



THE STATE OF DEFI SECURITY 2021





“

Centralization issues were the most common attack vector.

\$1.3 Billion

in user funds lost in total across 44 DeFi Hacks.

”

EXECUTIVE SUMMARY

- 1 DeFi grew at a faster pace than ever before in 2021. DEX volume tripled, Total Value Locked quadrupled, and Ethereum's transaction fees skyrocketed.
- 2 Competing L1s offering faster and cheaper transactions cut Ethereum's market share down by more than a third over the course of the year.
- 3 CertiK audited a total of 1,737 projects in 2021. Ethereum (42%) and Binance Smart Chain-based projects (36%) made up the vast majority of this number.
- 4 The market capitalization of CertiK-audited projects came in just over \$90 billion.
- 5 New industries such as NFTs and blockchain gaming went mainstream, giving newcomers their first taste of Web3.
- 6 With such explosive growth, blockchain security became more important than ever. While the dollar value of losses due to hacks and exploits increased, the proportion they represented of DeFi's market capitalization decreased year-over-year.
- 7 Centralization issues were the most common attack vector exploited in the \$1.3 billion in user funds lost in total, across 44 DeFi hacks. This underscores the importance of decentralization and highlights the fact that many projects still have work to do to reach this goal.

INTRODUCTION

As a blockchain and smart contract security firm, CertiK is committed to raising the level of security and transparency in crypto and DeFi. Yet too often security is treated as an afterthought until funds are lost and it's too late. In this report we will look at how the security landscape has changed in 2021 and what we expect to see moving forward, keeping you up to date on the latest exploits and new vulnerabilities that have emerged as DeFi grows in adoption and complexity. In 2021, \$1.3 billion in cryptocurrency was lost to hacks, exploits, and scams. This is an increase over the approximately \$500 million lost in 2020. However, contextualizing this number by looking at it as a percentage of total market capitalization provides a clearer picture. 2021's losses represented 0.05% of crypto's total market capitalization, a drop of 17% from 2020. CertiK audited a total of 1,737 projects in 2021. This YoY growth of more than 1,000% reflected the persistent demand for security solutions in a rapidly expanding industry.

A large proportion of this growth was driven by the rise of Binance Smart Chain. From January 1st to now, BSC's total value locked (TVL) grew from \$62 million to \$21 billion, a 31,000% increase. Users flocked to the EVM-compatible chain, attracted by the vibrant ecosystem and much cheaper fees.

It's our mission to raise the standard of security and transparency across all of crypto and DeFi. Our work towards this end has grown to encompass code auditing, real-time on-chain monitoring, the creation of accessible and educational content, and the provision of critical infrastructure services. Mirroring the growth seen in the diverse set of L1s that gained attention in 2021, the Security Leaderboard ended the year with 1,861 distinct projects listed and ranked according to on and off-chain security analyses.

The rise in value of DeFi protocols has made the reward for successful exploits even greater, while increased interoperability has opened up new vectors of attack. Bridges between L1s were exploited a number of times over the course of 2021. As competing L1s gain traction, Ethereum L2 scaling solutions are released, and the merge to Eth 2.0 draws closer, the importance and complexity of cross-chain interoperability will only increase.

These hiccups didn't dampen the appetite of DeFi users for new ecosystems, particularly ones with faster transactions and lower fees than the often-congested Ethereum blockchain. Competing L1s were some of the major winners of 2021, and we'll investigate their evolution in this report.

Overall, despite some growing pains, 2021 was an exciting year, full of major innovation and increased adoption. This report will examine the evolution of the space over the last year, the hurdles encountered along the way, and the macro trends that will continue to grow in importance as crypto continues to become established as a future-focused asset class.

1

VECTORS OF ATTACK

CertiK obtains unique insights into common smart contract vulnerabilities through our auditing work. Though these issues are ideally resolved by the project owners before deployment, they offer important lessons about the most prevalent pitfalls smart contract developers encounter and the necessity of comprehensive auditing.

By far the most common vulnerability found was centralization risk. CertiK auditors came across 286 discrete centralization risks throughout the 1,737 audits performed in 2021. Centralization is antithetical to the ethos of DeFi and poses major security risks. Single points of failure can be exploited by dedicated hackers and malicious insiders alike.

The DeFi protocol bZx was exploited for more than \$55 million in November as the result of private key mismanagement. This was an example of privileged ownership (found 76 times in audits) that allowed the attacker to gain complete control of all contracts the key controlled.

“After centralization, risks missing event emission were the next most common vulnerabilities found”

When a simple phishing email can compromise an entire protocol relatively easily, a single, non-multi signature setup is insufficient. If these privileged functions were protected by a timelock, delegated to a DAO, or managed by a multi-sig wallet, the centralized point of failure would have been resolved and the exploit averted.

After centralization risks, missing event emissions were the next most common potential vulnerabilities found (211 instances). Certain functions should emit events as notifications to users because they change the status of sensitive variables or call important processes. `setOracleAddress()` and `setLiquidityFeePercent()` are two examples of functions auditors found that should emit such notifications when invoked.

Another common code error found was the utilization of an unlocked compiler version (176 instances). An unlocked compiler version in the source code of the contract permits a user to compile it at or above a particular version. This, in turn, leads to differences in the generated bytecode between compilations due to differing compiler version numbers.

CertiK came across 104 lines of code that lacked proper input validation. Validating inputs (e.g. ensuring that a certain variable in a function is greater than zero) limits the functionality of an executable to a set of known possibilities. Limiting the ability to create unknown or potentially malicious events on a smart contract becomes essential, especially when users are given the flexibility to interact with all variables in the entirety of the smart contract.

