CYVERS

Overview Cyvers 2024 Report

Annual trends in security, fraud, scams, risk management and compliance.

Overview 5
About Cyvers 5
Executive Summary 6
Cyvers Key Security, Fraud and Compliance Trends in 2024 6
Executive Summary 6
1. Overview 6
2. Key Stats of Malicious Activity 6
3. Attack Types (2024): 7
4. Recovery Rate: 8
5. Quarterly Highlights: 8
6. Notable Incidents 9
7. Future Trends 10
8. Cyvers's Innovative Solutions 10
Conclusion 10
Types of Incidents 11
Access Control vs. Smart Contract Vulnerability Attacks 11
Attack Breakdown by Chain: 13
Annual Statistics 16
Quarterly Statistics 16
Number of incidents per quarter 16
Funds lost per quarter 16
Monthly Statistics 17
Number of incidents per month 17
Funds Lost per Month 18
Funds Recovery 20
Notable Recoveries in 2024 20
Top 10 Incidents for 2024 22
1st Quarter 22
CoinsPaid Hack (January 6, 2024) 22
PlayDapp Hack (February 9–13, 2024) 23
Duelbits Security Breach (February 13, 2024) 24
Prisma Finance Hack (March 28, 2024) 24
2nd Quarter 25
Hedgey Finance Exploit (April 19, 2024) 25
Address Poisoning Scam (May 3, 2024) 26
Sonne Finance Hack (May 14, 2024) 27
DMM Bitcoin Hack (May 31, 2024) 27
Kraken Bug Bounty Controversy (June 9, 2024) 28
UwU Lend Exploit (June 10, 2024) 29

BtcTurk Hack (June 22, 2024) 29
3rd Quarter 30
Dough Finance Flash Loan Attack (July 12, 2024) 30
LiFi Protocol Exploit (July 16, 2024) 31
WazirX Hack (July 18, 2024) 32
DeltaPrime Hacks (September and November 2024) 32
Penpie Hack (September 3, 2024) 33
Indodax Hack (September 11, 2024) 34
BingX Exchange Hack (September 20, 2024) 35
4th Quarter 36
Base Blockchain Exploit (October 25, 2024) 36
Radiant Capital Hack (November 1, 2024) 36
CoinPoker Hack (November 8, 2024) 37
Polter Finance Exploit (November 17, 2024) 38
M2 Exchange Hack (October 31, 2024) 39
Audited Yet Hacked: The Imperative of Real-Time Monitoring in Web3 41
The Role of Smart Contract Audits 41
Case Studies: When Audited Contracts Fail 41
The Missing Link: Real-Time Monitoring and Pre-Transaction Screening 41
The Importance of Crisis Management Mechanisms 42
Conclusion 42
The Ripple Effect of Crypto Hacks on Companies 43
Financial and Market Impact 43
Survival Rates After Hacks 43
Dependency and Reputational Risks 44
Operational and Talent Challenges 44
Legal and Regulatory Repercussions 44
Evolving Security Measures 44
Conclusion 44
The Rise of Multisig Wallet Attacks in 2024:
Techniques, Impact, and Lessons Learned 46
Quantum and AI: Accelerating the Cyber Arms Race 47
Tokenized Real-World Assets: Securing a Revolutionary Frontier 48
Bitcoin ETFs: A Double-Edged Sword for Security 49
Regulation: 51
Global: 51
The United States: 51
India: 52
European Union: 53
United Kingdom: 54
Standardization: 55

Real-Time Monitoring: A New Benchmark in Crypto Wallet Security 55
The New Requirement: Real-Time Wallet Monitoring 55
New solutions by Cyvers 56
1. Preemptive Protection for Wallets 57
2. Pig Butchering Protection 59
3. Dynamic Risk Assessment 61
Cyvers In the news 65

Overview

2024 has been a pivotal year in the Web3 ecosystem, marked by an increase in malicious activities, as compared to last year, and a corresponding evolution in defense strategies.

This report consolidates insights from Cyvers's proprietary threat detection systems, which continuously monitor blockchain activity, alongside data from open-source intelligence (OSINT) resources, industry reports from security providers auditors, bug bounty platforms, and more.

The report highlights the growing sophistication of attacks, including access control breaches, smart contract vulnerabilities, and advanced fraud schemes like pig butchering. It provides a comprehensive analysis of the year's major incidents, key trends, and the industry's strides in fund recovery and compliance.

About Cyvers

Cyvers is a leader in preventing threats and mitigating the risk of malicious activity in Web3. Cyvers employs geometric deep learning (GDL) and AI-driven graph-based anomaly detection as part of its advanced threat detection framework to analyze blockchain activity and identify malicious behaviors.

Cyvers serves a myriad of clients in the Web3 space, such as centralized exchanges, custodians, DeFi protocols, institutional platforms and more – helping them protect their assets, mitigate compliance risks and prevent fraudulent activity on their platforms.

Executive Summary

Cyvers Key Security, Fraud and Compliance Trends in 2024

Executive Summary

1. Overview

- The year 2024 saw a sharp rise in Web3 cyber threats, with over $6.3B lost in hacks, fraud, and scams.
- Hacking incidents and the resulting funds losses have climbed to over $2.3 billion lost across 165 incidents—a 40% increase from 2023.
- Access Control incidents were the main culprits, accounting for 81% of losses despite comprising 41.6% of incidents.
- Pig Butchering emerges as the biggest fraud threat to users, with over $4B in stolen funds detected by Cyvers this year on the Ethereum blockchain alone.

2. Key Stats of Malicious Activity

- Annual Trends: 40% increase in losses year-over-year; still 37% below the 2022 record.

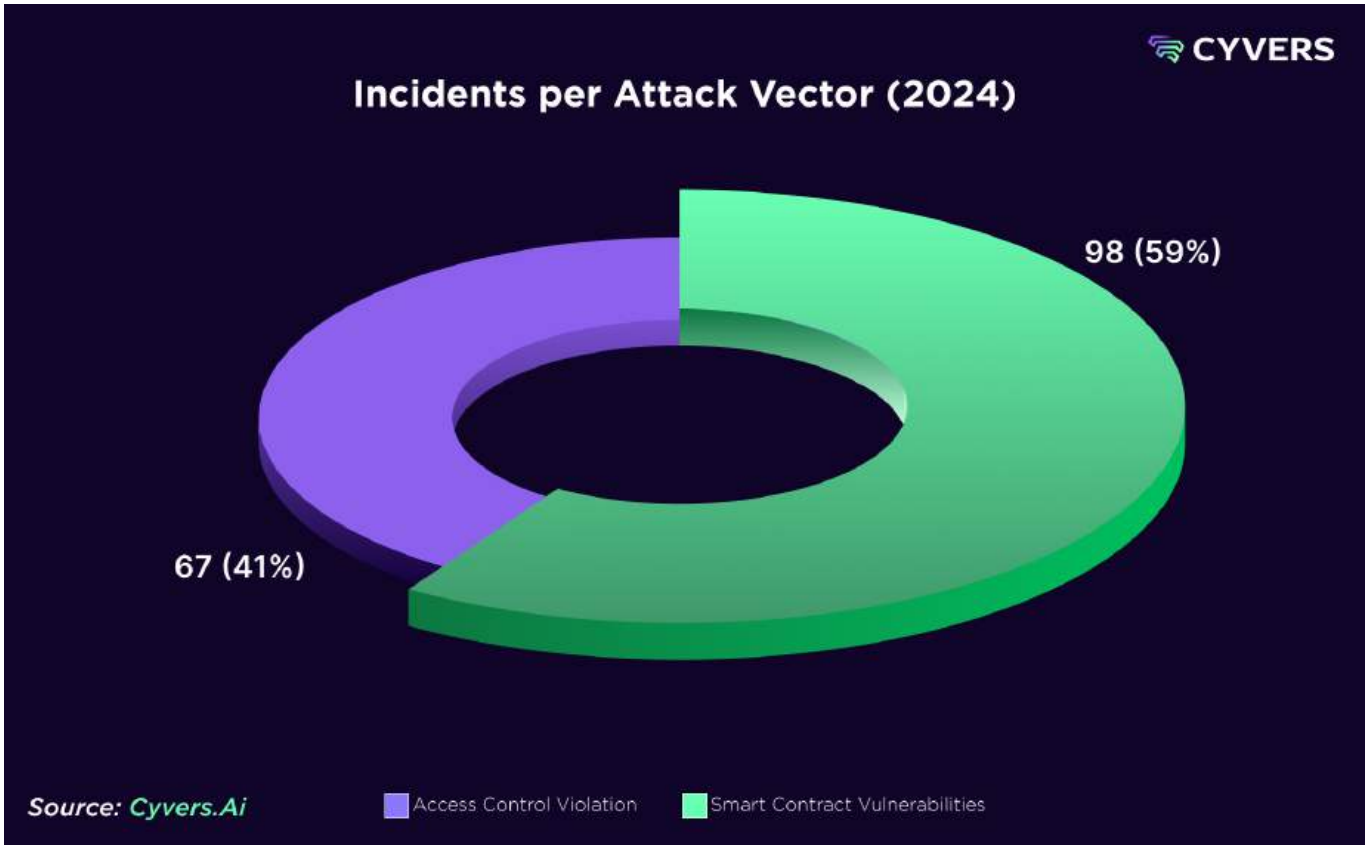
- Ethereum was the most affected blockchain, with over $1.2 billion in losses.

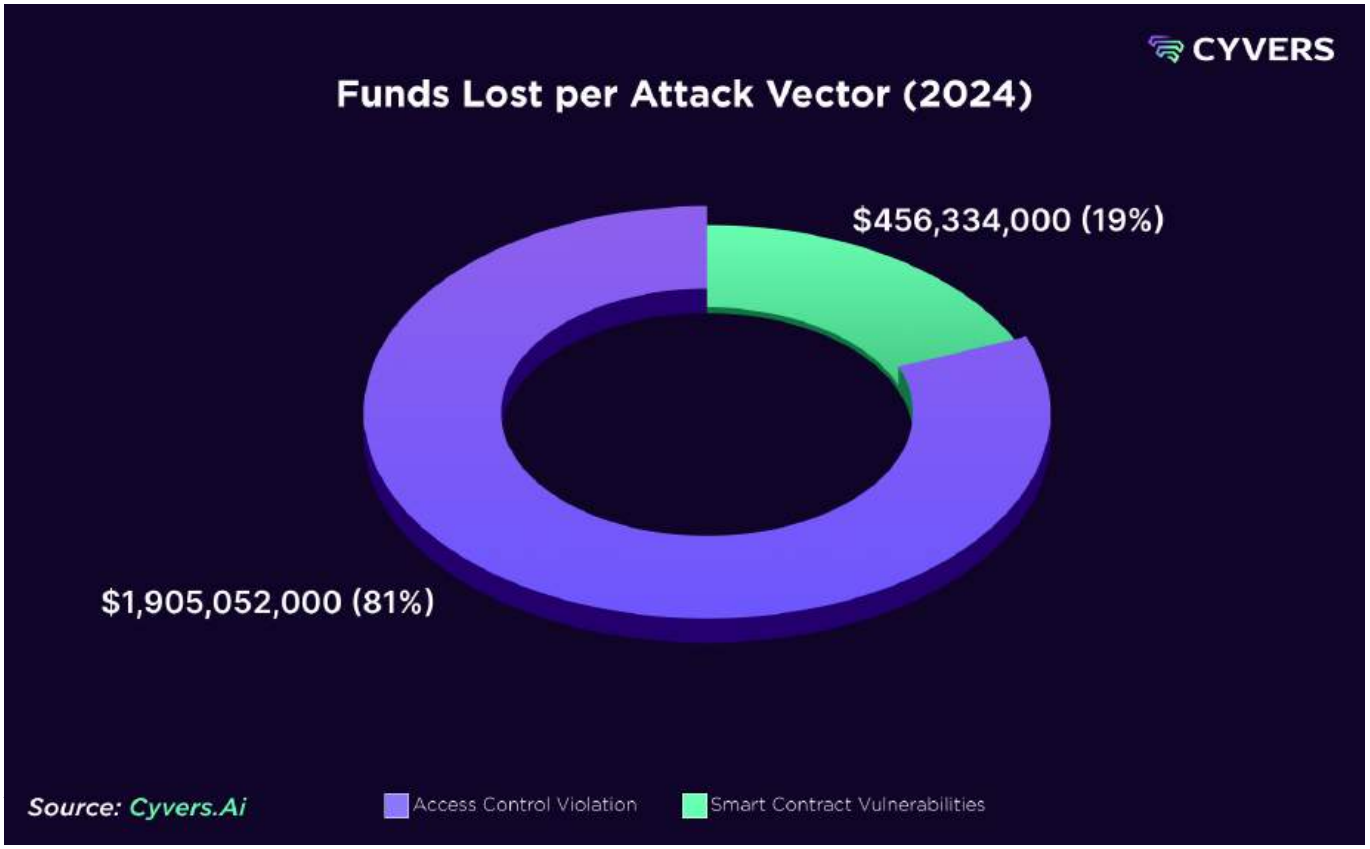
3. Attack Types (2024):

a. Access Control Breaches: $1.9B in 67 incidents

b. Smart Contract Exploits: $456.3M, in 98 incidents

c. Address Poisoning: $68.7M in one-single incident + numerous smaller incidents.



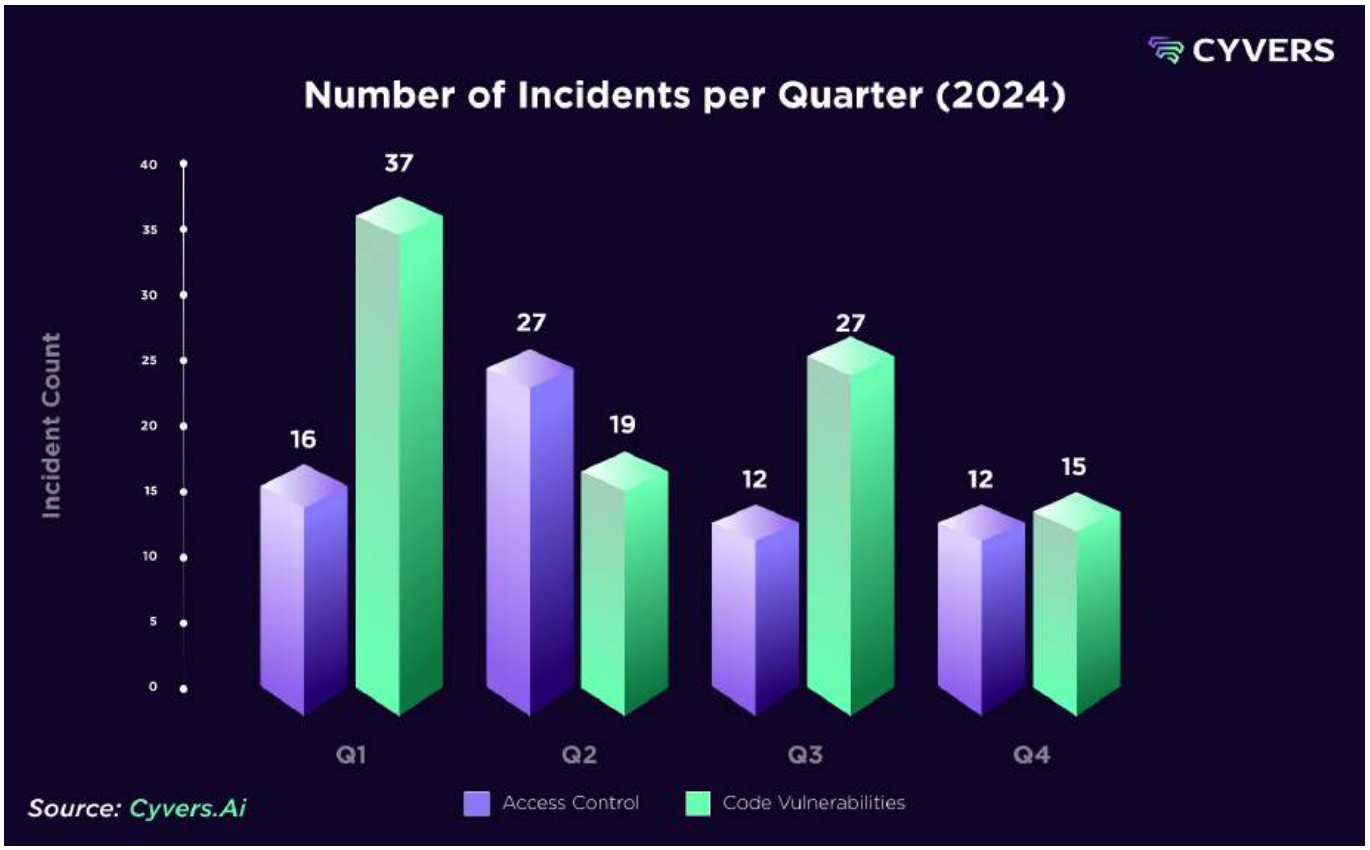


4. Recovery Rate:

According to aggregated data from leading recovery and bug-bounty services, more than $1.3B was recovered this year.

