Gate Research

From Hacking Attacks
to Regulatory Reflection:

Analysis of Cryptocurrency Security Status in 2024

Abstract

- From 2012 to November 2024, the blockchain ecosystem experienced 1,740 publicly reported security incidents, resulting in approximately $33.744 billion in losses;
- In 2024, the blockchain industry saw a surge in security incidents, with 369 cases causing around $2.308 billion in losses, with hacking being the primary threat;
- In 2024, private key leaks accounted for losses as high as $1.199 billion, representing 62.3% of all hacking-related losses, underscoring the critical importance of private key security within the industry;
- During the first three quarters of 2024, contract vulnerability attacks were the most frequent, with business logic flaws, reentrancy bugs, and access control vulnerabilities causing the most severe damages;
- Centralized exchanges (CEX) suffered the most significant losses, while DeFi remained the most vulnerable area to attacks;
- Ethereum, due to its mature ecosystem and large financial scale, became the primary target for hackers. Emerging ecosystems such as BSC and Arbitrum, with their rapid growth, also became new targets for attacks;
- Of the stolen funds in 2024, approximately 25.3% were frozen or recovered, but 58.7% remained in hacker addresses;
- Regulatory authorities in various countries are actively addressing money laundering and fraud in the cryptocurrency sector through measures such as enhanced KYC and stablecoin regulation to protect investors' interests.

Keywords:

Gate Research, Security Incidents, Hacking, Anti-Money Laundering

From Hacking Attacks to Regulatory Reflection:

Analysis of Cryptocurrency Security Status in 2024

1 Introduction

As Bitcoin reached a historic high of $90,000, meme coins also captured significant market attention. Coins like GOAT, PUNT, and BAN generated substantial wealth, fueling market enthusiasm. However, while investors dreamed of overnight riches, a sudden hacking incident shattered the market celebration. The decentralized exchange DEXX fell victim to an attack, leading to massive theft of user assets and causing several related meme coins to plummet in value. This incident highlighted the critical importance of security in the cryptocurrency market.

The DEXX incident exposed numerous security issues in decentralized exchanges, serving as a stark reminder that while enjoying the convenience of cryptocurrencies, we must emphasize security greatly. In fact, as the cryptocurrency market develops rapidly, security issues are becoming increasingly prominent. Hackers exploit various methods, such as system vulnerabilities, phishing attacks, and smart contract loopholes, to launch attacks on crypto assets, causing users to suffer significant losses.

This research paper provides an in-depth analysis of the state and trends in cryptocurrency security in 2024. We will review major security incidents of the year, analyze attackers' common methods, targets, and the resulting damages. Additionally, we will examine historical cases to distill valuable lessons. Furthermore, this article will explore the challenges and opportunities that the cryptocurrency security field may face in the future, discussing how regulators and industry participants can work together to address these challenges and build a more secure and reliable cryptocurrency ecosystem.

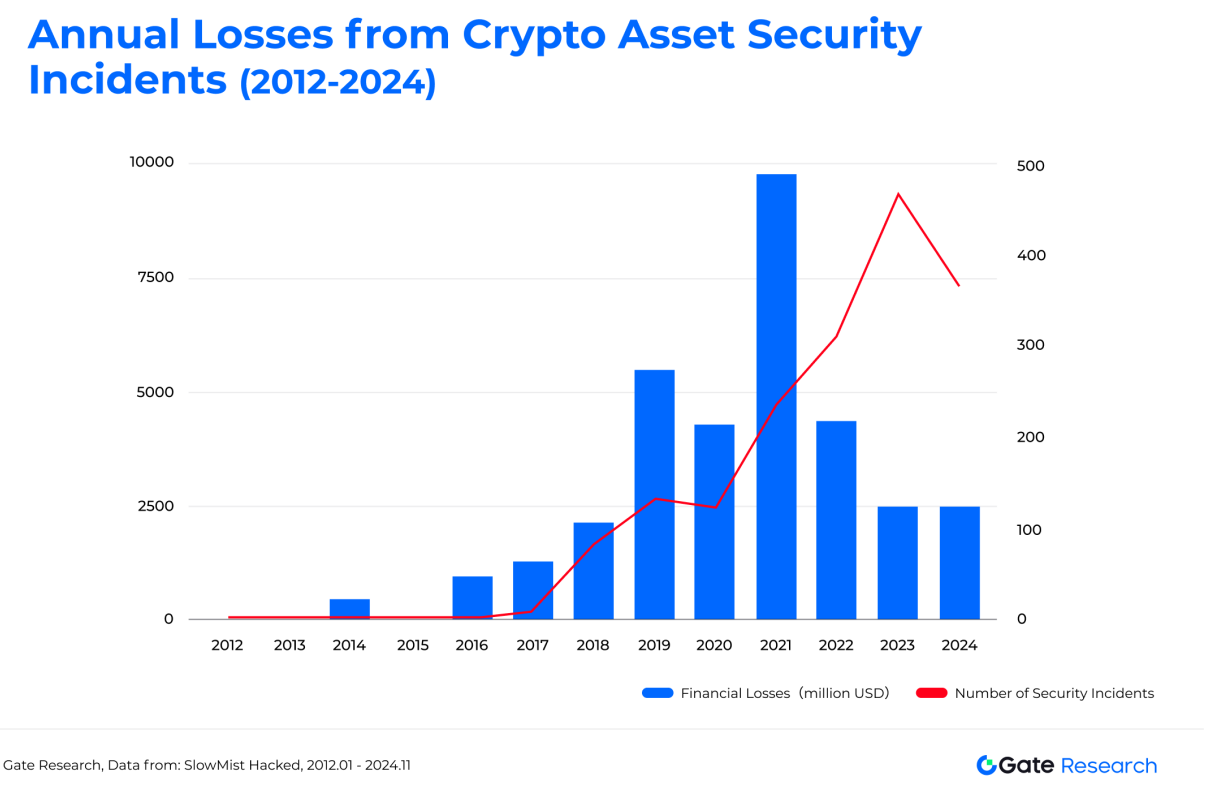
2 Overview of Historical Crypto Security Incidents

According to incomplete statistics from SlowMist Hacked, from 2012 to November 2024, 1,740 publicly disclosed crypto security incidents within the blockchain ecosystem have resulted in total losses of approximately $33.744 billion. Overall, the number of crypto security incidents and the corresponding financial losses have shown a year-on-year upward trend, peaking notably in 2021 and 2022.

Crypto security incidents increased steadily from 32 cases in 2012, peaking in 2021 before a slight decline. By 2024, there were still 369 incidents. As the cryptocurrency market grew and asset values increased, attacks on the blockchain ecosystem became more frequent. Financial losses followed a similar pattern, rising dramatically from $5.97 million in 2012 to$43.98 billion

in 2022. The number of attacks increased, and their financial impact grew more severe. The crypto market's rapid expansion attracted legitimate participants—and turned it into a lucrative target for hackers. This was particularly evident during the bull markets of 2021 and 2022, when soaring crypto prices drew in both investors and malicious actors. By 2023, however, both security incidents and financial losses decreased compared to 2022, likely due to market cooling and improved security awareness across the industry.

Figure 1: Annual Losses from Crypto Asset Security Incidents (2012-2024)



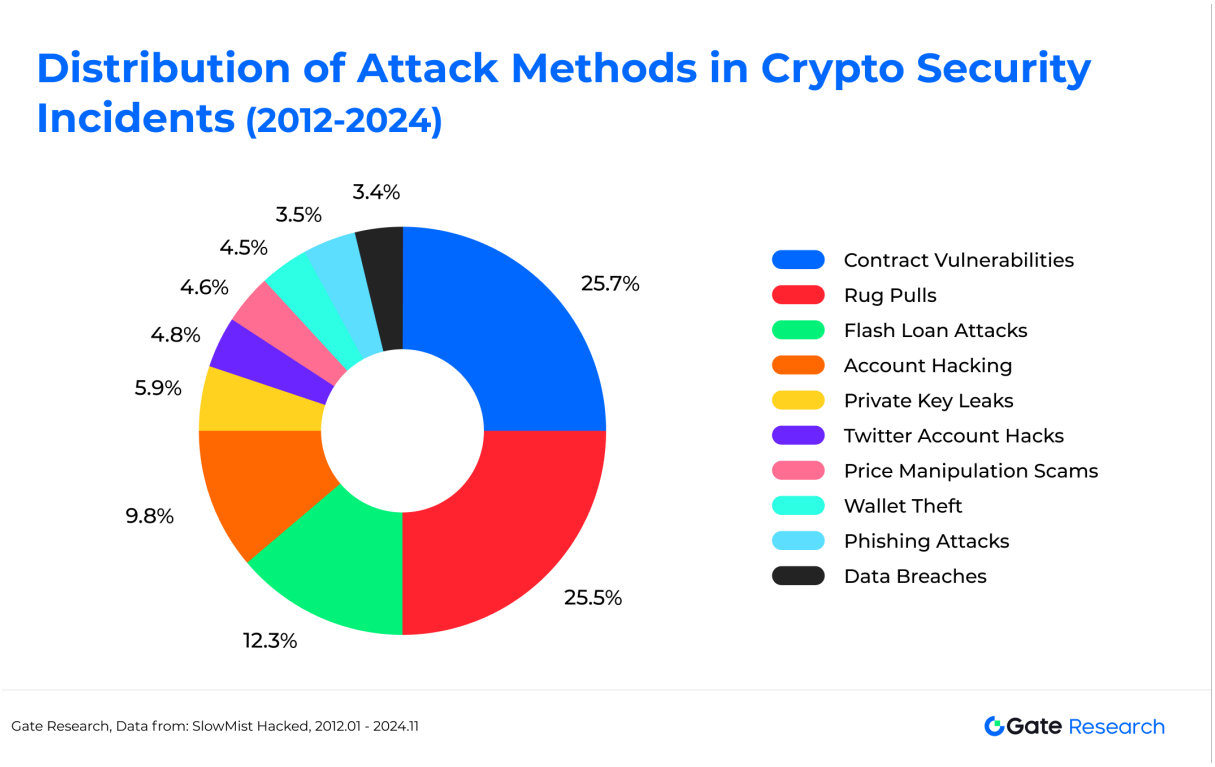
Historical crypto security incidents have involved ten main types of attacks: contract vulnerabilities, rug pulls, flash loan attacks, account hacking, private key leaks, Twitter account hacks, price manipulation scams, wallet theft, data breaches, and phishing attacks. In recent years, three attack types have dominated, accounting for over 50% of all incidents: contract vulnerabilities (25.7%), rug pulls (25.5%), and flash loan attacks (12.3%). This pattern highlights three key risk areas in the crypto space: smart contract security, project team trustworthiness, and DeFi protocol design.

