CERTIK

HACK3D

THE WEB3 SECURITY REPORT

2023

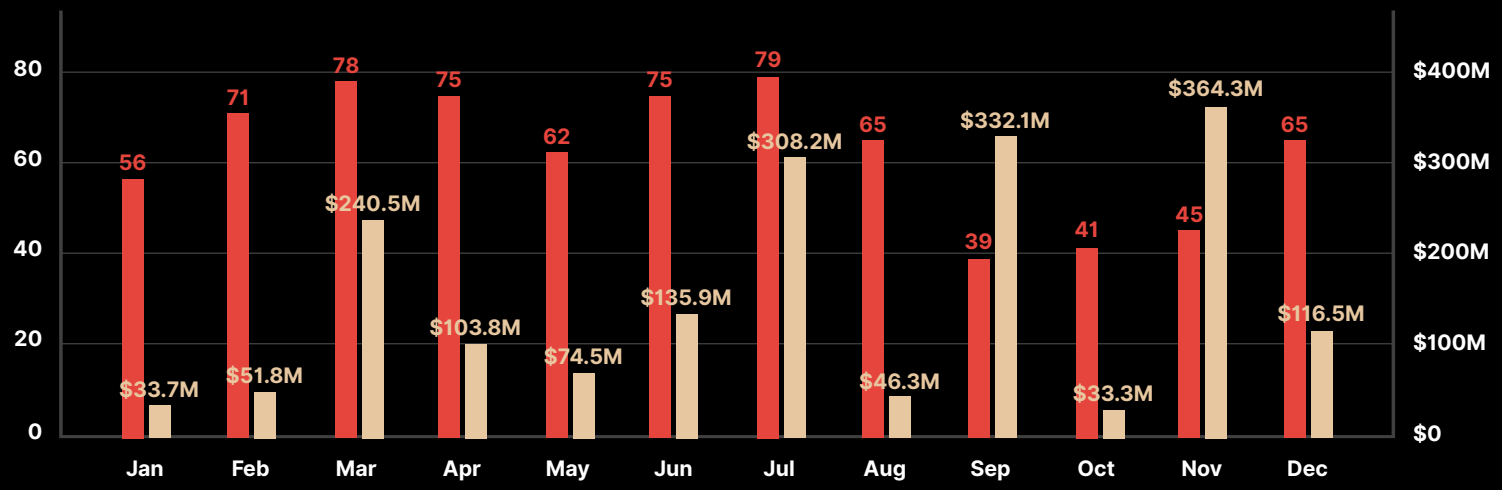
Securing the Web3 World

Executive Summary

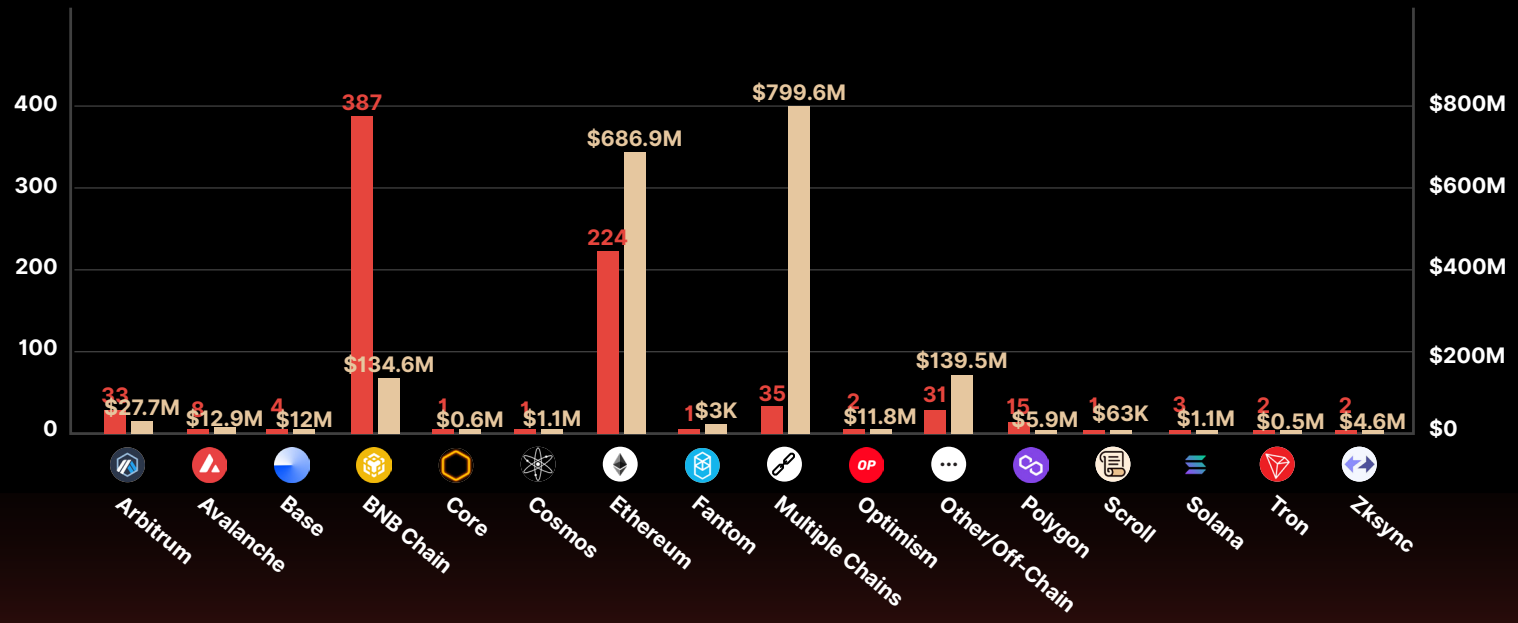
- A total of **$1,840,879,064** was lost across **751** security incidents in 2023.
- This represents a decline of **51%** from 2022's total of $3.7 billion, and an average of $2.45 million per incident. However, just the ten most costly incidents alone accounted for $1.11 billion, and the median loss per incident was much lower than the average, at $101,132.
- November was the most costly month of the year, with **$364,340,035** lost in 45 incidents.
- Q3 saw the most losses, at **$686,558,472**, from 183 hacks, scams, and exploits.
- Private key compromises were the most costly attack vector, with **$880,892,924** lost in just 47 incidents. This represents nearly half of all financial losses, though private key compromises accounted for just 6.3% of all security incidents.
- BNB Chain experienced the highest number of security incidents, with a total of **387** hacks, scams, and exploits leading to $134 million in losses. This resulted in an average of **$346,253** per incident.
- Ethereum saw a total of **224** incidents but $686 million in losses, for an average of $3.0 million per incident.
- Security breaches affecting multiple chains accounted for **$799million** of losses in just 35 incidents, highlighting the persistent pain-point that is cross-chain interoperability.
- Hack3d 2023 covers the stories and trends that defined the direction of Web3, the current state of the industry, and where the next twelve months may take us.

Statistics Graphs: 2023

BY MONTH



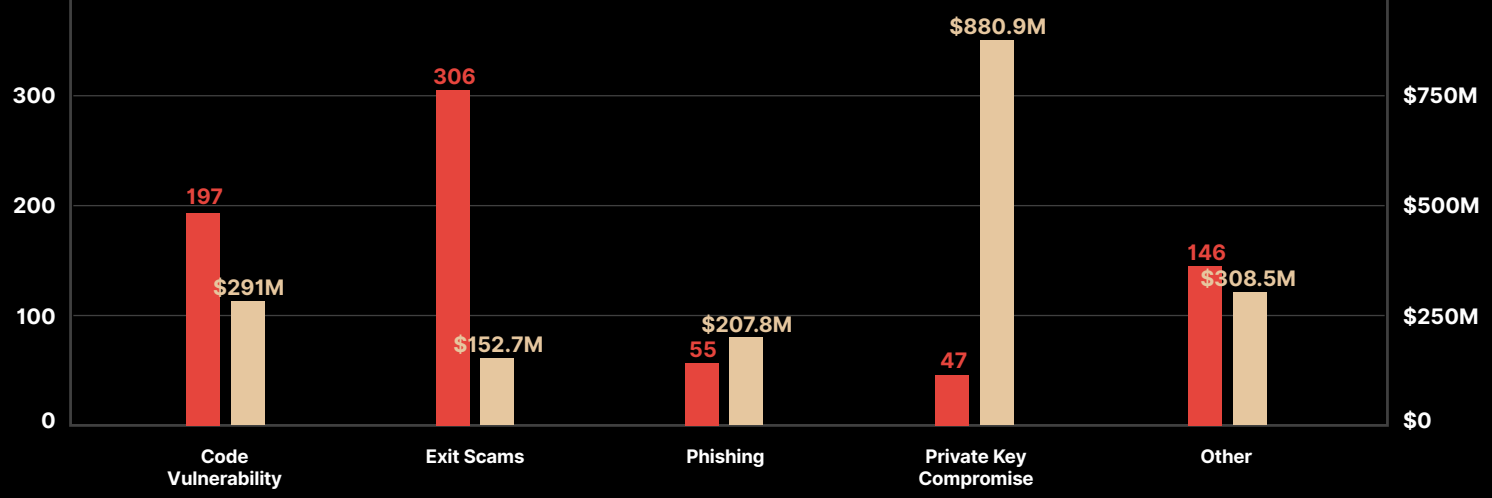
BY CHAIN



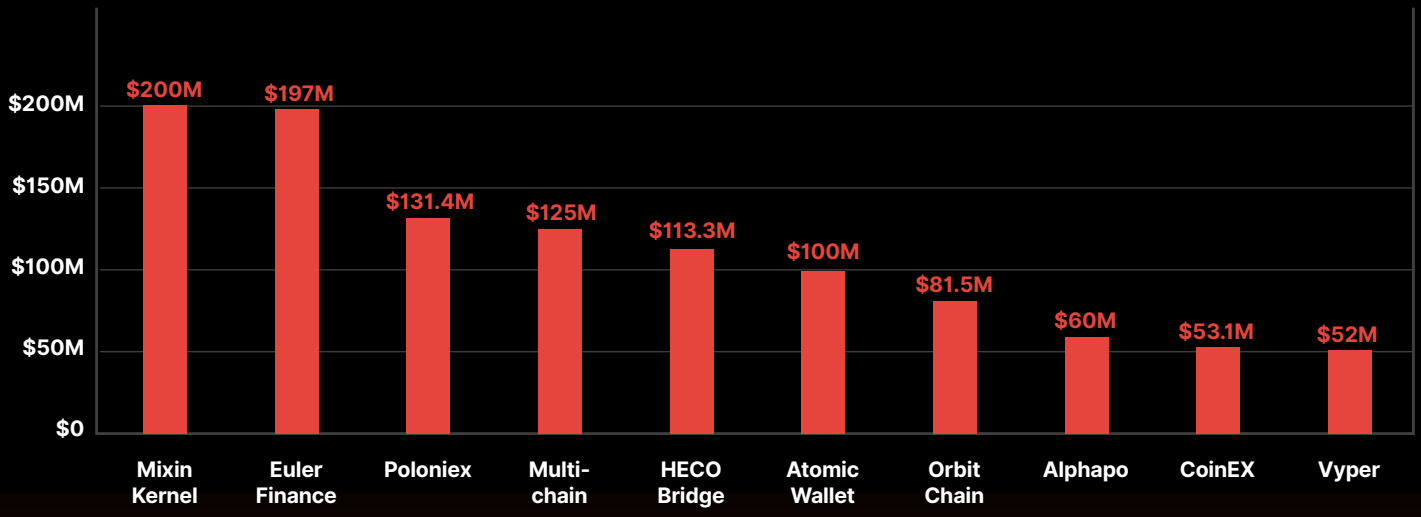
Numbers are approximate and may change with new information