5. Quarterly Highlights:

1. Q1: Most incidents (53); dominated by smart contract vulnerabilities.
2. Q3: The quarter with the highest losses ($790M).
3. Q4: Lowest activity and losses



- The third quarter was very dominant, both in 2023 and 2024.
- The last quarter of 2024 saw a decline of over 56%, compared to the same quarter of last year.

6. Notable Incidents

- ***WazirX Hack:*** $235M stolen due to multisig wallet exploit by what seems to be a misinformed approval by the signers, exposing gaps in preventive measures. Cyvers exposed the attack exclusively and its Pre-emptive Transaction Interceptor could have prevented this hack.
- ***Radiant Capital Attack:*** $50M lost via compromised devices; Cyvers was the first to uncover the attack.
- ***DMM Exchange Hack:*** A $305M breach, one of the largest in history, caused by a private key compromise in DMM Bitcoin's hot wallets.
- ***BingX Exploit:*** Singapore-based BingX lost $52M when attackers compromised its hot wallets and moved assets across multiple blockchains. Cyvers' detected the incident first and assisted in assessing the total loss across all chains
- ***Address Poisoning Scam:*** $68M stolen in this incident (which makes it the biggest in history) via malicious lookalike addresses, highlighting the need for address verification tools. Cyvers was the only system to identify the incident.

7. Future Trends

- ***Pig Butchering Scams:*** A growing threat, with victim funds losses exceeding $3.96B in 2023 (according to the FBI). Cyvers flagged over $4B billion in victim funds across more than 150K addresses and 800,000 transactions in 2024.
- ***CeFi Targeting:*** CeFi remains vulnerable due to centralized reserves; multisig wallets face heightened risks.
- ***Quantum and AI Risks:*** Advancements in these technologies will drive increasingly complex attacks.

8. Cyvers's Innovative Solutions

Cyvers introduced several groundbreaking tools in 2024 to combat emerging threats:

- ***Preemptive Protection for Wallets:***
- Combines transaction simulation and AI-powered technology to validate transactions for maliciousness before execution.
- Effective against access control breaches, such as the WazirX hack.

- ***Secure Signer with Custodians and Co-Signers:***
- A dual-layer security framework combining pre-transaction simulations with a co-signing mechanism for anomaly detection.
- Seamlessly integrates into infrastructures like Fireblocks, offering unparalleled security without complexity.

- ***Dynamic Risk Assessment:***
- Able to trace multi-hop transactions and evaluate wallet behaviors across chains.
- Identifies hidden affiliations and laundering schemes with unprecedented accuracy, ensuring regulatory compliance and enhanced security.

- ***Pig Butchering Protection:***
- Detects and disrupts fraudulent wallet networks using advanced AI and graph analysis.
- Assists crypto platforms in blocking suspicious wallets and preventing users' funds loss.

Conclusion

The Web3 ecosystem faces unprecedented security challenges. Cyvers' advanced tools provide proactive defenses, fostering trust and resilience against evolving threats. Platforms must adopt robust monitoring and prevention strategies to safeguard assets and maintain user confidence.

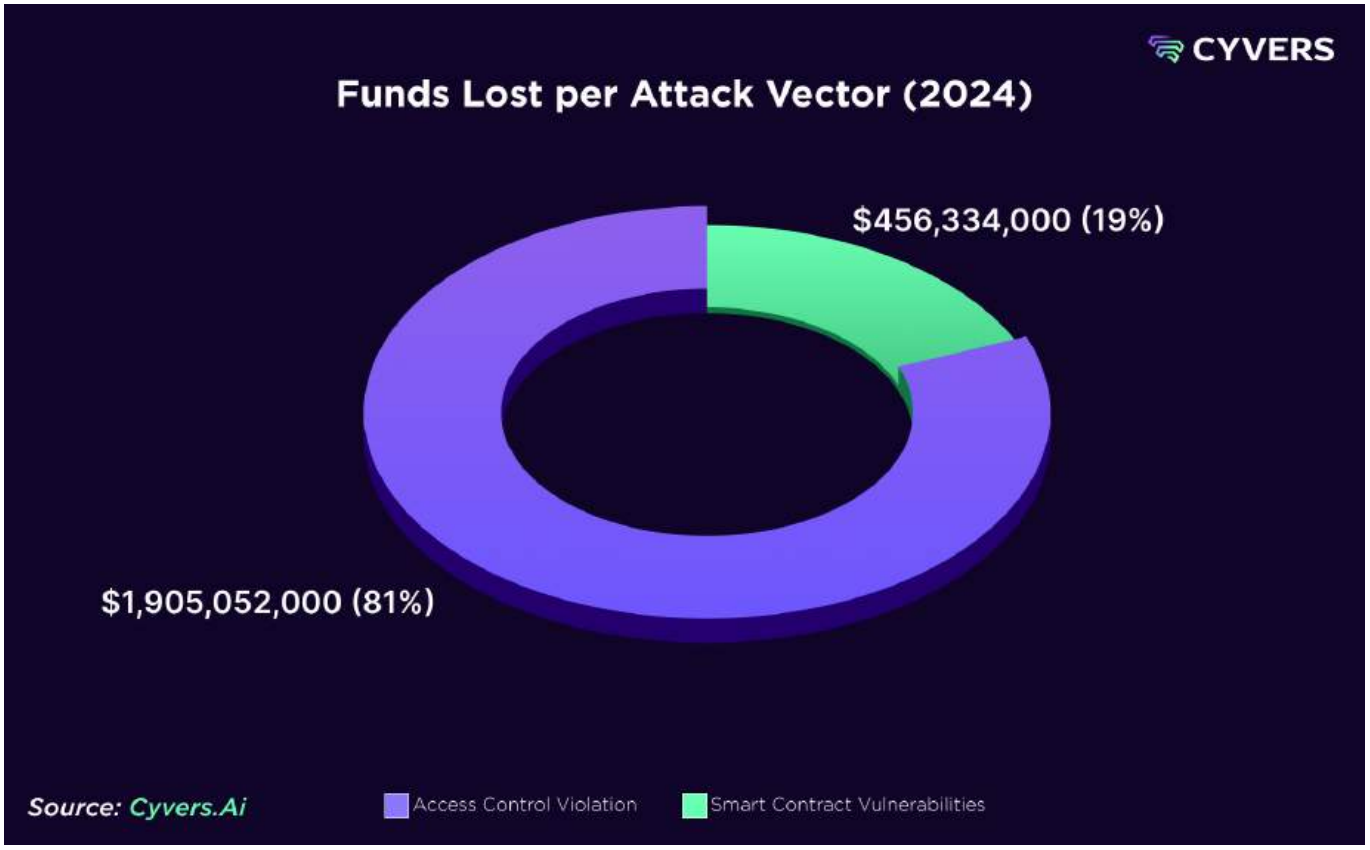
Types of Incidents

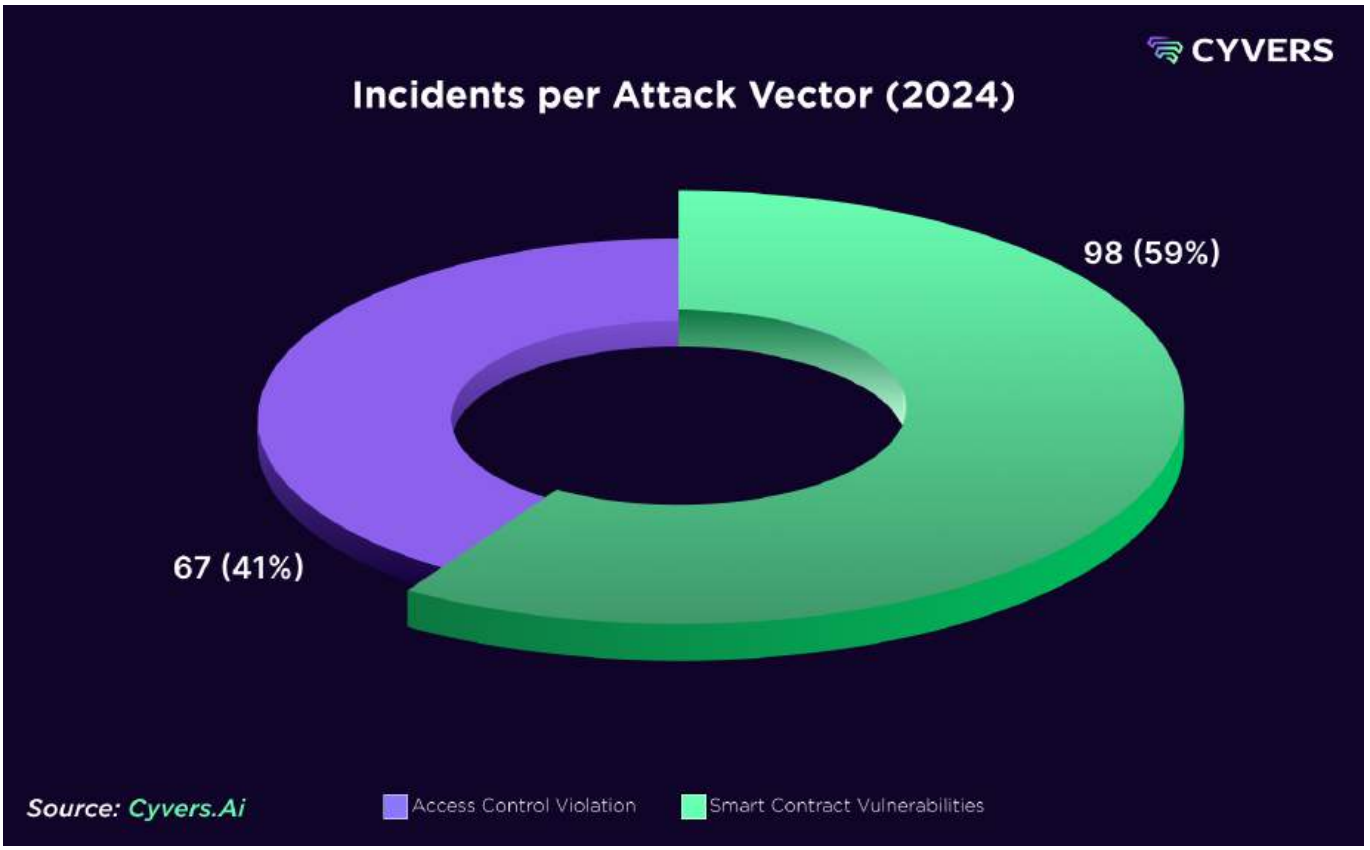
Access Control vs. Smart Contract Vulnerability Attacks

2024 marked a pivotal year as hackers shifted their focus to access control attacks, predominantly targeting centralized platforms. While smart contract attacks accounted for approximately 60% of the total incidents, their financial impact was relatively minor, contributing to just 19% of the stolen funds.

In contrast, access control attacks represented 41.6% of all recorded incidents but were responsible for an overwhelming 81% of the total financial losses. While the share of access control incidents declined slightly, from 46% in 2023 to 41% in 2024, this category's financial impact surged dramatically, making up 81% of total losses.

Losses from access control attacks skyrocketed by over 76%, increasing from approximately $1.08 billion in 2023 to around $1.9 billion in 2024. Meanwhile, losses associated with smart contract vulnerabilities fell by nearly 25%, dropping from roughly $607 million to $456 million.

