
- Algonaut.js
- Board
- Algocharts
- Algorand Name Service
- Svansy Coin
- Loozr
- MAGMA
- ASA Stats
- MoonX
- Soundmart
- xFinite Entertainment Token
- Quicknode
- genpyteal

DAO
- A Note Music
- Prismatic
- xBacked
- Vote Coin
- Quantoz
- Nimble
- Glitter Finance
- Gard
- CarbonStack
- VerdeX Finance
- STOI
- Humble DeFi
- Data History Museum
- Hallar
- Blockrank
- NFT Explorer
- AlgoExplorer
- Capi
- Choice Coin
- ASA Portfolio
- Birdbot
- Algo Curator
- AlgoScout
- Nekoin
- ASA Stats
- Anirand
- Algogems
- Lioncoin
- MoonX
- Mandalore
- Zest
- WAGMIswap.io
- QMG.finance

Exchange
- Archax
- Binance
- Coinbase
- Kucoin
- Huobi Global
- MEXC
- The Lovechain
- ExBerry
- Confluence
- Artquare.io
- Opulous
- FXDX
- Nexus ASA
- ELEMENT
- WAGMIswap.io

DeFi
- A Note Music
- Prismatic
- Yieldly
- Venue.one
- Securitize
- Algofi
- xBacked
- Upside finance
- Bleumi Payment
- Shosha
- Quantoz
- Ferrum Network
- Where Defi
- Tinychart
- Nimble
- Zone
- Glitter Finance
- Folks Finance
- Gard
- Mari Coin
- @Pay
- Hipo Protocol
- Opulous
- VerdeX
- Oystro
- ORIGINO
- STOI
- Humble DeFI
- Board
- Algo Charts
- C3 Protocol
- Capi
- AlgoScout
- Svansy Coin
- Nexus
- Defly
- SmileCoin
- Loozr
- ANIRAND
- MAGMA
- Nexus ASA
- Element
- MoonX
- Soundmart
- Mandalore
- Zest
- xFinite Entertainment Token
- Neomoon
- AlgoStake
- Pact
- WAGMIswap.io
- QMG.finance

Decentralized Identity
- SecureCerts
- Dizme Ecosystem
- CarbonStack
- Verida
- Hallar
- Blockrank
- NFT Explorer
- AlgoExplorer
- AlgoScout
- Algo Curator
- ASA Stats
- Algogems
- Mandalore
- MailChain
- QMG.finance

Governance
- Prismatic
- xBacked
- Alty
- Glitter Finance
- Dizme Ecosystem
- Gard
- Verida
- Artquare.io
- Ecosteer
- Choice Coin
- SecureCerts
- Loot Box ASA
- Algo Faucet
- Anirand
- Algogems
- Zest
- Seedbomb
- Mailchain
- WAGMIswap.io
- QMG.finance

News Sharing
- Alty
- Awesome Algorand
- Gard
- Algopulse
- The Lovechain
- Kryptonurd
- Algo Curator
- Algo Gaming Guild
- Citrust

Source: *Cointelegraph Research*

Figure 38 / part 2

Algorand ecosystem map

Algorand

NFT
- A Note Music
- X Finite
- Opulus
- Vesta Equity
- Securitize
- Dequency
- Shosha
- Epoch
- AI Goanna
- Sign.net
- Meadow Labs
- Zestbloom
- Zone
- Glitter Finance
- Dartroom
- Aorist
- Anterdit
- Algoworld
- AlgoFractals
- Musa NFT
- Flex NBA
- Algo Leagues
- Arcadian Tales
- The Lovechain
- SockHodler
- AB2 Gallery
- Algo Cleanup
- Affluence
- Artquare.io
- Opulous
- Abris.io
- NF Domains
- ORIGINO
- The Drone Racing League
- Kollektor.io
- Data History Museum
- Crazy Goose Flock
- DRINKITS
- Board
- US Algo
- M.N.G.O.
- Captain Squishy PFP
- Raccoon Squad
- Zenny Casino
- Algo Fotos

NFT
- Tinywhales
- Algowhales
- Octorand
- Rally
- AlgOcean
- The Parliament of AOWLS
- Birdbot
- tinyhorse
- The Algonauts
- Space Pilots of Algorand
- Nekoin
- Algo Gaming Guild
- Extremely Bullish
- Svansy coin
- Angry Penguins
- Algopard NFT Collection
- MASU
- Buzzy bees
- Lil Slashers
- Pyrenees Pack
- Anirand
- Aegir tactics
- Algogems
- alienprideart
- Algo Sprites
- Karen Coin
- MAGMA
- Randy Cones
- Randy Pixels
- 123NFT
- Element
- Soundmart
- Mandalore
- The GIF Economy
- xFinite Entertainment Token
- CodeX
- Kissbits
- Seedbomb
- Algocats
- WAGMIswap.io
- QMG.finance
- Industrial Punk
- Coffee DAO

P2E
- X Finite
- The Drone Racing League
- Rally
- AlgOcean
- AlgoVegas
- tinyhorse
- Extremely Bullish
- LootBox
- SmileCoin
- Parsec
- Lil Slashers
- Anirand
- Super
- Aegir tactics
- MAGMA
- AlgoSprites
- WAGMIswap.io
- QMG.finance
- MoonX