Statistics Graphs: 2023

BY TYPE



TOP 10 MOST COSTLY INCIDENTS

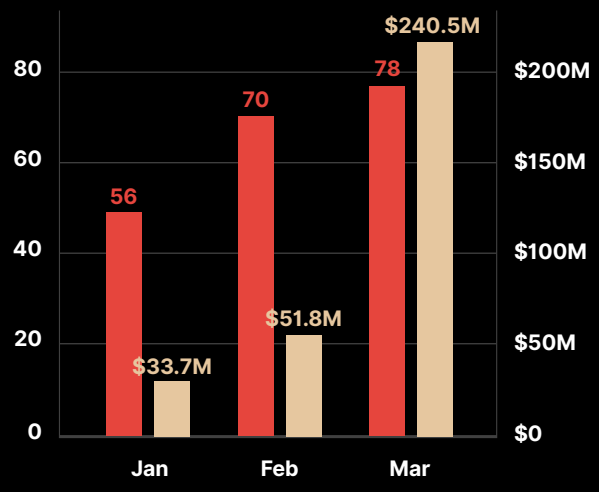


Numbers are approximate and may change with new information

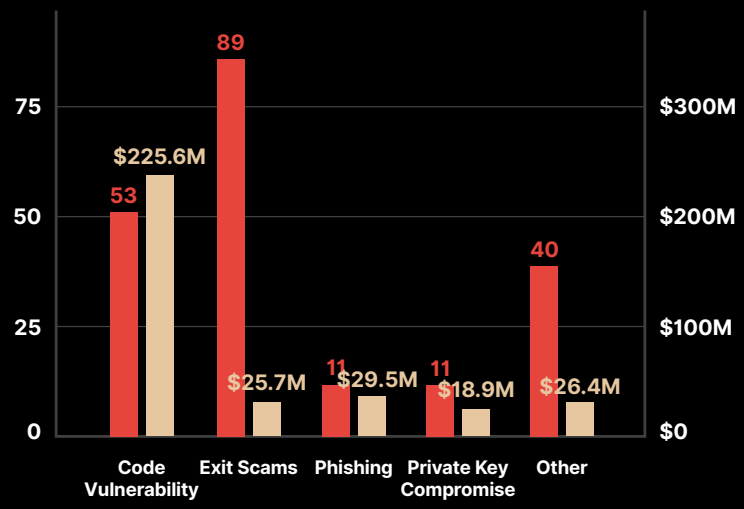
Statistics Graphs: Q1

Incident Count $Amount

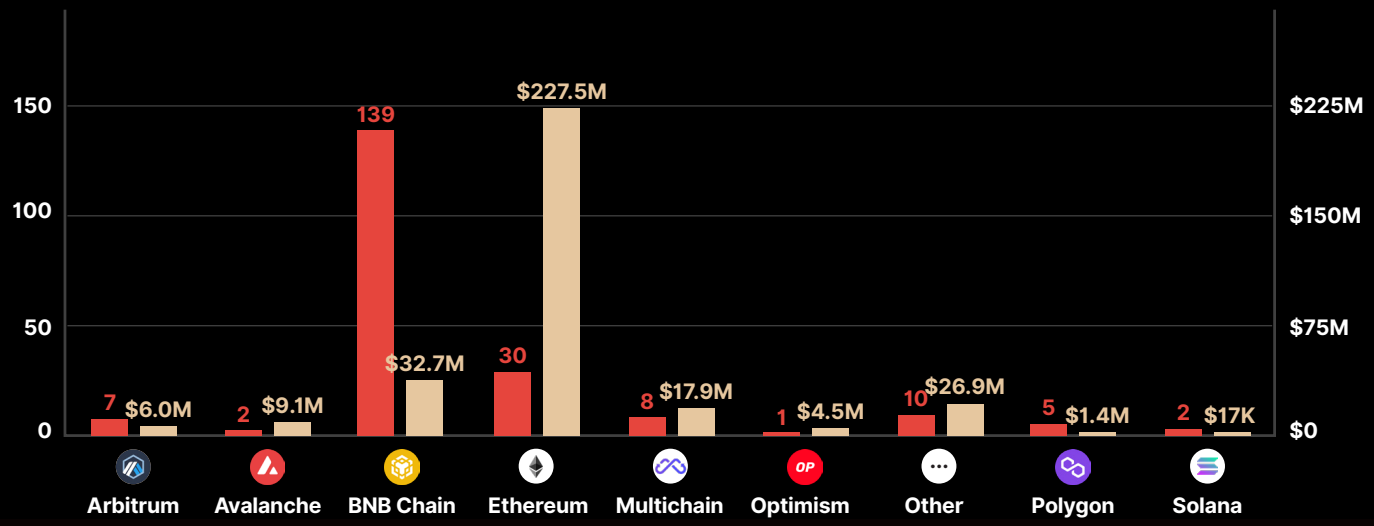
BY MONTH



BY TYPE

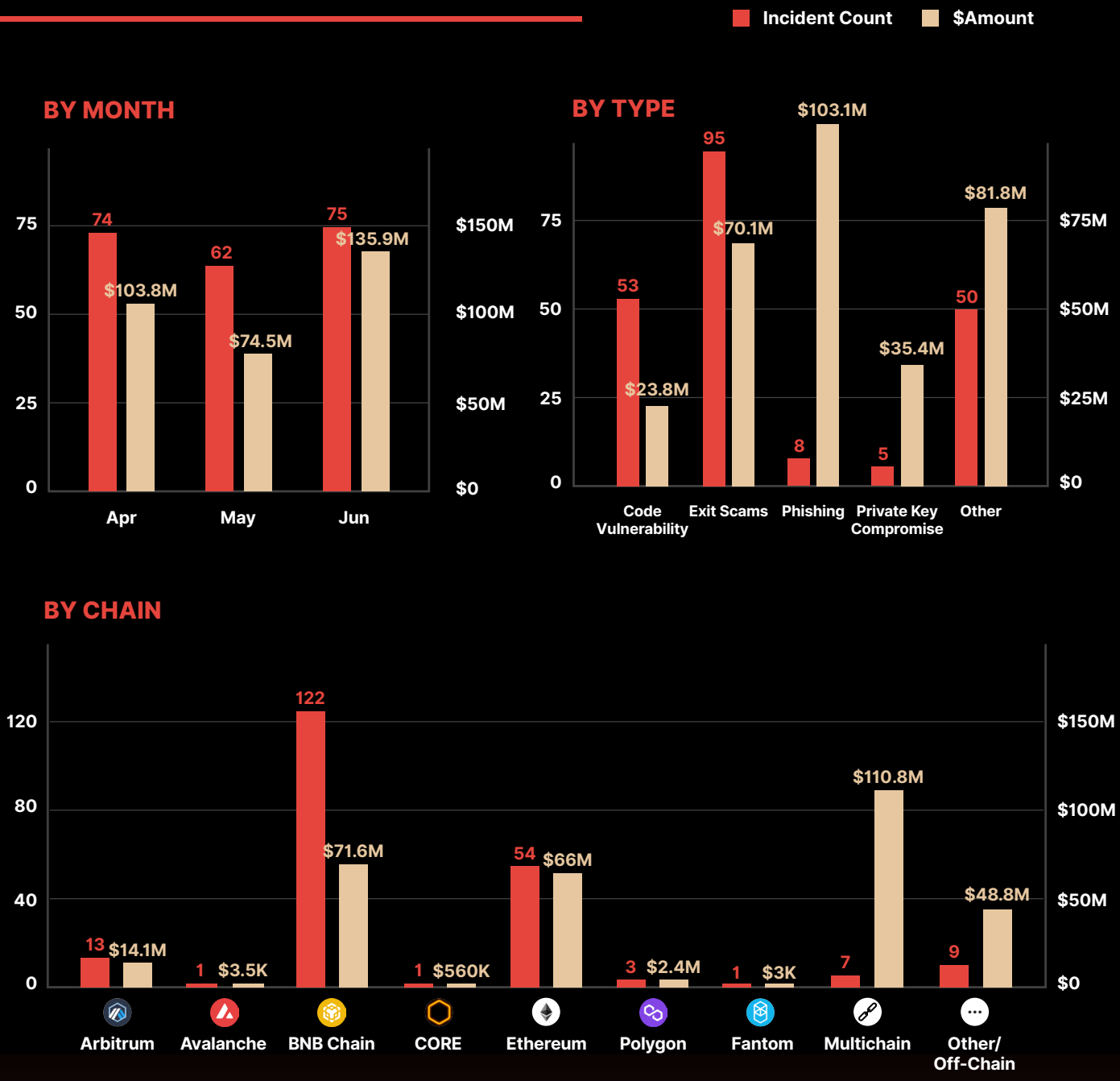


BY CHAIN



Numbers are approximate and may change with new information

Statistics Graphs: Q2

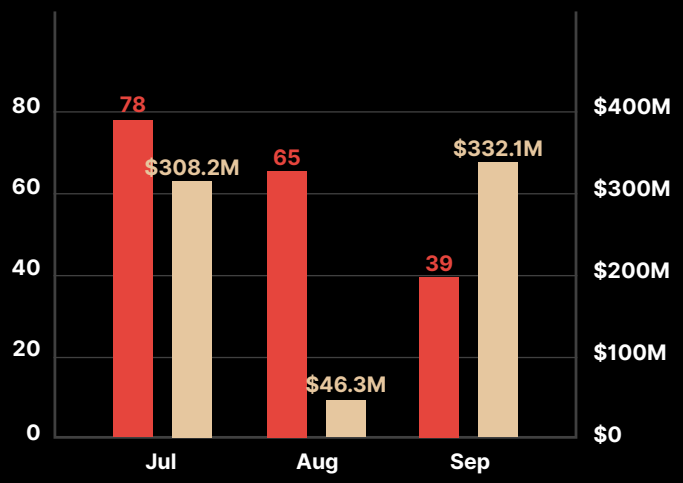


Numbers are approximate and may change with new information

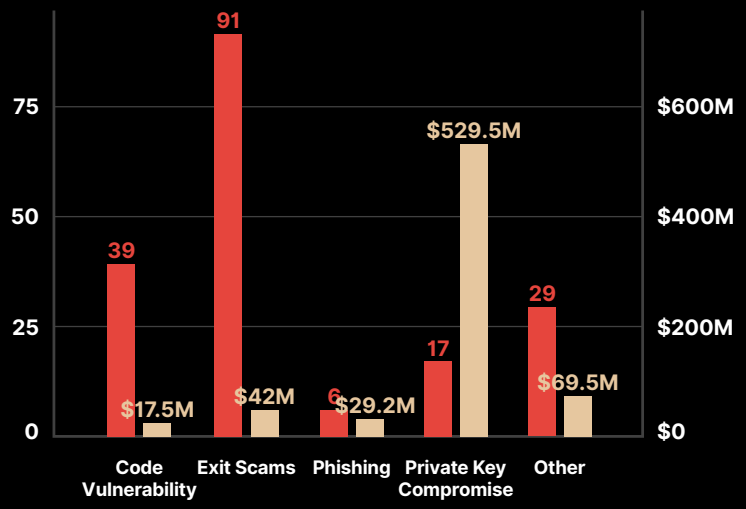
Statistics Graphs: Q3

Incident Count $Amount