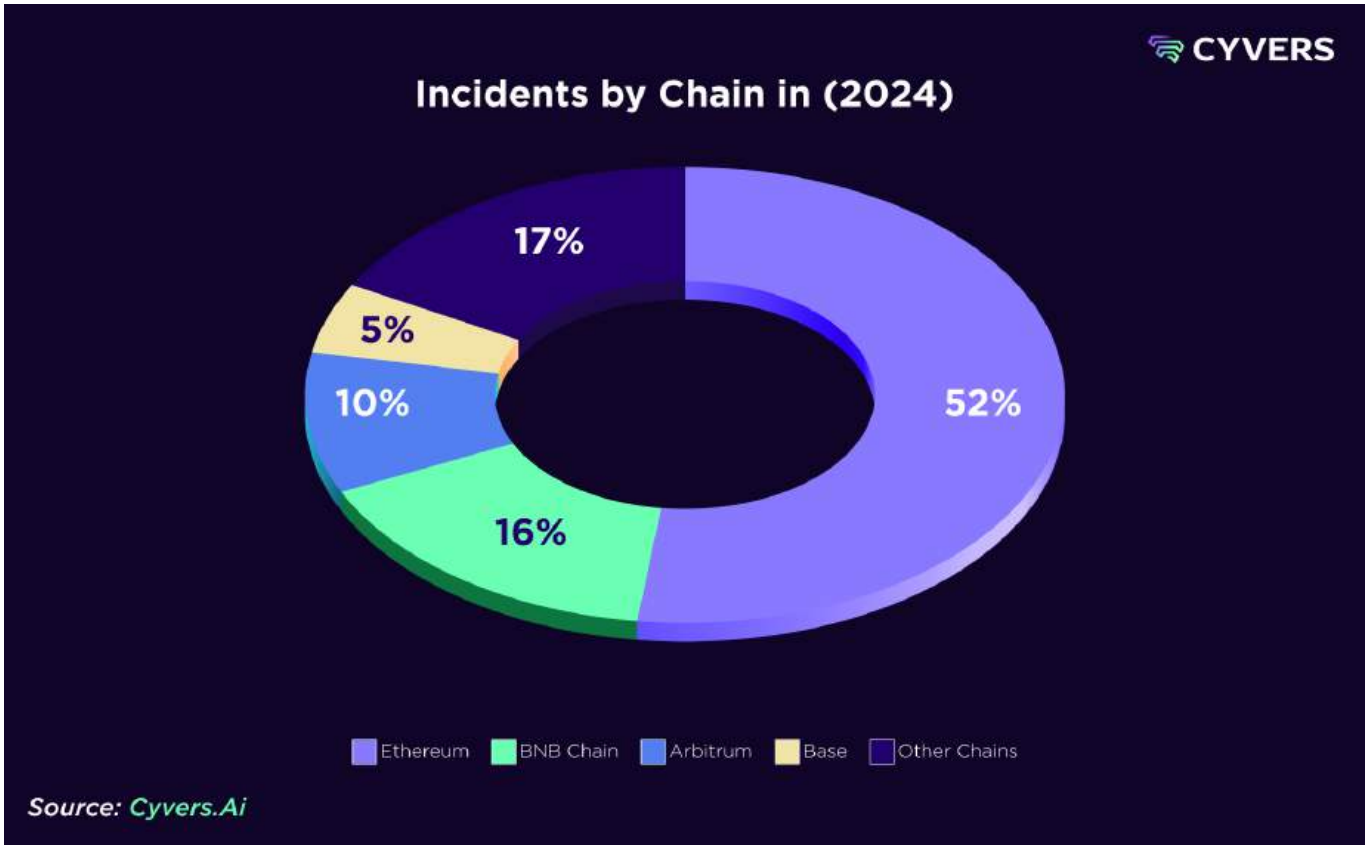


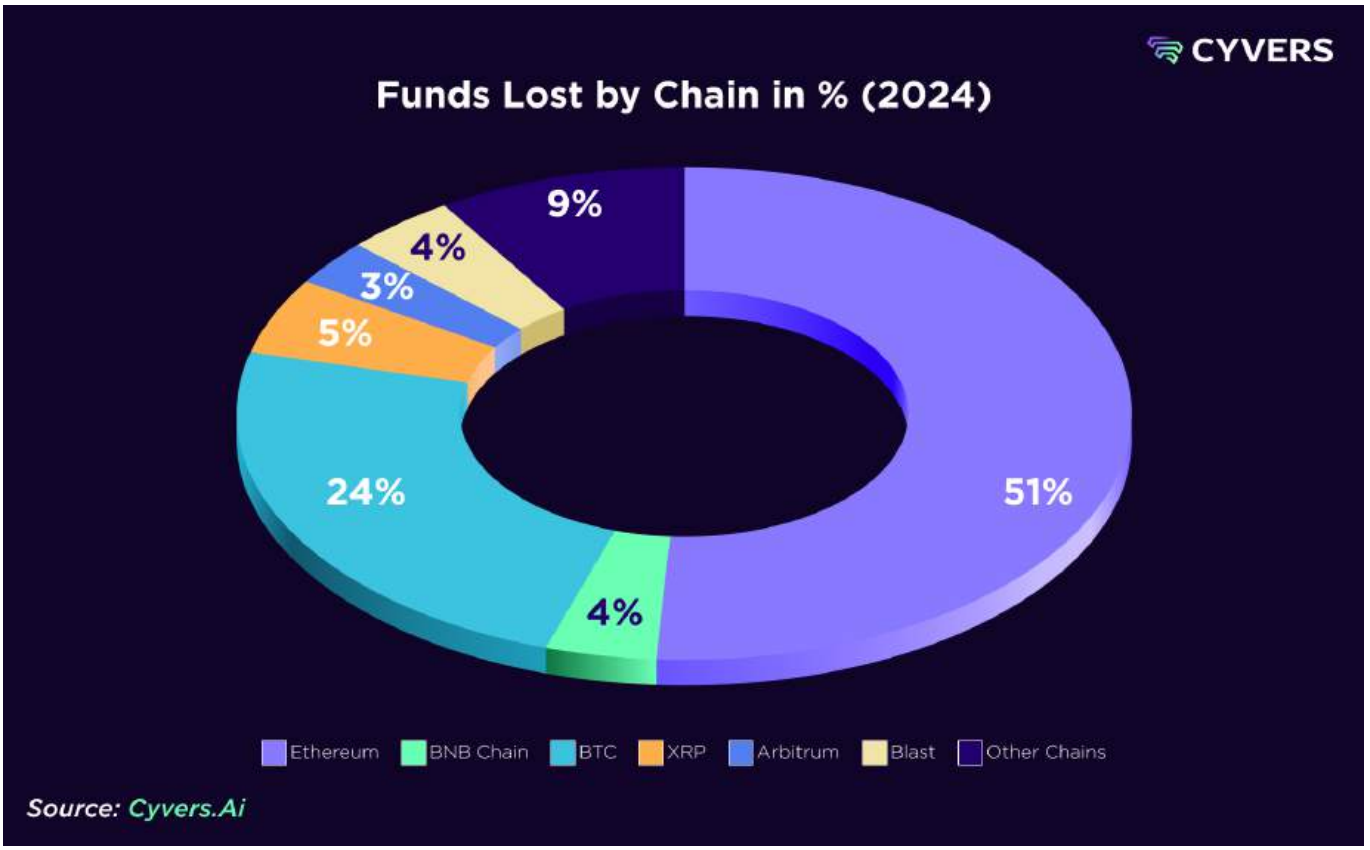


Attack Breakdown by Chain:

- ***Ethereum as the Primary Target*** - The Ethereum blockchain bore the brunt of attacks in 2024, experiencing 83 incidents—representing about 52% of all recorded attacks. These incidents led to losses exceeding $1.2 billion, accounting for nearly 51% of the total funds stolen. Ethereum's widespread popularity and the high value of assets it secures likely made it a prime target. Cybercriminals leveraged smart contract exploits, phishing schemes, and wallet attacks to inflict damage.

- ***Bitcoin: Quality Over Quantity*** - The Bitcoin blockchain saw fewer incidents, with only five significant attacks recorded. However, these incidents resulted in losses approaching $580 million, highlighting the disproportionate impact of each breach.





CYVERS

2024 Statistics

Annual Statistics

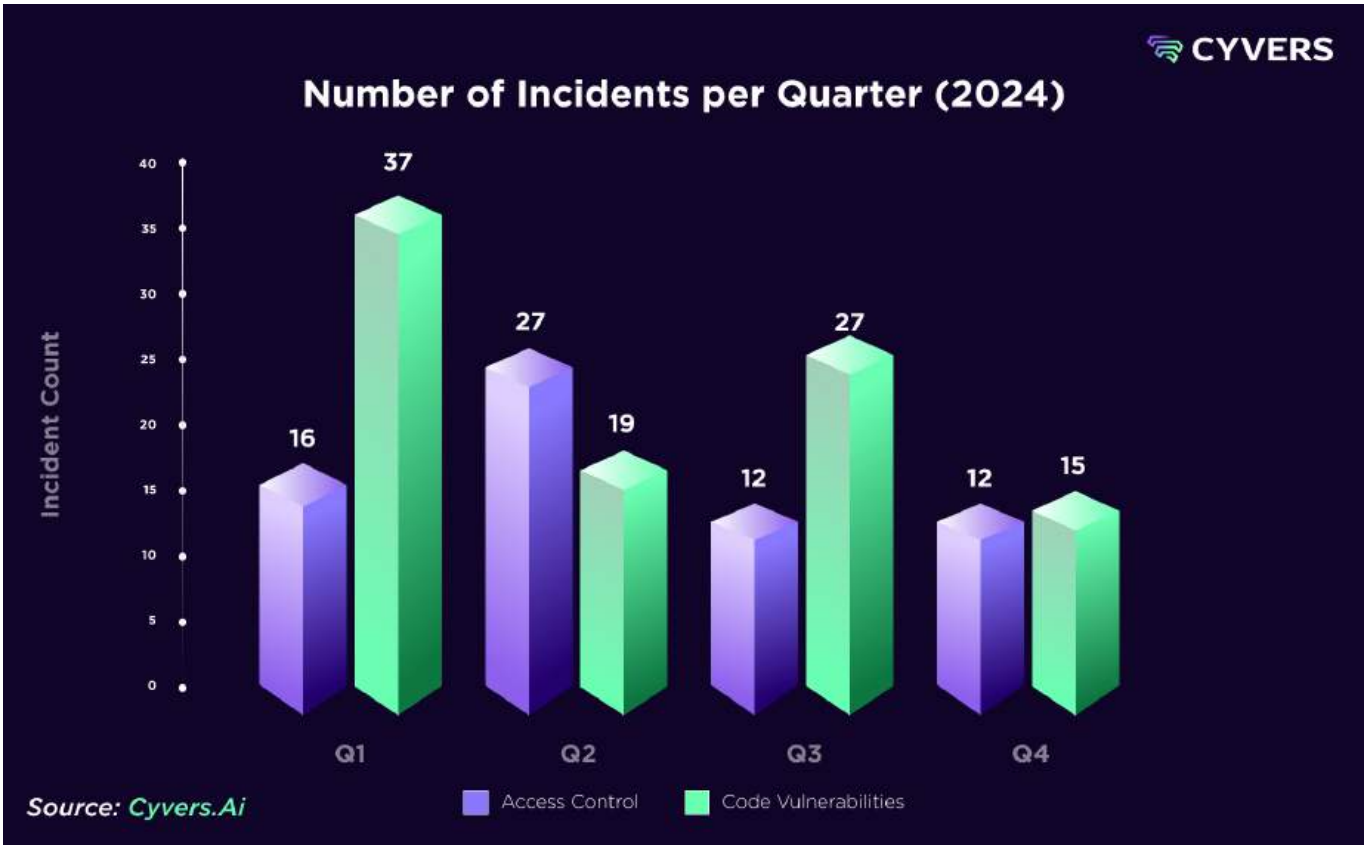
The Web3 space witnessed a sharp rise in both the frequency and financial magnitude of attacks in 2024 (as compared to last year's statistics). Hackers managed to steal over $2.3 billion across 165 incidents—a nearly 40% increase compared to 2023. Despite this surge, the total losses were still 37% lower than the record $3.7 billion stolen in 2022.

Although the year was marked by billions in stolen funds, the distribution of incidents and losses was uneven across quarters and months.

Quarterly Statistics

Number of incidents per quarter

The first quarter of 2024 was the most active for hackers, with 53 attacks primarily targeting smart contract vulnerabilities. Incident numbers steadily decreased throughout the year, with Q4 recording the fewest attacks. Interestingly, Q2 was the only quarter where access control breaches outnumbered smart contract vulnerability exploits (27 versus 19).



Funds lost per quarter

Financial losses did not consistently align with the number of incidents. The third quarter saw the most significant losses, with over $790 million stolen, while Q4 incurred the least at the time of writing.

A similar trend was observed in 2023, with Q3 being the most financially damaging quarter. This year, Q4 saw a 56% decline in losses compared to the same period last year.

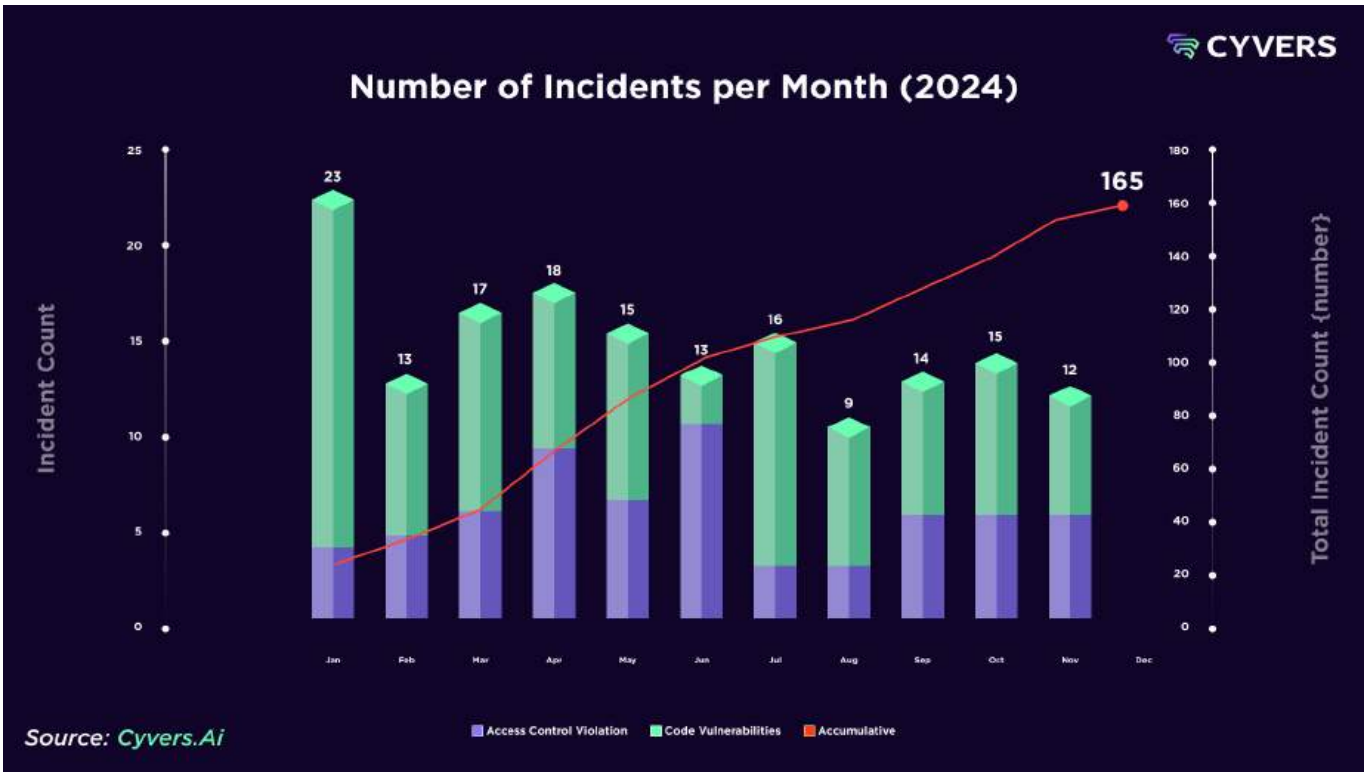
Monthly Statistics

Some months were very intense and stuck out in terms of the number of incidents, or the amount of funds lost. It is important to highlight that there is no direct correlation between the two parameters, given that one single attack can be much more harmful than dozens of smaller ones.

Moreover, looking at the statistics from the previous year, one can easily see that the distribution per month is quite arbitrary and doesn't rely on reasonable temporal attribution, but rather on a coincidental loophole that was taken advantage of by a hacker each time.