- Rug Pull is a common cryptocurrency scam. Fraudsters create an appealing crypto project to lure investors with false promises of success. After accumulating substantial funds, the project creators disappear with the money, leaving investors with worthless tokens or an abandoned project that causes severe financial losses.
    - Thodex, a Turkey-based cryptocurrency exchange, abruptly shut down in April 2021. Its founder, Faruk Fatih Özer, fled with billions of dollars, leaving approximately 391,000 users with losses exceeding $2 billion. This became one of the most severe rug pull incidents in cryptocurrency history.

- Smart Contract Vulnerabilities refer to security flaws in the code of smart contracts, which hackers can exploit to launch attacks, leading to losses of user assets.
    - In June 2016, a hacker exploited a reentrancy vulnerability in The DAO's smart contract. By repeatedly invoking the contract's withdrawal function, the attacker executed a reentrancy attack and successfully stole about 3.6 million ETH, valued at approximately $50 million at the time.

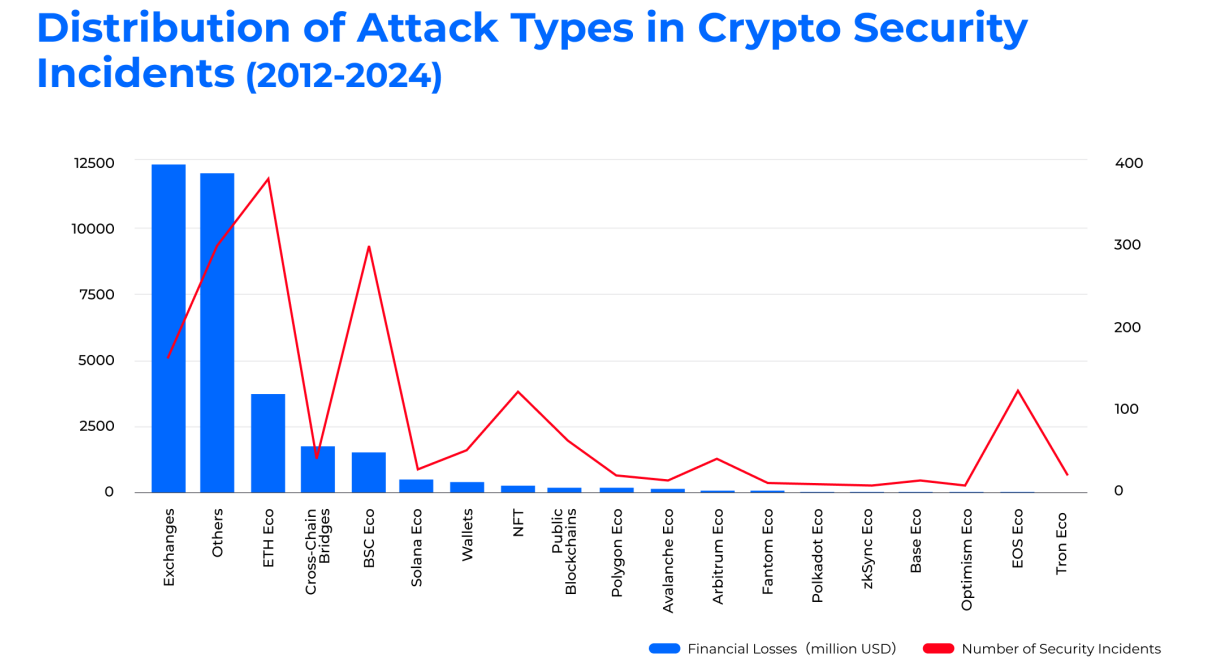
- Flash Loan Attacks exploit the instant borrowing feature of DeFi platforms/protocols. Attackers borrow a large sum within a single transaction, manipulate market prices, or exploit price discrepancies to engage in arbitrage, reaping illicit gains.
    - On March 13, 2023, the DeFi lending protocol Euler Finance suffered a flash loan attack. The attacker borrowed a massive flash loan and executed high-leverage operations, triggering the protocol's liquidation mechanism and ultimately stealing approximately $197 million.

Figure 2: Distribution of Attack Methods in Crypto Security Incidents (2012-2024)



Regarding financial losses from attacks, exchanges remain the hackers' primary targets. Exchange-related losses have reached $12.374 billion, significantly higher than other sectors. This vulnerability stems from exchanges' role as centralized repositories of user assets, making successful breaches extremely lucrative. The ETH ecosystem and cross-chain bridges have also become attractive targets with their complex interconnections and high transaction volumes. The ETH ecosystem in particular, given its maturity and diverse range of projects, has experienced 379 security incidents, the highest number of any platform.

Figure 3: Distribution of Attack Types in Crypto Security Incidents (2012-2024)



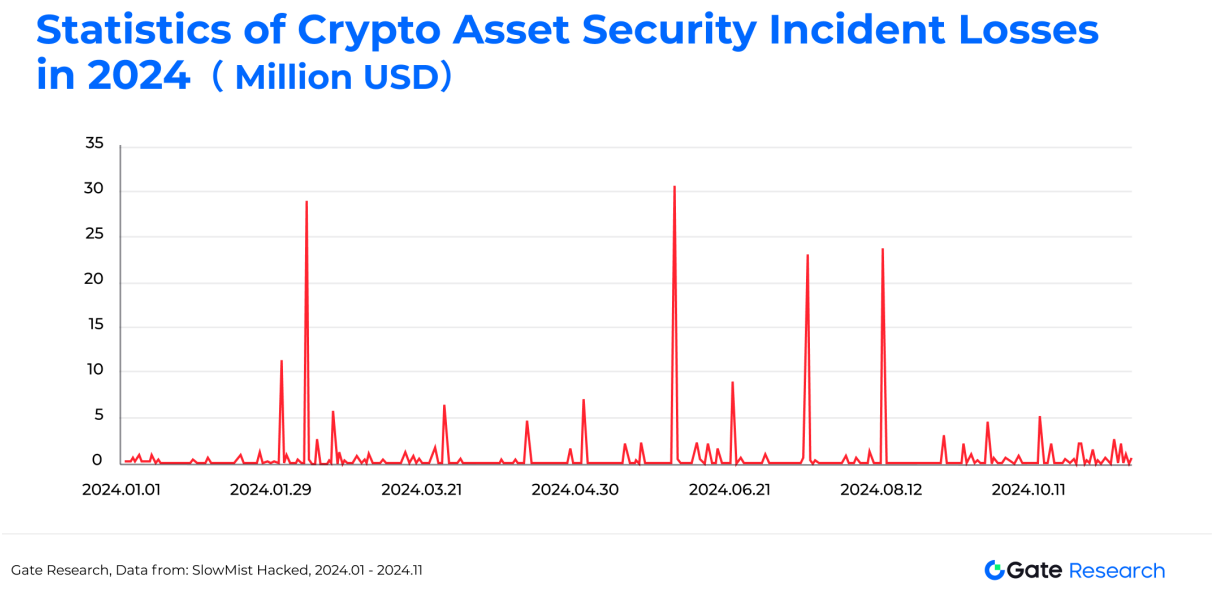
Gate Research, Data from: SlowMist Hacked, 2012.01 - 2024.1

Gate Research

3 2024 Overview of Crypto Security Incidents

According to incomplete statistics from SlowMist Hacked, the blockchain ecosystem reported 369 publicly disclosed crypto security incidents in 2024, resulting in total losses of approximately $2.308 billion. These figures highlight the pressing nature of crypto asset security issues, with frequent security incidents imposing significant economic damage on the industry.

Figure 4: Statistics of Crypto Asset Security Incident Losses in 2024

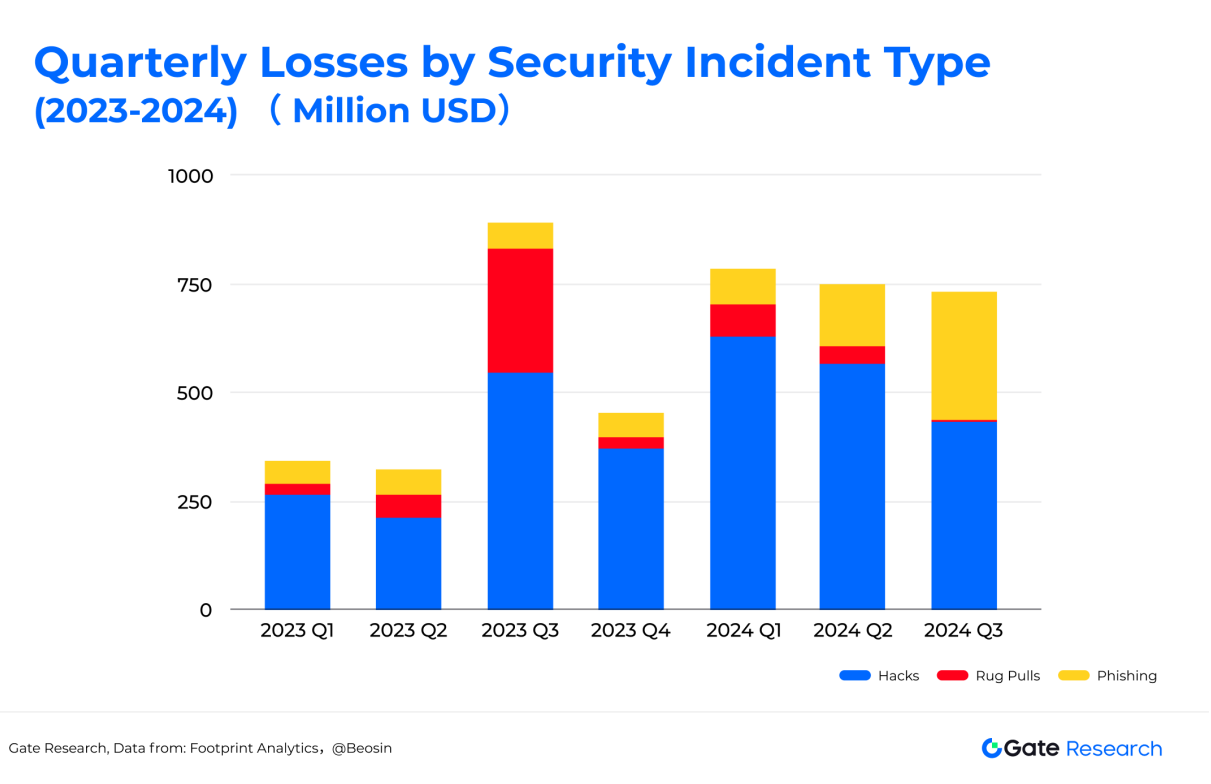


3.1 Analysis of Security Incident Types

The attack methods from previous years—such as contract vulnerabilities, flash loan attacks, account hacks, private key leaks, social media hacks, wallet theft, and data breaches—are collectively categorized as Hacks. Phishing scams and price manipulation frauds are grouped under Phishing. Thus, historical attack methods can be broadly divided into three categories: Hacks, Rug Pulls, and Phishing scams.