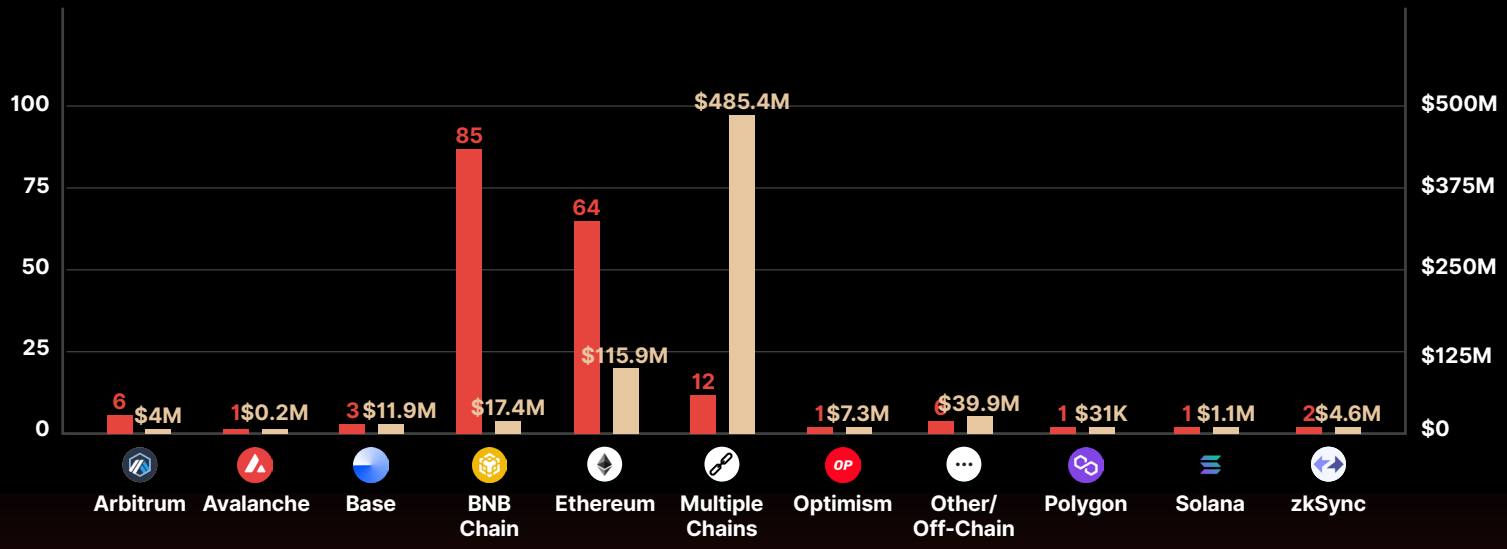
BY MONTH



BY TYPE



BY CHAIN

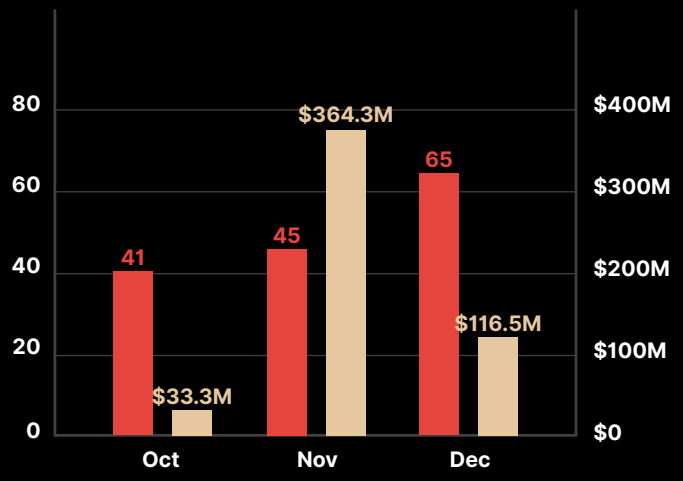


Numbers are approximate and may change with new information

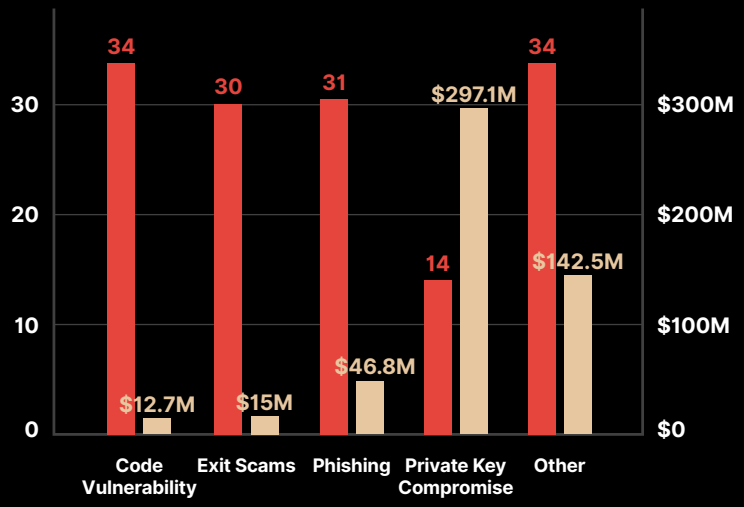
Statistics Graphs: Q4

Incident Count $Amount

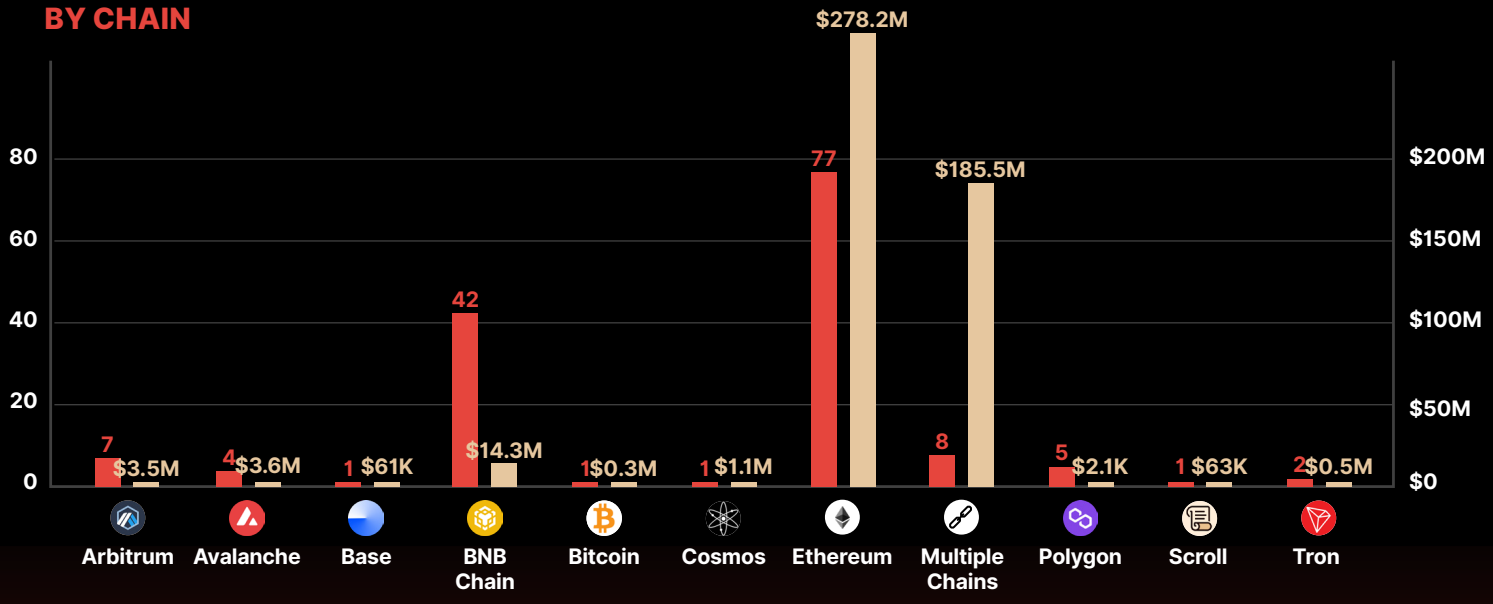
BY MONTH



BY TYPE



BY CHAIN



Numbers are approximate and may change with new information

Introduction

2023 saw a 51% decline in the value lost to hacks, scams, and exploits in Web3. Still, $1.8 billion is nothing to sneeze at, and in this report, we'll examine the major incidents and exploits that led to this ten-digit number.