Number of incidents per month

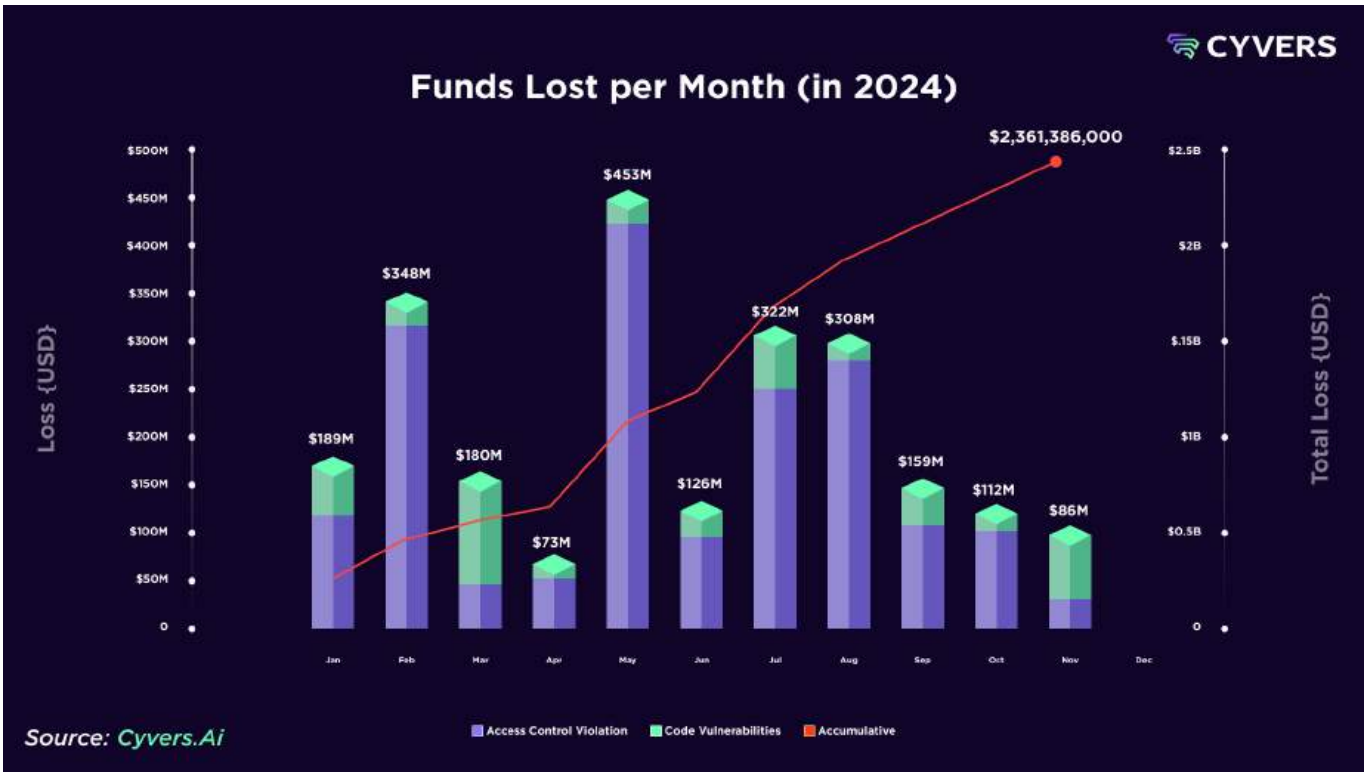
January was the most active month, with 23 incidents, smart contract vulnerabilities. This marked a stark contrast to 2023, where January was the least eventful month. April followed 18 incidents, split evenly between access control and smart contract exploits. Conversely, August was the quietest month, with only nine incidents.



Funds Lost per Month

May emerged as the most financially damaging month, with over $450 million lost—primarily due to access control breaches. February followed with nearly $350 million in losses. Surprisingly, April reported the lowest monthly losses, at “just” $73 million.

Last year, July, September, and November were the costliest months, with losses exceeding $300 million each. Access control breaches were the primary contributors to losses in both years.



Funds Recovery

Despite the challenges of 2024, the year also saw advancements in crypto recovery efforts, reflecting the industry's resilience against cyber threats. Recovery initiatives, often led by prominent firms like Hacken, ImmuneFi, and SlowMist, reclaimed over $1.3 billion in stolen funds.

The breakdown of the recovery successes per quarter indicated very fruitful recovery efforts by the various services during the first two quarters of 2024:

Notable Recoveries in 2024

- ***Q1:*** CertiK's $77.9 million recovery from the Munchables exploit.
- ***Q2:*** ImmuneFi recovered $26.7 million across four cases, complemented by $68 million retrieved from a May dust attack.
- ***Q3:*** SlowMist and Beosin recovered $34.4 million and $16.9 million, respectively, while $27 million stolen from the Penpie Protocol was returned.
- ***Q4:*** Thala Labs secured $25.5 million in November, underscoring the importance of collaboration between firms and regulators.

CYVERS

Prominent incidents and analysis

Top 10 Incidents for 2024

2024 witnessed several record-breaking hacks, with at least three making it into both the annual and all-time top 10 lists of the most significant breaches. Cyvers played a pivotal role in identifying these incidents, further demonstrating the growing sophistication of attacks in the Web3 ecosystem.

1st Quarter

CoinsPaid Hack (January 6, 2024)

Company: CoinsPaid

Amount Lost: $7.5 million

Attack Vector: Unauthorized transactions due to inadequate access controls

Incident Overview:
On January 6, 2024, CoinsPaid, an Estonian-based crypto payment gateway, experienced its second security breach within six months, resulting in unauthorized transactions totaling approximately $7.5 million. The assets involved included Tether

(USDT), Ether (ETH), USD Coin (USDC), and CoinsPaid's native token, CPD. The breach was attributed to inadequate access controls, allowing attackers to execute unauthorized withdrawals.

Cyvers' Role:
Cyvers' artificial intelligence system detected multiple irregular transactions on January 6, 2024, enabling the identification of unauthorized withdrawals amounting to $6.1 million in various digital assets. Further analysis revealed additional unauthorized transactions involving Binance Coin (BNB) worth over $1 million, bringing the total amount stolen to nearly $7.5 million. Cyvers promptly reported these findings, highlighting the critical need for robust access controls to prevent such breaches.

Aftermath:
Following the breach, CoinsPaid has not yet issued an official statement regarding the incident. This security breach underscores the importance of implementing stringent access control measures and continuous monitoring to safeguard digital assets. The recurrence of such incidents within a short timeframe highlights the necessity for organizations to reassess and strengthen their security protocols to prevent future breaches.

PlayDapp Hack (February 9–13, 2024)

Company: PlayDapp, a Web3 gaming platform and NFT marketplace.

Funds Stolen: Approximately $290 million USD.

Vector of Attack: Unauthorized minting through a private key compromise.

Backstory:
Between February 9 and 13, 2024, an attacker exploited PlayDapp's deployer address, compromising its private key. They added themselves as an authorized minter and minted 1.79 billion PLA tokens in two stages: 200 million tokens inflated the token supply, causing severe financial and reputational damage.

Aftermath:
PlayDapp halted smart contract operations to prevent further losses and began migrating to a new contract. The company offered a $1 million bounty for the return of stolen funds and threatened legal action, including FBI involvement, if they weren't returned. Collaboration with blockchain analytics firms and exchanges helped trace portions of the stolen funds, though recovery remained challenging. The PLA token's value dropped significantly, eroding user trust in the platform.

Cyvers Angle:
Cyvers detected the exploit in real time, identifying the unauthorized addition of a minter and suspicious minting activity. This early detection provided crucial insights, enabling PlayDapp to act swiftly to contain the breach. The incident underscores the necessity of robust private key management and continuous monitoring to safeguard Web3 platforms.

Duelbits Security Breach (February 13, 2024)

Date: February 13, 2024

Company: Duelbits

Amount Lost: $6.7 million

Attack Vector: Access control violation

Incident Overview:
In February 2024, Duelbits, a cryptocurrency casino platform, suffered a significant security breach resulting in the loss of $6.7 million. The breach was attributed to a access control violation, where unauthorized parties gained access to the platform's cryptocurrency wallets. Despite prior warnings about suspicious transactions totaling $4.6 million, the company did not take adequate measures to secure their assets, leading to substantial loss.

Cyvers' Role:
Cyvers was instrumental in identifying the suspicious transactions from Duelbits' wallets. Our real-time monitoring systems detected the unauthorized transfers, highlighting the critical need for robust access controls. This incident underscores the importance of proactive security measures and the value of vigilant monitoring in safeguarding digital assets.

Aftermath:
The breach serves as a stark reminder of the vulnerabilities inherent in inadequate access control mechanisms. It emphasizes the necessity for implementing stringent security protocols, such as multi-signature setups and distributed storage solutions, to protect against unauthorized access and potential financial losses.

Prisma Finance Hack (March 28, 2024)

Company: Prisma Finance, a decentralized finance (DeFi) protocol.

Funds Stolen: Approximately $11.6 million USD.

Vector of Attack: Smart contract vulnerability in the MigrateTroveZap contracts.

Backstory:
The attacker exploited a flaw in the MigrateTroveZap contracts, which are designed for migrating user positions between trove managers. This vulnerability allowed the attacker to manipulate the contract's behavior and withdraw funds illegally. Approximately 3,257.7 ETH was drained during the attack. Cyvers' real-time monitoring detected the initial suspicious transactions and flagged them, revealing the extent of the exploit.

Aftermath:
Prisma Finance suspended the protocol immediately to prevent further exploitation and advised users to disable delegate approvals. The attack caused Prisma's Total Value Locked (TVL) to drop from over $220 million to $115 million, significantly impacting user confidence. The Prisma Governance Token (PRISMA) saw a 30% price drop but showed signs of recovery. The attacker claimed to act as a "whitehat" and opened communication with Prisma Finance, suggesting potential negotiations for fund recovery.

Cyvers Angle:
Cyvers was instrumental in detecting and analyzing the exploit in real time. Its monitoring systems provided early alerts, enabling Prisma to respond swiftly. Cyvers also traced the movement of stolen funds, which were swapped for ETH and partially funneled through Tornado Cash. This case highlights Cyvers' critical role in safeguarding DeFi protocols and mitigating the impacts of high-stakes security breaches.

2nd Quarter

Hedgey Finance Exploit (April 19, 2024)

Company: Hedgey Finance, a decentralized finance (DeFi) platform.

Funds Stolen: Approximately $44.7 million USD.

Vector of Attack: Flash loan exploit targeting the createLockedCampaign function.

Backstory:
The attacker exploited a vulnerability in Hedgey Finance's createLockedCampaign function by using flash loans. This allowed the manipulation of token approvals and the unauthorized withdrawal of funds. The exploit resulted in losses of $42.8 million on the Arbitrum network and $1.9 million on Ethereum. These dual exploits highlighted gaps in input validation and smart contract design.

Aftermath:
Hedgey Finance acknowledged the breach and worked with security auditors to investigate the vulnerability. The team advised users to cancel active claims

contributed to growing concerns over the DeFi sector's security, with over $500 million lost to similar breaches in early 2024.

Cyvers Angle:
Cyvers' proactive monitoring systems highlighted the critical need for robust defenses in DeFi platforms. By advocating for reentrancy guards, improved input validation, and regular security audits, Cyvers underscores the importance of real-time threat detection in preventing large-scale losses like the Hedgey exploit.

Address Poisoning Scam (May 3, 2024)

Individual: An unidentified cryptocurrency trader.

Funds Stolen: Approximately $68 million USD (1,155 Wrapped Bitcoin, WBTC).

Vector of Attack: Address poisoning scam.

Backstory:
On May 3, 2024, an unknown trader became the victim of an address poisoning scam, losing 1,155 WBTC, valued at approximately $68 million. Address poisoning exploits users' reliance on transaction history by sending small amounts from addresses designed to resemble trusted ones. This manipulates users into copying malicious addresses, resulting in inadvertent transfers to attackers. The victim's wallet, identified as "0x1E," was drained of 97% of its assets, highlighting the devastating impact of this tactic.

Aftermath:
The substantial loss brought attention to the growing prevalence of address poisoning scams. The victim's holdings were almost entirely wiped out, sparking discussions about the need for user education and robust transaction verification practices in the cryptocurrency ecosystem.

Cyvers Angle:
Cyvers was the only Web3 security provider to detect and report the incident in real time, showcasing its unmatched monitoring capabilities. By identifying the systems and user-centric protections, such as address whitelisting and verification protocols, to prevent such exploits. This case underscores Cyvers' leadership in safeguarding the crypto space through advanced threat detection.

Sonne Finance Hack (May 14, 2024)

Company: Sonne Finance, a decentralized lending protocol on the Optimism blockchain.

Funds Stolen: Approximately $20 million USD.

Vector of Attack: Smart contract exploit leveraging a "donation" attack in Compound v2 forks.

Backstory:
The attacker has exploited a vulnerability in Sonne Finance's contracts by manipulating the token exchange rate using a "donation" method. This involved artificially inflating the collateral value by donating large amounts, which tricked the protocol into miscalculating balances. This enabled the attacker to withdraw unauthorized funds across multiple assets, including WETH, VELO, soVELO, and Wrapped USDC. Cyvers' monitoring system detected the initial suspicious activity targeting Sonne's USDC and WETH contracts, identifying $3 million stolen in the early stages.

Aftermath:
Sonne Finance promptly paused all markets on Optimism to prevent further losses. Despite attempts to negotiate with the hacker through a bug bounty offer, the stolen assets were moved to new wallets, swapped for Ether (ETH) and Dai (DAI), and further obfuscated. This incident led to extensive discussions on the need for continuous auditing and updates to DeFi protocols to address known vulnerabilities.

Cyvers Angle:
Cyvers' AI-driven monitoring system was instrumental in identifying the exploit in real time, flagging the attack before the full extent of the loss was realized. This proactive detection demonstrated the value of advanced security tools in mitigating threats and reducing potential damage in the Web3 ecosystem.

DMM Bitcoin Hack (May 31, 2024)

Company: DMM Bitcoin, a Japanese cryptocurrency exchange.

Funds Stolen: Approximately $308 million USD (4,502.9 Bitcoin).

Vector of Attack: Hot wallet breach (specific details undisclosed).

Backstory:
On May 31, 2024, DMM Bitcoin reported an unauthorized leak of 4,502.9 Bitcoin from its wallets. The exact method of the breach remains unclear, but it is suspected to involve vulnerabilities in wallet management. The attack occurred during heightened

scrutiny of security protocols across centralized exchanges in 2024, contributing to growing concerns over asset safety.

Aftermath:
DMM Bitcoin assured customers that lost deposits would be reimbursed through support from its parent company. The Japanese Financial Services Agency launched a formal investigation, and DMM Bitcoin imposed restrictions on services to prevent further losses. By December 2024, the exchange announced plans to cease operations, transferring its assets and customer accounts to SBI VC Trade, a subsidiary of the SBI Group, by March 2025.

Kraken Bug Bounty Controversy (June 9, 2024)

Company: Kraken, a leading cryptocurrency exchange.

Funds Involved: Approximately $3 million USD.

Vector of Incident: Alleged unauthorized withdrawal during vulnerability testing.

Backstory: In early June 2024, Kraken's Chief Security Officer, Nicholas Percoco, reported that a security researcher exploited a critical vulnerability within Kraken's system, withdrawing $3 million from the exchange's treasury before reporting the bug. The researcher, later identified as blockchain security firm CertiK, claimed the withdrawal was part of a standard bug bounty procedure to alleging that the firm withheld the return of funds pending a payment linked to potential damages had the vulnerability not been disclosed.

Aftermath:
The incident ignited a significant debate within the crypto community regarding ethical practices in vulnerability disclosure and bug bounty programs. CertiK admitted to the exploit but faced criticism for allegedly sending the withdrawn funds through Tornado Cash, a mixing service under U.S. sanctions, raising concerns about fund traceability. On June 20, 2024, Kraken confirmed the recovery of the missing funds, effectively concluding the dispute. This event underscored the necessity for clear protocols and trust between security researchers and organizations in handling vulnerabilities.

Cyvers Angle:
Cyvers' analysis of on-chain data revealed that an address associated with CertiK had created a suspicious contract on the Base network 26 days prior to the reported vulnerability discovery, and another on Polygon 14 days beforehand. This activity suggested that similar vulnerabilities might have been tested on other exchanges, such as OKX and Coinbase, casting doubt on CertiK's timeline of discovery and

highlighting the importance of proactive security measures and transparent communication in the Web3 ecosystem.

UwU Lend Exploit (June 10, 2024)

Company: UwU Lend, a decentralized finance (DeFi) lending protocol.