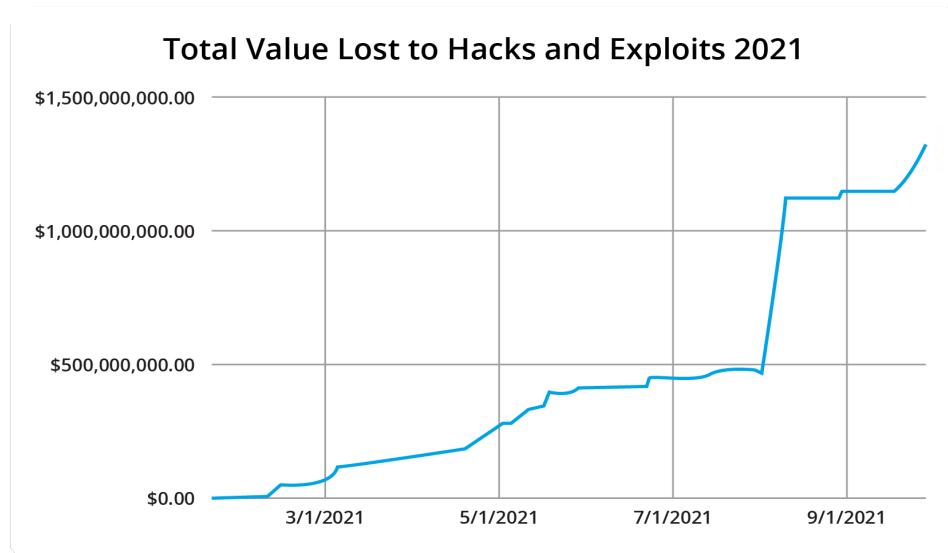
Reliance on third-party dependencies (102 instances) should be avoided as much as possible. A developer can only control the security of their own code, not that of the external contracts with which theirs interact. While tools such as the Security Oracle can act as a failsafe by ensuring external contracts meet a predetermined level of security before an interaction is approved, the goal of DeFi is to remove centralization in all its forms. Interoperability magnifies the power and potential of each of its constituent smart contracts, but it also requires that they all meet a certain standard of security and decentralization.

CertiK categorizes findings into six rankings: critical, major, medium, minor, informational and discussion. Critical errors jeopardize the functioning of an entire project, while informational or discussion findings often relate to best practices in smart contract development. In addition to addressing critical and major errors as soon as they arise, CertiK's mission to raise the standard of security in the ecosystem involves establishing such norms and best practices. Solidity – the language in which EVM smart contracts are written – is only seven years old. Developers are still exploring the possibilities of smart contract code, and there is no better time than these early days to make security a foundational concern and protect users well into the future.



2

HACKERS FIND NEW WAYS TO PLAY OLD TRICKS



The value lost to hacks and exploits crossed the billion-dollar mark in late 2021, making it clear that meaningful security remains a challenge for the industry. The proliferation of hasty forks, unaudited deployments, and outright scams led to hundreds of millions of dollars of unnecessary losses.

Disappointingly, the majority of DeFi platforms exploited in 2021 were unaudited. This highlights the amount of work to be done before DeFi is seen as a secure place to invest and innovate in.

For an example of the kinds of errors that can lead to huge losses, Uranium Finance, an unaudited fork of Uniswap deployed on BSC, lost \$57 million of user funds due to a single character in their source code.

“A byte sized piece of code can have multimillion-dollar ramifications”

This is the original, audited Uniswap code:

```
uint balance0Adjusted = balance0.mul(1000).sub(amount0In.mul(3));
uint balance1Adjusted = balance1.mul(1000).sub(amount1In.mul(3));
require(balance0Adjusted.mul(balance1Adjusted) >=
uint(_reserve0).mul(_reserve1).mul(1000**2), 'UniswapV2: K');
```

And Uranium Finance's forked code:

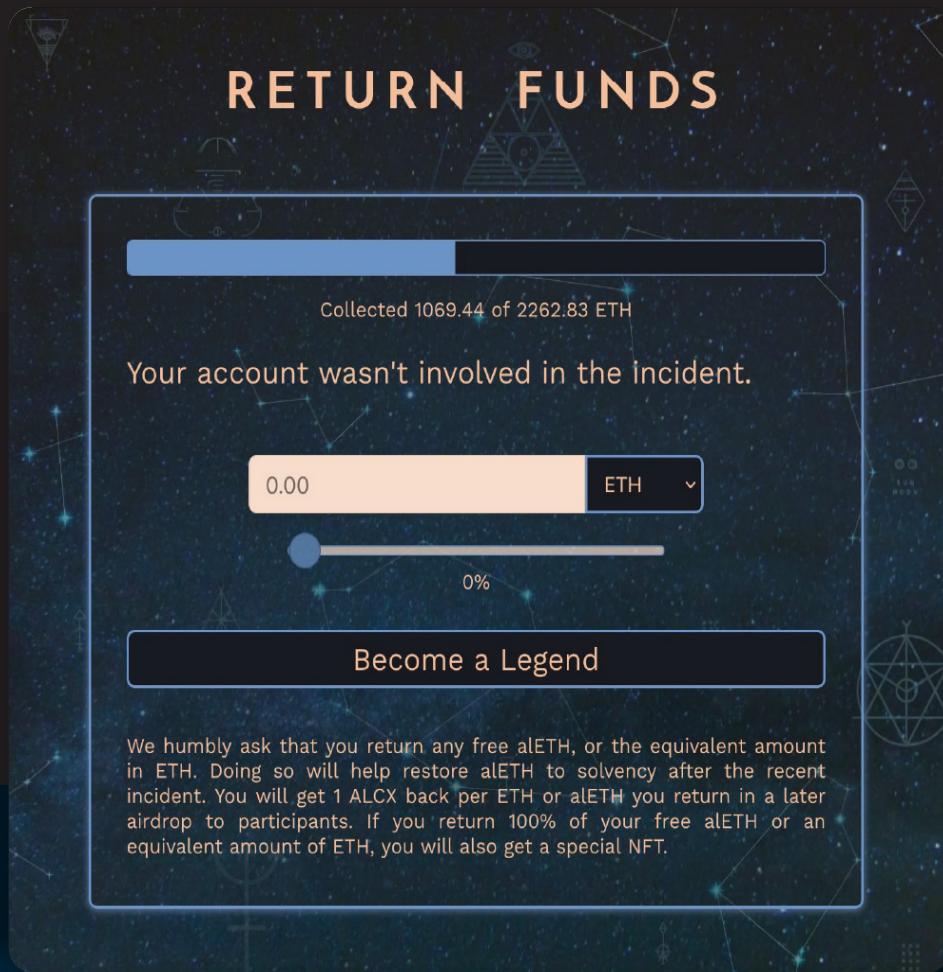
```
uint balance0Adjusted = balance0.mul(10000).sub(amount0In.mul(16));
uint balance1Adjusted = balance1.mul(10000).sub(amount1In.mul(16));
require(balance0Adjusted.mul(balance1Adjusted) >=
uint(_reserve0).mul(_reserve1).mul(1000**2), 'UraniumSwap: K');
```