The crypto industry faced legal and regulatory headwinds throughout 2023, with the U.S. Securities and Exchange Commission (SEC) bringing charges against the two largest exchanges: Coinbase and Binance. The SEC's actions indicated a move away from focusing solely on smaller platforms and individuals to targeting more significant players in the crypto space. The year also saw one of the most significant players – Binance founder Changpeng Zhao (CZ) – step down from his role as CEO after the exchange's $4.3 billion settlement with federal prosecutors in the US. CZ is currently out on a $175 million bond as he awaits sentencing in February.

Meanwhile, the FTX saga came one step closer to resolution in November with the conviction of Sam Bankman-Fried on seven counts, including fraud and money laundering. FTX creditors are still yet to see any fraction of their assets returned.

On the bright side, Q4 saw a recovery in crypto asset prices, a welcome reversal in the market after eighteen months of declining values. As the saying goes, bear markets are for building, and we have seen plenty of progress made on all fronts: from the technical to the regulatory.

Now is the time to look back on the last year, celebrate the achievements, recognize the missteps, and look forward to the future (hint: it's bright).

But first, a toast to those who make crypto what it is, the indefatigable few who stand defiant in the face of regulatory crackdowns, widespread skepticism, and the occasional 90% drawdown. On-chain actors stand at the forefront of innovation and risk. They are the guinea pigs of a new system; the proof of the pudding for those who see the potential of blockchain technology but lack the risk tolerance for getting involved on the far left side of the adoption curve. As they navigate through challenges such as usability hurdles, security lapses, and the journey towards establishing a solid product-market fit, their resilience is continually tested. Moreover, they face frequent skepticism from established players outside the industry, who exaggerate failures and minimize victories.

Despite these obstacles, the dedication of these degens, investors, hobbyists,

and technologists paves the way for future advancements in the field. And the rewards for these pioneers are significant. Early adopters gain access to exclusive opportunities, like lucrative airdrops and the thrill of being at the forefront of technological innovation. Their endeavors not only shape the industry but also build a foundation for future participants. They experience the excitement of shaping cutting-edge developments and accrue both knowledge and value, both of which will grow exponentially across coming cycles. As blockchain technology begins to gain traction among institutional entities, who wield trillions of dollars in financial influence, its potential becomes increasingly evident. We anticipate transformative impacts across sectors like finance, gaming, art, and digital experiences.

One bright spot on the horizon is the potential (or likely, depending on who you ask) approval of up to almost a dozen Bitcoin ETFs (exchange traded funds) in early January 2024. In the latter half of 2023, the SEC scrutinized a series of Bitcoin ETF proposals, notably extending review periods for applications from major firms like BlackRock, ARK, and Fidelity. This came after a D.C. Circuit Court ordered the SEC to reevaluate rejections like Grayscale Investments' case, ruling that it was wrong to reject Grayscale's application for a Bitcoin ETF on the grounds that it had previously approved Bitcoin futures ETFs which were "materially similar" to a spot Bitcoin ETF.

Regardless of the SEC's decision, which must be delivered by January 10, the crypto industry will continue its volatile but ever-upward path to maturity. At CertiK, we are at the forefront of securing this digital frontier. We all have our part to play, and CertiK's mission is to secure the Web3 world. To this end, we've audited more than 4,200 platforms and detected over 60,000 vulnerabilities. Our mission is ongoing, and 2023 has seen achievements like the release of the SkyInsights crypto compliance and risk management platform. This platform marks a significant milestone in our commitment to enhancing digital security. Recognition in Apple and Samsung patches for our mobile device security contributions underscores our impact on the broader technology ecosystem. Additionally, bug bounty payouts from SUI and Wormhole highlight the effectiveness

of our proactive security measures in 2023. These accomplishments demonstrate our commitment to enhancing the security and reliability of the Web3 world.

While the future of the industry is brighter than ever, challenges still remain. Although $1.8 billion is a significant decline from last year, it's still too much.

In our Hack3d reports, we aim to distill the signal from the noise. There were well over 700 security incidents in Web3 over the course of 2023 (nearly 300 exit scams alone)—far too many to examine individually. Instead, we focus on the standouts that highlight systemic vulnerabilities and the industry's capacity to respond with resilience.

First, we analyze the degree to which declining losses are a function of declining asset values, posing the question of whether we as an industry are learning our lessons. Next, we highlight the ongoing prevalence of devastating private key compromises, a disappointing phenomenon as password management predates blockchain technology entirely. The recent Ledger exploit highlights the dangers of phishing and supply chain attacks, while our examination of retroactive bug bounties sheds light on the effectiveness of this last-ditch effort to reclaim funds after an attack. We then move on to coverage of the dramatic KyberSwap hack, investigate a framework-level vulnerability in the integration of two specific standards, and finally take a look at where the trend of institutional adoption of blockchain led in 2023.

These selected trends and incidents provide clear examples of the challenges we face, but more importantly, they showcase the Web3 industry's collective response and adaptability. They tell a story of an industry that, despite setbacks, is making steady progress toward securing a more robust digital future.

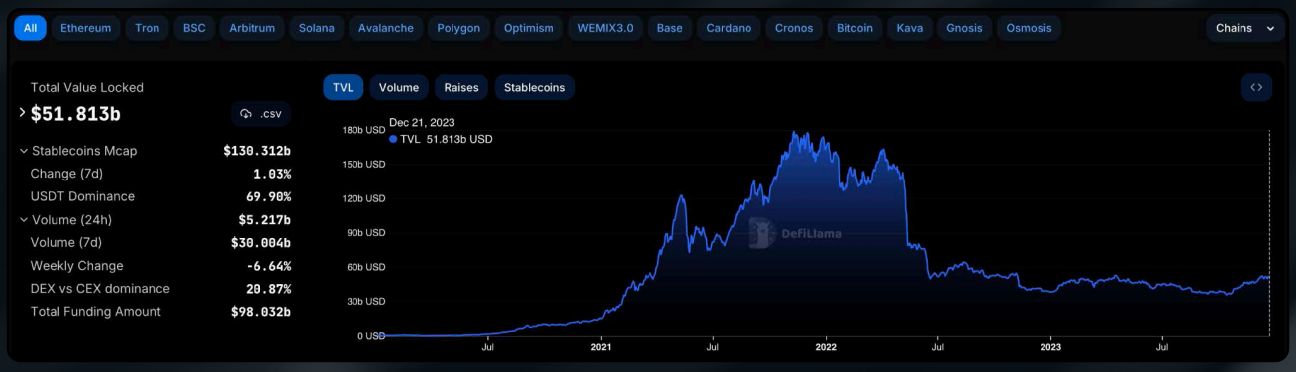
Statistical Analysis: Are We Learning Our Lessons?

2023's headline figure of a 51% decline in losses from 2022 is worth investigating. Is it simply the result of declining asset valuations? To answer this question, we'll examine the relationship between Total Value Locked (TVL) and losses to hacks, scams, and exploits in Web3.

TVL is one of the most important metrics in DeFi. It's a measure of the value of assets deposited in decentralized financial protocols, and as such is representative of the demand for DeFi's offerings.

While many tokens deposited in DeFi protocols are stablecoins, many are not, which means they are subject to market fluctuations. Thus, TVL is influenced by overall market conditions, as well as user demand. This makes it a useful metric for gauging the true active engagement and growth in the DeFi space, beyond just surface-level market capitalization. Unlike crypto's total market cap, which primarily reflects the valuation of assets, TVL offers insight into how much capital is actually being utilized within the DeFi ecosystem.

As of the time of writing in late 2023, DeFi's TVL stands at about $50 billion, down from a peak of $170 billion in November 2021 but up 40% from a low of $36 billion in October of this year.

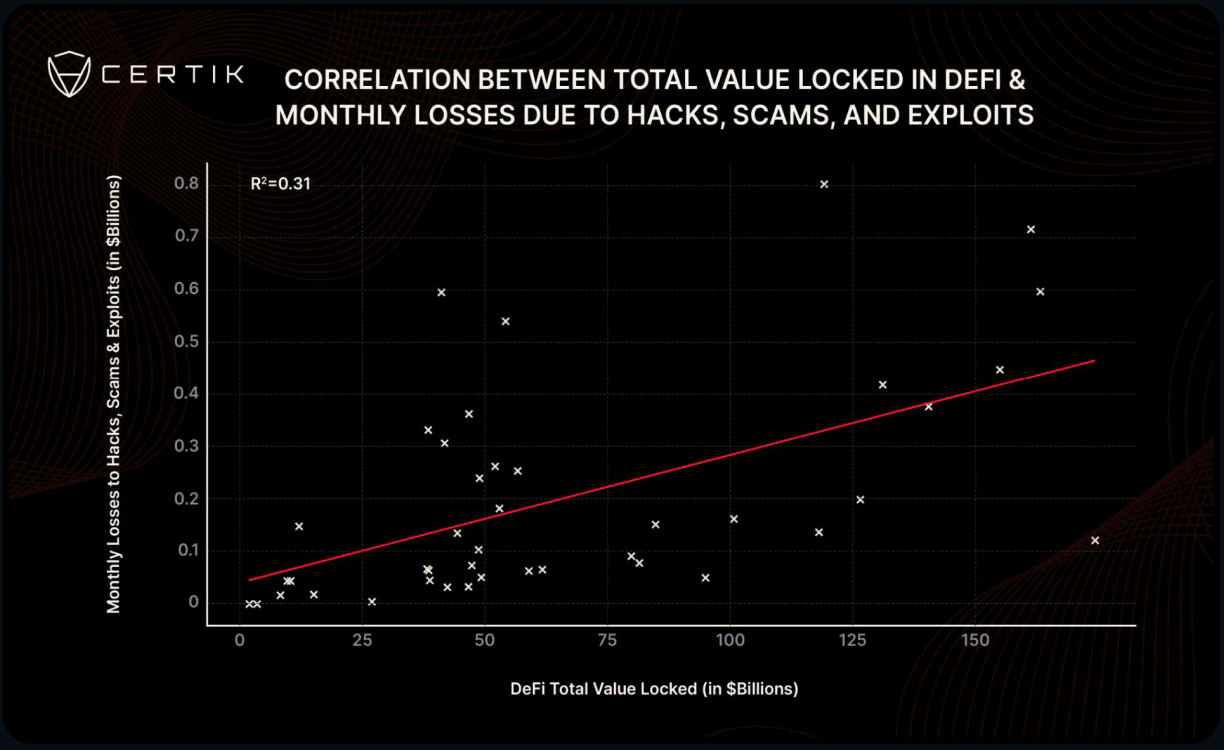


Source: DeFiLlama

The decline in losses to security incidents from 2022 to 2023 mirrors the decline in time-weighted average TVL in 2023 compared to 2022, which is down approximately 46%.