Funds Stolen: $23 million USD.

Vector of Attack: Smart contract exploit through oracle manipulation.

Backstory:
The attack began with a record-setting $3.796 billion flash loan from multiple DeFi protocols. The hacker used half the borrowed assets to inflate the value of sUSDE on UwU Lend's oracle by targeting five price sources, creating an artificially high price. This manipulation rendered their leveraged position insolvent, triggering liquidations. Through calculated actions, the attacker repeatedly liquidated their position, extracting

large amounts of uWETH. Once the attack was complete, the manipulated prices were reversed, and the flash loan was repaid, leaving the hacker with substantial profits.

Aftermath:
The stolen funds were converted into ETH and distributed across multiple wallets. UwU Lend paused its protocol to prevent further exploits. However, three days later, a second attack exploited residual vulnerabilities, leading to the theft of an additional $3.72 million. This second breach further underscored the heightened risks faced by already compromised platforms, emphasizing that recovery measures must include comprehensive monitoring and proactive threat mitigation to prevent subsequent exploits.

Cyvers Angle:
Cyvers' advanced real-time monitoring system detected suspicious flash loan activity as it unfolded. Unlike traditional detection methods, Cyvers identified the anomaly before any external alert systems, offering exclusive insights into the manipulation process. Our AI-powered system flagged unusual price movements in the oracle, providing actionable intelligence to stakeholders early on. This proactive detection not only showcased Cyvers' multi-layered defense solutions but also highlighted their critical importance in safeguarding DeFi platforms from persistent threats.

BtcTurk Hack (June 22, 2024)

Company: BtcTurk, Turkey's largest cryptocurrency exchange.

Funds Stolen: Approximately $55 million USD.

Vector of Attack: Hot wallet breach.

Backstory:
On June 22, 2024, attackers compromised ten of BtcTurk's hot wallets, leading to unauthorized withdrawals of approximately $55 million. While the exchange's cold wallets remained secure, the attackers targeted hot wallets due to their cryptocurrencies, including significant amounts of Avalanche's AVAX tokens.

Aftermath:
BtcTurk immediately suspended cryptocurrency deposits and withdrawals to prevent further losses and assured users that its financial reserves were sufficient to cover the stolen funds, ensuring user balances remained unaffected. Binance, a leading global exchange, collaborated with BtcTurk by freezing over $5.3 million in stolen funds that had moved through its platform. Despite these recovery efforts, the market saw a significant decline in AVAX's value, which dropped 10%, hitting a six-month low.

3rd Quarter

Dough Finance Flash Loan Attack (July 12, 2024)

Company: Dough Finance, a decentralized finance (DeFi) protocol.

Funds Stolen: Approximately $1.8 million USD.

Vector of Attack: Flash loan attack exploiting a vulnerability in the "ConnectorDeleverageParaswap" contract.

Backstory:
The attacker exploited a flaw in Dough Finance's contract, which failed to validate call data properly. This oversight allowed unauthorized manipulation of the contract, enabling the siphoning of 608 ETH. The attacker leveraged Railgun, a zero-knowledge protocol, to obscure the source of their transactions and swapped stolen USDC for ETH. The exploit targeted Dough Finance's lending mechanism without impacting other pools, such as Aave's.

Aftermath:
Dough Finance responded by issuing a public ultimatum to the attacker, demanding the return of funds within two days to avoid legal action. The protocol has since begun a thorough review of its security practices to address the vulnerabilities exploited in the attack. The event underscores the pressing need for rigorous contract validation and robust defensive mechanisms in the DeFi sector.

Cyvers Angle:
Cyvers' advanced real-time monitoring detected the attack as it unfolded, providing immediate alerts to the community. By swiftly identifying the affected contract and ensuring transparency, Cyvers played a critical role in minimizing further risks. This case highlights the importance of proactive security monitoring in safeguarding DeFi protocols against emerging threats.

LiFi Protocol Exploit (July 16, 2024)

Company: Li.Fi Protocol

Funds Stolen: Approximately $11.6 million USD

Vector of Attack: Smart contract exploit due to a vulnerability in a newly deployed contract facet

Backstory:
On July 16, 2024, Li.Fi Protocol, a cross-chain bridging and swapping platform, suffered a significant security breach. The attack exploited a vulnerability in the recently deployed GasZipFacet contract, which lacked proper validation for contract calls. This flaw allowed the attacker to execute arbitrary calls via the depositToGasZipERC20() function, leading to unauthorized transactions. The breach primarily affected users who had granted infinite approvals to the compromised contract, enabling the attacker to drain funds from these users' wallets.

Aftermath:
Li.Fi promptly disabled the affected contract facet across all chains to contain the exploit. The team released an incident report detailing the breach and announced a voluntary compensation plan to reimburse 100% of the stolen funds to affected users. They also engaged law enforcement and collaborated with security teams to trace the stolen assets. The incident highlighted the critical importance of rigorous code validation and cautious deployment processes in decentralized finance (DeFi) protocols.

Cyvers Angle:
Cyvers' advanced monitoring systems detected the suspicious transactions in real-time, identifying the specific contract address involved in the exploit. By promptly alerting the community and recommending the revocation of approvals to the malicious contract, Cyvers played a crucial role in mitigating further losses. This incident underscores the vital importance of real-time threat detection and proactive security measures in protecting the Web3 ecosystem.

WazirX Hack (July 18, 2024)

Company: WazirX, one of India's leading cryptocurrency exchanges.

Funds Stolen: $235 million USD (45% of WazirX's total reserves).

Vector of Attack: Multi-signature wallet breach.

Backstory:
The hack targeted WazirX's multi-signature wallet, which required 4 out of 6 signatures (3 from WazirX and 1 from custodian Liminal) for transactions. Hackers prepared by funding wallets through Tornado Cash on July 10. On July 18, the wallet was compromised, enabling unauthorized transactions that drained $235 million worth of digital assets, including a significant portion of WazirX's reserves. The breach highlighted vulnerabilities in the wallet's security framework and a lack of robust preventative measures.

Aftermath:
WazirX collaborated with cybersecurity experts and law enforcement agencies to investigate the breach. Efforts to recover stolen funds have seen partial success, with some assets blocked by exchanges, but 43% of customer funds remain irreversibly lost. WazirX engaged its community, proposing recovery plans, while facing legal battles and scrutiny under India's IT Act. The hack spurred regulatory discussions in India, emphasizing the need for stronger security protocols and international cooperation.

Cyvers Angle:
Cyvers' advanced monitoring system detected the suspicious activity first, transactions in real time. CyVers has reached out to the founder of the exchange and was the first to notify him about the incident. Despite this early warning, the scale of the breach highlights the necessity of integrating Cyvers' real-time threat detection and AI-driven monitoring to preemptively stop such attacks. Cyvers' tools could have identified compromised keys and anomalous wallet behavior, providing actionable insights before the breach escalated. This case serves as a testament to the critical role Cyvers plays in securing the Web3 ecosystem against evolving threats.

DeltaPrime Hacks (September and November 2024)

Company: DeltaPrime, a decentralized finance (DeFi) lending platform operating on Arbitrum and Avalanche blockchains.

Funds Stolen: Approximately $6 million USD in September; $4.8 million USD in November.

Vectors of Attack: September 2024: Compromised private key leading to unauthorized contract upgrades.

November 2024: Smart contract vulnerability in the reward claiming mechanism.

Backstory:
September 2024 Attack: Attackers gained access to DeltaPrime's ProxyAdmin private key, allowing them to perform malicious upgrades on proxy contracts. This breach enabled the draining of approximately $6 million from liquidity pools on the Arbitrum network.

November 2024 Attack:
A flaw in input validation within the reward claiming mechanism was exploited. The attacker created a malicious trading pair, converting loan collateral into reward tokens, which were then withdrawn, leaving the platform with bad debt. This resulted in a $4.8 million loss across Arbitrum and Avalanche networks.

Aftermath:
September Attack Response: DeltaPrime paused operations on affected chains and collaborated with security firms to investigate. The incident highlighted the critical importance of securing administrative keys and implementing multi-signature protections.

November Attack Response:
Following the second breach, DeltaPrime again halted protocol activities to prevent further losses. The recurring security failures raised concerns about the platform's vulnerability management and prompted calls for comprehensive security audits.

Cyvers Angle:
Cyvers' real-time monitoring systems detected both breaches promptly, providing early alerts that were crucial for initiating immediate response measures. These incidents underscore the necessity of integrating advanced security solutions like Cyvers' to identify and mitigate threats proactively, ensuring the integrity of DeFi platforms against sophisticated attacks.

Penpie Hack (September 3, 2024)

Company: Penpie, an independent protocol built on Pendle.

Funds Stolen: Approximately $27 million USD.

Vector of Attack: Smart contract exploit (reentrancy vulnerability).

Backstory:
The attacker exploited a reentrancy vulnerability in the PendleStaking contract, which lacked a reentrancy guard. By creating a counterfeit SY token and linking it to valuable PENDLE-LPT market tokens through untrusted market arguments, the attacker manipulated the batchHarvestMarketRewards function. This allowed them to repeatedly enter the contract, deposit, withdraw minted shares, and inflate their reward balance. The vulnerability enabled the hacker to drain substantial funds from the protocol.

Aftermath:
The Penpie and Pendle teams froze their protocols immediately upon discovering the breach to prevent further losses. Despite these efforts, the stolen funds were laundered through Tornado Cash, complicating recovery. This exploit highlighted significant gaps in smart contract security and emphasized the importance of implementing robust reentrancy defenses.

Cyvers Angle:
Cyvers was the first Web3 security company to identify this exploit in real time, offering critical insights into the vulnerability and attacker methods. Our advanced monitoring and proactive detection showcased the importance of vigilant security measures to protect the Web3 ecosystem against evolving threats. Cyvers continues to lead efforts in safeguarding decentralized platforms from similar vulnerabilities.

Indodax Hack (September 11, 2024)

Company: Indodax, Indonesia Digital Asset Exchange.

Funds Stolen: Approximately $20.58 million USD (other estimates suggest up to $22 million).

Vector of Attack: Hot access control violation.

Backstory:
On September 11, 2024, Indodax experienced a significant security breach targeting its hot wallets. Cyvers' real-time monitoring flagged 160 critical red flags at the onset, beginning with a transfer of 660 $ETH. The attack spanned multiple blockchains and compromised various assets, including $13.3M in ETH, $2.5M each on TRON and Polygon, $1.4M in BTC, and $883K in OP tokens. Security experts identified over 150 suspicious transactions, with stolen funds swiftly converted and moved across chains.

Preliminary analyses suggested vulnerabilities in Indodax's withdrawal system, and the attack bore hallmarks of the Lazarus Group, known for their rapid asset transfers and sophisticated operational patterns.

Aftermath:
Indodax temporarily suspended operations to assess the breach and assured users that their balances remained safe. Collaborating with blockchain security firms like PeckShield, SlowMist, and Cyvers, Indodax launched an investigation and implemented enhanced security measures. While some funds were traced, the conversion and movement of assets complicated recovery efforts. The breach highlighted gaps in Indodax's security framework and shook user trust, prompting promises of more rigorous checks to prevent similar incidents.

Cyvers Angle:
Cyvers' monitoring systems detected the breach in real time, providing detailed insights into the attack's scope and execution. By flagging anomalous transactions early, Cyvers enabled immediate damage control measures. This incident underscores the critical role of Cyvers' advanced security solutions in preemptively detecting threats and safeguarding digital assets in an increasingly sophisticated threat landscape.

BingX Exchange Hack (September 20, 2024)

Company: BingX, a Singapore-based cryptocurrency exchange.

Funds Stolen: Approximately $52 million USD.

Vector of Attack: Compromised hot wallets across multiple blockchains.

Backstory:
On September 20, 2024, BingX detected abnormal network access, indicating a potential hacker attack on its hot wallets. The breach resulted in unauthorized transfers of various cryptocurrencies, including Ethereum (ETH), Binance Coin (BNB), and Tether (USDT), among others. The attackers swiftly moved the stolen assets across multiple blockchains, complicating tracking and recovery efforts.

Aftermath:
BingX promptly initiated emergency protocols, including the suspension of withdrawals and the transfer of assets to secure wallets. The exchange assured users that all losses would be covered from its capital reserves and began collaborating with blockchain security firms and law enforcement agencies to investigate the breach. Approximately $1 million of the stolen funds were frozen with the assistance of security firms. Withdrawals and deposits were gradually restored within 24 hours, and BingX committed to enhancing its security measures to prevent future incidents.

Cyvers Angle:
Cyvers' threat intelligence system played a crucial role in assessing the total loss across all chains, providing a comprehensive estimate of $52 million. This incident

underscores the importance of real-time monitoring and advanced threat detection systems in identifying and mitigating security breaches promptly. Cyvers' proactive approach highlights the necessity for continuous vigilance and robust security protocols in the rapidly evolving cryptocurrency landscape.

4th Quarter

Base Blockchain Exploit (October 25, 2024)

Company: Base, a Layer 2 blockchain platform.

Funds Stolen: Approximately $1 million USD.

Vector of Attack: Smart contract exploit through oracle price manipulation.

Backstory:
On October 25, 2024, an attacker exploited vulnerabilities in unverified lending contracts on the Base blockchain. They manipulated the price of Wrapped Ether (WETH) using a flawed oracle reliant on a single pair with limited liquidity (~$400K), inflating WETH's value artificially. Leveraging the inflated value, the attacker borrowed assets against the manipulated collateral, resulting in the theft of $1 million.

Aftermath:
The attacker moved stolen funds to the Ethereum network, depositing a portion into Tornado Cash to obscure their trail. The exploit highlighted the importance of reliable oracle mechanisms and rigorous contract verification. This incident sparked discussions in the DeFi community about enhancing security to prevent such breaches.

Cyvers Angle:
Cyvers' advanced monitoring system was the first to detect the suspicious transactions. Real-time alerts flagged the exploit as it occurred, providing actionable insights that could have facilitated immediate response efforts. This case exemplifies the critical role of Cyvers' solutions in identifying threats proactively and safeguarding DeFi ecosystems.

Radiant Capital Hack (November 1, 2024)

Company: Radiant Capital, a decentralized lending and borrowing platform.

Funds Stolen: $50 million USD.

Vector of Attack: Compromised device enabling the signing of malicious payloads.

Backstory:
Radiant Capital's robust security measures, including Safe Multisig wallets, Ledger hardware wallets, transaction simulations, and manual checks, were compromised

when a device allowed a malicious payload to be blindly signed. The attack exploited vulnerabilities in the trust model of secure wallet systems, leading to a $50 million theft.

Aftermath:
Radiant Capital launched an investigation in collaboration with cybersecurity experts to determine the breach's root cause. The attack highlighted significant gaps in even the most secure frameworks, sparking renewed industry discussions about strengthening wallet security and transaction validation.

Cyvers Angle:
Cyvers' advanced Transaction Firewall offers critical protection against such sophisticated attacks. By verifying transactions in real-time and blocking even when signers are compromised. This breach underscores the necessity of adopting proactive and innovative solutions like Cyvers' to prevent high-stakes vulnerabilities.

CoinPoker Hack (November 8, 2024)

Company: CoinPoker, a blockchain-based poker platform.

Funds Stolen: $2 million USD.

Vector of Attack: Access control violation involving a third-party provider.