Investment Fund
- Securitize
- Hivemind Capital
- Ferrum Network
- Dizme Ecosystem
- Meld Ventures
- The Lovechain
- Verida
- @Pay
- Opulous
- Board
- Xpand Capital
- SecureCerts
- Element
- Soundmart
- Mandalore
- Zest
- Mailchain
- QMG.finance

Infrastructure
- XP Network
- VoteCoin
- Algomint
- Ferrum Network
- Prismatic
- Algonode.io
- Nimble
- Dizme Ecosystem
- Gard
- CarbonStack
- Verida
- @Pay
- Hipo Protocol
- asalp
- Blockrank
- Choice Coin
- Wayru
- Openfabric
- SecureCerts
- Algoneer
- Lioncoin
- Zest
- Neomoon
- QuickNode
- AlgoSTake
- Mailchain
- QMG.finance

Services Provider
- Caffe Barbera
- Prismatic
- A Note Music
- bountyblock
- Securitize

Wallets
- VerdeX Finance
- Pera Wallet
- Securitize
- The Drone Racing League
- Kollektor
- MyAlgo Wallet
- Algogator.finance
- Defly
- WAGMIswap.io

LaunchPad
- Dizme Ecosystem
- Verida
- VerdeX Finance
- Polynize
- Airsho.io
- Algofund
- Capi
- AlgoDAO
- SecureCerts
- Element
- Mailchain
- QMG.finance

Metaverse
- X Finite
- Dequency
- Shosha
- Epoch
- Dizme Ecosystem
- Musa NTF
- The Lovechain
- Verida
- Affluence
- Abris.io
- The Drone Racing League
- Data History Museum
- TruYou
- Rally
- Extremely Bullish
- Svansy coin
- SecureCerts
- Loozr
- Anirand
- MAGMA
- Mailchain
- WAGMIswap.io
- QMG.finance

Stablecoin
- USDC
- Tether USDT

Source: *Cointelegraph Research*

Insider Insight

How is the blockchain impacting the music investment world?

Grégoire Mathonet, CTO and co-founder at ANote Music

When new technologies and traditional markets meet, you can usually expect something big to happen. That's exactly the kind of impact blockchain is making within the investment world and the music industry. Both industries are undergoing a great period of growth and innovation right now, and we're probably just at the start of unlocking the full potential blockchain technology will bring along.

Any kind of investment requires a high level of trust among the involved parties, the confidence needs to be there that allocated funds will receive the rightful amount of shares/returns. The addition of blockchain to the traditional investment methods mark a huge leap forward in that matter. We are proud of the partnership we have with Algorand and the opportunity it provides to our investors to allocate their capital confidently and securely. Our platform's integrated blockchain technology provides infrastructure for transparent financial transactions between investors and artists, fostering trust between the two parties and eliminating the need for onerous two-way audits. Blockchain improves the speed of execution, virtually eliminating the need for ex-post reconciliations, as well as allowing flawless payment of different fiat currencies, in the preferred cryptocurrencies.

For the music industry, blockchain technology is unlocking artistic freedom for creators, while simultaneously bringing a lot more transparency to an industry that often operated behind closed doors. Blockchain applications create easier, more secure and clearer tracking of royalty flows across the entire process of collection, repartition and distribution. At the same time, it's removing counterparty risks with automated royalty payments through smart contracts, eliminating the risk of human error. Of course, the benefits blockchain provides to the music industry as a whole are much wider than just the possible better collection and fairer remuneration, or tracking of watermarked pieces. Some new NFT applications based on utility or collectible functionalities enable investments in artists independent of the actual cash flows or royalties the artists generate. Web3.0 will without a doubt further boost the music sector and push it to new record highs.

At ANote Music, we took the best of those two worlds and merged them into an innovative investment platform. By doing so, we want to make music even more valuable to even more people and position ourselves as one of the pioneering companies in listing music rights to retail investors on the blockchain and allowing those investors to receive royalty payouts as a return on their investments, all while giving a boost to the music industry. It marks the first time fragmented ownership of music rights is enforced through a database that is not dependent on one single company or institution. The integration with Algorand's ergonomic framework underpins our objective to democratise investment in music royalties by delivering seamless user experience at high speed, in an ecological way and at low cost.

To capitalize on the network's upgraded capabilities, Algorand launched its series of accelerator programs — a 12 week initiatives focused on spurring the development of the blockchain's ecosystem via providing funding resources (in partnership with Eterna and borderless capital) and mentorship (technological, economical, marketing) for aspiring projects hoping to build on top of the blockchain. The first iteration, Algorand's Asia accelerator program, which ended in early January 2021, wanted to ameliorate Finance 3.0 as its focal point and saw a curated list of projects accepted into the program to build the foundational stage of financial services. **[Figure 39]**

Some of the inductees included DEXTF (an asset management protocol), StakerDAO (a DAO for governing financial assets), Yieldly (the first full-suite of DeFi services on Algorand), and VeriTX (digital commerce marketplace for exchanging physical assets like medical equipment).

The second half of 2021 was the biggest growth catalyst thus far. First, Algorand's technological stack was updated to include the AVM 1.0 upgrade, which was necessary to predicate the roll-out of more complex smart contracts. It was an equally eventful biannual for the network's funding as borderless capital set forth a $25-million Miami-based fund for investing in projects harnessing Algorand's technology. This was followed by Arrington capital's $100-million advertised fund to back Algorand-focused protocols back in June. In September, SkyBridge Capital allocated another $250-million fund to fuel the growth of DApps building on top of the network.