So, is this correlation the only explanation for 2023's lower losses? Do we have no reason to celebrate? Have we once again failed to learn our lessons, and will any forthcoming appreciation in asset values necessarily mean we return to record-breaking sums lost to hacks and scams?

Let's look at the data:



This scatter plot charts the correlation between monthly losses to hacks and scams in Web3 with the TVL in DeFi. It covers the 41 months from June 2020 – when DeFi first crossed the $1 billion TVL threshold – to November 2023.

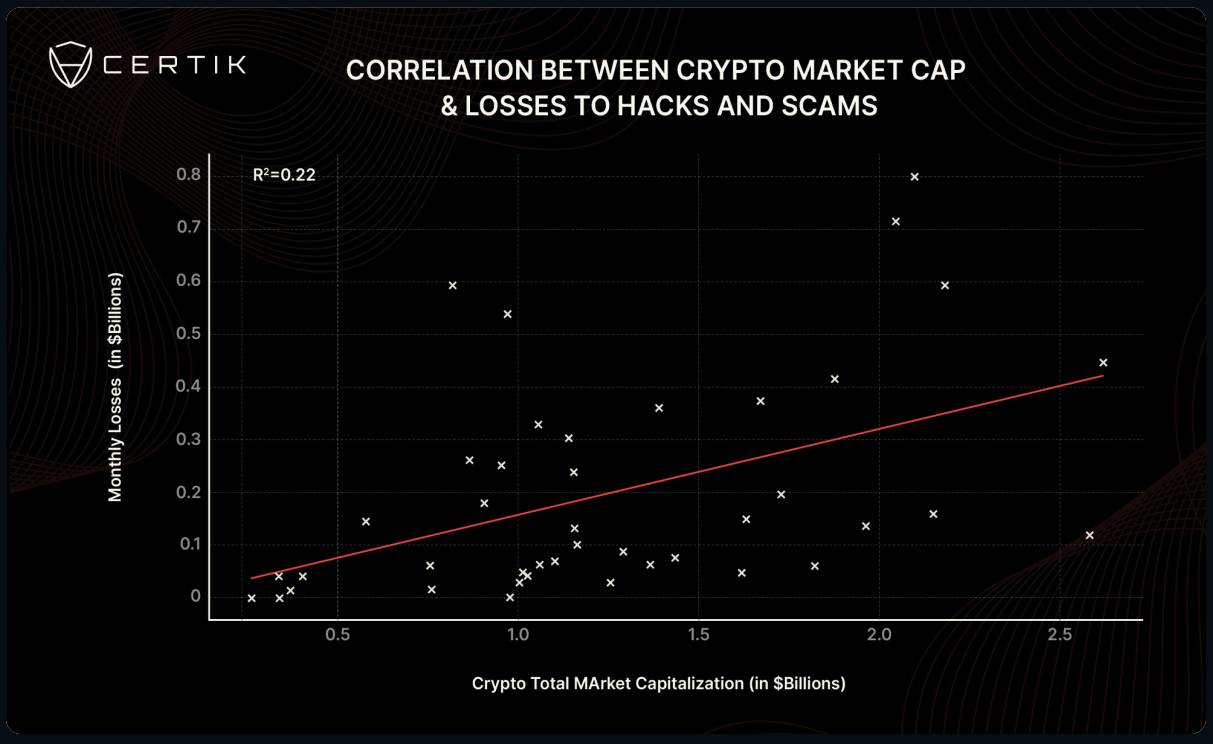
TVL values are taken on the last day of each month from DeFiLlama's dataset. Value lost to hacks and scams are monthly totals from CertiK's own data.

There is a moderate positive correlation between TVL and monthly losses, with an R2 value of 0.31. This suggests that approximately 31% of the variability in monthly losses can be statistically attributed to changes in DeFi's TVL, which itself is a proxy for both asset valuations and user demand. The trend line's positive

gradient indicates that as TVL increases there is a tendency for losses from security incidents to rise as well, albeit not in a strictly proportional manner. This correlation, while statistically significant[1], leaves a substantial 69% of the variability unexplained by TVL alone, suggesting other factors also play important roles in influencing the losses within the ecosystem.

The R2 value of 0.31 for this analysis is approximately 50% greater than that of the same analysis performed on a dataset matching monthly losses to security incidents with cryptocurrency's total market capitalization, which leads to an R2 value of 0.22.

> **"31% of the variability in monthly losses can be statistically attributed to changes in DeFi's TVL"**



[1]Our analysis yielded an F-statistic of 17.65, leading to a very small p-value of 0.000144. This low p-value rejects the null hypothesis of no effect, indicating that our findings are not simply due to chance. The regression coefficient for TVL was 2.417e-12, implying that changes in TVL are likely to influence the losses experienced. The p-value for our TVL variable was effectively zero, allowing us to confidently conclude that there is a statistically significant relationship between TVL and losses. The 95% confidence interval around our coefficient further validates these results.

The correlation between losses to security incidents and DeFi's TVL is stronger than that between losses and total cryptocurrency market capitalization.

This indicates that TVL is a more effective metric for understanding the dynamics of losses within the DeFi sector compared to just evaluating the overall market capitalization of cryptocurrencies. While market cap gives a broad view of the crypto industry's market value, TVL specifically reflects the active engagement and real-time utilization of assets within DeFi protocols. The stronger correlation with TVL underscores the direct impact of DeFi activities and investor behavior on the security landscape. These insights suggest that factors specific to DeFi, such as the sophistication of protocols, user behavior, and the effectiveness of security measures, are more closely correlated with the value of losses from security incidents than the broader macro trends indicated by the total market capitalization.

Market conditions, such as bull or bear trends, certainly do affect the attractiveness of DeFi platforms to both users and attackers. In bull markets, increased activity and higher asset values can present more lucrative targets for attackers, driving an uptick in the frequency and scale of security incidents. Conversely, during market downturns, reduced asset and treasury valuations lowers the impact of attacks, but the desperation of some actors may lead to more aggressive tactics.

It's important to note that the relationship between DeFi's TVL and losses to hacks and scams only explains roughly a third of the fluctuations in value lost to security incidents. There are clearly other factors at play, which suggests that participants in Web3 have a significant degree of influence to put to use.

For example, with each major hack or scam, the collective knowledge base of the industry grows. Protocols learn from past mistakes, implementing stronger security measures and fostering a culture of vigilance. For example, the increased use of bug bounty programs, improved coding practices, and the wider adoption of risk mitigation strategies (such as comprehensive pre-deployment security reviews and ongoing monitoring once live) all point to an industry that is learning and adapting. As platforms

and protocols evolve and patch known vulnerabilities, attackers continuously refine their methods, employing more advanced techniques to exploit newer, more obscure weaknesses. This open-source arms race between attackers and defenders is essential to consider as a fundamental driver of the incident rate.

Looking ahead, the real test of DeFi's improved security protocols awaits in the resurgence of a bull market. The expectation isn't to eliminate losses entirely — an unrealistic goal in an industry that prides itself on cutting-edge innovation — but to continue reducing the correlation between TVL and losses to hacks and scams. Such a trend would be the clearest indicator of a maturing industry that takes security seriously. The proof of the pudding will indeed be in the eating — and for DeFi, the next taste test could define its legacy and ultimate viability.

Not So Private: Compromised Keys Unlock Millions

> **Six of the ten most costly security incidents over the course of 2023 were due to private key compromises**

In 2023, the Web3 world continued to grapple with the threats posed by private key compromises. Accounting for nearly 50% of total losses, and amounting to $880 million, these compromises were a painful reminder of the importance of secure private key management. These losses stemmed from just **47** incidents, representing only **6.3%** of total security incidents throughout the year yet over half of the losses.

Notably, six of the ten most costly security incidents over the course of 2023 were due to private key compromises.

Highlighting the severity of this issue was the July compromise of Multichain, which resulted in a **$125 million** loss. Behind the scenes, it was revealed that, contrary to its claims of decentralization, Multichain's multi-party computation servers and private keys were solely controlled by its CEO. This vulnerability was exposed when the CEO was arrested, leaving $1.5 billion in TVL on the Multichain bridge inaccessible to users. The situation worsened as funds began moving to unknown wallets, underscoring the vulnerability inherent in centralized private key control.

To combat such centralization risks, CertiK partnered with Safeheron, an enterprise private key self-custody service provider. This collaboration has yielded a novel verification mechanism, allowing users to confirm that projects have integrated secure private key management systems. This initiative is crucial as many Web3 projects, either through smart contracts or individual account addresses, inadvertently create single points of failure.

We highlight these centralization risks in the course of our security reviews, but implementing the required solutions ultimately rests with the project owners. Our collaboration with Safeheron has introduced interfaces enabling both security firms and end-users to validate whether a project's address is secured by a key custodian solution, enhancing transparency and confirming the implementation of decentralization measures.

PRIVATE KEY MANAGEMENT BEST PRACTICES

1. Multi-Signature Wallets: Utilize multi-signature wallets to distribute control among multiple parties, reducing the risk of single-point failures.
2. Hardware Wallets: Consider hardware wallets for high-grade key storage and cryptographic operations, which help ensure private keys are never exposed in plain text.
3. Secure Backup Procedures: Keep backups of private keys in secure, offline environments like safety deposit boxes or vaults.
4. Access Control Policies: Define strict access control policies, ensuring only authorized personnel have access to private keys.
5. Encrypted Storage: Store private keys in encrypted formats, preferably using strong encryption standards.
6. Audit and Monitoring: Regularly audit and monitor the use of private keys to detect any unauthorized access or anomalies.
7. Cold Wallets for Long-Term Storage: Use cold wallets (offline storage) for long-term storage of private keys, minimizing exposure to online threats.
8. Employee Training: Train all relevant employees on best practices for key management, emphasizing the importance of security and confidentiality.
9. Multi-Party Computation (MPC): Consider MPC for key management to enable key sharing without exposing the entire key to a single party.
10. Use of Key Management Services: Employ professional key management services or solutions, especially for enterprise-level operations, to ensure compliance with industry standards.