Backstory:
The breach was triggered by a vulnerability in a third-party payment gateway mechanism. The hacker created a fake deposit worth $2 million, generating a fraudulent balance in their account. They systematically withdrew the funds in 82 small increments ($25K or less) across Ethereum, Binance Smart Chain, and Polygon to bypass detection mechanisms. The entire operation was completed within 50 minutes.

Aftermath:
The stolen funds were laundered through Tornado Cash, with incremental deposits obfuscating their origin, rendering recovery efforts extremely challenging. CoinPoker publicly acknowledged the breach and attempted to negotiate with the attacker via on-chain messages, offering a potential bounty for the return of funds. This incident underscored the risks of relying solely on custodian-defined limits without additional security measures.

Cyvers Angle:
Cyvers' AI-driven real-time monitoring system detected the very first suspicious $10K USDT transaction on Ethereum, marking the initial test of the exploit. Our system flagged the unusual pattern of repetitive $25K transfers across multiple chains,

providing early alerts well before the exploit concluded. This proactive detection highlights Cyvers' unmatched ability to identify and analyze malicious activity in real time, offering a critical opportunity to mitigate losses and secure pre-transaction validation, Cyvers could have thwarted the attacker at multiple stages, making this an avoidable tragedy with the right tools in place.

Polter Finance Exploit (November 17, 2024)

Company: Polter Finance, a decentralized non-custodial lending and borrowing platform operating on the Fantom blockchain.

Funds Stolen: Approximately $12 million USD.

Vector of Attack: Smart contract exploit through oracle price manipulation.

Backstory:
The attacker initiated the exploit by transferring funds through Tornado Cash to obscure their origin, then bridging them from Ethereum to the Fantom network. They exploited a vulnerability in Polter Finance's newly launched SpookySwap (BOO) market by manipulating the token's price oracle. This manipulation allowed the attacker to artificially inflate the value of BOO tokens, enabling them to secure loans far exceeding the actual value of their collateral. The attack drained approximately $12 million from the platform's total value locked (TVL).

Aftermath:
Polter Finance promptly paused its platform to prevent further losses and notified bridge operators. The pseudonymous founder, "Whichghost," filed a police report in Singapore and reached out to the attacker via an on-chain message, offering negotiation and potential immunity in exchange for the return of the stolen funds. Despite these efforts, skepticism arose within the community, with some speculating potential insider involvement. The incident underscores the critical importance of thorough security audits and robust oracle mechanisms in DeFi protocols.

Cyvers Angle:
Cyvers' advanced real-time monitoring system detected the exploit as it unfolded, identifying the suspicious transactions and the attacker's use of Tornado Cash to obscure fund origins. Our system provided immediate alerts, enabling stakeholders to respond swiftly to the breach. This proactive detection continuous monitoring and rapid threat identification, highlighting the necessity of advanced security solutions in the evolving DeFi landscape.

M2 Exchange Hack (October 31, 2024)

Company: M2Exchange, a cryptocurrency exchange platform.

Funds Stolen: Approximately $13 million USD.

Vector of Attack: Access control violation.

Backstory:

On October 31, 2024, Cyvers' advanced AI monitoring system detected unauthorized access to M2Exchange's wallets across Ethereum, Solana, and Bitcoin networks. Over a 16-minute attack window, hackers drained $13M in assets, including 3.78M $USDT, 97M $SHIB, 1,378 $ETH, and 41 $BTC. The stolen funds were converted entirely into $ETH, with $10M still remaining on the Ethereum chain as of the last update. Despite Cyvers' attempts to alert M2Exchange in real time, the warnings went unanswered, allowing the attack to progress unchecked.

Aftermath:

M2Exchange responded swiftly, claiming full responsibility and assuring users that all customer funds were fully restored. However, the exchange's lack of transparency regarding the exact failure points raises concerns about whether all vulnerabilities were adequately addressed. While their rapid compensation is commendable, true preventative measures and proactive transparency are crucial for maintaining trust in the crypto community.

Cyvers Angle:

Cyvers was the first to detect and report the breach, showcasing the effectiveness of its real-time monitoring system. By identifying suspicious multi-chain transactions and flagging them immediately, Cyvers provided a vital opportunity for mitigation that was unfortunately missed by M2Exchange. This incident underscores the importance of leveraging Cyvers' solutions for preventing breaches before they occur.

CYVERS

Trends and insights

Audited Yet Hacked: The Imperative of Real-Time Monitoring in Web3

In the dynamic realm of Web3, security challenges loom large for crypto companies. Many rely primarily on pre-deployment smart contract audits, assuming these checks will safeguard projects and client funds. However, a startling statistic reveals that **90% of smart contracts hacked had undergone pre-deployment audits,** exposing a critical gap in this approach.

The Role of Smart Contract Audits

Smart contract audits play a vital role in identifying vulnerabilities and security flaws pre-deployment. Companies often use multiple auditors to ensure comprehensive coverage. While these efforts reduce risks, they fail to address every threat, particularly new, sophisticated attack vectors that arise post-deployment. Audits alone cannot provide foolproof security.

Case Studies: *When Audited Contracts Fail*

Several high-profile hacks in 2023 and 2024 demonstrate the limitations of relying solely on audits:

- **Dough Finance** (July 2024): Lost **$1.8M** despite an audit labeling their contracts "low risk."
- **UwU Lend** (June 2024): Suffered **$19.3M** in two separate hacks, even with prior audits.
- **Radiant Capital** (January 2024): Experienced a **$4.5M** loss after four audit reviews by top firms.
- **Euler Finance** (May 2023): Lost **$197M** following audits by four leading firms.
- **LI.FI** (July 2024): Lost **$11M**, two years after boasting of audits from two prominent providers.

The Missing Link: Real-Time Monitoring and Pre-Transaction Screening

Beyond audits, real-time monitoring and pre-transaction screening are essential components of a robust security framework:

1. Real-Time Monitoring:

- Continuously oversees deployed smart contracts.
- Detects and responds to threats, including scams, fraud, and exploits, as they happen.
- Reduces the window for hackers, enabling rapid mitigations.

2. Pre-Transaction Screening:

- Analyzes transactions before execution to identify risks.

- Blocks malicious actors and fraudulent activities.
- Ensures only legitimate transactions proceed, bolstering overall security.

The Importance of Crisis Management Mechanisms

Crisis management tools such as pause functions and circuit breakers are critical in reacting to detected threats. Whether automated or manual, these mechanisms enable swift responses to mitigate damages when real-time alerts signal issues.

Conclusion

While audits are indispensable, they represent just one layer of Web3 security. To truly protect crypto projects and their stakeholders, a **holistic security approach** is necessary. Integrating **real-time monitoring, pre-transaction risk assessment, and robust crisis management tools** can transform how companies defend against evolving threats, ensuring the resilience and trustworthiness of the Web3 ecosystem.

The Ripple Effect of Crypto Hacks on Companies

In the high-stakes world of cryptocurrency, hacking incidents leave devastation beyond the immediate financial loss. Recent researches, including Cyvers's data, ImmuneFi's 2024 report, the 2024 report from the University of British Columbia (UBC), Cozy Finance data, and other expert analyses, highlights the multifaceted impact of these events on companies, spanning financial damage, reputational harm, and operational setbacks.

Financial and Market Impact

The average crypto hack costs companies $16 million, with significant market repercussions. Token prices often drop by 52% within six months following a hack, as detailed in Immunefi's comprehensive analysis of 2021-2023 data. The financial consequences of these attacks ripple out further, with recovery costs often exceeding the stolen funds. The 2024 report from UBC states that the costs of implementing post-hack security measures and responding to legal actions can be as much as 1.5 times the direct financial loss of the incident.

For example, the DMM Bitcoin hack in May 2024 resulted in $305 million in losses, but the full financial impact was far greater due to prolonged market volatility, compliance overhauls, and operational adjustments.

Survival Rates After Hacks

Contrary to common perceptions, projects have a higher chance of surviving a hack than many founders assume. According to data from Cozy Finance, 39% of projects survived for at least one year after being hacked. Survival chances increase even further if funds are recovered, or users are reimbursed:

- **Fund Recovery Rates:**
  Cozy Finance's findings show that 44% of hacked projects recover some portion of lost funds, either through technical intervention, negotiation with attackers, or law enforcement. Recovered funds lead to a survival rate of 50%, compared to just 31% for projects that recover nothing.

- **Impact of User Reimbursement:**
  Reimbursing users significantly boosts survival rates. Projects reimbursing users at a high rate (>80%) had a 65% survival rate, compared to just 14% for those reimbursing at a low rate (<25%). The 2024 report from UBC also highlights that projects offering transparency and swift reimbursement see greater retention of their user base and investor confidence.

Dependency and Reputational Risks

Hacks create ripple effects beyond immediate losses, including reputational damage and ecosystem disruptions. For example, the WazirX hack in 2023, which exposed wallet vulnerabilities and led to a $235 million loss, prompted Indian regulators to increase scrutiny of the crypto industry. The 2024 report from UBC notes that such regulatory responses often lead to increased compliance costs but can also drive better security practices across the sector.

Dependency-related impacts are also significant. A compromised protocol can affect the entire ecosystem it supports, eroding user confidence and inhibiting new integrations. Immunefi notes that these effects can amplify over time, undermining even unrelated parts of the ecosystem.

Operational and Talent Challenges

The operational aftermath of a hack is extensive. The 2024 report from UBC highlights that hacked companies often face a productivity decline of up to 30% for three months post-incident, as resources are diverted to damage control. This aligns with findings from Cozy Finance, which notes that recovery efforts typically consume three months of development time. Talent churn is another common challenge; the loss of key security personnel or leadership during or after a hack disrupts long-term stability and strategy.

Legal and Regulatory Repercussions

Legal challenges often follow hacking incidents, with regulators enforcing stricter compliance protocols. The WazirX hack prompted Indian regulators to demand higher transparency and adherence to security standards, setting an example for how governments worldwide may respond to such crises. The 2024 report from UBC states that regulatory responses can increase compliance costs by up to 40% over two years, particularly for companies operating in jurisdictions with evolving crypto regulations.

Evolving Security Measures

To combat the increasing sophistication of cyberattacks, platforms like Cyvers.ai are investing in real-time monitoring and mitigation tools. Their work in detecting and addressing threats—such as the Stake.com and Pump.fun hacks—illustrates how proactive measures can reduce both financial and reputational damage. The 2024 report from UBC highlights the importance of incorporating AI-driven systems to identify threats earlier and more effectively than traditional methods.

Conclusion

Crypto companies must adopt robust, multi-layered security frameworks to withstand and mitigate the impacts of hacking incidents. The data from Cozy Finance and the

2024 report from UBC emphasize the importance of fund recovery, user reimbursement, and proactive communication in determining long-term project viability. Coupled with AI-driven monitoring and tighter compliance, these measures not only minimize damage but also restore user trust and ensure the sustainability of the Web3 ecosystem.

The Rise of Multisig Wallet Attacks in 2024: Techniques, Impact, and Lessons Learned

In 2024, attackers increasingly targeted **multisig wallets**, exploiting their complex authorization mechanisms to execute high-profile heists. Multisig wallets, designed to enhance security by requiring multiple approvals for transactions, became lucrative targets as hackers developed sophisticated strategies to bypass their safeguards. Notable incidents, including the $235 million WazirX breach, the $50 million Radiant Capital attack, and the $305 million DMM Bitcoin hack, exposed critical vulnerabilities in wallet systems and transaction signing processes.

Techniques Used

1. **Compromising Shared Responsibility:**

Hackers exploited weaknesses in distributed signing schemes. In the WazirX breach, attackers gained unauthorized access to a quorum of signers by phishing team members and deploying malicious software. This enabled them to siphon funds while bypassing the intended safeguards of the multisig setup.

2. **Manipulating Transaction Displays:**

Using spoofed transaction data, attackers crafted fraudulent transactions that appeared legitimate in wallet interfaces. This method deceived users into approving malicious actions. Such techniques were pivotal in incidents like the **DMM Bitcoin hack**, where tampered transaction details misled signers into authorizing the transfer of $305 million in funds.

3. **Exploiting Smart Contract Logic in Multisig Systems:**

In the Radiant Capital breach, attackers identified and manipulated a flaw in the multisig smart contract's logic. They injected unauthorized code during a contract update, enabling malicious transactions to bypass the quorum of required signers. This highlighted how poorly implemented contract upgrades or governance procedures can open doors for exploits.

4. **Malware-Assisted Signature Hijacking:**

Attackers deployed malware on hardware wallets and signing devices to intercept and alter transaction details mid-signing, compromising the integrity of multisig workflows.

Quantum and AI: Accelerating the Cyber Arms Race

Quantum computing and artificial intelligence (AI) are revolutionizing cybersecurity, creating both unprecedented opportunities and alarming threats. Quantum advancements threaten the backbone of blockchain technology: cryptography. Within a decade, quantum computers may be capable of breaking encryption, leaving blockchain-based assets exposed.

Concurrently, AI is turbocharging cybercrime. Hackers now deploy AI-driven algorithms to identify vulnerabilities, automate phishing attacks, and optimize laundering strategies. These technologies allow adversaries to scale operations, making threats both more frequent and harder to predict.

The Web3 ecosystem must embrace post-quantum cryptography and integrate AI-driven threat detection tools to counter these risks. Platforms like Cyvers are leading the charge, leveraging machine learning to monitor real-time blockchain activity, flagging anomalies, and neutralizing threats. As technology evolves, so too must the defense strategies that safeguard the digital frontier.

Tokenized Real-World Assets: Securing a Revolutionary Frontier

Tokenized real-world assets (RWAs) are bridging traditional finance and decentralized crypto ecosystems. By enabling fractional ownership of tangible assets like real estate and artwork, tokenization democratizes access to investments, fostering inclusivity and liquidity. However, as noted by Cyvers CEO Deddy Lavid, this transformative innovation introduces unique security challenges.

Key risks include vulnerabilities in smart contracts, digital wallets, and pseudonymous blockchain transactions. Hackers exploit these gaps through attacks like flash loan

exploits and address poisoning. Cyvers addresses these threats with its Address Reputation Score, a machine-learning-powered tool that evaluates blockchain addresses for risk. This solution empowers users to assess transaction counterparties, mitigating fraud and safeguarding investments.

As RWAs redefine asset management, security innovations like Cyvers' Address Reputation Score are critical. By ensuring trust and integrity in transactions, they enable secure scaling of this emerging financial paradigm, building a resilient foundation for the future.

Bitcoin ETFs: A Double-Edged Sword for Security

The introduction of Bitcoin spot ETFs in 2024 marked a watershed moment for cryptocurrency, attracting significant institutional investment. However, this development has also made the digital asset sector a prime target for state-sponsored hackers, particularly the North Korean Lazarus Group. Leveraging advanced techniques, these actors exploit vulnerabilities in wallets, centralized exchanges, and new financial instruments tied to ETFs.

The Lazarus Group's focus on crypto assets is tied to geopolitical strategies, using stolen funds to bypass sanctions and finance state initiatives. Attacks often target weak key management systems, phishing vulnerabilities, and unmonitored exchange interactions. These exploits underline the urgent need for robust, real-time threat monitoring.

Cyvers has played a pivotal role in mitigating such risks, leveraging AI and blockchain analytics to monitor and neutralize threats before they materialize. This proactive approach ensures that while Bitcoin ETFs expand access to cryptocurrency, they do so within a secure framework. As ETFs continue to grow, the industry must adopt a defense-in-depth approach, blending technology, compliance, and education to safeguard against an evolving threat landscape.

CYVERS

Regulation and Standardization

Regulation:

Global:

IOSCO:
IOSCO's recent policy recommendations aim to regulate crypto markets with the same rigor as traditional financial markets.