Activity truly began to forge ahead following Algorand Foundation's decision to launch the $300-million Viridis fund in September, which is focused on growing DeFi on the emerging network, as manifested by the increase of active addresses from last September shown above. Precisely, the capital was to be deployed for bankrolling applications relating to money markets, NFT platforms and synthetics issuance — the ground-laying infrastructure for DeFi. Tinyman, an Algorand-based automated market maker, raised $2.5 million following the fund's announcement and in hopes of securing the required liquidity at launch. The DEX went live on mainnet on Oct. 31, marking the first true passageway to DeFi on the growing blockchain. Yieldly and Tinyman are the only two DeFi applications live on Algorand's mainnet where they attribute a sum of $85 million in total value locked.

The upgrade capabilities, combined with the inflow of capital, unequivocally stirred the development of more complex primitives, such as Algofi (a lending, borrowing market), Algodex (an order-book-based DEX), Mese (a micro-equity exchange), Algomint (a synthetics platform), and saw their deployment to testnet.

Prismatic is an up-and-coming member in the Algorand ecosystem. Prismatic is a treasury management solution and builds tooling for crypto organisations with maximum security and transparency. Treasury management includes efficient multi-sig tooling to save crypto organisations time & money with an on-chain treasury management protocol focused on being a service for decentralized communities and crypto businesses. One of the issues facing these communities is idle assets not being deployed in any useful way. Prismatic leverages Algorand's blockchain capabilities to help these businesses to develop strategies for different market conditions easily, inexpensively, and securely. While Prismatic is on Algorand, it is not limited to helping only decentralized communities on Algorand but any blockchain ecosystem. This expands the reach of Prismatic and Algorand's involvement in the entire DeFi and cryptocurrency space.[33]

Looking into the future of Algorand, the infant blockchain is expected to undergo a performance boost that will witness the block finalization time reduced to 2.5 seconds from 4.5, while the capacity for processing transactions per second will grow to reach 25,000. The improved latency will surmise as a result of adopting an encoding mechanism that utilizes hex transactions (32 bits) over protracted names (with relation to how transactions are specified and

Figure 39

Source: *Defi Llama*

[33] Learn more about Prismatic here

called), while the enhanced transaction throughput will be enabled through the truthful block pipelining mechanism. This is a conceptually similar approach to sharding where a block is proposed without waiting on the finalization of its preceding block.

Considering the influx of VC funding and the blockchain's elevated capabilities, Algorand should be in for a fruitful journey ahead assuming applications gather significant adoption in the coming year. Once the DeFi stack of protocols reaches a relatively mature level and becomes more entrenched, the Algorand Foundation's next move will potentially be launching its own liquidity mining program.

Valuing Algorand

Due to Algorand's fledgling state of development, the network's ecosystem hasn't reached a level of fruition that would make it sensible to conduct an analysis into either its revenue for deducing a P/R Ratio or inferring the network's value based upon its generated fees. Even though a good number of protocols are being built on the network's mainnet, it will still be a while before Algorand's ecosystem matures and enough data can be extracted out of it. Algorand is still in its infancy when compared to other functioning smart contracts-based platforms and layer-one blockchains. This juxtaposition corroborates that ALGO has a long way to go before catching up with a corresponding market sizing similar to its competitors — representing only 2% of Ether's current market value.

Risks

Compared to most Layer-one blockchains, apart from Ethereum, Algorand's mainnet went live just shy of two years ago. In this period, activity had only recently begun ramping up due to the network's new capabilities that accommodate the plethora of complex smart contracts and long tail of Web3 applications. However, with only two DApps live on the mainnet, it shows that Algorand's technology is even less battle-tested than other relatively functioning blockchains, such as Solana and Avalanche, which have hundreds of deployed apps and still have their fair share of issues that are in the process of being addressed. Seeing the big picture nevertheless depicts how early Algorand is to the layer-one blockchain wars.

Seeing how Algorand's operating system AVM now supports creating DApps with five different programming languages, caution should be exercised, as two out of the five (Clarity and Reach) are quite experimental languages that don't have a provable record of stability yet, notwithstanding their prospects.

An issue that originally plagued the blockchain was the degree of centralization present in who ran the introductory round of relay nodes. Even though there are around 100 relay nodes distributed geographically around the world, they're all vetted and appointed through the Algorand Foundation so that that they satisfy the necessary performance requirements and avoid clogging the blockchain. However, this is being addressed with Algorand's community relay pilot program, launched on Nov. 2, 2021, where it began accepting and onboarding more users to increase the diversity of relay nodes, eventually leading to more decentralization.

Finally, due to the network's approach of increasing the block size while reducing block time, the full ledger size of the Algorand blockchain was estimated at 647GB back in May. For context, this figure is aggregated over two years in contrast to Bitcoin's 360GB aggregated over 11 years. So, considering it has exceeded 1 trillion GB by this stage, average users will soon be quoted out of participating as relay nodes due to the unfeasible hardware requirements. Possible workarounds could include introducing zero-knowledge proofs to compress transaction history, or adopting decentralized data storage solutions, such as Arweave.

Blockchains diverting away from EVM compatibility risk sacrificing on the network effect accrued from Ethereum's ecosystem of developers and users accustomed to the workings of the architecture. Algorand has decided to take a longer path by rebuilding from scratch and bootstrapping its own operating system. Thus, adopting Algorand as the go-to platform for underpinning complex smart contracts is predicated on developers appropriating the new developmental environment to create competing DApps to those found on the more familiar EVM-compatible chains.