Read more:

- ↗ What are Public and Private Keys?
- ↗ Web3 Mobile Wallet Apps: A Secret Key Protection Perspective
- ↗ What is Multi-Party Computation (MPC)?
- ↗ Exploring the Efficiency of MPC Algorithms in Crypto Wallets
- ↗ Multi-Party Computation (MPC) in Wallets: A Review of Current Strategies

Ledger's Library Leak

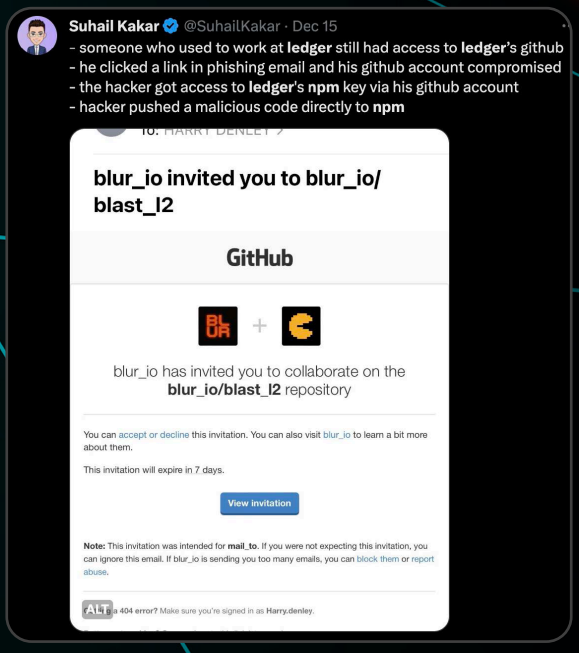
Wallet drainers have continued to be a persistent threat in Web3 throughout 2023. These drainers are a type of malicious software or script that allow scammers to "drain" assets from a victim's wallet to their own. The scammers typically trick users into granting token permissions through deceptive means like phishing websites and fraudulent applications.

We've uncovered some major players in the wallet drainer space, who have targeted thousands of users and stolen millions of dollars. The typical advice is to use a hardware wallet and to always avoid granting token permissions to sites you haven't completely verified. Sites like revoke.cash can help you manage the sites to which you've granted permissions. It's good practice to revoke permissions that you don't use anymore or don't recognize.

However, on December 14, Ledger, one of the largest manufacturers of crypto hardware wallets, confronted a cybersecurity nightmare that left many Web3 users unsure of where they could turn for a secure wallet provider.

A former employee fell victim to a sophisticated phishing attack, which enabled the attacker to gain access to the company's Ledger Connect Kit, a JavaScript library used for connecting websites to Ledger wallets. Losses from the exploit totaled $610,000 – a relatively modest payday for the attacker – but the damage to Ledger's reputation is harder to quantify.

The successful phishing attack gave control of the employee's NPMJS account, a critical node in the JavaScript package ecosystem. The breach allowed the attackers to upload a malicious file to Ledger's NPMJS.



This file was designed to appear as a legitimate update, but it contained a malicious payload. The code specifically targeted the interaction between Ledger wallets and various decentralized applications (dApps) that utilized the Connect Kit.

Once the file was in place, the infected Ledger Connect Kit operated as a Trojan horse. When users attempted to connect their Ledger hardware wallets to these dApps, they were unknowingly exposed to the exploit. Instead of establishing a secure link between their wallet and the application, the malicious code rerouted the connection through a fake WalletConnect protocol.

While the exploit was active for approximately five hours, the period during which funds were drained was less than two hours.

Ledger deployed an update within 40 minutes of discovery. This fix involved updating NPMJS to remove and deactivate the malicious code, effectively neutralizing the immediate threat posed by the exploit.

This exploit is proof of the continued threats posed by a number of distinct trends we've talked about extensively:

- The ongoing and far-reaching effects of centralization in Web3
- The impact of Web 2.0 systems (in this case NPMJS) on Web3 platforms and architectures
- Phishing as an effective attack vector

Despite the decentralized ethos of blockchain and cryptocurrency, there are elements within the ecosystem, such as NPMJS accounts and software libraries like the Ledger Connect Kit, that represent centralized points of vulnerability. And it just took a successful phishing attack on a single employee's account to lead to a breach that affected a wide range of users and dApps.

The Ledger Connect Kit exploit is a reminder of the inherent challenges in balancing the decentralization ideals of blockchain with the practical realities of software development and maintenance.

Retroactive Bug Bounty Negotiations

We saw a trend of "retroactive bug bounties" emerge in 2023, with $219 million returned across 36 events. This represents 12% of the $1.8 billion lost in total, and a 54% increase in negotiated returns in 2023 compared to previous years.

The term “retroactive bug bounty” is an ironic one, as negotiations are heavily skewed in the attacker’s favor in the aftermath of a successful exploit. Many would see these negotiations as extortion attempts, but regardless of one’s views on the matter it is an incontestable fact that a number of protocols have successfully negotiated “gray-hat” bounties that lead to the return of significant portions of stolen funds.

Euler Finance takes second spot on the leaderboard of most-costly security incidents of 2023, with $197 million lost in March. The exploit was executed through malicious flash loans and targeted Euler's donateToReserves() function across five separate pools. The attacker created a highly leveraged insolvent position using Euler’s mint() function and liquidated their position in the same transaction to gain a large number of derivative eTokens before draining the pool. The stolen funds were primarily in the form of DAI, WETH, WBTC, stETH, and USDC, and were later converted to ETH and DAI.

After the exploit, Euler Finance offered a $1 million bounty for information leading to the arrest of the attackers and demanded the return of the stolen funds. The attacker initially moved some of the stolen funds to Tornado Cash, seemingly ignoring Euler Finance's ultimatum. However, the exploiter, identifying themselves as "Jacob," then sent a message to an Ethereum address linked to Euler, expressing a willingness to start a dialogue and no intention of keeping the remainder of the stolen assets.

Between March 25 and March 28, the Euler exploiter returned a total of 84,951 ETH, worth approximately $147.8 million, and $29.9 million in the DAI stablecoin. The hacker expressed remorse for the attack, acknowledging the impact on

others' money, jobs, and lives and claimed that the delay in returning the funds was due to concerns for their own safety.

The Euler team responded positively to these developments, stating that as the hacker "did the right thing," they would no longer accept new information leading to the hacker's arrest, and the $1 million reward was no longer available.

Retroactive bug bounty negotiations have become an often-critical component of the post-attack response. While the strategy has yielded varying degrees of success, Web3 projects cannot rely on this approach. Comprehensive bug bounty platforms that pay out enough to incentivize white-hat hackers to disclose vulnerabilities before they're exploited for profit are essential.

Read more:

- A Grey Area: Retroactive Bug Bounty Negotiations
- Shifty Negotiations: Are Projects Still Benefiting From Negotiating With Their Attackers?
- Euler Finance Incident Analysis

The KyberSwap Hack

One platform that has so far failed to negotiate a “retroactive bug bounty” is KyberSwap, which on November 22, 2023 fell victim to a sophisticated exploit leveraging flash loans that drained approximately $47 million worth of assets across several blockchains.

- **Flash loan:** a type of loan in decentralized finance (DeFi) where a borrower can take out a large amount of cryptocurrency instantly and without collateral, with the condition that it must be repaid within the same transaction block. If the loan is not repaid within that single transaction, it is as if the loan never happened, reverting all actions taken. This unique feature makes flash loans useful for a variety of financial maneuvers in the DeFi space, such as arbitrage, collateral swapping, and self-liquidation.

KyberSwap’s model, inspired by Uniswap v3, introduced concentrated liquidity market makers, allowing liquidity providers (LPs) to add liquidity within specific price ranges, termed "ticks." Each LP position was uniquely tracked, as liquidity became non-fungible within these pools.

- **Tick:** a specific price point within a liquidity pool of a decentralized exchange. Liquidity providers can choose to add liquidity to the pool at these discrete price levels, creating a series of concentrated liquidity zones. Each tick represents a price threshold, and the liquidity is active only when the pool's price is within the range of these ticks. This mechanism allows for more efficient capital utilization and better control over the price ranges in which liquidity providers wish to participate.

The KyberSwap hack involved multiple attacks all using the same method. Let's consider the USDC-ETHX pair for illustration. The attacker first borrowed 500 ETHx through a flash loan from Uniswap and targeted the KyberSwap v2 Reinvestment Token (KS2-RT) pool. By trading a large amount of ETHx for USDC, they exhausted the pool’s liquidity and significantly increased the pool's current tick value.

With only a small amount of ETHX and USDC left in the pool, the attacker then created a new liquidity pool in a narrow tick range, strategically positioning it to exploit this artificially inflated price range. They partially removed liquidity from this range but left enough to manipulate the next set of transactions.

The attacker's subsequent ETHx for USDC swap appeared unusual, as they were the sole liquidity provider in that range. However, this was a setup for the next phase of the exploit. KyberSwap's `computeSwapStep()` function, which determines if a swap crosses a tick range, was manipulated by the attacker's precise input amounts. This manipulation prevented the function from updating the next price, creating false liquidity in the pool.

Finally, the attacker reversed the swap, exchanging USDC for ETHx, which lowered the price and allowed them to exploit the falsified liquidity, thereby draining the pool of USDC for profit. This technique was replicated across various KyberSwap pairs on multiple chains, leading to substantial losses on each.