Key Impacts:

- **Security:**
  Recommends "same activity, same risk, same regulation" principles, requiring crypto platforms to meet high standards for client asset protection and cybersecurity.
- **Compliance:**
  Calls for rigorous governance and risk management practices, including clear disclosure requirements for DeFi and stablecoin providers.
- **Fraud Prevention:**
  Focuses on reducing fraud through cross-border regulatory cooperation, ensuring consistent enforcement and oversight globally.

Why It Matters:
IOSCO's recommendations highlight the need for robust fraud detection mechanisms and heightened consumer protection in the growing DeFi sector.

The United States:

The Strategic Bitcoin Reserve Bill: *A Transformative Initiative*

Senator Cynthia Lummis' **Strategic Bitcoin Reserve Bill,** set to be introduced in early 2025 under President Trump's administration, represents a bold vision for integrating cryptocurrencies into U.S. financial strategy. If approved by the Senate, this landmark legislation could position Bitcoin as a strategic reserve asset, akin to gold, solidifying its role in the nation's economic stability and financial security.

Key Provisions:

- **National Bitcoin Reserve:** The bill proposes establishing a federally managed Bitcoin reserve, signaling long-term confidence in digital assets and encouraging mainstream adoption.
- **Streamlined Regulatory Framework:** It introduces a unified regulatory approach, reducing compliance barriers for blockchain businesses and fostering innovation.

- **Incentives for Innovation:** Provisions for tax incentives and federal grants aim to support blockchain startups focused on critical infrastructure, security, and scalability.
- **Global Competitiveness**: By adopting this forward-looking policy, the U.S. seeks to assert its dominance in the blockchain space, encouraging other nations to follow suit.

Implications of the Bill

1. **Institutional Adoption:** The establishment of a Bitcoin reserve could drive institutional confidence, leading to increased investments from traditional financial sectors and asset managers.
2. **Enhanced Security Needs:** Managing a national Bitcoin reserve will necessitate advanced security protocols, including state-of-the-art wallet systems, multi-signature authorization, and real-time threat detection.
3. **Market Stabilization:** A federally backed reserve could mitigate Bitcoin's volatility, encouraging broader adoption and enhancing market stability.
4. **Global Ripple Effects:** The bill may prompt other nations to adopt similar strategies, fostering global competition and accelerating blockchain innovation.

Challenges and Criticisms:

- **Legislative Hurdles:**
  The bill's approval may face resistance from lawmakers concerned about Bitcoin's volatility and environmental impact.
- **Security Risks:**
  Managing a national reserve introduces significant cybersecurity challenges, requiring robust safeguards against insider threats and external attacks.

India:

In the wake of the significant security breach at WazirX, where approximately $235 million was stolen, Indian regulatory bodies are intensifying their focus on the cryptocurrency sector to enhance security and compliance.

Regulatory Developments:

Multi-Regulatory Framework Proposal: The Securities and Exchange Board of India (SEBI) has proposed a collaborative regulatory approach, suggesting that multiple regulatory bodies oversee various aspects of cryptocurrency activities. This proposal contrasts with the Reserve Bank of India's (RBI) earlier stance favoring a complete ban on cryptocurrencies.

Financial Intelligence Unit (FIU) Actions:
The FIU has taken decisive steps against non-compliant offshore crypto exchanges, including issuing show-cause notices and imposing penalties. For instance, Binance was fined 188.2 million rupees ($2.25 million) for operating in violation of local anti-money laundering regulations.

Department of Economic Affairs (DEA) Consultation Paper:
The DEA is preparing to release a consultation paper aimed at shaping a comprehensive crypto policy for India. This initiative reflects the government's intent to establish a balanced and inclusive regulatory framework for digital assets.

Implications for Crypto Exchanges:

- **Enhanced Compliance Requirements:**
  Exchanges may be required to implement more robust Know Your Customer (KYC) and Anti-Money Laundering (AML) procedures to align with stricter regulatory standards.
- **Operational Transparency:**
  There will likely be increased demands for transparency in operations, including regular audits and disclosures, to build trust and ensure adherence to regulations.
- **Security Protocols:**
  Exchanges will need to bolster their cybersecurity measures to protect against breaches and instill confidence among users and regulators.

European Union:

MiCA :
MiCAR, fully effective by December 2024, introduces a unified regulatory framework across the EU for crypto service providers.

Key Impacts:

- **Security:** Crypto Asset Service Providers (CASPs) must implement enhanced risk management, including protection against cyber threats and operational risks.
- **Compliance:** Transparency requirements for stablecoins include proof of reserves and regular audits to reduce risks of insolvency or fraud.
- **Fraud Prevention:** Stronger customer protection rules mandate rigorous KYC processes and transaction monitoring to identify and mitigate fraudulent activity.

Why It Matters: MiCAR minimizes regulatory fragmentation, ensuring consistent security and compliance standards across the EU.

DORA:

DORA, applicable from January 17, 2025, sets ICT risk management requirements for financial entities, including crypto firms operating in the EU.

Key Impacts:

- **Security:** Firms must implement robust frameworks for cyber risk identification, response, and recovery, alongside continuous monitoring of ICT systems.
- **Compliance:** Regular stress testing and third-party risk management evaluations are mandatory to maintain operational resilience.
- **Fraud Prevention:** Enhanced incident reporting ensures timely communication of security breaches, aiding in fraud detection and mitigation.

Why It Matters: DORA mandates a proactive approach to operational risks, ensuring crypto companies are better equipped to handle sophisticated cyberattacks and disruptions.

United Kingdom:

FCA Regulation on APP Fraud

On October 7, 2024, the United Kingdom implemented mandatory reimbursement rules for authorized push payment (APP) fraud, requiring payment service providers (PSPs) to reimburse customers who fall victim to such scams. While the regulation currently applies to traditional PSPs, the broader principles may soon affect crypto platforms, especially as regulators increasingly align crypto services with traditional financial standards.

What the New Rules Mean for Crypto Platforms

APP fraud, where victims are deceived into authorizing payments to fraudsters, is becoming a rising concern in the crypto space. The decentralized and irreversible nature of crypto transactions exacerbates these risks, making fraud detection and prevention critical. If regulators extend APP fraud protections to crypto platforms, operators may face significant financial liabilities for reimbursing victims, regardless of fault.

Proactive Fraud Prevention: A Must for Crypto Platforms

To avoid losses and align with evolving standards, crypto platforms must enhance fraud prevention measures:

1. **Real-Time Transaction Monitoring:** Platforms should implement robust systems to monitor for anomalies such as unusual transaction patterns, rapid fund withdrawals.or flagged wallet addresses AI-powered detection tools can provide actionable insights in real time.
2. **Real-Time Wallet Screening:** Strengthened protocols for wallet address verification can minimize the risk of fraudulent activity.
3. **Automated and Accurate Reporting Systems** Flagging and time-stamping high-risk addresses and tracking the money-trail can assist in countering unsubstantiated demands for reimbursement.

Conclusion

The industry should view the new APP Fraud rules as a call to action. Proactively adopting fraud prevention services not only minimizes financial losses but also reinforces user trust—an essential factor in the rapidly growing crypto ecosystem.

Standardization:

Real-Time Monitoring: A New Benchmark in Crypto Wallet Security

The upcoming version (V.9) of the CryptoCurrency Security Standard (CCSS) introduces **real-time wallet monitoring** as a mandatory requirement for certification. By continuously tracking operational and organizational wallets for anomalous behavior, this update emphasizes proactive threat detection, enabling entities to respond swiftly and reduce the impact of attacks. This evolution reflects the CCSS's commitment to strengthening security practices in an increasingly vulnerable crypto landscape.

The New Requirement: Real-Time Wallet Monitoring

Requirement Wording: *Internal operational and organizational wallets are continuously monitored for anomalous behavior, generating alerts. Appropriate personnel address the alerts generated.*

Rationale: By detecting unusual wallet activity, entities can mitigate threats promptly, ensuring reduced damage and heightened asset protection. This proactive approach aligns with the growing need for enhanced security in cryptocurrency operations.

What is the CryptoCurrency Security Standard (CCSS)?

The CCSS is a global framework that sets benchmarks for securing cryptocurrency systems, including wallets, exchanges, and custodial services. Managed by the

CryptoCurrency Certification Consortium (C4), it emphasizes robust practices like key management and operational security. With real-time monitoring now mandatory, CCSS V.9 raises the bar for safeguarding digital assets against evolving threats.


New solutions by
CYVERS

1. Preemptive Protection for Wallets

The Problem: Wallets as the primary target for hackers

Access control breaches are among the most critical threats in the Web3 ecosystem. These breaches occur when malicious actors bypass security measures to gain unauthorized access to private keys, wallets, or transaction signing mechanisms. In 2024, centralized platforms saw a staggering 1,000% increase in access control attacks, with major incidents like the WazirX hack, which resulted in a $234.9 million loss, highlighting the vulnerabilities in current systems. Similarly, Radiant Capital suffered losses due to a failure in safeguarding its access controls, further underscoring the inadequacy of traditional wallet security measures.

These attacks exploit weak access controls, phishing campaigns, and malware targeting wallet infrastructures. For institutional investors transitioning to self-custody solutions like Fireblocks, the problem is compounded by centralization risks and operational challenges, as revealed by recent failures in multi-party computation (MPC) wallet services. Without proper safeguards, these black-box solutions leave critical gaps that hackers can exploit.

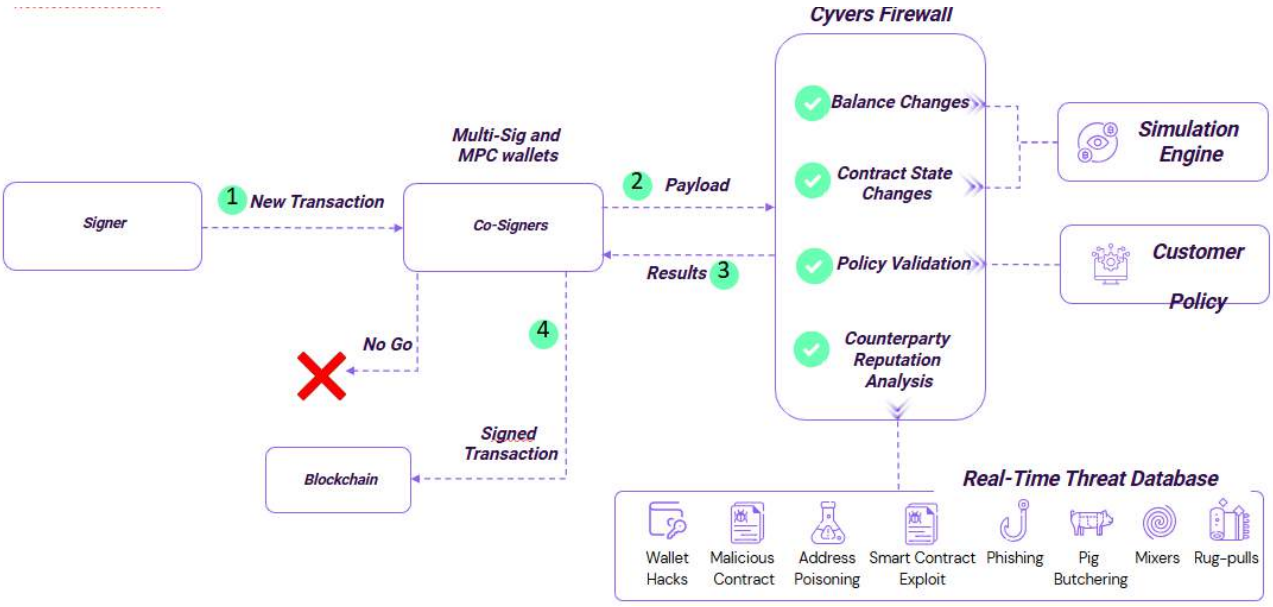
Cyvers's Solution:

Cyvers addresses this challenge with its **Preemptive Threat Interceptor and Secure Signer**, two groundbreaking solutions designed to mitigate access risks.

The Threat Interceptor operates by simulating and validating transactions—whether simple peer-to-peer or complex atomic transactions—before execution. Once a

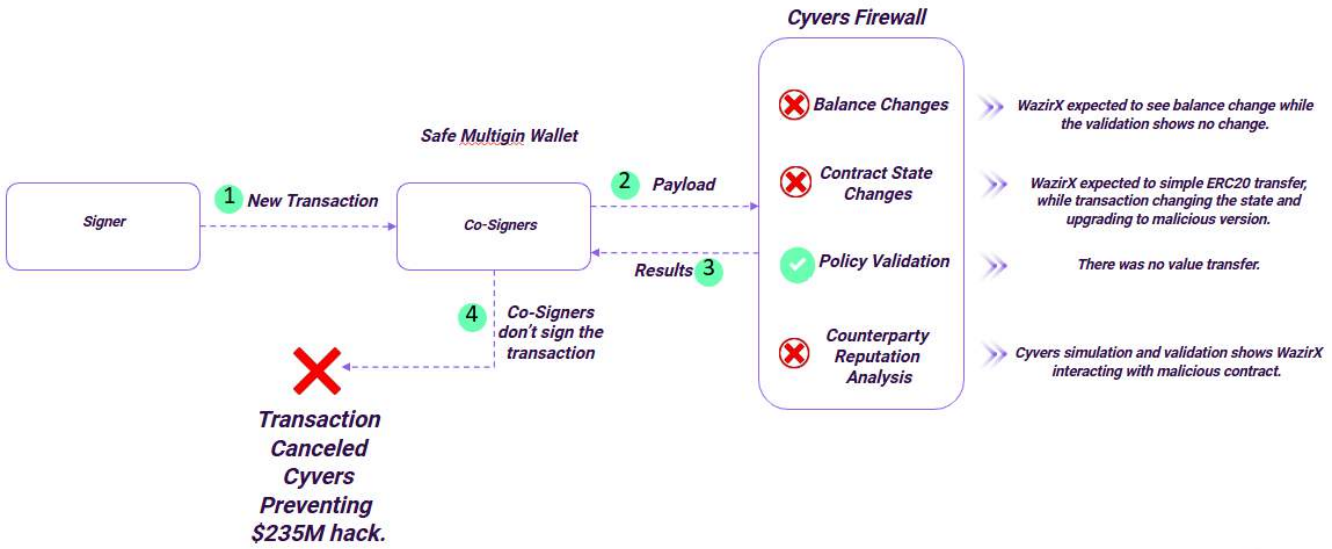
transaction payload is generated, it is transmitted to Cyvers's system, which simulates it on-chain and uses its AI-powered engine to analyze it. The system evaluates each milestone of the transaction, scrutinizing wallets or smart contracts, assessing their risk and potential maliciousness. This fully customizable tool aligns with user-defined security preferences and operational policies, empowering users to either manually or automatically approve or block transactions based on Cyvers' risk assessment.

The solution easily integrates with custodians and wallet providers to allow a seamless user experience.



This proactive mechanism not only prevents hacks, scams, and compliance risks but could have mitigated losses in incidents like the sophisticated WazirX hack, which drained $235M from India's largest exchange. By addressing vulnerabilities at the transaction level, Cyvers offers unparalleled security to institutional and individual users alike.