Beosin Alert data shows that Web3 security incidents were frequent in the first three quarters of 2024, with total losses reaching $2.276 billion—a 45% increase from the previous year. Hacking attacks inflicted the most damage at $1.624 billion, up 59.18% year-over-year, with increasingly sophisticated techniques threatening Web3 ecosystem security. Phishing scams saw a dramatic 191.26% year-over-year increase to $528 million, particularly in early 2024, as hackers refined their methods of exploiting user psychology through deceptive websites and misleading information to obtain private keys and initiate unauthorized transfers. However, Rug Pull losses decreased significantly to $122 million, down 66.54% year-over-year, likely due to heightened community awareness and stronger regulatory oversight.

Figure 5: Quarterly Losses by Security Incident Type (2023-2024)

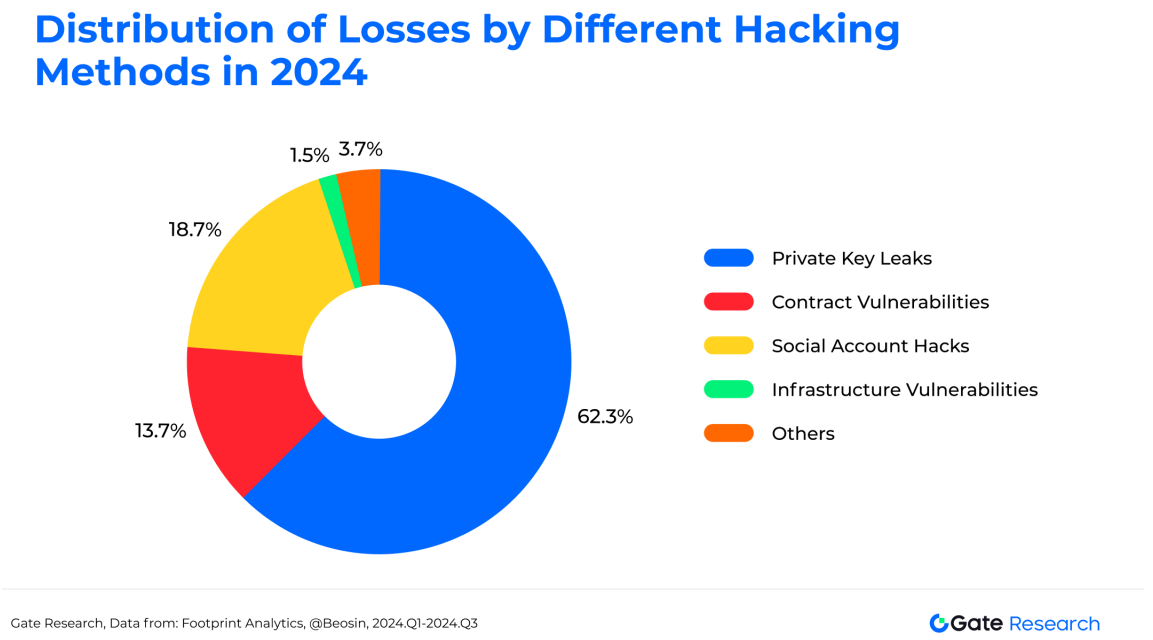


3.2 Analysis of Hacking Techniques

In the first three quarters of 2024, private key leaks accounted for the highest financial losses at $1.199 billion, representing 62.3% of all hacking-related losses. This was followed by losses from social account hacks, with contract vulnerabilities ranking third, contributing 13.7% of total losses.

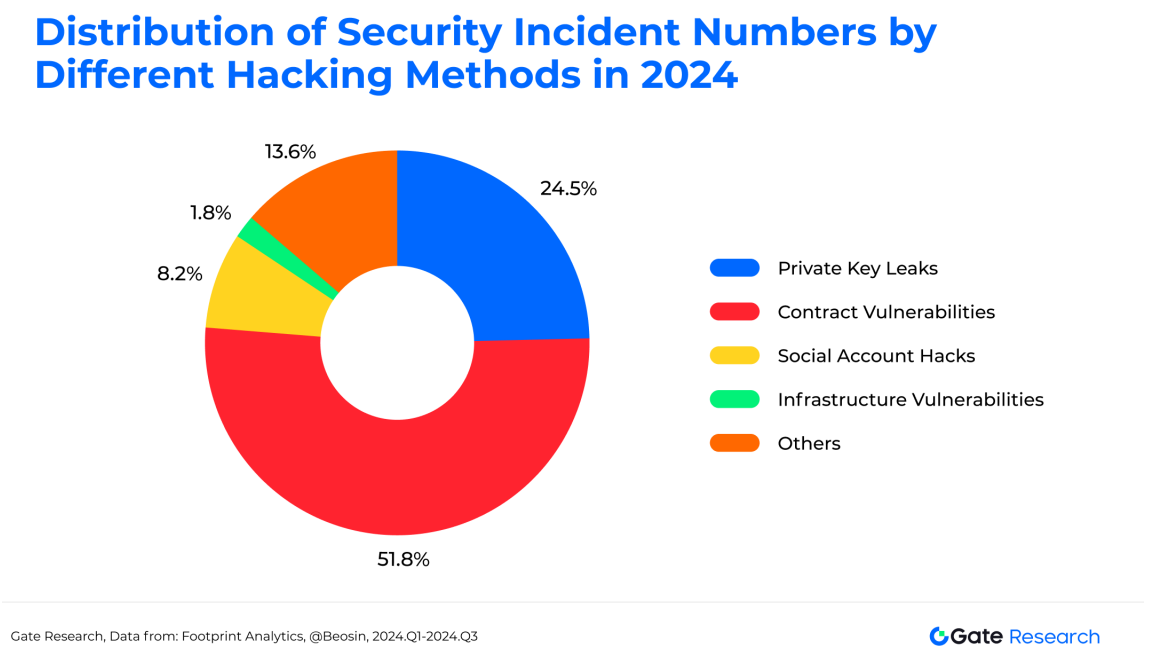
In 2024, multiple platforms and individuals suffered major losses due to private key leaks, including DMM Bitcoin ($308 million), PlayDapp ($290 million), WazirX ($230 million), Ripple co-founder Chris Larsen ($112 million), BtcTurk ($55 million), BingX ($45 million), and Indodax ($22 million). These incidents demonstrate that private key security remains one of the biggest challenges in the cryptocurrency industry.

Figure 6: Distribution of Losses by Different Hacking Methods in 2024



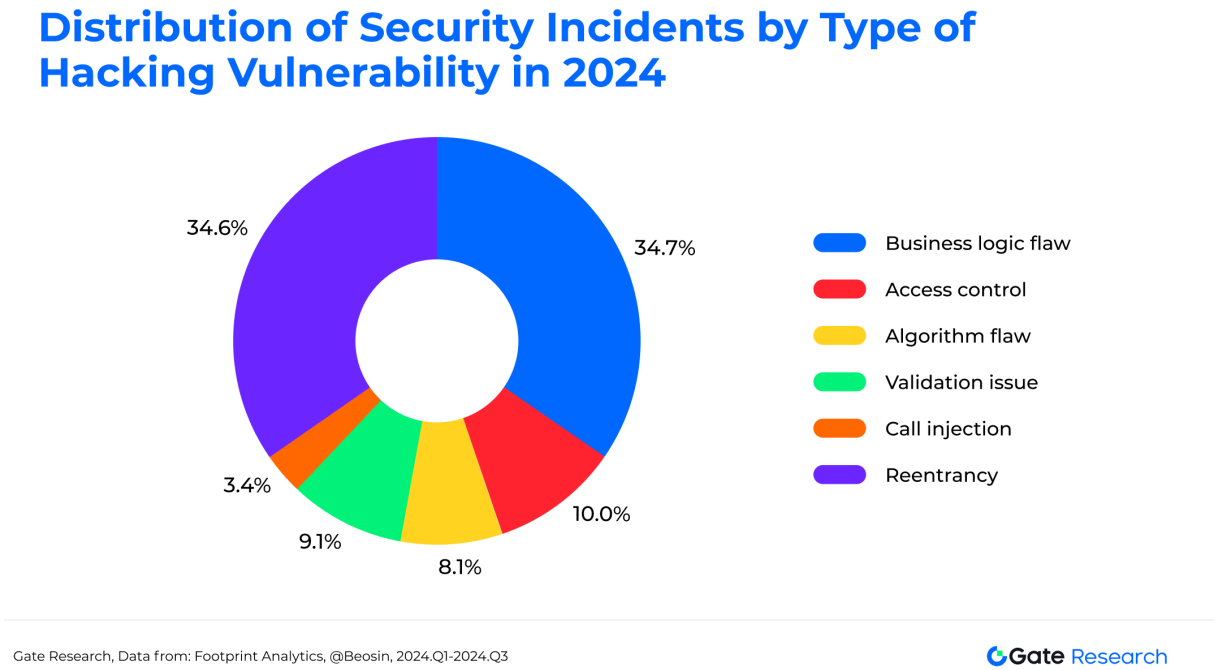
Contract vulnerability attacks dominated security incidents in the first three quarters of 2024, making up 51.8% of all cases. Hackers targeted weaknesses in smart contract code to execute various attacks and steal user assets. While the financial losses from these vulnerabilities (13.7%) were lower than those from private key leaks, their high occurrence rate poses a significant concern. Projects with poorly designed contracts proved particularly vulnerable to these attacks.