Another emerging issue, despite its irrelevance at the moment, comes down to instituting a reliable incentivizing mechanism to remunerate early backers of relay nodes after 2024, as their advertised allocation

(25% of ALGO's total supply) will have run out by then. There currently isn't a rewarding mechanism for new entities hoping to join the relay node force.

Summary

Algorand uses a zero-knowledge proof algorithm to solve the blockchain trilemma. Its new consensus mechanism enables the system to be efficient and secure while being sufficiently decentralized. In theory, Algorand's blocks can reach their final state in seconds, and the transaction throughput of the entire blockchain network will be comparable to that of large financial networks. Given the current adoption metrics, it is hard to imagine that Algorand is a threat to Ethereum; however, if the Algorand public chain is fully realized, the project and the entire blockchain industry will benefit greatly. No matter which dimension is analyzed, the project will not lack market attention. With the likes of crypto companies such as Circle developing solutions on the Algorand chain and the government of El Salvador choosing Algorand as the backbone of the nation's blockchain infrastructure, the longer-term picture looks constructive.

The Casper Association is the not-for-profit entity that oversees the ongoing evolution and decentralization of the Casper Blockchain. It provides resources to help accelerate the adoption of the Casper proof of stake (PoS) layer 1 protocol and its growing ecosystem of decentralized applications. Casper is designed to make full use of open web programming standards to quickly build blockchain applications that meet the needs of startups as well as enterprise environments.

Why Casper?

CBC-Casper proof-of-stake

Casper was built off the original CBC Casper specifications designed by Ethereum developers.

Scalable

Projects can choose to build private, permissioned or fully public applications on the network. Casper has weighted Key Management for Accounts and account-level permissions for keys and contracts.

Enterprise Grade

Casper's PoS architecture will enable sharding, a database-scaling solution. What is more, Casper Infrastructure is highly modular making it much easier to upgrade.

Future Proof

Casper has Upgradable Contracts for changing startup and Enterprise Requirements as well as predictable gas fees, and is built using Rust and Web Assembly which ensure Casper evolves as businesses do.

Overview about Entity Structure within the Casper Ecosystem

There are three major organizations in the Casper ecosystem: (1) The Casper Association, (2) CasperLabs, and (3) the Developers DAO. The Casper Association, CasperLabs, and the DEVxDAO are independent of each other but have complementary missions in the Casper ecosystem. They each have their own resources and budgets, and they do not share any directors, officers or employees.

About Casper

The Casper Network is the first live proof-of-stake blockchain built off the Casper CBC specification. Casper is designed to accelerate enterprise and developer adoption of blockchain technology today and evolve to meet user needs in the future. Casper enables full use of open web programming standards for developers to get started quickly using languages they already know including Rust and Web Assembly. Casper is an enterprise grade and highly adaptable future proof blockchain. In that way, it is arguably the only fully decentralized, highly secure, and scalable blockchain.

The CSPR Token

CSPR is the native token to the Casper Network. As a proof-of-stake blockchain, Casper relies on CSPR to reward the validators that participate in the PoS consensus mechanism to secure and uphold the network. Casper users also rely on CSPR to pay network fees for on-chain actions.

Casper's developer grant program

CasperLabs is now partnered with the DEVxDAO to collaborate with the Emerging Technology Association (ETA), a Swiss association, to onboard prospective developers, researchers and scientists who are looking for decentralized infrastructure project funding.

"The team at CasperLabs has built an essential blockchain platform for real-world applications without sacrificing the essential components of usability, cost, decentralization, or security."

Tim Draper, *Founder, Draper Venture Network & Draper Associates*

Learn more

7 Radix

Radix — the layer-one for mainstream DeFi

The rise of DeFi is not only limited by scalability, the focus of the majority of 'Ethereum killers', but also by the complexity of smart contract development that leads to both frequent DeFi hacks (over $1.5Bn to date) and an extreme shortage of DeFi developers. 18 months of research by the Radix team with developers and DeFi project leaders led them to this conclusion — with most projects they talked to citing lack of talent as a more urgent problem than even high fees due to poor scalability. Radix, a layer-1 protocol focused specifically on the DeFi industry, is a solution under development that will not only scale massively, but also make it far easier for developers to build and deploy DeFi dApps in a more intuitive and safe manner.

The chronic lack of developer talent in DeFi — and the shockingly high occurrence of smart contract exploits — are both directly caused by how insecure, unintuitive and complex DeFi development is made by the existing smart contract development paradigm created by Solidity and the Ethereum Virtual Machine (EVM).

Radix spent more than eight years researching and creating fundamental technology approaches for a public ledger network that will not only be scalable, secure and decentralized, but will also deliver a new development experience that will finally allow developers to build mainstream-suitable DeFi apps. Bringing innovation at multiple levels, Radix claims to be one of the industry's leaders with the Cerberus consensus protocol design that is linearly scalable without compromising composability between dApps — and a smart contract development paradigm enabled by a new "asset-oriented" Scrypto smart contract language and Radix Engine virtual machine that is secure, easy-to-use, and tailored specifically for the needs of the DeFi industry.