Source: [rekt](#)

Uranium Finance changed **balance0** and **balance1** from **1,000** to **10,000**, but neglected to update the third instance. The result was that the attacker was able to receive 98% of the swap's output token in return for just 1 wei of the input token.

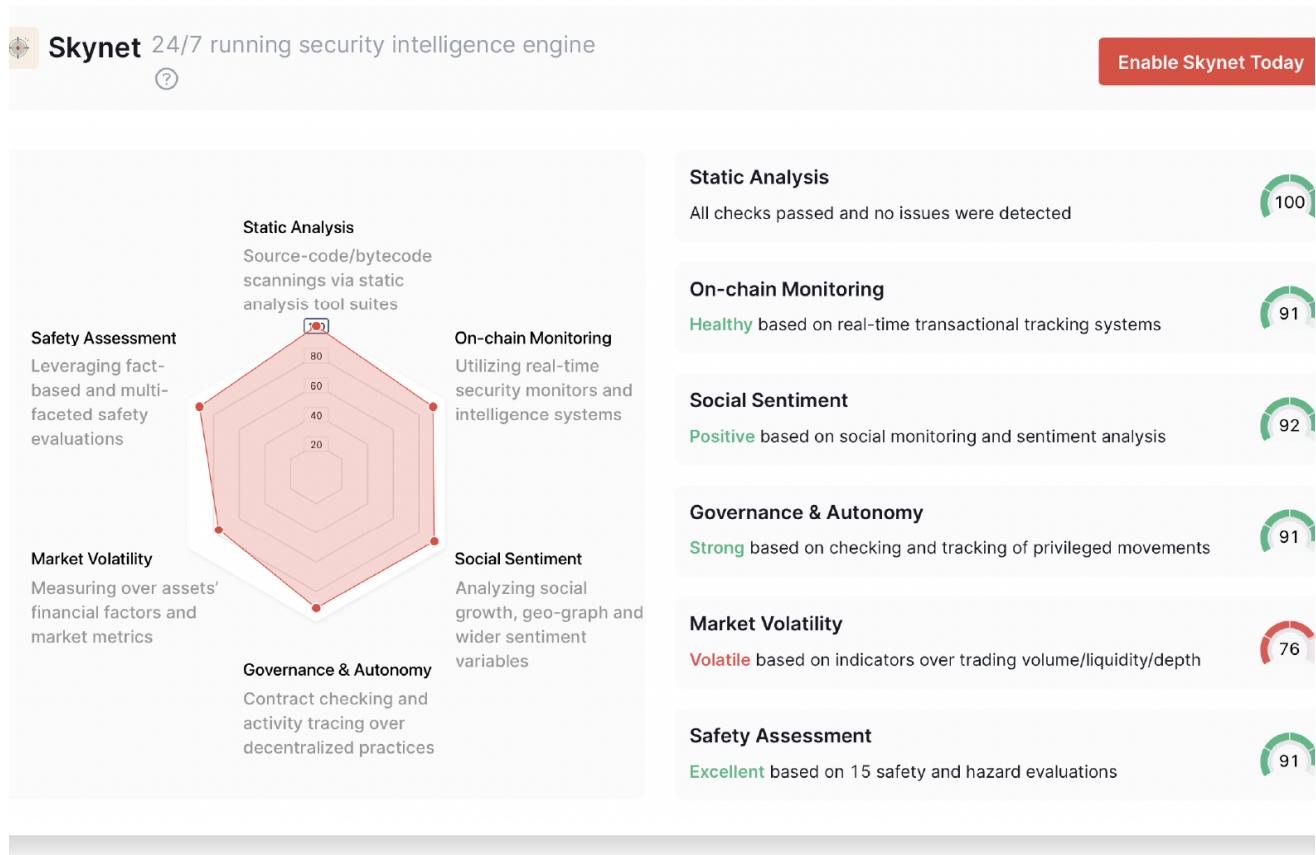
While these kinds of rushed forks of projects proved to be low-hanging fruit, a number of exploits targeted platforms working at the cutting-edge of the industry. Alchemix and Compound – two high-profile DeFi platforms – suffered multimillion dollar losses as the result of bugs in their code. Any changes to a platform's code should be reviewed and audited, no matter how small the initial modification is. As we've seen, a byte-sized piece of code can have multimillion dollar ramifications.