Figure 7: Distribution of Security Incident Numbers by Different Hacking Methods in 2024



From the perspective of vulnerability types, the top three vulnerabilities causing the most significant losses in the first three quarters of 2024 were: business logic flaws (34.7%), reentrancy vulnerabilities (34.6%), and access control vulnerabilities (10%). Business logic flaws were also the most frequently occurring type of vulnerability, followed by validation issues.

Figure 8: Distribution of Security Incident by Type of Hacking Vulnerability in 2024



Gate Research, Data from: Footprint Analytics, @Beosin, 2024.Q1-2024.Q3

Gate Research

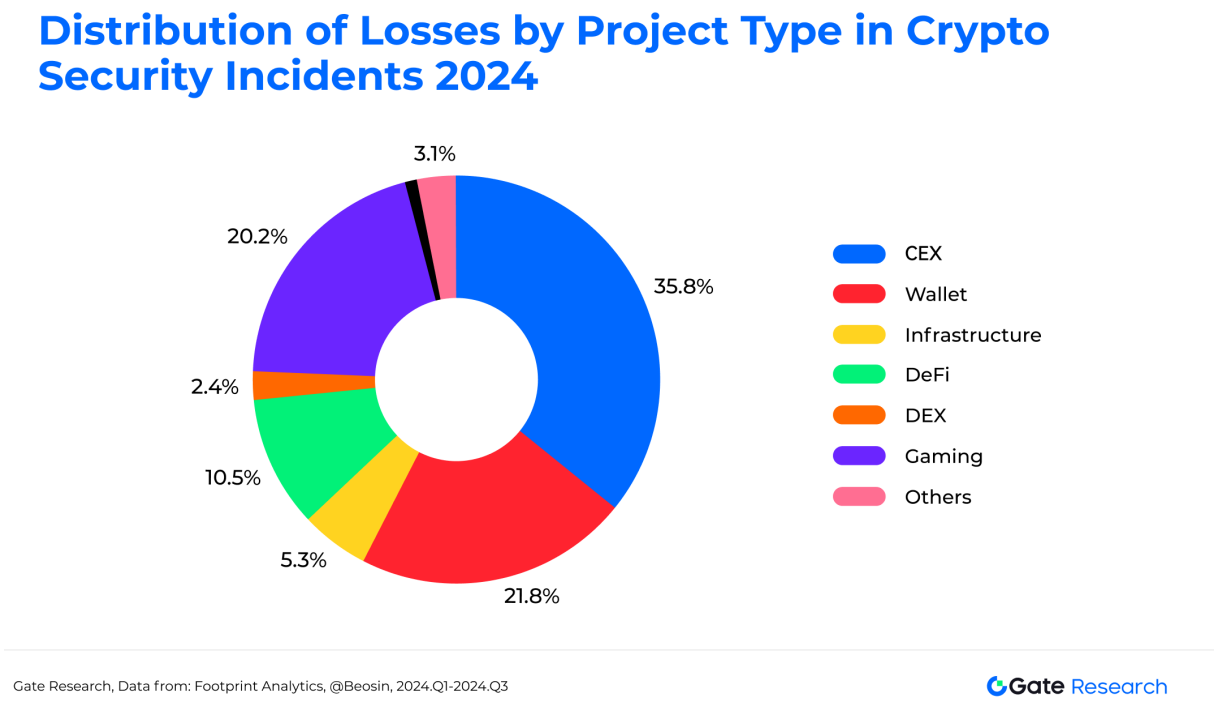
3.3 Analysis of Targeted Projects

From the perspective of project categories, centralized exchanges (CEX) suffered the most significant losses in the first three quarters of 2024, accounting for 35.8% of total losses, amounting to $688 million. Among these, the DMM Bitcoin incident was the most severe, with losses totaling $308 million. This incident ranks as the seventh-largest crypto hacking loss in history and the most significant security event of 2024. It also marked Japan's third-largest cryptocurrency exchange theft after the Mt.Gox incident in 2014 and the Coincheck incident in 2018. Due to the centralized nature of CEXs, which store many user assets, they are prime targets for hackers. While the frequency of security incidents involving CEXs is relatively low, the losses per incident tend to be substantial, posing significant threats to the security of the entire exchange ecosystem.

Additionally, wallets and gaming projects also incurred significant losses, accounting for 21.8% and 20.2% of total losses, respectively. Wallets, being the primary choice for users to store cryp-

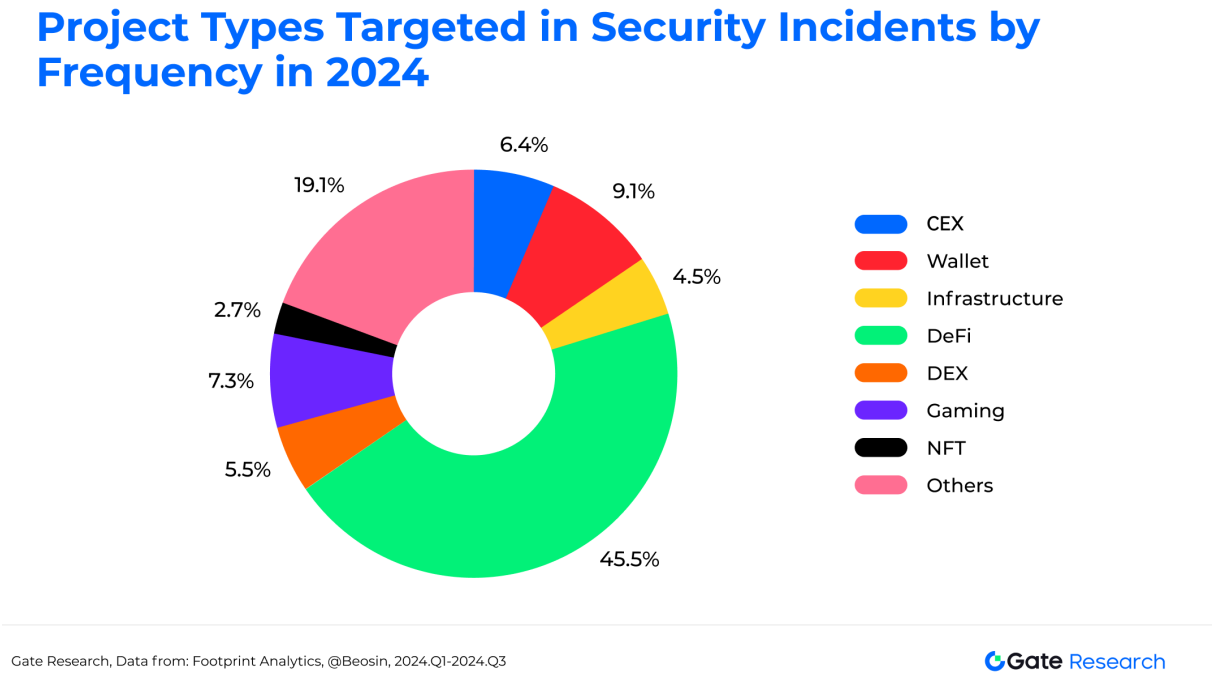
to assets, are particularly devastating when breached. Gaming projects, due to their large user base and extensive virtual asset transactions, have become high-risk targets for hackers. For example, on May 20, Gala Games was attacked when the attacker minted a large number of tokens and quickly exchanged them for other mainstream cryptocurrencies, causing significant losses to the platform.

Figure 9: Distribution of Losses by Project Type in Crypto Security Incidents 2024



In terms of the number of attacks, DeFi is the most frequently targeted sector. According to Beosin Alert data, in the first three quarters of 2024, attacks on DeFi projects accounted for 45.5% of all incidents, making DeFi a primary focus for hackers. The high frequency of attacks is primarily due to the complexity of DeFi protocols, high concentration of funds, and frequent security vulnerabilities. In contrast, centralized exchanges (CEX) and wallet projects, while also targeted, experience relatively fewer attacks thanks to the implementation of multiple security measures. However, while DeFi projects face the highest attack frequency, the direct financial losses per incident are generally smaller than CEX. This is because CEX platforms store a large volume of user assets, making any breach potentially far more devastating.

Figure 10: Project Types Targeted in Security Incidents by Frequency in 2024



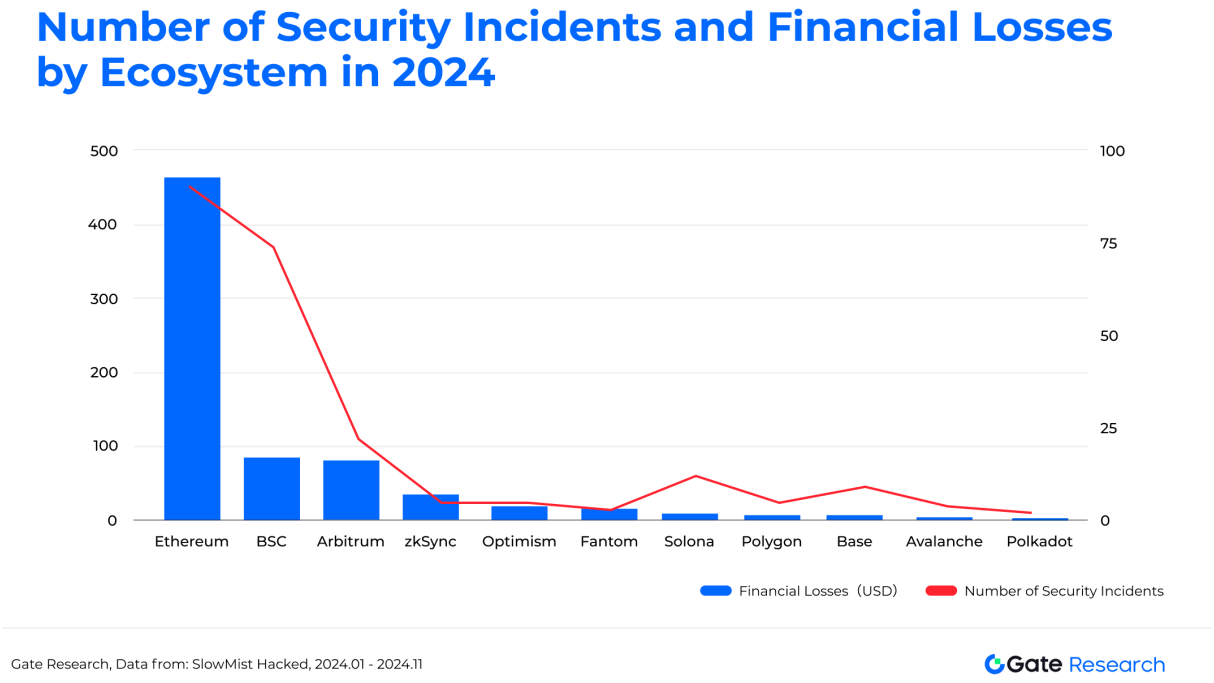
3.4 Analysis of Targeted Ecosystems

In 2024, Ethereum remained the blockchain ecosystem with the highest financial losses, totaling $460 million. It was followed by BSC (Binance Smart Chain) with losses of approximately $86.08 million, and Arbitrum with losses of about $83.23 million. Ethereum's status as the largest smart contract platform, with its extensive ecosystem and significant locked funds, makes it the primary target for hackers. Similarly, BSC, as a competitor to Ethereum, also faced many attacks, with losses second only to Ethereum.