The Radix mainnet went live in July 2021 with its Olympia release including core token functionality. The next Radix release, Alexandria, occurred on December 15, 2021. This was not an update to mainnet, but it does bring a set of development tools to allow developers to start experimenting with building DeFi apps using Scrypto and a Radix Engine simulator. The next release will be Babylon, expected towards the end of 2022, which will be a major update to mainnet enabling deployment of Scrypto-based dApps as well as a decentralized developer royalty system. Then the Xi'an release expected in 2023 will bring another major mainnet update for Cerberus and full unlimited scalability for dApps.

Cerberus Consensus

One of the most important features of DeFi is the ability for a user to be able to call multiple DeFi applications all at once, and all inside a single transaction. For example on Ethereum, being able to borrow some USDC from Aave, swap the USDC for some wBTC on Uniswap, only to swap that wBTC back for USDC on SushiSwap and then repay the loan of USDC on Aave — all in the time it takes for a single block.

This type of typical DeFi user behavior is technically enabled by a network feature called "atomic composability". While it is quite technical in nature, it underpins a huge amount of the liquidity that is powering the Ethereum ecosystem today. Unfortunately scaling solutions like Ethereum 2.0, Polygon, Optimism, Avalanche, Near and Polkadot

all massively compromise or eliminate this very important feature for DeFi.

At the heart of Radix lies Cerberus, a novel consensus algorithm with theoretically unlimited scalability without compromising atomic composability. Cerberus is able to make use of a data structure with 2^256 individual shards through the world's only truly atomic cross-shard consensus algorithm. With Cerberus, all transactions are cross-shard, with consensus across the relevant shards for a given transaction being "braided" together for that single, atomic transaction, while all other unrelated operations are able to happen in parallel. This allows for uncompromising parallelization of unrelated transactions without stopping the kind of DeFi transactions described above from working. Consequently, this lets Cerberus deliver the kind of scalability that is perfect for the needs of DeFi.

Current scalability solutions, such as Ethereum 2.0, aim to increase their blockchain's throughput, either by using a form of sharding that is unable to support cross-shard atomic composability — and therefore encourage developers to minimize the number of cross-shard transactions — or simply look to use layer 2 solutions like Optimism or Polygon that also do not allow atomic composability between arbitrary dApps on the layer 1. In short, with these solutions the ability to freely compose transactions between DeFi apps in a single block is lost. Hence, current solutions cannot satisfy the need for DeFi and a new solution is needed.

Cerberus, developed by Radix, is a solution to this issue that ultimately takes an entirely different approach to parallelization and sharding that is tightly integrated with the Radix Engine application layer. Cerberus provides "linear scalability" — meaning that the addition of nodes to the network can continue to add additional throughput to the overall network at the same rate without limit. Ultimately this means that Cerberus will give Radix not just an extremely high fixed maximum TPS throughput value, but practically unlimited scalability as more nodes may be economically incentivized to add additional throughput to meet real world demand.

Cerberus's design has not yet been implemented into the Radix mainnet. But to help ensure the design is sound and can achieve the claims made for it, Radix asked consensus researchers at the University of California Davis to validate Cerberus. That team came to the same conclusions, stating that Cerberus can operate in general-purpose fault-tolerant environments and provide linear scalability without significant costs to recover from attacks. Hence, Radix has successfully created an innovative solution capable of competing with the industry leaders, resolving the blockchain trilemma.

Cerberus' predecessor, Tempo, while using a different consensus mechanism demonstrated the underlying sharding approach, delivering 1.4 million TPS in a test deployment.

Finality time is another often-neglected aspect of scalability and Radix Olympia already provides finality well below 5 seconds, while fees are also much lower than those of Ethereum, and should forever remain low due to the unlimited linear scalability of Cerberus.

Scrypto Smart Contract Language

Building deployment-ready smart contracts for DeFi is currently surprisingly complicated. This is because Solidity and other languages used for smart contract development are not adequately tailored to the concept of the needs of finance. For example, tokens, NFTs and other digital assets — used in every DeFi application and transaction — must implement the entire concept of a digital asset and how it behaves from scratch as ERC-20 (or similar) smart contracts each time. The smart contract logic to manage and manipulate those assets then must be built to interact with these thousands of separate smart contracts — and must be very carefully written as each smart contract interaction is another opportunity for error. This makes the whole ecosystem extremely vulnerable to exploits and hacks, as well as to basic human error if a developer fails to catch a potential exploit.

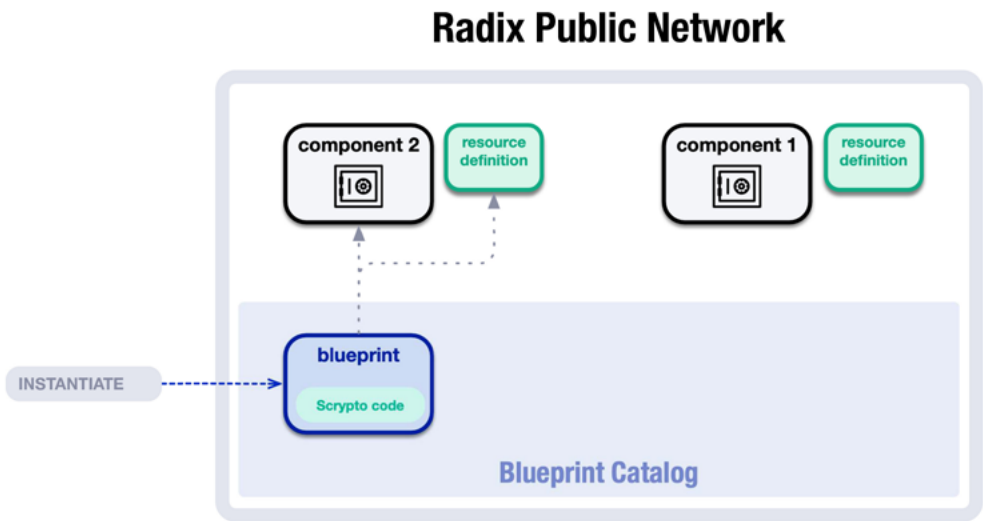
While this is not such a problem for something as simple as a token transfer, coding anything even slightly more complex requires huge amounts of additional time and, potentially, large developer teams. Hence, many resources are spent (and wasted) in the development phase, application functionality is kept as minimal as possible, and the learning curve for deployment-ready Solidity is years long.