In a sign of good faith from the community, more than 55% of the 2262 ETH mistakenly released by the Alchemix protocol was returned after a public appeal. Those who returned 100% of the aLETH they had erroneously been able to claim were rewarded with 1 ALCX token per ETH or aLETH returned, plus an Alchemix Legend NFT.



Though the end result was about as good as could be hoped for, restitution should not be left to the goodwill of the community. The best security is a combination of a comprehensive pre-deployment audit and on-chain monitoring tools that analyze and protect contracts in real time.

Alchemix currently uses [CertiK Skynet](#) to guard its on-chain protocol activity and provide users and investors with an easily readable overview of the security and overall health of the project.



While there will always be risks involved when pushing the boundaries of what's possible in DeFi, security does not need to come at the cost of innovation. In fact, the two can go hand in hand.

The open-source and collaborative nature of DeFi has led to developers from different projects coming together and establishing "war rooms" in the event of a vulnerability being discovered. The end result is a safer experience for all users and a stronger ecosystem.

Security products have also come a long way in the last year. The range of tools available to retail users and professionals is expanding rapidly.

The Security Leaderboard – with a total of 1861 completed and on-boarded projects at the end of 2021 – allows DeFi users to leverage the expertise of our auditing and security teams in order to equip themselves with a deeper knowledge of security risks. These users push the whole ecosystem to new heights, while we provide the data that helps them make informed decisions.

Skynet actively monitors hundreds of DeFi platforms in real-time, using a combination of on-chain transaction monitoring and off-chain data such as social sentiment to ultimately arrive at a comprehensive security analysis. Skynet Premium – unveiled in 2021 – integrated continuously-evolving machine learning to grow in lockstep with the constantly shifting smart contract risk environment, getting more and more advanced as it encounters new threats and vulnerabilities. The Premium platform includes an analytics dashboard which enables enterprise clients to monitor and manage their risk in real-time.

CertiK's Security Oracle allows developers to leverage real-time security scores provided by a decentralized network of nodes to ensure that their contract's interactions with other smart contracts meet an acceptable level of security. This allows developers to take advantage of the powerful interoperability of DeFi while protecting their own contracts against failures of third-party dependencies.

SkyTrace is an intelligent, intuitive tracing tool to help analyze and visualize transaction data across Ethereum and BSC wallets. This tool provides actionable insights into identifying and tracing suspicious flows to and from one's own personal wallet or a project's team wallet.



3

THE “DEATH OF ETH” OR BIRTH OF A MULTI-CHAIN WORLD?

Ethereum has suffered from success over the last year. In what could be seen as the first flippening, the network's fee revenue outstripped Bitcoin's by a factor of more than 60. At the time of writing, **Ethereum averaged \$53 million in daily fee revenue**. Bitcoin's daily revenue was just over \$1 Million. Ethereum also processed more than four times the number of transactions per day than the bitcoin network, at 1.28 million compared to 293,000.



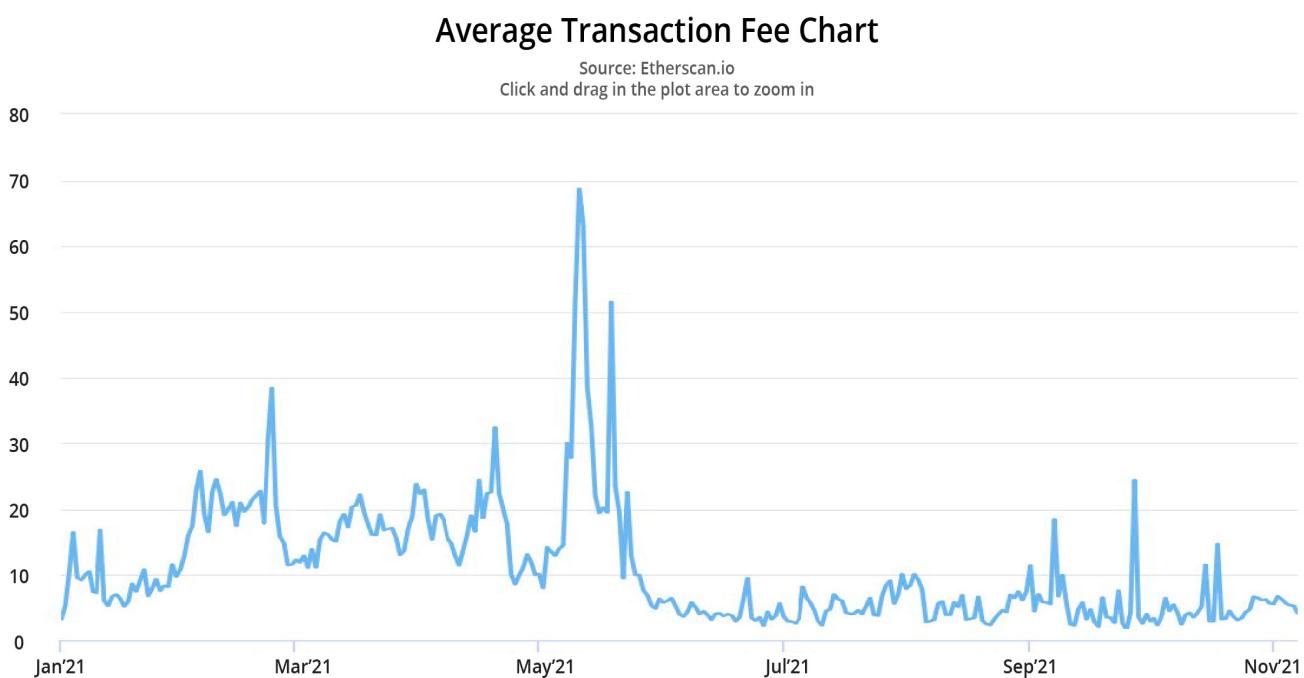
source: [cryptofees](https://cryptofees.info)

Three largely Ethereum-based applications also beat Bitcoin to make the top five. Uniswap does 99.2% of its volume on Ethereum, SushiSwap 85.4%, and AAVE 66.9%.