After the attack, the hacker made a series of highly unconventional demands:

> To ALL relevant and/or interested parties,
>
> I thank you for your attention and patience during this uncertain time for Kyber (the protocol/DAO) as well as Kyber (the company). Below I have delineated a treaty for us to agree to.
>
> My demands are as follows:
>
> * Complete executive control over Kyber (the company)
>
> * Temporary full authority and ownership over the governance mechanism (KyberDAO) in order to enact legislative changes. My current wallet address is fine for this.
>
> * All documents and information related to company / protocol formation, structure, operation, revenues, profits, expenses, assets, liabilities, investors, salaries, etc.
>
> * Surrender of all Kyber (the company) assets. This is both On-chain and Off-chain assets. It includes but is not limited to: shares, equity, tokens (KNC and non-KNC), partnerships, blogs, websites, servers, passwords, code, social channels, any and all creative and intellectual property of Kyber.
>
> Once my demands have been met, I will provide the following:
>
> * Executives, you will be bought out of the company at a fair valuation. You will be wished well in your future endeavors. You haven't done anything wrong. A small error was made, rounding in the wrong direction, it could have been made by anyone. Simply bad luck.
>
> * Employees, under the new regime your salary will be doubled. It is understandable that many current employees will want to leave regardless. The employees who don't want to stay will be given a 12-month severance with

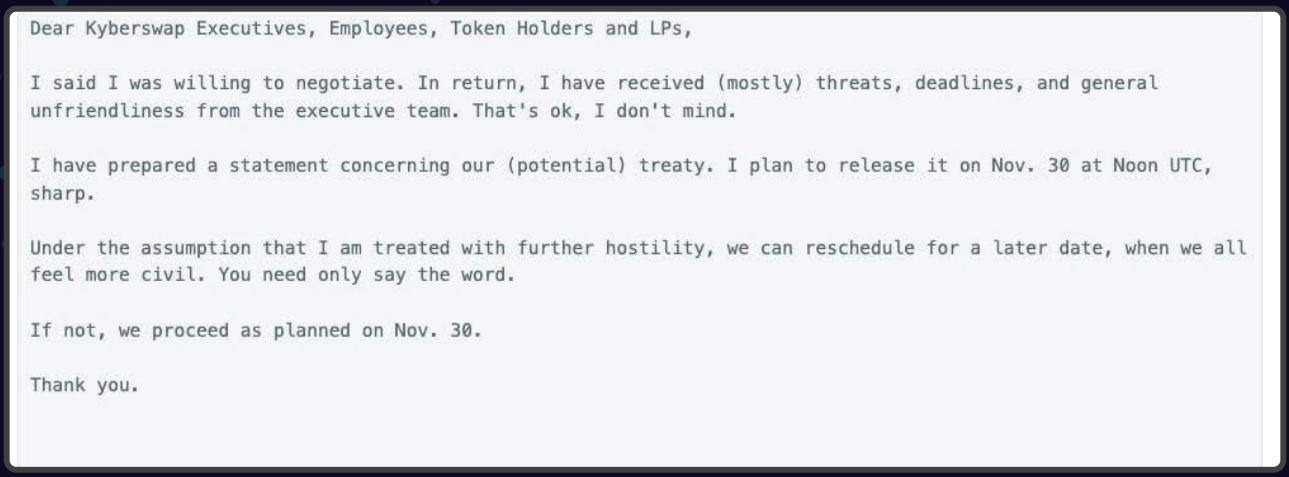
> full benefits and assistance in finding a new career, no questions asked.
>
> * Token Holders and Investors, under this treaty, your tokens will no longer be worthless. Is this not sweet enough? I'll go further still. Under my management, Kyber will undergo a complete makeover. It will no longer be the 7th most popular DEX, but rather, an entirely new cryptographic project.
>
> * LPs, you will be gifted a rebate on your recent market-making activity. The rebate will be for 50% of the losses you have incurred. I know this is probably less than what you wanted. However, it is also more than you deserve.
>
> This is my best offer. This is my only offer.
>
> I require my demands to be met by December 10, otherwise, the treaty falls through.
>
> Additionally, should I be contacted by agents from any of the 206 sovereignties, concerning the trades I placed on Kyber, the treaty falls through. In this case, rebates will total to exactly 0.
>
> Kyber is one of the original and longest-running DeFi protocols. No one wants to see it go under.
>
> To assist with this transition of leadership, I may be contacted on telegram: @Kyber_Director
>
> Thank you.
>
> - Kyber Director

Source: Etherscan

KyberSwap responded by offering a bounty to the hacker, proposing that if 90% of the stolen funds were returned, the attacker could keep the remaining 10%. However, when the hacker did not immediately comply, KyberSwap escalated the situation by threatening legal action and involving law enforcement.

The attacker demanded a more respectful tone from the team. The hacker threatened to delay any negotiations unless they felt the KyberSwap executives were being sufficiently civil towards them.

The hacker stated in their on-chain message: *"I said I was willing to negotiate. In return, I have received (mostly) threats, deadlines, and general unfriendliness from the executive team... Under the assumption that I am treated with further hostility, we can reschedule for a later date, when we all feel more civil."*



Dear Kyberswap Executives, Employees, Token Holders and LPs,

I said I was willing to negotiate. In return, I have received (mostly) threats, deadlines, and general unfriendliness from the executive team. That's ok, I don't mind.

I have prepared a statement concerning our (potential) treaty. I plan to release it on Nov. 30 at Noon UTC, sharp.

Under the assumption that I am treated with further hostility, we can reschedule for a later date, when we all feel more civil. You need only say the word.

If not, we proceed as planned on Nov. 30.

Thank you.

Despite the impasse in negotiations with the attacker, KyberSwap has managed to reclaim a portion of the stolen funds, with $4.67 million being returned by operators of front-running bots involved in the exploit. Meanwhile, KyberSwap introduced a grant initiative funded from its treasury, aimed at providing financial compensation to those affected by the security breach.

This grant, equating to the USD value of the lost assets, is intended to make users whole and demonstrate KyberSwap's commitment to its userbase.

Read more:

↗ KyberSwap Incident Analysis

The ERC-2771 Vulnerability: A Ticking TIMEbomb

On December 7, attackers exploited the TIME protocol, resulting in the loss of 89.5 ETH. They accomplished this by manipulating the Forwarder contract, which is generally trusted to execute transactions on behalf of legitimate senders, to burn $TIME tokens. This incident arose from an error in the Forwarder contract's application of the ERC-2771 standard, which is intended to facilitate user-friendly interactions with dApps by subsidizing gas fees.

The ERC-2771 standard enables users to interact with dApps without requiring Ether for gas, thereby promoting more user-friendly experiences. However, this facilitation introduces certain complexities that must be addressed.

The core of the ERC-2771 vulnerability lies in its handling of transaction relays. This standard was designed to allow for meta-transactions, where a third party can sponsor the gas fees of a transaction. However, the vulnerability arises from the way these transactions are processed and verified, leading to issues where the identity of the actual transaction initiator is obscured or misrepresented. The breach, which led to the TIME token incident, stems from a vulnerability within the standard's transaction processing mechanism, particularly in the ERC2771Context and Multicall contracts, which allows an attacker to spoof transaction sender addresses.

To exploit this vulnerability, an attacker must carefully craft transactions that manipulate the trustedForwarder check, which the ERC2771Context relies upon to validate the actual sender of the transaction. By doing so, the attacker can make the contract believe that the transaction is coming from a trusted address when, in fact, it is not. This misrepresentation can lead to unauthorized actions being executed within the contract.

```
function verify(ForwardRequest calldata req, bytes calldata signature) public view returns (bool) {
    address signer = _hashTypedDataV4(
        keccak256(abi.encode(TYPEHASH, req.from, req.to, req.value, req.gas, req.nonce, keccak256(req.data)))
    ).recover(signature);

    return _nonces[req.from] == req.nonce && signer == req.from;
}

function execute(ForwardRequest calldata req, bytes calldata signature)
    public
    payable
    returns (bool, bytes memory)
{
    require(verify(req, signature), "MinimalForwarder: signature does not match request");
    _nonces[req.from] = req.nonce + 1;

    // solhint-disable-next-line avoid-low-level-calls
    (bool success, bytes memory result) = req.to.call{ gas: req.gas, value: req.value }(
        abi.encodePacked(req.data, req.from)
    );

    if (!success) {
        // Next 5 lines from https://ethereum.stackexchange.com/a/83577
        if (result.length < 68) revert("Transaction reverted silently");
        assembly {
            result := add(result, 0x04)
        }
        revert(abi.decode(result, (string)));
    }
    // Check gas: https://ronan.eth.link/blog/ethereum-gas-dangers/
    assert(gasleft() > req.gas / 63);
    return (success, result);
}
```

TIME's verify function contained a flawed logic check that incorrectly equated the signer of a transaction with the from address, allowing an attacker to spoof this address and authorize transactions that should otherwise be restricted.

The implications of this are significant. For users, it undermines the security and trust they place in dApps utilizing the ERC-2771 standard. For developers and projects, it reveals an urgent need for a comprehensive audit and security review of their contracts, especially those that involve complex interactions like meta-transactions.

In response to the discovery of this vulnerability, the security community has rallied to patch the exploit and fortify the framework against future attacks.

Institutional Adoption: How Soon is Now?

2023 saw significant strides towards institutional adoption, signaling a possible tipping point in the upcoming when Proofs of Concept (POCs) begin to move into live production. Spearheading this shift are influential financial entities like Swift, the Hong Kong Monetary Authority, and the Australia and New Zealand Banking Group (ANZ), all of which have made major moves in integrating blockchain technology into their operations.

Swift, the global financial messaging network, has taken notable steps towards blockchain interoperability, with a specific focus on tokenized asset settlement. In 2022, Swift demonstrated its infrastructure's capability to connect various private blockchain tokenization platforms and in August of 2023 announced extensions to include public blockchains like Ethereum for settlement purposes. This paints an optimistic picture of a future where public networks operate seamlessly with private networks, and individuals and organizations can leverage the benefits of both.

ANZ, one of Australia's Big Four banks with assets under management (AUM) exceeding $1 trillion, ventured into digital assets in 2022 with the launch of the country's first ever private stablecoin (A$DC) and the trading of tokenized carbon credits using cross-chain infrastructure. The bank emphasizes the complementary nature of potential Central Bank Digital Currencies (CBDCs) and private-sector innovations, such as tokenized bank deposits that can be used as cash equivalents, in the payments space.

Innovation in Asia-Pacific continued with the Hong Kong Monetary Authority's (HKMA) February issuance of $100 million in tokenized green bonds.

Project Evergreen not only champions technological progress but also aims to set a precedent for future regulatory adaptations. The HKMA's report on its own issuance process highlights the importance of strategies that balances security, efficiency, and compliance, ideally ailored to integrate with established systems.