Notably, the Solana ecosystem, which experienced rapid growth in 2024, also attracted significant attention from hackers. For example, on May 16, the Solana-based token launch platform pump.fun suffered a flash loan attack, resulting in losses of up to $80 million. This incident highlights the considerable security challenges that remain within the Solana ecosystem.

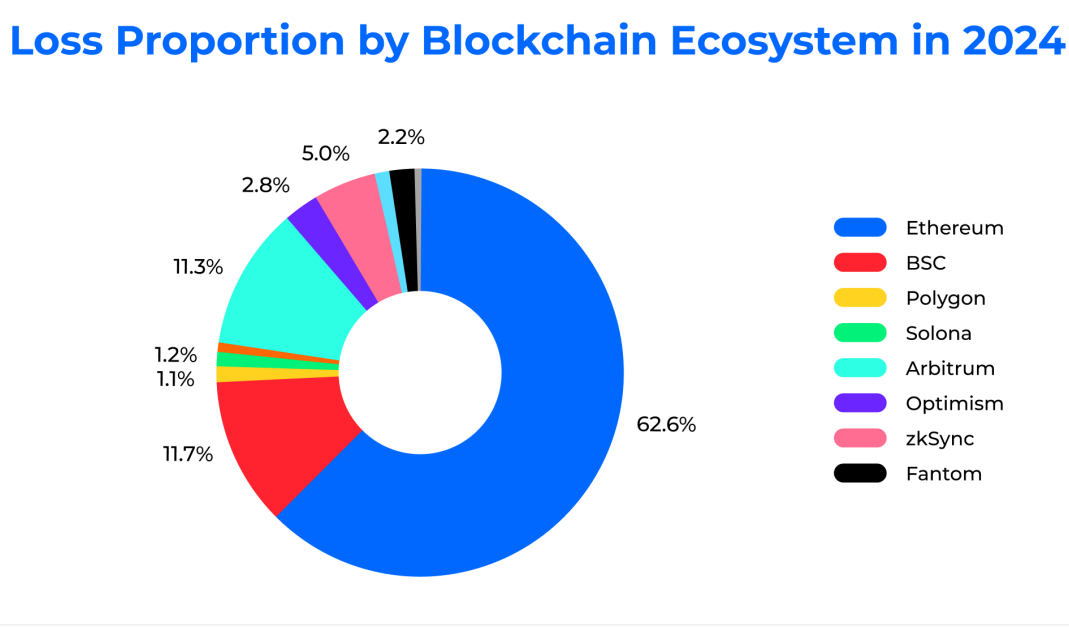
In addition, the rise of Layer 2 solutions, such as Arbitrum and Optimism, has drawn increased focus on their security. While these ecosystems have implemented several technical optimizations, they have not been immune to hacker attacks.

Figure 11: Number of Security Incidents and Financial Losses by Ecosystem in 2024



Additionally, comparing the loss proportions and the number of incidents across ecosystems in 2024 reveals that Ethereum accounted for 62.6% of total financial losses, far exceeding other ecosystems. While it experienced only 39% of total security incidents, the losses per attack were significantly higher. This discrepancy reflects Ethereum's position as the largest smart contract platform, with a rich DeFi ecosystem and substantial locked funds, making any breach particularly devastating. In contrast, BSC saw 32% of total security incidents, comparable to Ethereum, but its loss proportion was only 11.7%, indicating that while incidents were frequent, the financial impact per attack was relatively smaller.

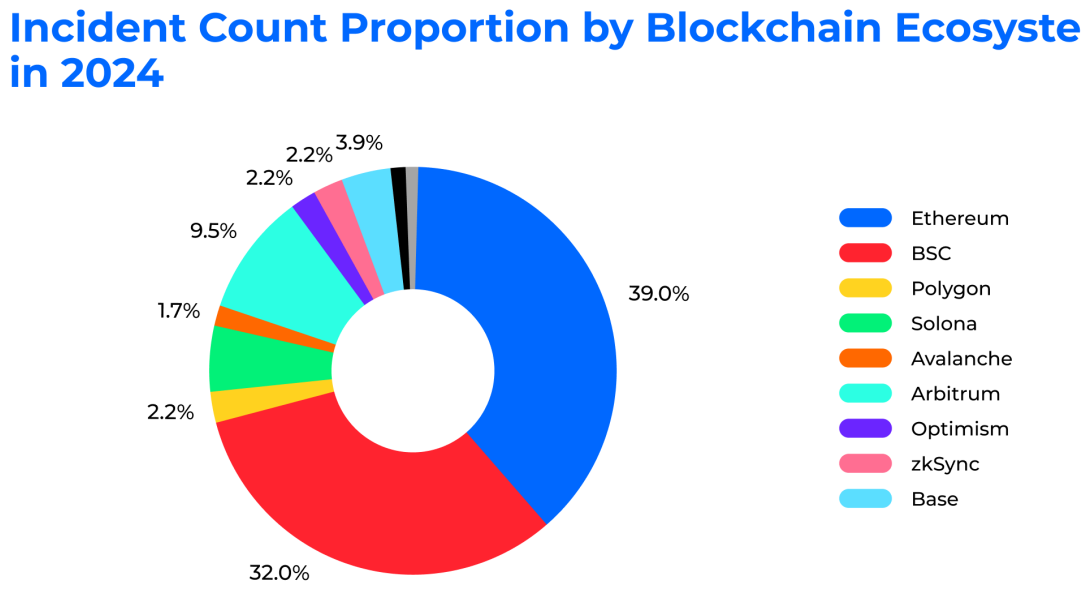
Figure 12: Loss Proportion by Blockchain Ecosystem in 2024



Gate Research, Data from: SlowMist Hacked, 2024.01 - 2024.11

Gate Research

Figure 13: Incident Count Proportion by Blockchain Ecosystem in 2024



Gate Research, Data from: SlowMist Hacked, 2024.01 - 2024.11

Gate Research

3.5 Review of 2024 Attach Incidents

In 2024, the cryptocurrency industry faced a severe security landscape, with frequent hacking incidents causing substantial economic losses. Below is a summary of some major security incidents from the first three quarters of 2024, highlighting various attack methods and significant financial losses:

Figure 14: Typical Security Attack Incidents in 2024

Typical Security Attack Incidents in 2024

Incident	Loss Amount	Attack Method	Description
DMM Bitcoin	$308M	Private Key Leak	May 31st: Japanese crypto exchange DMM Bitcoin was attacked, with hackers stealing approximately $308M in Bitcoin. The stolen funds were distributed across more than 10 addresses.
PlayDapp	$290M	Private Key Leak	Feb 9th: Blockchain gaming platform PlayDapp was hacked, with attackers minting 200M PLA tokens worth $36.5M. On Feb 12th, after failed negotiations, hackers minted another 1.59B PLA tokens worth $253.9M.
WazirX	$230M	Wallet Theft	Crypto exchange WazirX released preliminary investigation results, reporting that one of their multi-signature wallets was compromised, resulting in losses exceeding $230M.
BtcTurk	$55M	Private Key Leak	Turkish crypto exchange BtcTurk acknowledged a hack affecting ten hot wallets containing various cryptocurrencies. The exchange suspended deposits and withdrawals while cooperating with law enforcement.
Hedgey	$44.7M	Flash Loan Attack	Hedgey Finance suffered two attacks on both Ethereum and Arbitrum networks, leading to total losses of $44.7M.
FixedFloat	$26.1M	Third-party Vulnerability	Crypto exchange FixedFloat confirmed a hack resulting in stolen funds, working to improve security and investigate.
Gala Games	$21.8M	Private Key Leak	May 20th, 2024: Web3 gaming platform Gala Games was attacked, with perpetrators minting and quickly selling large amounts of GALA tokens.
Thala	$25.5M	Security Vulnerability	Aptos ecosystem DeFi project Thala lost assets due to a security vulnerability, implemented measures to pause contracts and negotiate asset recovery.
DEXX	$21M	Unknown	On-chain trading terminal DEXX users lost funds totaling $21M.
BingX	$45M	Unknown	BingX's security system detected unauthorized access to a hot wallet.
U.S. Government-Controlled Wallet	~$20M	Unknown	A U.S. government-controlled wallet reportedly transferred tokens worth nearly $20M, with some funds later returned to government addresses.