This highlights the phenomenal growth of Ethereum over the past 12 months. In late 2020, Bitcoin was pulling in roughly double the revenue of Ethereum. Since then, Ethereum has grown by more than 50x, while **Bitcoin's daily revenue declined by 66%**.

While Bitcoin remains the undisputed leader and figurehead of the crypto world, there is clearly a voracious appetite for the smart contract-driven decentralized applications that Ethereum enables. DeFi, NFTs, and other applications such as ENS (Ethereum Name System) have all contributed to this growth.

However, one consequence of this demand is that Ethereum's blockspace is trading at an expensive premium. The massive increase in revenue necessarily entails a massive increase in the fees paid by users. Average transaction fees reached an all time high of \$68.72 in May. This was the average cost for a simple token transfer, interacting with the complicated smart contracts powering DeFi protocols can cost many multiples more.



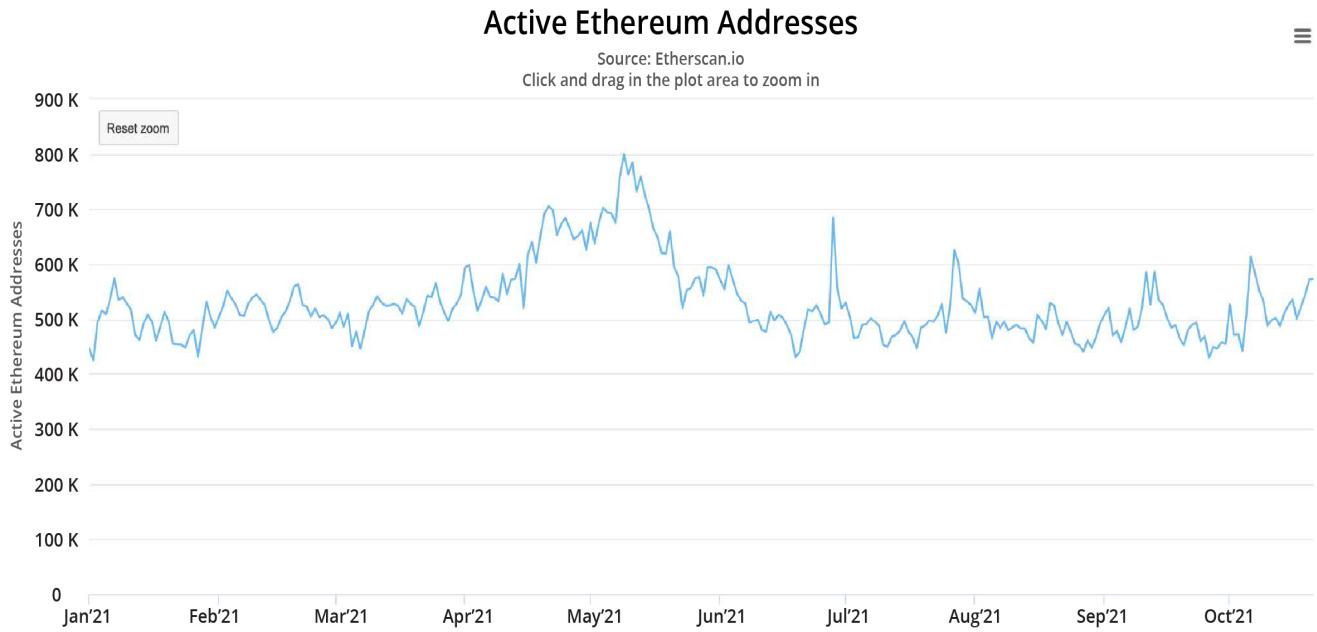
The eye-watering cost of transacting on the Ethereum blockchain drove many users to seek out cheaper alternatives. At the beginning of 2021, applications on the Ethereum blockchain held 98.2% of all value locked in DeFi protocols. By the time of writing, that figure had dropped by more than a third to 67%. The big winners were Binance Smart Chain, Solana, Terra, Avalanche, Fantom, and Polygon, which made up the next six places by TVL.¹