IF WazirX Used Cyvers

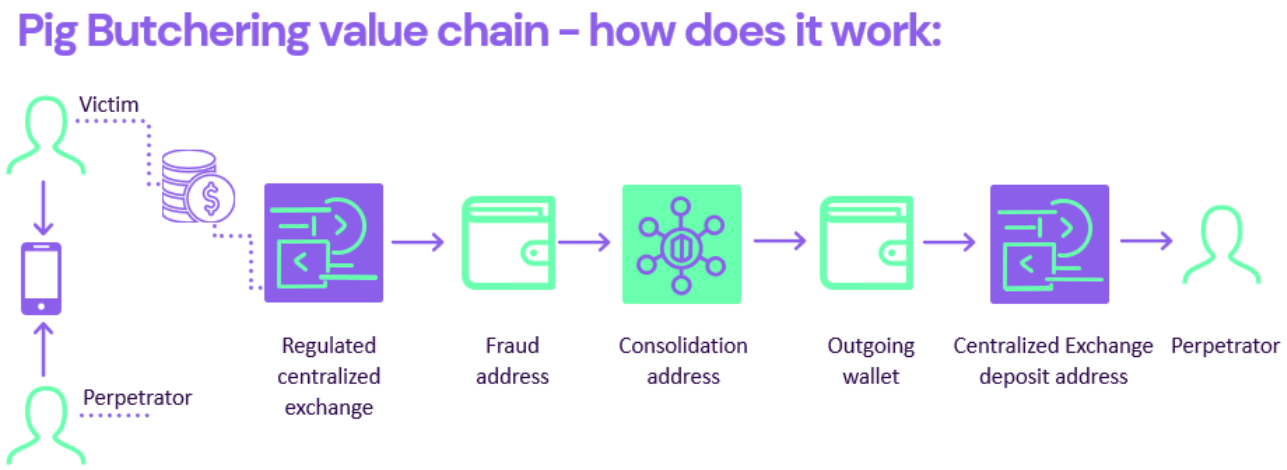


Meanwhile, the Secure Signer, developed in partnership with **Station70**, extends this protection with a dual-layer security framework. It combines pre-transaction simulations and a co-signing mechanism that identifies anomalies before transactions are executed on-chain. This seamless integration ensures that users of infrastructures like Fireblocks can adopt enhanced security measures without complexity.

2. Pig Butchering Protection

The Problem:

"Pig Butchering" represents a sophisticated and escalating form of authorized fraud within the cryptocurrency ecosystem. Fraudsters build trust with victims over time, persuading them to invest in fraudulent platforms. These scams involve a complex series of steps: funds are funneled into fraudulent wallets, layered through multiple transfers to obscure their origin, and laundered across regulated and unregulated exchanges.



The scale of this phenomenon is staggering, with victims numbering in the hundreds of thousands and annual losses reaching billions of dollars. The FBI's Internet Crime Complaint Center (IC3) reported that pig butchering scams accounted for over $5.6 billion in losses in 2023 (ABC News). It is also estimated that more than 200,000 people are involved in activating those schemes, mostly in call and messaging centers in developing countries. These scams are not limited to obscure or small platforms; they often involve major exchanges and employ intricate cross-chain laundering techniques.

Fraudsters have increasingly turned to social media and messaging platforms to lure victims, as highlighted in reports from Meta and New York Attorney General Letitia James (NY Post). Many schemes exploit emotional vulnerabilities, particularly through romance scams, with individual losses often exceeding $1 million. These operations use advanced technologies like AI to clone voices and develop fake investment materials, while platforms themselves are targeted through fake crypto apps and websites. Fraudsters further obscure their tracks using tools like atomic swaps and cross-chain bridges. The U.S. Securities and Exchange Commission (SEC) reported a 21% increase in investment fraud losses in 2023, with cryptocurrency scams rising by 53%, adding to a $3.96 billion toll (Finance Magnates). These findings reveal the

intersection of technology, emotional manipulation, and regulatory gaps that continue to fuel this alarming trend.

Recognizing the severity of this issue, global regulators have begun imposing greater accountability on crypto platforms. Among the most proactive measures is the UK's Financial Conduct Authority (FCA) Authorized Push Payment (APP) Fraud regulation introduced in 2024. This regulation mandates that crypto platforms reimburse victims of fraudulent activity, underscoring the critical need for robust fraud prevention mechanisms.

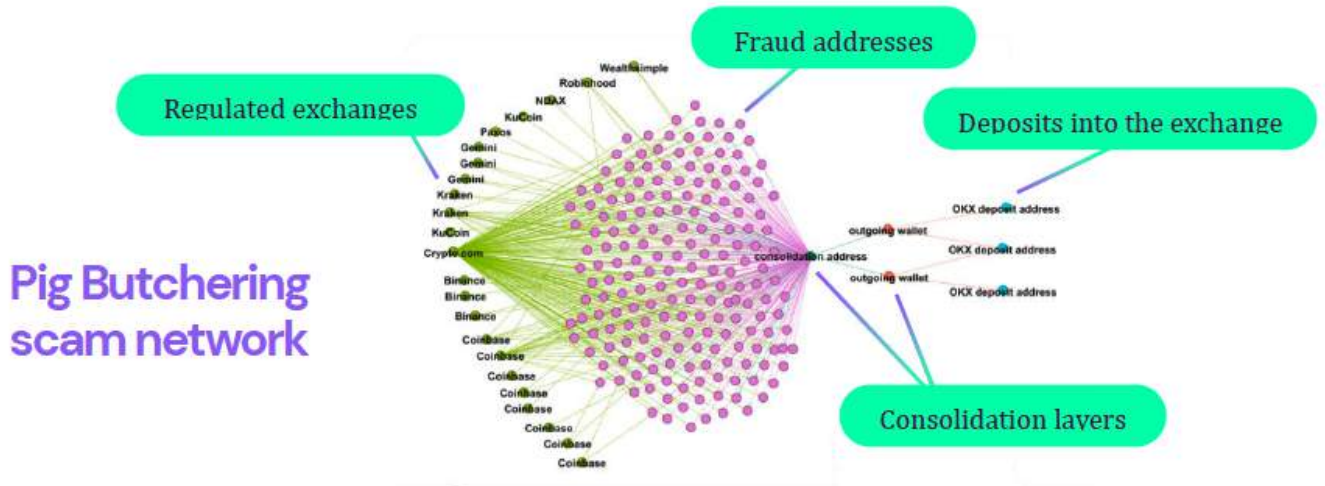
Cyvers's Solution:

Cyvers has pioneered a comprehensive pig butchering detection and mitigation framework, powered by advanced AI and graph analysis technologies.

In 2024 alone, Cyvers identified more than 180 fraud networks operating over 160,000 wallets, which collectively received over $4 billion from victims through almost 1 million transactions.

With real-time flagging mechanisms, Cyvers detects and disrupts pig butchering schemes as they unfold, providing crypto platforms with proactive protection. By flagging wallets linked to pig butchering networks, Cyvers enables platforms to take decisive action—whether by blocking these addresses or warning users before engaging with them.

Beyond safeguarding users, Cyvers helps platforms mitigate regulatory risks, avoiding fines, legal liabilities, and reputational damage. This holistic approach not only curbs fraud but also enhances user trust and fosters a safer cryptocurrency ecosystem.



3. Dynamic Risk Assessment

The Problem:

Know Your Transaction (KYT) and address screening are essential for detecting illicit funds, malicious activities and assessing the risk that may arise from interacting with wallets and smart contracts. However, current tools often fall short, offering incomplete insights into wallet histories or affiliations. Many AML solutions lack cross-chain and cross-token tracing capabilities, leaving institutions with blind spots in their compliance efforts. These systems are “shortsighted” when assessing the risk and maliciousness of a certain address. Most systems can not trace beyond one “hop”, and don’t have the capabilities of tracing the funds in complex DeFi transactions. Moreover, the latency of these systems further hinders their effectiveness, as it often takes days to detect suspicious transactions, by which time the funds have already been laundered.

For example, a wallet flagged as “clean” by traditional tools was later found to have ties to Tornado Cash and other mixers when analyzed through Cyvers's dynamic tracing engine. Such oversights leave platforms vulnerable to regulatory penalties and expose users to financial risks.

Cyvers's Solution:

Cyvers' **Dynamic Risk Assessment** provides a real-time, comprehensive solution for compliance and risk management. By integrating machine learning, behavioral analysis, and graph algorithms, the platform offers full transparency into wallet/smart contract activities.

This system excels in tracing multi-hop transactions (of tens of hops) across chains and tokens, providing instantaneous insights with a very low latency. Unlike other tools, Cyvers enables platforms to uncover hidden affiliations and risky behaviors in wallets, whether they involve sanctioned entities, mixers, fraud networks and more.

For instance, Cyvers identified a complex laundering scheme that funneled funds through Li.Fi. protocol where they were swapped and sent across multiple wallets in a single atomic transaction. The target wallet of this complex sequence was flagged as

safe by the existing solutions, while Cyvers labelled it as risky, with a full breakdown of the money trail.

This is what you see with current AML tools

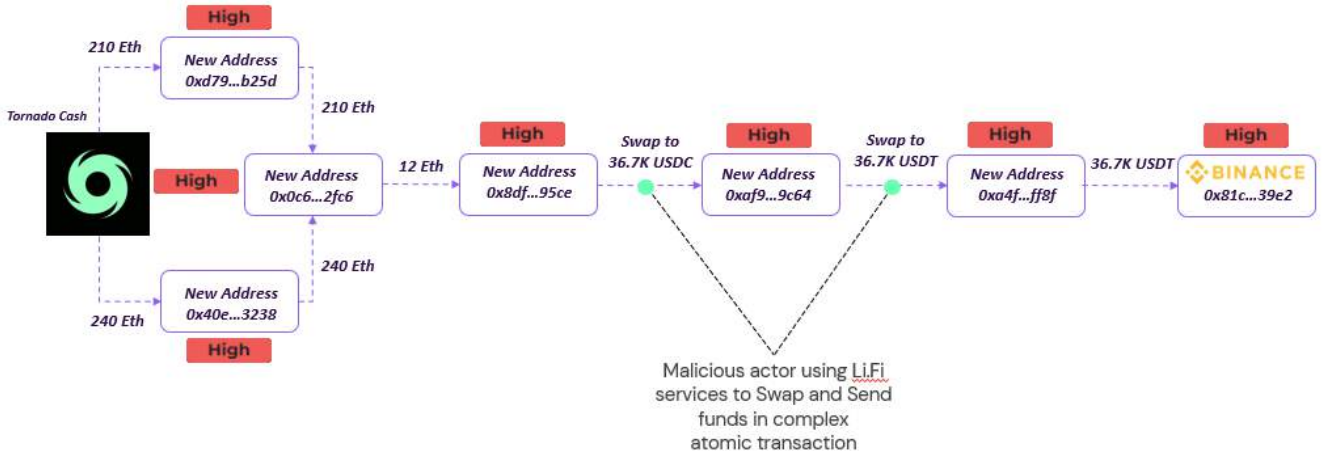
This is what you will see if you will screen this Binance Deposit address (0x81CFe11dC6e670e2aF62F200917FbB77A30339E2) in Chainalysis, Elliptic and TRM.

Chainalysis ELLIPTIC TRM

LOW

Address has no exposure to any malicious funds, so Binance approved the deposit

This is what you see with Cyvers



The platform's ability to trace the full flow of funds, even in such complex scenarios, ensures that no suspicious activity goes unnoticed.

It also provides a full clickable map that illustrates the flow of funds throughout all the steps of the way.

By providing actionable insights and automated responses, Cyvers empowers platforms to remain compliant, safeguard assets, and maintain user trust. Its superior tracing capabilities position it as the leading solution in an increasingly regulated digital economy.


CYVERS
in the News

COINTELEGRAPH
The future of money

News Indices In Depth Learn Research Podcasts About

ZOLTAN VARDAI NOV 20, 2024

Cyvers launches institutional crypto security tool for $4B vulnerability

Cyvers and Station70's solution uses an AI-powered real-time threat detection system to protect institutional-grade crypto transfers, aiming to bolster mass adoption.

Bitcoin.com News

Crypto Exchange M2 Confirms $13.7 Million Breach, Says Issue Resolved Within 16 Minutes

M2 Exchange recovered from a $13.7 million security breach within 16 minutes. A security firm said the incident highlights the growing vulnerability of crypto exchanges.

Cybersecurity firm Cyvers detected suspicious transactions involving the exchange across the Ethereum, Solana, and Bitcoin networks. Cyvers characterized the breach as an access control violation, saying the affected address had received 3.7 million USDT, 97 million Shiba Inu tokens, and 1,378 ETH. The digital assets were subsequently converted into ether.

HACKERNOON

Cyvers Early Detection Of Sonne Finance Hack and The Importance Of AI In Web3 Security

COINTELEGRAPH
The future of money

News Indices In Depth Learn Research Podcasts About

ZOLTAN VARDAI SEP 11, 2024

Bitcoin ETFs are next major target for North Korean hackers — Cyvers

North Korean hackers could be eying the infrastructure around Bitcoin ETFs, lured by the $52 billion worth of cumulative holdings.

BE(IN)CRYPTO News Rankings Learn Bonus Hunter Advertise Learn-to-Earn Newsletters Web3 Jobs Top Picks

Trusted

Attackers Shifted from DeFi to CeFi: Cyvers' Web3 Security Report Q2 2024

6 mins

By Lynn Wang 8 July 2024, 12:59 GMT+0000 Updated by Lynn Wang 8 July 2024, 12:56 GMT+0000

Bloomberg

North Korean Hackers Are Suspected in $235 Million Crypto Theft

By Sidhartha Shukla
18 липня 2024 р. at 11:17 GMT+3
Updated on 18 липня 2024 р. at 15:30 GMT+3

Save Translate Listen 2:38

WazirX, in a statement on its X account, didn't give an estimate of the amount of crypto that may have been lost. Blockchain security firm Cyvers said $234.9 million of assets have been drained from the exchange and moved to a new address.

BE(IN)CRYPTO News Rankings Learn Bonus Hunter Advertise Learn-to-Earn Newsletters Web3 Jobs Top Picks

Trusted

Radiant Capital Suffers $50 Million Hack; Second Major Attack in 2024

2 mins

By Landon Manning 17 October 2024, 04:19 GMT+0000 Updated by Harsh Notariya 17 October 2024, 04:19 GMT+0000

Blockchain lending protocol Radiant Capital lost more than $50 million in a major hack Wednesday. Cyvers Alerts first recognized this news, detecting a series of suspicious transactions involving Radiant Capital on multiple chains. Cyvers warned users to avoid all interactions with Radiant until further notice.

CryptoPotato
Everything Hot in Crypto

Crypto News Margin Trading Guides DeFi & NFT Buy Language

Trump's Win Is Big for Crypto, But Let's Keep Expectations in Check (Op-Ed)

Author: Guest Author • Last Updated Nov 14, 2024 @ 15:01

Authored by:

Michael Pearl is a seasoned executive in fintech and blockchain with over a decade of experience in business development and growth. Before joining Cyvers, he was the COO of Intentable and served as Director of Content at Finance Magnates and global economy editor at Calcalist. Michael is also the host of the "Free and Decentralized" podcast and is launching a new podcast called "Web3 Watchdogs." He is a lawyer and holds a Master's degree in International Relations and a Bachelor of Law from the University of Haifa.

Cryptopolitan

BTC | ETH | NORTH KOREA | UKRAINE

2024 sees nearly $1.4 billion in crypto thefts so far

Web3 security company Cyvers has reported that $1.38 billion has been stolen in crypto so far in 2024. This is way higher than last year's, which was only $657 million.

Get started with Cyvers today!

Book a Demo