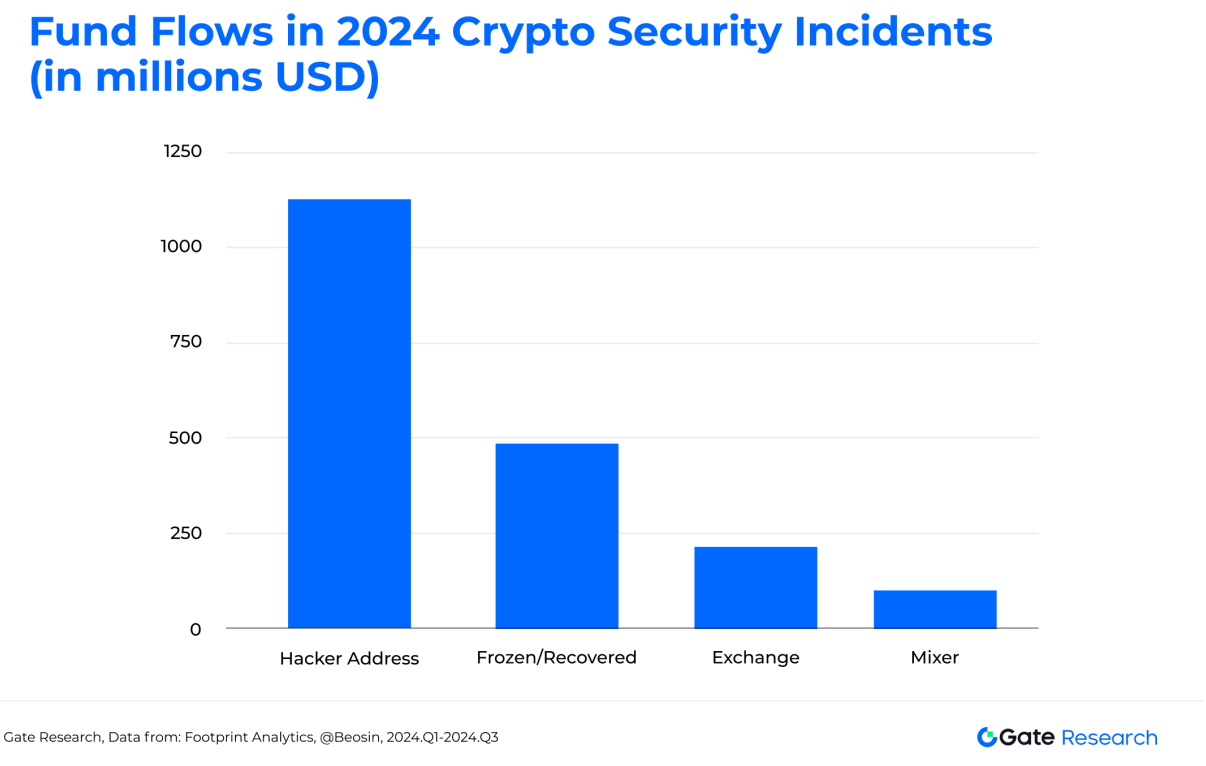
Gate Research, Data from: SlowMist Hacked

4 Fund Flows in 2024 Crypto Security Incidents

4.1 Analysis of Stolen Funds Flow

According to Beosin KYT data, in 2024, approximately 25.3% ($486 million) of stolen funds were frozen or recovered, a significant improvement from 2023. About 58.7% ($1.129 billion) remained in hacker addresses. With increased global anti-money laundering efforts, it has become more challenging for hackers to launder stolen funds. As a result, hackers often initially transfer funds to on-chain addresses to facilitate further operations. Approximately 10.9% ($209 million) of stolen funds were sent to exchanges, a higher proportion compared to 2023, while only 5.1% ($98 million) were laundered through mixers, reflecting a significant decrease in mixer usage for laundering stolen funds.

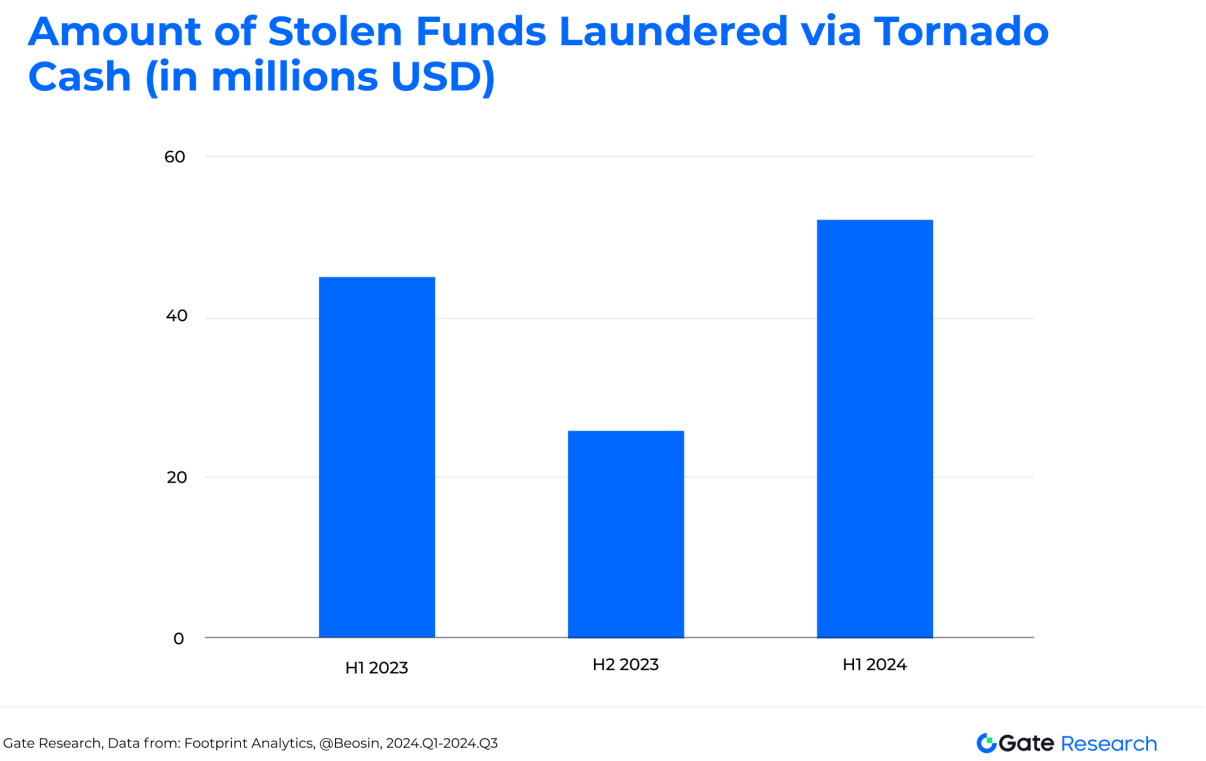
Figure 15: Fund Flows in 2024 Crypto Security Incidents (in millions USD)



The data reveals four primary destinations for stolen funds: frozen/recovered, retained in hacker addresses, sent to exchanges, or laundered through mixers. Among mixers, Tornado Cash remains one of the most frequently used tools. It allows users to mix transactions to enhance privacy but is also exploited for illicit activities like money laundering. Beosin KYT data shows a notable increase in laundering through Tornado Cash in the first half of 2024 compared to 2023,

with a 15.42% growth compared to the first half of 2023 and a 103.42% growth in the second half. This indicates hackers' growing reliance on Tornado Cash to obscure the origins of funds.

Figure 16: Amount of Stolen Funds Laundered via Tornado Cash (in millions USD)



As criminals increasingly use mixers like Tornado Cash for laundering, regulatory scrutiny of cryptocurrency mixing services has intensified. The U.S. Treasury's sanctions on Tornado Cash in August 2022 marked a significant step in addressing the balance between cryptocurrency privacy and anti-money laundering (AML). This action brought compliance and risk management to the forefront of the industry. Governments worldwide are strengthening regulations on cryptocurrency mixing services to prevent money laundering and terrorism financing activities.

4.2 Money Laundering Methods for Stolen Funds

Recently, the methods for laundering stolen cryptocurrency have become increasingly sophisticated. Hackers have innovated various techniques, including multi-layered transfers, mixing services, decentralized exchange (DEX) trading, and using privacy-focused coins to obscure the source of funds. One of the most active groups in these activities is North Korea's Lazarus Group, which has repeatedly targeted financial institutions and cryptocurrency exchanges, causing significant losses. Examples include the Axie Infinity Ronin Bridge attack and the DMM

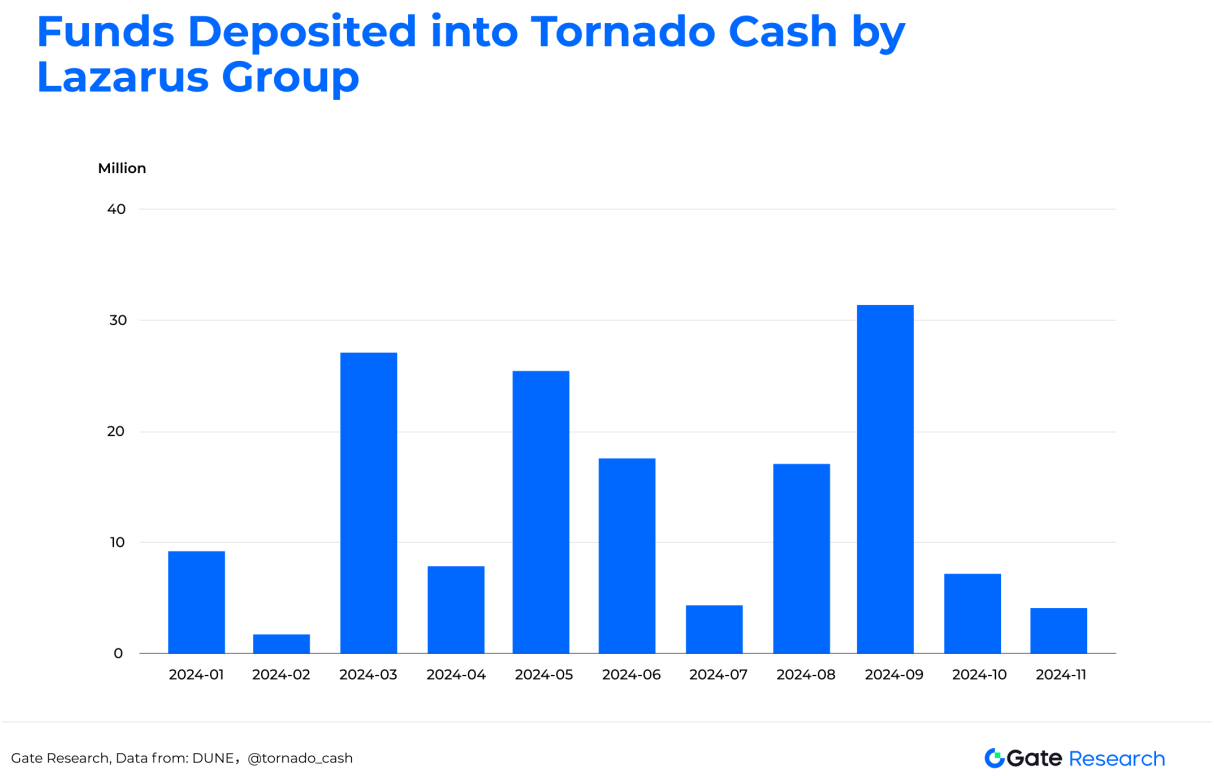
Bitcoin breach, which rank among the largest hacks in cryptocurrency history.