This is why Radix has developed a new programming language, based on Rust, called Scrypto. While leveraging Rust's familiar syntax and toolchain, Scrypto adds a large amount of DeFi specific syntax

and functionality making it a purpose-built language for DeFi. This allowed it to be designed to both significantly simplify development of production-grade DeFi apps and make the result more secure — without reducing flexibility as it is still Turing complete.

Scrypto simplifies DeFi development by making "assets" a first-class part of the language — something Radix calls asset-oriented programming. Issuing a token, NFT, or other digital asset is done as a direct system call to the platform for a customized "resource" that automatically provides the desired asset behavior without any development effort. These resources are intrinsically part of the platform provided by Radix Engine. And Scrypto provides a variety of first-class elements like vaults, buckets, and "take/put"-style functions for interacting with resource-based assets intuitively and simply. The end result for developers is smart contracts that are both simpler and much more secure at the same time. For example, a dApp similar to Uniswap can be written with a mere 150 lines using Scrypto.

Scrypto-based smart contracts will be initially deployed to the Radix network as "blueprints" — reusable templates that define core logic, but are not active for use and cannot hold resources. Blueprints are then instantiated into active "components" that can be interacted with via transactions or other Scrypto logic. This separation of smart contracts into blueprints and components means more modularity, more reusability, and a much shorter path to creating standards for common functionality.



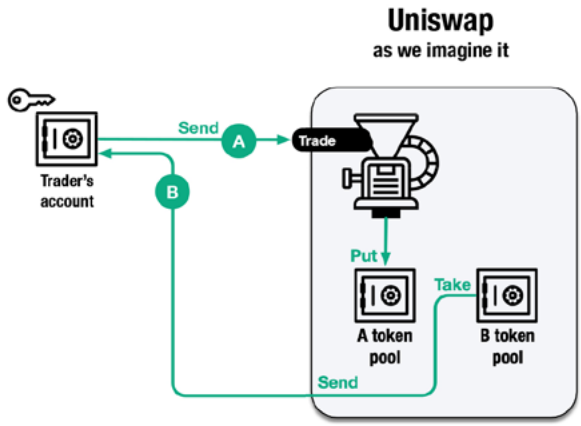
The Radix network will also include a blueprint catalog that will further accelerate development by making blueprints deployed by other developers available for re-use directly. It can be thought of as an onledger repository that developers may use so that common, proven functionality does not have to be re-implemented over and over and can be accessed without additional code. Using a blueprint isn't the same as importing code into a project off-ledger — it is directly requesting functionality that is operational on the network. Hence, Radix aims to create a convenient, safe, and genuinely decentralized open development environment that would attract millions of developers to decentralized finance.