¹ <https://defillama.com/chains>

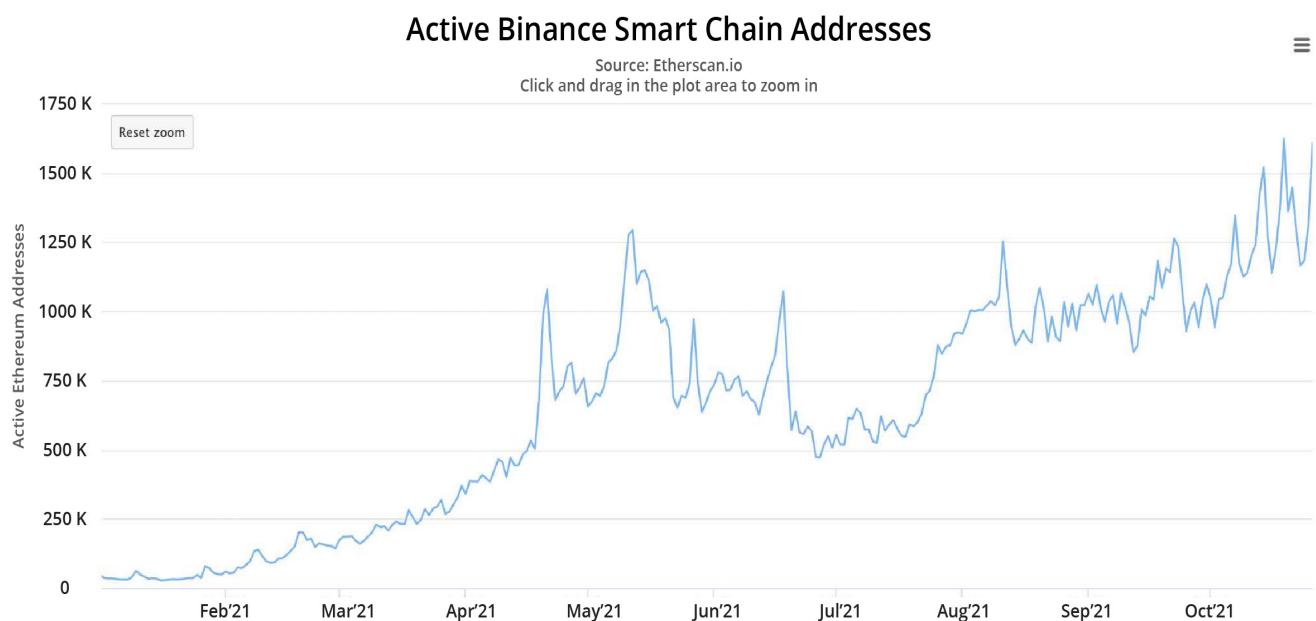
4

2021 STATISTICS: NUMBER OF ADDRESSES, YOY GROWTH

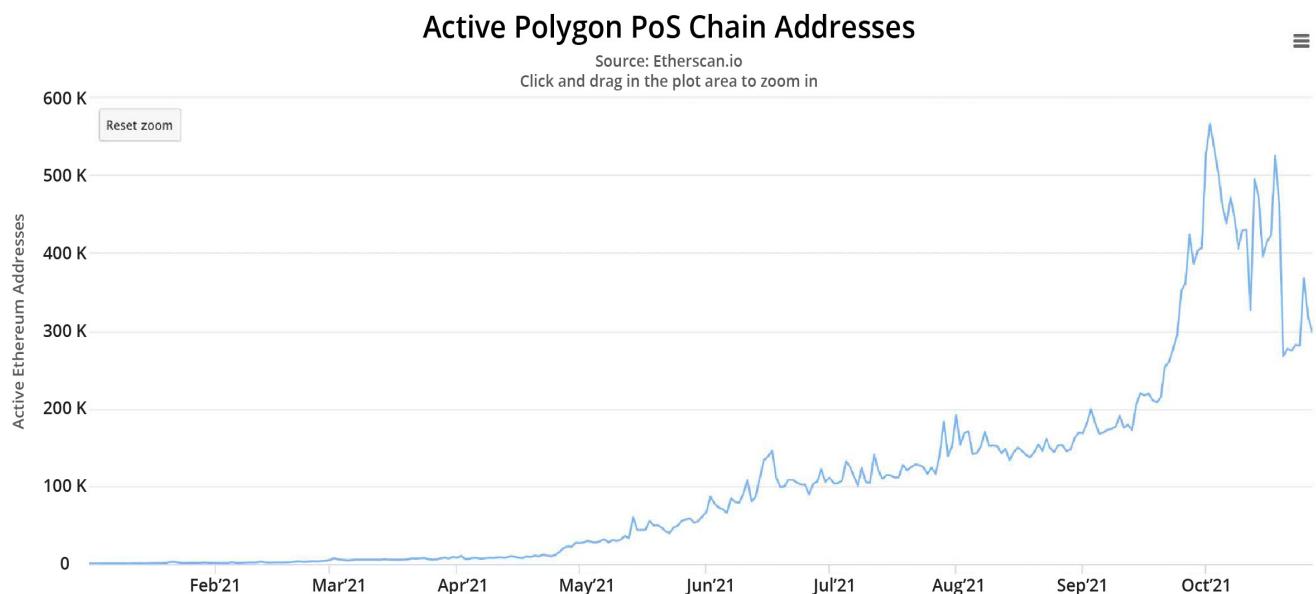
Ethereum: Jan. 1st: **426,000** daily active addresses to now current: **558,000** - peak in May of **800,000**. \$153 billion TVL