> Inter-operability with other conventional systems, such as existing custody systems and payment systems, is technologically complex. However, overcoming this hurdle can support the inclusion of every component of a bond transaction on-chain.
>
> – Bond Tokenisation in Hong Kong, HKMA (pg. 21)

The HKMA put significant emphasis on aligning tokenized bonds with existing securities regulations. The report also recognizes the continuous need for legal and regulatory updates to nurture the growth and adoption of blockchain technology. It cautions against the risks of market fragmentation and highlights the vast potential of blockchain across the broader financial domain.

These advancements indicate a maturing understanding and acceptance of blockchain's potential in traditional financial sectors. Swift's efforts in facilitating interoperability and ANZ's practical foray into tokenized assets and stablecoins exemplify the growing confidence in blockchain as a viable and necessary component of the financial ecosystem.

As these institutions continue to innovate and integrate blockchain solutions, they pave the way for a significant influx of capital into the blockchain space. Tokenization is poised to be a key driver in this shift, potentially heralding the arrival of a multi-trillion dollar wave of institutional capital onto blockchains.

Read more:

- ↗ Digital Assets:From Fringe to Future, BNY Mellon
- ↗ Larry Fink's Annual Chairman's Letter to Investors, Blackrock
- ↗ Relevance of On-chain Asset Tokenization in 'Crypto Winter', Boston Consulting Group

2023 at CertiK

2023 was a big year at CertiK. In addition to expanding our security services to new projects operating on new platforms, we:

- Discovered and safely disclosed a bug in Wormhole's Aptos contracts
- Were recognized in Apple's security updates for identifying vulnerabilities in iOS and iPadOS software (twice). We have a total of eight published CVEs, with more on the way.
- Were awarded a $500K bounty by Sui for the discovery of a critical vulnerability, codenamed "HamsterWheel", that had the potential to disrupt the entire Sui Layer one chain
- Were proud to see our co-founder, Professor Ronghui Gu, honored with the VMware Systems Research Award
- Became the first Web3 auditing firm to achieve SOC II Type I and II Compliance
- Verified The Open Network's (TON) transaction per second record
- Released SkyInsights, a crypto compliance and risk monitoring platform
- Formally verified HyperEnclave, a cross-platform Trusted Execution Environment (TEE) from Ant Group's Trust Native Technology team
- Audited XLS-30d, an AMM built on the XRP Ledger
- Partnered with Alibaba Cloud to bring blockchain security to the cloud
- Joined Finschia as a governance member and node validator after our audit
- Discovered an XSS vulnerability in WalletConnect's Verify API
- Produced a formally verified compiler for smart contracts, which we call DeepSEA
- Unmasked a million-dollar scammer
- Evaluated Safeheron's key sharding solution, identified and helped resolve a vulnerability
- Partnered with Coala Pay to streamline humanitarian aid funding
- Explored the and limitations of AI-powered auditing
- Formally verified OpenZeppelin's ERC-20 implementation
- Exposed the scammers behind a popular wallet drainer kit
- Identified an organized scammer group actively deploying malicious fake wallets

- Helped leading exchanges like OKX and wallet providers like ZenGo uncover and resolve vulnerabilities
- Saw our Skyfall team's proactive mobile security research recognized by Samsung with multiple CVEs

...and, as always, we published a wealth of content on our blog, underscoring our commitment to providing meaningful education and research in Web3. Here are some highlights from 2023:

SMART CONTRACT AND BLOCKCHAIN SECURITY FUNDAMENTALS

- A Short Introduction to Zero Knowledge Proofs
- Web3 Mobile Wallet Apps: A Secret Key Protection Perspective
- What is Formal Verification in Smart Contract Auditing?
- What is a Soulbound NFT?
- What is Multi-Party Computation (MPC)?
- How We Audit: A Comprehensive Guide to CertiK's Auditing Methodology
- Exploring the BRC-20 Token Standard: An Introduction
- What is Account Abstraction?
- Multi-Party Computation (MPC) in Wallets: A Review of Current Strategies
- Key Consensus Algorithms
- The Proliferation of Honeypot Contracts in Web3
- Tokenomics In DeFi Staking
- Soft Spots in Hard Tech: Mobile Security Challenges in Web3
- Scaling with Layer 2s: Rollups vs Sidechains
- Beyond the Bot: Unpacking Telegram Bot Tokens

ADVANCED BLOCKCHAIN SECURITY

- Cross-Function Reentrancy Attacks in Kadena Smart Contracts
- Runtime Environments and Smart Contract Security Modeling
- Critical Infrastructure: Secure Engineering of Blockchain Bridges
- The Move Prover: Quality Assurance of Formal Verification
- Diamond Proxy Contracts: Best Practices
- Why Memory-Safe Blockchain RPC Nodes are Not Panic-Free
- Formal Verification of TON Master Chain Contracts
- Auditing With Finite State Machines: A Complementary Methodology

- ↗ Challenges Encountered In the Formal Verification of ERC-20 Contracts
- ↗ Secure Smart Contract Programming in FunC: Top 10 Tips for TON Developers
- ↗ Gas Optimization in Ethereum Smart Contracts: 10 Best Practices
- ↗ Top 10 Security Tips for BNB Chain Builders
- ↗ How AI Can Enhance Cybersecurity: A Primer on Deep Learning and its Applications
- ↗ A Closer Look at Deep Learning Techniques for Software Security
- ↗ Exploring the Efficiency of MPC Algorithms in Crypto Wallets
- ↗ Fortifying ZenGo: Unearthing and Defending Against Privileged User Attacks
- ↗ Modal Phishing in Web3 Mobile Wallets
- ↗ How to Formally Verify A Cosmos SDK Standard Module

THREATS AND INTEL

- ↗ The Rug Pull Report
- ↗ How Pro-Russian Groups Are Fundraising on Telegram to Evade Sanctions
- ↗ How Safe is SafeMoon? Analyzing the FETA and BEVO Exploits
- ↗ KYC Actors are Ramping Up Their Game
- ↗ KYC'd Wallet Sales on Dark Net Markets
- ↗ On-Chain Ransomware - The Conti Group: Part One
- ↗ On-Chain Ransomware - The Ryuk Group: Part Two
- ↗ Chasing Shadows: A Decade of Criminal Crypto Seizures
- ↗ How Hackers Use DNS Hijacking Attacks to Steal Funds and Clone Websites
- ↗ BGP Hijacking: How Hackers Circumvent Internet Routing Security to Tear the Digital Fabric of Trust
- ↗ Intelligence Infiltration of Web3 Projects
- ↗ FinSoul: The Fintoch Fraud Continues
- ↗ The Rise of Stablecoins in Unstable Times
- ↗ Dirty Laundry: The Bitcoin Network's Growing Role in the Laundering of Stolen Crypto

CertiK's Security Suite

As part of our mission to secure the Web3 world, CertiK provides a number of tools designed to help projects and investors take an end-to-end approach to security.

CertiK KYC provides comprehensive and private identity verification for project teams. This process includes an ID authenticity inspection using AI-based detection systems, as well as liveness checks to ensure the individual is indeed real and matches the ID. CertiK will also undertake a live video call with each team member to verify their identity and other parameters as needed. As team anonymity increasingly enables high-risk behaviors, CertiK KYC helps to build accountability around projects to enable investors to move forward in trust. Projects that earn a Bronze, Silver, or Gold KYC Badge demonstrate to their community that they are willing to stand behind their project, sending a powerful message that they can be trusted to carry out the project's mission.

Penetration Testing is the final component of a comprehensive approach to securing crypto applications in a runtime environment. Our penetration testing services uncover even the smallest weaknesses by leveraging proprietary tooling, powered by an experienced team of ethical hackers.

CertiK Bug Bounty Program crowdsources intelligence from the world's top ethical hackers to uncover vulnerabilities before malicious actors can exploit them. CertiK's expert security engineers screen and qualify submissions and work with clients to implement the right fixes. Our 0% fee model reduces the payout pressure for projects and allows white hat hackers to receive the full bounty.

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.

Get the most out of Web3 by partnering with **CertiK Advisory**. Our team of seasoned analysts deliver a comprehensive range of services, including technical evaluations, proprietary research, and strategy recommendations.

CertiK Security Score Leaderboard lists and ranks projects according to their Security Score. The Security Score is generated using a proprietary algorithm that takes into account a project's Code Security, Fundamental Health, Operational

Resilience, Community Trust, Market Stability, and Governance Strength.

The Verified Teams Leaderboard lists and ranks projects based on the status of their CertiK KYC Badge. Project teams that successfully undergo a rigorous background investigation are granted the CertiK KYC Badge, which comes in Gold, Silver, and Bronze.

The Influencer Score Leaderboard lists and ranks Web3 influencers based on their influence score, which reflects the impact and reach of their content and online presence. This leaderboard is helpful for users who are interested in identifying influencers who are shaping the conversation in Web3.

Exchange Audit allows users to conduct due diligence on centralized exchanges (CEXs) by displaying the on-chain asset holdings in the wallet addresses controlled by the exchanges. This is an important first step for proof-of-reserve verification.

Skynet Alerts is a system that provides timely notifications on rugpulls and exploits in the cryptocurrency space. Skynet Alerts constantly monitors various sources of information to identify and report on potential rugpulls and exploits as they happen.

Smart Money Wizard is the access point for the Wallet Analyzer feature, and enables users to directly search for wallet addresses, view trending wallet searches, top smart money wallets, and top liquidity pairs. The Wallet Analyzer feature provides insights on wallet addresses and makes it easy to decipher on-chain transactions between wallets by displaying key wallet characteristics, visualizing wallet relationships and token trading activity.

Check out Skynet for Community platform today, read more on the Skynet education hub, and watch the masterclass on using Skynet to level up your due diligence research.

SkyInsights is a comprehensive crypto compliance and risk management platform. It offers wallet screening, real-time transaction monitoring, risk scores, and customizable alerts to help financial institutions, small-to-medium firms, and crypto-native platforms manage compliance complexities effectively. SkyInsights helps crypto-exposed organizations navigate regulatory

landscapes efficiently while maintaining efficient processes and enhancing client trust.

Supported Ecosystems: CertiK's security services are available for all projects on all blockchains. A list of ecosystems we've worked with includes:

- Algorand
- Aptos
- Arbitrum
- Avalanche
- BNB Chain
- Cardano
- Cosmos
- Cronos
- Ethereum
- Fantom
- Ferrum
- Harmony
- IoTeX
- Near
- OKTC
- Optimism
- Polkadot
- Polygon
- Solana
- Terra
- TON
- Tron
- WEMIX
- zkSync