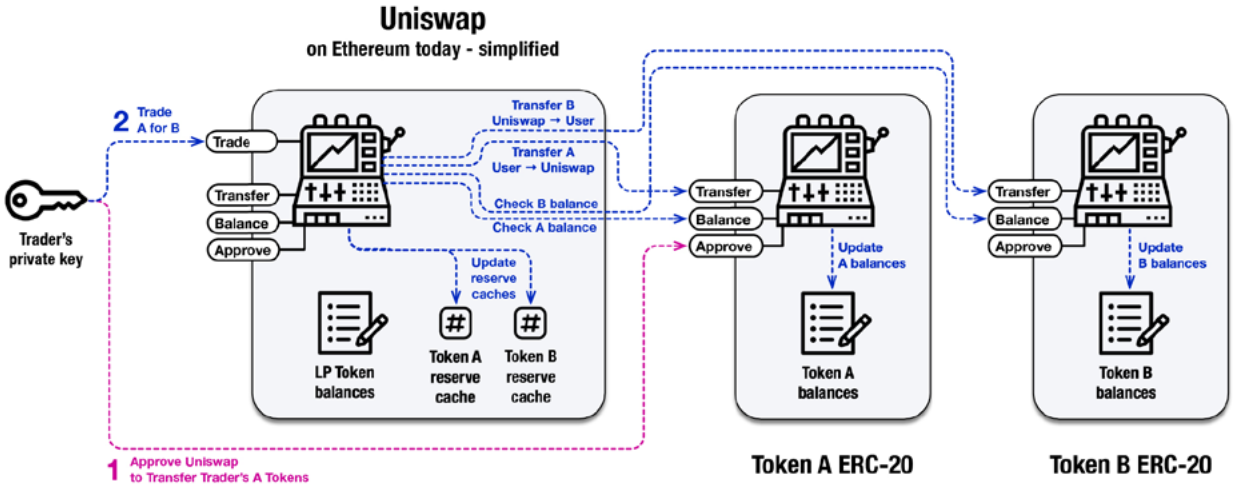
Radix Engine Virtual Machine

The asset-oriented development approach of Scrypto is made possible by the Radix Engine. Radix Engine is Radix's virtual application environment, which provides the asset-oriented functionality for Scrypto-based DeFi smart contracts that Ethereum Virtual Machine (EVM) does not. The main issue EVM faces is that all functionality, from dApps to tokens themselves, must be created by smart contracts and communication between smart contracts. Such an approach is highly inefficient and time-consuming — especially when dealing with assets, which form the great majority of interactions (and opportunities for error) in DeFi. Radix Engine implements assets at a platform level as the

customizable "resources" described above — not as standalone smart contracts.

It also implements other common platform features around this universal resource-based asset model. For example, accounts aren't simply public/private key pairs that may be looked up across many token smart contracts as with the EVM. On Radix, accounts are components that own vaults that are actual containers for resource-based tokens, NFTs, or other assets. An example of how this asset-oriented model simplifies smart contracts and transactions can be seen via a brilliant example of how much simpler Uniswap is with Radix Engine rather than with EVM:





Radix Engine's resources are implemented using the finite state machine (FSM) model. FSM-based logic is conventionally used in systems where extreme reliability and predictability are required. Radix Engine uses an FSM model specifically to implement automatically reliable, predictable, intuitive resource-based asset behavior as a feature of the platform. This allows developers to write Scrypto code that is direct, and to be relieved from the large amounts of logic to safely manage and interact with smart contract-based token functionality.

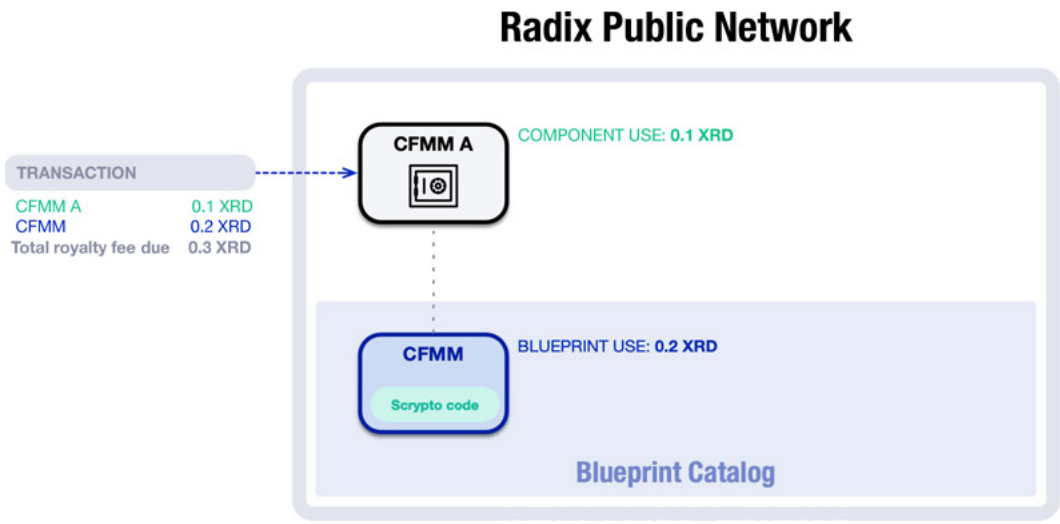
Developer Royalties System

To facilitate consistent developer participation, Radix is taking a different approach to many 'Ethereum killers', which usually encourage development on the platform through contests, prizes, or grants. Yet, only those projects selected by the fund managers receive the money, and others are left with nothing. Furthermore, once the rewards run out, developers who were attracted by those rewards move on to the next platform offering rewards. Independent development

of a complex dApp, on the other hand, faces all sorts of issues. Ultimately, the complexity of coding on Solidity, together with the lack of earnings at early stages until more users are attracted, significantly reduces the willingness of developers to move into DeFi.

Rather than just relying on grants provided by prominent funds and teams of initial developers, Radix is introducing a self-incentivizing, decentralized model for third-party developers. Upon submitting code in the on-ledger Blueprint Catalog, a developer can set their own fee for each use of their code in a transaction. This royalty fee is paid alongside typical network fees in each transaction. Hence, each developer can directly earn money for development of truly useful functionality, instead of aiming to produce a large-scale solution, spending a lot of financial and time resources, hiring other developers, trying to appeal to developer fund managers, etc. Notably, the appropriate royalty set by the developer is guaranteed to be correctly collected for each developer by the Radix system itself.

An example of how Radix's royalty system model works can be seen here:



To summarize, Radix's sequence of technology releases represent an ultimate solution, which not only successfully can solve the blockchain trilemma, but additionally can revolutionize the development of the DeFi industry, attracting myriads of developers and stimulating them to contribute with high-quality code, resulting in high-quality, easy-to-understand, secure and easy-to-write dApps and accelerating the growth of the whole market segment.

8 Conclusion

Ethereum is currently at the top of the food chain in the DeFi universe. In all of the TVL in DeFi, Ethereum has clear percentage dominance in the entire space. Almost every up-and-coming chain or application makes sure to include EVM compatibility so that it is not left out in the cold from the Ethereum community. As the leader of the "altcoins" (alternatives to Bitcoin), Ethereum has disrupted, inspired, or spawned many of the other alts in existence farther down in the rankings of market capitalization.