Lazarus Group has developed a sophisticated and mature money laundering system over the years, typically following these steps:

1. Initial Obfuscation: Deposit stolen cryptocurrency into mixers like Tornado Cash to sever the transaction chain and achieve preliminary anonymity.
2. Cross-Chain Transfers: Use cross-chain protocols like Thorchain to convert funds into different cryptocurrencies, making tracking more difficult.
3. Funds Obfuscation: Perform multiple transactions across various addresses. For example, funds may be transferred to the Bitcoin network via tBTC protocol before being moved back to Ethereum, adding further complexity.
4. Dispersed Storage: Distribute funds across multiple addresses and transfer them to less-regulated blockchains like TRON.
5. Over-the-Counter (OTC) Trading: Convert cryptocurrency to fiat or other cryptocurrencies using OTC platforms like Paxful or Noones to bypass KYC scrutiny.

Industry analysis indicates a strong correlation between Lazarus Group's activities and Tornado Cash usage, underscoring Tornado Cash's critical role in laundering operations. Data shows a fluctuating but rising trend in ETH deposits into Tornado Cash by Lazarus Group, reflecting sustained laundering activity. Despite increasing regulatory oversight, the group's use of innovative laundering techniques—such as multi-layered transfers and cross-chain movements—continues complicating enforcement efforts. Regions must adapt to these evolving strategies to combat cryptocurrency-related crimes effectively, enhance international cooperation, and strengthen oversight mechanisms.

Figure 17: Funds Deposited into Tornado Cash by Lazarus Group



4.3 Tracking Stolen Funds from 2024 Crypto Security Incidents

4.3.1 DMM Bitcoin Hack: Suspected Lazarus Group Involvement

4.3.1.1 Background

In May 2024, DMM Bitcoin, a prominent Japanese cryptocurrency exchange, suffered a severe cyberattack, resulting in the theft of a significant amount of Bitcoin. The attack caused massive financial losses, prompting DMM Bitcoin to cease operations. On December 2, the company announced the transfer of all user accounts and company assets to SBI VC Trade, a subsidiary of SBI Group. This asset transfer is expected to be completed by March 2025.

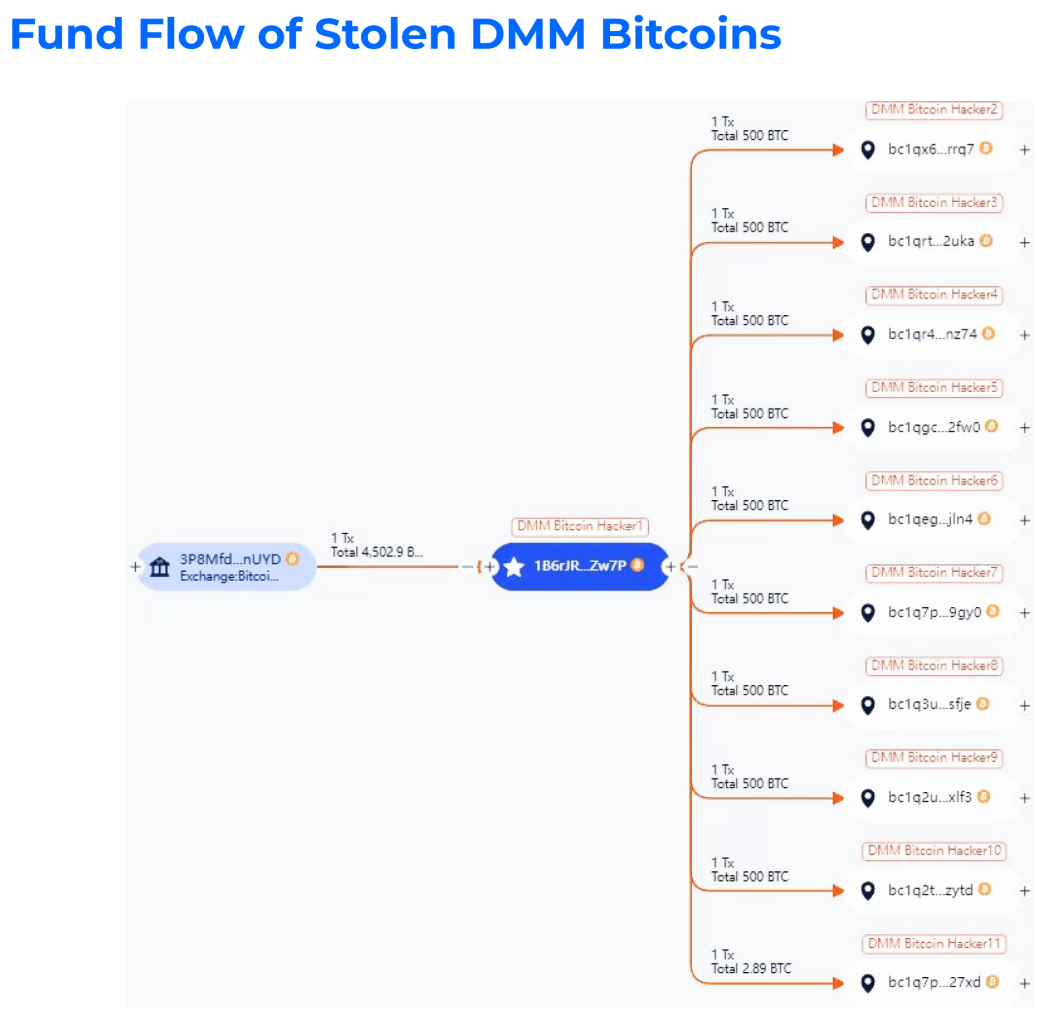
On May 31, 2024, hackers infiltrated the DMM Bitcoin platform and stole 4,502.9 BTC, valued at approximately $308 million. By December 2, the value of these stolen Bitcoins had increased to over $429 million. Following the incident, DMM Bitcoin imposed restrictions on withdrawals and cryptocurrency purchases to mitigate losses. However, these measures were insufficient to prevent further financial damage and negatively impacted user services.

4.3.1.2 Fund Pathway

Blockchain security experts discovered that the stolen Bitcoin was quickly dispersed across multiple wallets and laundered through suspicious platforms like Huione Guarantee. The attack methods and laundering patterns strongly suggest the involvement of the North Korea-backed hacker group Lazarus Group.

Beosin Trace tracked the stolen 4,502.9 BTC to 10 newly created addresses. Blockchain investigator ZachXBT revealed that Lazarus Group had laundered over $35 million of the stolen DMM Bitcoin funds via Huione Guarantee, operating in Cambodia.

Figure 18: Fund Flow of Stolen DMM Bitcoins



Gate Research, Data from: BEOSIN

4.3.1.3 Regulatory Challenges

The incident raised significant concerns about the security of cryptocurrency exchanges. The closure of DMM Bitcoin highlighted the severe security challenges faced by exchanges and attracted close scrutiny from regulatory authorities. An investigation by Japan's Financial Services Agency (FSA) revealed severe deficiencies in the company's risk management practices, including a lack of independent audits, centralized security functions, and non-compliance with cryptocurrency trading regulations.

The investigation found that DMM Bitcoin failed to establish a robust risk management framework. Internal audits were largely ineffective, leaving the company unable to safeguard against the theft of crypto assets. Risk management responsibilities were concentrated in the hands of a few individuals, and critical logs needed for investigating the theft were not retained, violating relevant regulations. The FSA issued a "business improvement order" to the company, emphasizing significant shortcomings in its system risk management and response to crypto asset leaks.

This incident ranks as one of the most significant cryptocurrency thefts of 2024 and the second-largest illegal outflow of crypto assets in Japan's history. It underscores the escalating cybersecurity threats in the digital asset space and has sparked widespread calls for increased regulation of cryptocurrency exchanges. The DMM Bitcoin hack serves as a stark reminder of the immense security risks exchanges face. To safeguard user assets, exchanges must continually strengthen security measures. Simultaneously, regulators must intensify oversight of the cryptocurrency market to maintain order and prevent similar incidents from recurring.

4.3.2 Turkey's Crypto Ponzi Scheme: Stolen Fund Tracking

4.3.2.1 Background

On May 30, 2024, Turkish police conducted a large-scale raid on a cryptocurrency project called Smart Trade Coin (STC), arresting 127 suspects on charges of fraud and seizing substantial assets and firearms.

Since its launch in 2021, the STC project attracted many Turkish investors with promises of high returns, claiming to connect multiple cryptocurrency exchanges and enable unified management of various trading accounts. Over time, however, suspicions grew that the project was a Ponzi scheme. Lawyers representing the victims estimated that as many as 50,000 Turkish investors were affected, with total losses potentially exceeding $2 billion. Many users reported