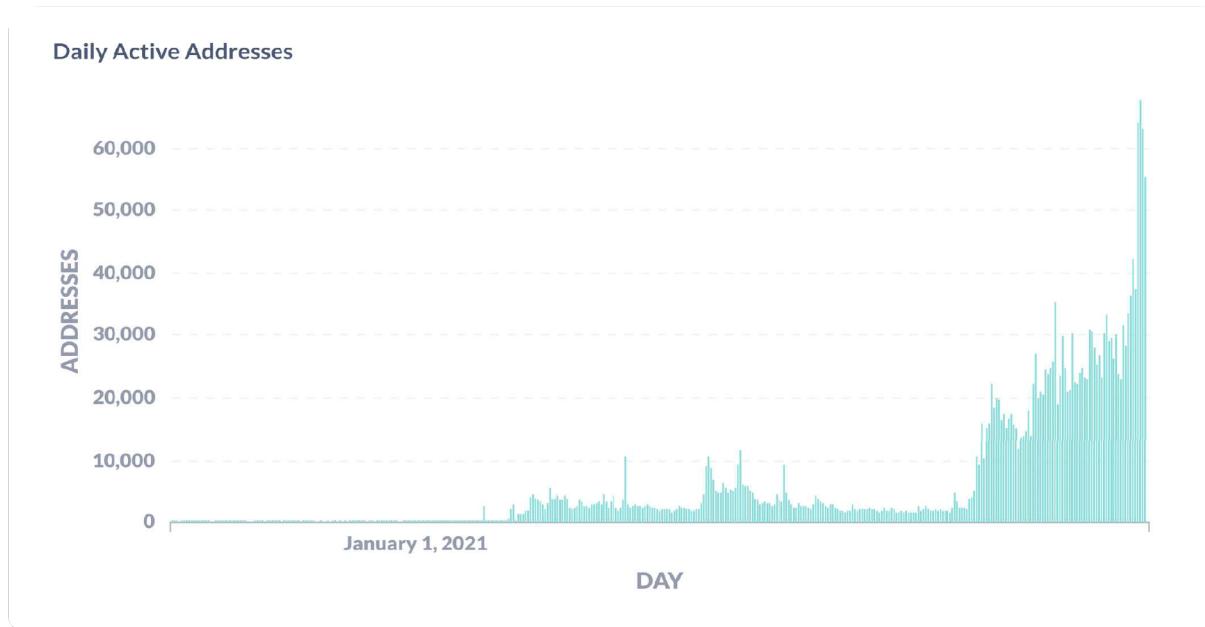
BSC: Jan. 1st: **49,500** daily active addresses to now current **1,313,223** - peak in mid-October at **1,624,000**. \$19.07 billion TVL



POLYGON: Jan. 1st: **759** daily active addresses to now current **367,346** - peak beginning October **566,000**. \$4.59 billion TVL



AVALANCHE: Jan. 1st: **22** daily active addresses to now current **67,000**.
\$8.2 billion TVL



Each of these new Layer 1s comes with its own comparative advantages and trade-offs to Ethereum. There is still no permanent solution to the blockchain trilemma of speed, security, and decentralization, meaning at least one of the three needs to be sacrificed to a degree for the sake of the other two components. Ethereum generally sacrifices speed – measurable not just in transaction throughput but also in transaction cost – for security and decentralization. The ~2500 mainnet nodes that perform the intensive Proof of Work (PoW) mining that secures the network make it extremely costly to successfully compromise the trustless blockchain.

Binance Smart Chain takes a different approach. There are 21 trusted validators that work according to a Proof of Staked Authority (PoSA) consensus mechanism. The result is greatly increased speed and decreased transaction fees at the cost of decentralization.

The pitfalls of reduced decentralization and security were evident in September when Solana suffered a distributed denial of service (DDoS) attack and was knocked off-line for more than 18 hours. Despite this loss of service, users flocked back to the ecosystem as soon as it was back on-line, proving that for many the main incentive driving their choice of preferred Layer 1 is cheap, quick transactions.

While there have been many debates about the merits of each blockchain's design choices, the flourishing of multiple competing Layer 1s shows that the market has a place for each of them. Users who value Ethereum's decentralization and track record of security will pay the high fees necessary to transact on the network, while those who prefer faster, cheaper confirmations will look to other blockchains utilizing more novel consensus mechanisms.

Ethereum's DeFi dominance dropped significantly during 2021, yet its fee revenue and TVL grew massively. This is a positive sign for the health of the industry as a whole and the continuation of innovation that competition brings.

5

2021 MACRO TRENDS

NFTs For You and Me

Non-fungible tokens (NFTs) and blockchain gaming went mainstream in 2021. Christie's auction of Beeple's First 5000 Days NFT for \$69 million in February made headlines as the art world took its first steps into the metaverse. This came as the physical art market contracted 22%, due in part to the global pandemic but perhaps also to the growing interest in digital forms of art². NFTs promise to revolutionize proof of authenticity, ownership, provenance, and scarcity – all of which will be essential in a digital world.

Blockchain gaming also took off in a big way, with games such as Axie Infinity and platforms like Immutable reaching millions of users. Many of these users took advantage of the *play-to-earn* model of blockchain gaming, where NFT technology and token rewards mean in-game assets have real-world value.

While in the past few years prices of in-game assets such as weapons and skins in Fortnite and Counter-Strike have been the subject of media attention, these assets are limited to the closed world of the video game. NFT technology allows users to take the digital assets they have spent countless hours obtaining outside the video game, holding it instead in their blockchain wallet and using it all across Web3. They are free to trade their NFT skins or items on platforms such as Immutable X or display them in the virtual trophy case of the player's wallet. More applications will spring up as the intersection of gaming and blockchain technology is built out.

² <https://www.artmarketmonitor.com/2021/03/16/2021-art-basel-global-market-report-reveals-22-percent-drop-in-2020-sales-to-50-billion/>

Facebook Goes Meta

Facebook's bold re-brand to Meta was dismissed by some sceptics as little more than a calculated ploy to distract from the negative attention the company has received lately. Yet Zuckerberg's insistence on the importance of the Metaverse points to something that's more ideological than it is Machiavellian.

While many people will have qualms about the degree to which Meta will adopt and embrace the open, collaborative nature of Web3 and blockchain, the fact remains that the company is staking its existence on the growth of the Metaverse. Regardless of their intentions, it is inevitable that the world's largest social media platform promoting and advancing the Metaverse will be a powerful catalyst for its adoption.