Although, most up-and-coming chains include EVM compatibility to leverage the network effects and developer tools of the Ethereum community, some blockchain projects such as Radix are purposefully not building EVM compatibility in order to reduce vulnerabilities that can lead to losses worth millions of dollars from hacks and exploits.

The history of TradFi shows us that no matter how big a firm is, it can lose its standing in industry or even cease to be. Standard Oil, Blockbuster, Texaco, TWA, Pan AM, E.F. Hutton, WorldCom, Bear Stearns, Kodak, U.S. Steel, and the list goes on. All these giant behemoths have been some of the largest companies the world has ever known. They all were at the top of their prospective markets at one point or another. Times change and competitors start evolving and moving their way up the food chain. In crypto, it was not that long ago that others were the number two in market rankings until Ethereum came along.

And the race to claim the title has already begun. The famous title, "Eth Killer," has been used to describe all of the blockchains detailed in this report. Each blockchain, Solana, Polkadot, Algorand, and Radix has its own unique reasons for claiming the title of Eth Killer. But some major things have to happen which would open the door to these potential dethroning

First, the Ethereum Foundation, Vitalik Buterin, and the entire Ethereum community are acutely aware of the state of Ethereum at the moment. They are also aware of the shortcomings, including high gas fees and diminished TPS compared to some of its competitors. Ethereum's transition from 1.0 to ETH 2.0 has already been pushed back from many of its original expected rollouts. This continued pushback in the past is exactly the incentive the market needed to look to faster blockchains like Solana and Algorand. If Ethereum continues to prolong the transition to ETH 2.0 or does structured roll-outs of features and benefits touted in the transition, this will only further investors, developers, and interest to look for chains that deliver the goods.

If Ethereum 2.0 falters, Solana would have to firm up its TPS and strengthen its network from distributed denial-of-service attacks, as it has had in the past. Every time a network is attacked, however, if the team addresses the discovered problem, it only makes the network stronger going forward. Solana has the venture capital backing needed to improve and grow, which is an important factor not to be overlooked.

Polkadot's ability to be a multi-chain ecosystem is the critical component to its potential rise. Interoperability is an important concept, allowing a host of different blockchains to interact seamlessly. This ease of use may be key in enticing people into using Polkadot applications, NFTs, and DeFi. Polkadot also has some decent venture capital backing and some of the most brilliant minds in the entire crypto-blockchain space. The technology is not yet proven, but interest from the developer community is high, which is always a good sign for emerging technologies.

Algorand has the advantage of being brought into existence by Silvio Micali, the man who inspired many of the elements of cryptography used throughout the entire industry. Algorand is still a developing ecosystem, and its 1,000 TPS is not as much as that purported by Solana or Polkadot. However, the Algorand network has never gone down since its launch in 2019, which bodes well for the strength of the network. Conversely, its large ledger size can be a limiting factor moving forward, as this would require more centralized storage space unless further changes are adapted to the blockchain.

Radix has its own maverick approach to DeFi development, and in its quest for the scalability required for mainstream DeFi, does away with the notion of a blockchain altogether. But Radix's most innovative technologies are not scheduled to even start being released until the end of this year, and so for now, Radix is still unproven.

No one knows for sure if any of these "Eth Killers" will have what it takes to get to the number two spot in the crypto rankings. But the game is partly each one of the "Eth Killers" to win and partly Ethereum's to lose.

Disclaimer

Neither Cointelegraph Research is an investment company, investment advisor, or broker/dealer. This publication is for information purposes only and represents neither investment advice nor an investment analysis or an invitation to buy or sell financial instruments. Specifically, the document does not serve as a substitute for individual investment or other advice. Readers should be aware that trading tokens or coins and all other financial instruments involves risk. Past performance is no guarantee of future results, and I/we make no representation that any reader of this report or any other person will or is likely to achieve similar results. The statements contained in this publication are based on the knowledge as of the time of preparation and are subject to change at any time without further notice. The authors have exercised the greatest possible care in the selection of the information sources employed; however, they do not accept any responsibility (and neither does Cointelegraph Consulting or Crypto Research Report) for the correctness, completeness, or timeliness of the information, respectively the information sources made available as well as any liabilities or damages, irrespective of their nature, that may result therefrom (including consequential or indirect damages, loss of prospective profits or the accuracy of prepared forecasts). In no event shall Cointelegraph Consulting or CryptoResearch. Report be liable to you or anyone else for any decision made or action taken in reliance on the information in this report or for any special, direct, indirect, consequential, or incidental damages or any damages whatsoever, whether in an action of contract, negligence or other tort, arising out of or in connection with this report or the information contained in this report. Cointelegraph Consulting and CryptoResearch.Report reserve the right to make additions, deletions, or modifications to the contents of this report at any time without prior notice.
The value of cryptocurrencies can fall as well as rise. There is an additional risk of making a loss when you buy shares in certain smaller cryptocurrencies. There is a big difference between the buying price and the selling price of some cryptocurrencies and if you have to sell quickly you may get back much less than you paid. Cryptocurrencies may go down as well as up and you may not get back the original amount invested. It may be difficult to sell or realize an investment. You should not buy cryptocurrencies with money you cannot afford to lose.