This Metaverse is in the very early days of being built, but the popularity of NFTs and blockchain gaming this year has proven there is strong demand for virtual experiences and digital assets. It's hard to conceptualize exactly what the Metaverse will look like in ten or twenty years, but it wouldn't be an outlandish bet that it will come to permeate our lives as much as the Internet has.

Going Green – Miners Bet Big on ESG

Not everybody embraced blockchain throughout 2021, however. Arguments emerged against NFTs, criticizing the environmental cost of transactions on the Ethereum blockchain. Steam – a major video game distribution platform – banned all games that issue NFTs or cryptocurrencies, quoting the prevalence of scams. Some observers wondered if the platform's main concern was in fact ensuring its control over the trading of in-game items, as NFTs can be bought and sold on decentralized markets.

Tesla's announcement in February that it had bought \$1.5 billion of Bitcoin and would accept the cryptocurrency as payment pushed the price of BTC 20% higher, though the company's reversal in May marked the beginning of a strong sell-off across the whole asset class. Environmental, Social, and Governance (ESG) concerns remain front of mind for many organizations.

Musk, Twitter and Square CEO Jack Dorsey, and Cathie Wood, CEO of ARK Invest, held a live discussion in July headlined The  Word: Bitcoin as a Tool for Social Empowerment. Musk confirmed that Tesla would resume accepting Bitcoin as payment once the network is powered by at least 50% renewable energy.

In the medium term, Ethereum's upcoming transition to Proof of Stake and the growing use of renewable energy in Bitcoin mining continue to push the industry towards a greener future. A number of renewable-focused Bitcoin miners have gone public this year, aiming to cash in on what may by necessity be the future of the industry.

Regulatory Headwinds on the Horizon

Crypto's continued rise has attracted the attention of regulators and mainstream financial institutions around the world. These approaches have varied from El Salvador becoming the first sovereign nation to make Bitcoin legal tender, to China's crypto crackdown and the exodus of miners from the mainland.

Authorities in the U.S. have also taken a keen interest in DeFi. In April 2021, the SEC appointed a new chairman who is well-versed on the ins and outs of blockchain technology. Gary Gensler taught a graduate-level course on blockchain at the Massachusetts Institute of Technology in 2018. However, his recent remarks pertaining to crypto have signaled the possibility of broader enforcement of securities laws in the near future.

While Gensler made it clear that it was not within the purview of the SEC to ban cryptocurrencies, he did reiterate his belief that many tokens – particularly those that launched with an Initial Coin Offering (ICO) – are in fact securities.³

Stablecoins are another area that have come under close scrutiny. Tether and Bitfinex settled with the Commodity Futures Trading Commission (CTFC) to the tune of \$42.5 million, ending the civil lawsuit against them that alleged the two crypto companies "made untrue or misleading statements and omission of material facts about the U.S. dollar tether token stablecoin being fully backed by U.S. dollars."⁴ Previously, in February Tether and Bitfinex had also settled a lawsuit brought by the New York Attorney General's office for the sum of \$18 million, with neither company admitting any wrongdoing.

In the absence of clear guidance from regulatory bodies, the crypto industry pushed forward with self-regulation. Paxos, TrustToken, and EURS all implemented cryptographic Proof of Reserves (PoR), giving on-chain proof that their stablecoin offerings are backed by real assets in real bank accounts.⁵

³ <https://en.cryptonomist.ch/2021/10/06/gary-gensler-cryptocurrencies-are-securities/>

⁴ <https://www.ctfc.gov/PressRoom/PressReleases/8450-21>

⁵ <https://data.chain.link/ethereum/mainnet/reserves>

6

CONCLUSION

2021 was a year of record growth for all things DeFi. Just about every metric tracking the industry's growth increased by many multiples over the course of the year.

Ethereum now creates more than 64x the fee revenue of Bitcoin, and more than 4x the number of daily transactions. This growth throughout 2021 is perhaps even more remarkable due to the intense competition Ethereum faced from newer L1s. Their shared success proves that there is demand for multiple blockchain ecosystems, each with their own unique value proposition.

While the percentage of total market capitalization lost to hacks and exploits decreased in 2021, the rise in value locked meant the dollar value lost was greater than in 2020. This is a definite step forward, but it shows that the ecosystem still has progress to make before DeFi feels like a safe place in which to deploy capital.

CertiK's audits of 1,737 projects in 2021 revealed some trends which we have outlined in this report. Going forward, security will continue to be inextricably tied to the future of DeFi. Without meaningful security that protects users and secures platforms, innovation will suffer and interest will die off. Fortunately, the demand for DeFi is vastly outpacing the negative consequences of the small number of hacks and exploits that harm the space.

But for this to continue, a couple of things need to happen. Auditing needs to become a default standard for all projects. The fact that a large majority of projects exploited in 2021 were unaudited is disappointing, if not exactly surprising. Tools such as real-time monitoring and on-chain analytics can help fill the gaps that are inevitably created when code is deployed into the wild world of DeFi.

As we move deeper into a multi-chain world, cross-chain interoperability will become all the more important. This represents an opportunity to incorporate security best practices into the foundations of new cross-chain protocols, which is something we hope to see realized in the short to medium-term.

Despite all the major advancements in security, adoption, and regulatory approval, digital assets are still an emerging market. The future is being built as we speak. Taking the opportunity to leverage and expand on blockchain's security-by-design will ensure the technology continues to create new opportunities for all people, all around the world.

This report has been an opportunity to pause and reflect on the developments of the last year in blockchain technology. Looking back on 2021, CertiK is proud to say this year's all time highs have not just been in price, but in interest, innovation, and adoption.