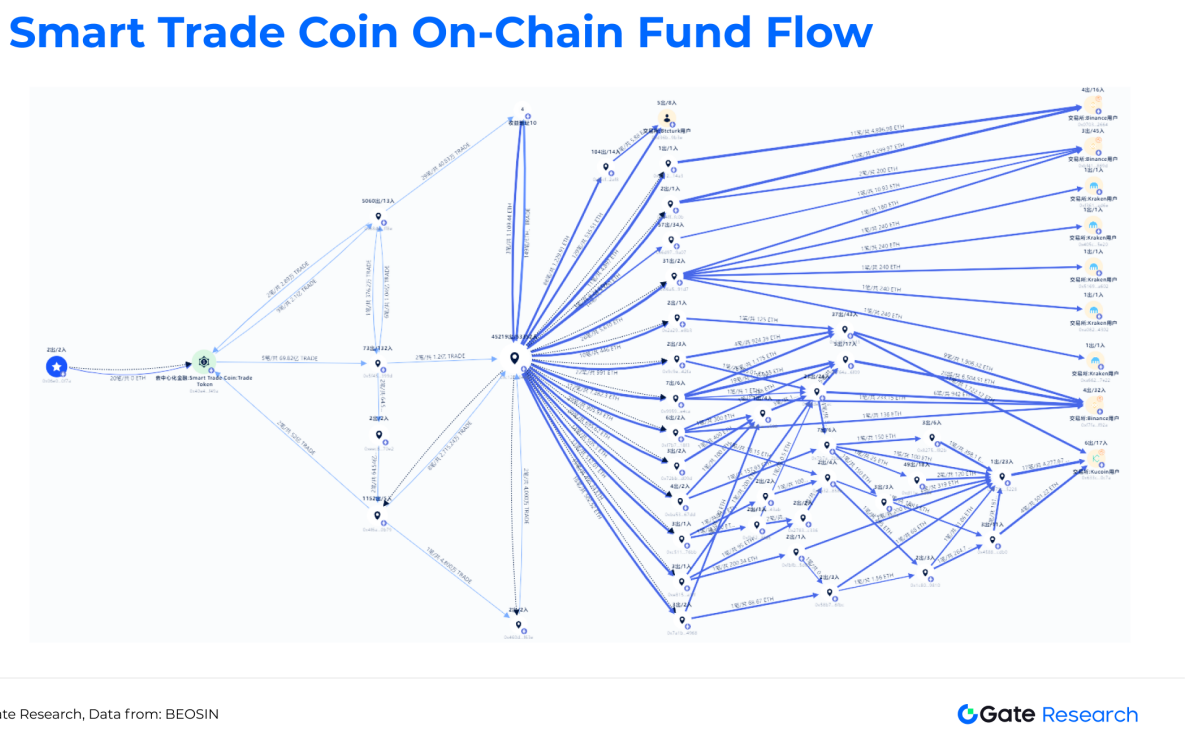
losing 95% of their savings and were unable to verify whether the funds had been misappropriated by the STC team.

4.3.2.2 Fund Pathway

Beosin KYT’s on-chain analysis of Smart Trade Coin revealed that most funds from the STC token contract were transferred through the 0x5f45 address and ultimately deposited into the 0xc12c address. Further tracking showed that the 0xc12c address conducted numerous large outbound ETH transactions, with amounts nearly matching the estimated total losses. Additionally, all transaction fees for ETH transfers were paid from the 0xc12c address, further confirming its role in distributing the stolen funds.

The chart below highlights only part of the fund flows. The 0xc12c address facilitated over 20,000 outbound transactions. Based on tracked transaction data, the stolen funds were distributed into two primary channels: one portion was directly sent to major exchanges, while the other underwent complex processes such as splitting, merging, and obfuscation before eventually being deposited into exchanges.

Figure 19: Smart Trade Coin On-Chain Fund Flow



4.3.2.3 Regulatory Challenges

This incident underscored the severe lack of regulation in Turkey’ s cryptocurrency market. While the government has encouraged innovation, the absence of an effective regulatory framework has left room for illicit activities, harming the interests of numerous investors. Local authorities must urgently establish a robust regulatory system to protect investors and promote the healthy development of the cryptocurrency industry.

Turkey’ s experience illustrates that pursuing unrestricted cryptocurrency freedom is not sustainable. Alongside fostering innovation, it is essential to strengthen regulation and establish a compliant, transparent market environment. Only by doing so can cryptocurrencies truly realize their potential as tools for economic growth and risk hedging. Governments and the industry must collaborate to develop comprehensive regulatory policies, enhance market oversight, and improve transparency to create a safe and reliable environment for cryptocurrency investments.

5 Anti-Money Laundering Regulations for Crypto Security Incidents

Money laundering activities in the cryptocurrency space have grown increasingly severe, posing significant threats to financial security. In 2024, regulatory efforts targeting cryptocurrency have intensified globally to address this challenge. Authorities in various countries have mandated virtual asset service providers to enhance KYC/AML compliance and actively participate in international regulatory cooperation. However, balancing investor protection with fostering innovation remains a key challenge for regulators. The cryptocurrency industry must also adapt to this regulatory landscape and balance compliance and business growth.

Anti-money laundering regulatory practices vary across countries. Taking Hong Kong, Singapore, the United States, Europe, Japan, Canada, Australia, South Korea, Turkey, and Malaysia as examples, these regions have implemented corresponding regulatory policies focusing on several key aspects: First, strengthening supervision of virtual asset trading platforms, requiring them to obtain relevant licenses; second, enhancing anti-money laundering and counter-terrorism financing measures, such as implementing the Travel Rule (which requires financial institutions handling crypto asset transfers to pass customer information to the next institution, including sender and recipient names and addresses) and strengthening KYC verification; third, focusing on stablecoin regulation, requiring increased transparency and capital reserves; fourth, protecting investor interests and combating fraud and cybercrime.

These regulatory measures indicate a growing global consensus on strengthening cryptocurrency market regulation to maintain financial stability and protect investor interests.

Figure 20: Anti-Money Laundering Regulatory Measures for Cryptocurrencies by Country

Smart Trade Coin On-Chain Fund Flow

Country/Region	Regulatory Authorities	Key Regulatory Measures
Hong Kong, CN	1. Hong Kong Monetary Authority 2. Securities and Futures Commission	1. Established licensing system for virtual asset OTC trading services, requiring all related services to obtain licenses. 2. Launched regulatory sandbox for stablecoin development and issuance. 3. SFC: Oversees crypto exchanges and security tokens, ensuring compliance with securities and AML regulations.
Singapore	Monetary Authority of Singapore	1. Revised Payment Services Act to enhance requirements for DPT (Digital Payment Token) service providers, addressing AML and financial stability. 2. Introduced stablecoin regulatory framework; compliant issuers can apply for "MAS-regulated stablecoin" designation.
United States	1.SEC 2.Office of Foreign Assets Control (OFAC) 3.Financial Crimes Enforcement Network(FinCEN) 4. OCC and Federal Reserve 5. State-level regulators	1. Crypto institutions must obtain MSB (Money Services Business) license for legal operation. 2. SEC pursues cases against crypto lending products and fraud, emphasizing investor protection. 3. OFAC sanctions Russian entities and cybercrime groups evading sanctions. 4. FinCEN: Handles crypto AML and customer identity verification. 5. OCC and Federal Reserve: Oversee financial institutions' crypto compliance. 6. Stablecoin regulations require higher transparency and capital reserves.
Europe	1.European Securities and Markets Authority (ESMA) 2.European Central Bank (ECB) 3. National financial regulators	1. Strengthened AML/CFT laws, established AMLA to monitor high-risk entities. 2. EU implementing MiCA for unified crypto standards, effective June 2023. 3. EU countries regulate through financial licenses: German BaFin, French AMF/ACPR. 4. UK requires crypto companies to register with FCA and meet regulatory requirements.
Japan	Financial Services Agency	1. Mandatory Travel Rule implementation for crypto exchanges, requiring collection and transmission of transaction party identities. 2. Regulates virtual currency exchanges under 2017 Virtual Currency Act. 3. Crypto-related financial services require FSA approval.
Canada	1.Canadian Securities Administrators (CSA) 2.Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) 3.Investment Industry Regulatory Organization of Canada (IIROC) 4.Provincial Securities Commissions	1. Regulates crypto asset securities trading, requires certain platforms to register as securities dealers. 2. Requires crypto platforms to register as MSBs (Money Services Business) and comply with AML/ATF regulations. 3. Canadian MSB licensing.
Australia	1. Australian Securities and Investments Commission (ASIC) 2. Australian Transaction Reports and Analysis Centre (AUSTRAC) 3. Reserve Bank of Australia (RBA)	1. Crypto services providers need AFSL license for financial products. 2. AUSTRAC registration required for crypto trading, wallet management, custody services. 3. Payment license needed for crypto payment services under RBA supervision.
South Korea	1. Financial Services Commission (FSC) 2. Korea Financial Intelligence Unit (KFIU)	Parliament passed a Special Financial Transactions Information Act amendment requiring VASPs to register with FSC and comply with AML and KYC regulations.
Turkey	Capital Markets Board, Banking Regulation and Supervision Agency	Unauthorized crypto service providers face 3-5 years imprisonment, up to 22 years for severe cases. Capital Markets Board responsible for provider authorization and regulation.
Malaysia	1.Bank Negara Malaysia (BNM) 2.Securities Commission Malaysia (SC)	Cryptocurrency trading incorporated into AML Act, requiring exchanges to implement strict KYC and report suspicious transactions.

A comparison of regulatory measures across countries reveals key similarities and differences. Most nations prioritize anti-money laundering (AML) and counter-terrorism financing (CTF), requiring cryptocurrency platforms to implement KYC compliance and obtain proper licenses. However, countries differ in their approach to stablecoin regulation, investor protection measures, and support for blockchain innovation. These variations demonstrate how each nation strikes its own balance between fostering innovation and maintaining regulatory oversight.

6 Summary

The security landscape for crypto assets remains challenging in 2024. Hackers are evolving their techniques, creating significant obstacles to industry growth. While traditional threats like rug pulls, smart contract vulnerabilities, and private key leaks persist, the situation has grown more complex due to low-security awareness among users and emerging attack methods. Recent major security incidents have revealed critical vulnerabilities in decentralized exchanges and other asset protection systems, emphasizing the pressing need for stronger security measures.

Recent incidents like the DMM Bitcoin hack and the Turkish crypto Ponzi scheme have prompted regulators worldwide to strengthen their cryptocurrency market oversight. Regulatory authorities are enhancing anti-money laundering (AML) and KYC measures to protect investors, fight financial crime, and ensure market stability. Countries globally have rolled out comprehensive measures, including licensing requirements, stricter AML protocols, investor safeguards, and stablecoin regulations. Notable examples include Hong Kong's new licensing system for virtual asset OTC platforms, Singapore's enhanced supervision of digital payment token services, the U.S. SEC's heightened scrutiny of crypto lending products, and Europe's implementation of the Markets in Crypto-Assets Regulation (MiCA) to create unified cryptocurrency market standards. These regulatory efforts aim to balance innovation and risk, creating a safer, more transparent, and compliant ecosystem for the cryptocurrency industry.

The crypto industry must maintain a delicate balance between innovation and security. The industry can effectively tackle evolving cyber threats through enhanced technology, robust security measures, and refined regulatory frameworks. Moreover, collaboration between regulatory bodies worldwide is essential for sharing intelligence and creating consistent oversight approaches. This coordinated effort will strengthen the crypto ecosystem's safety and transparency, enabling sustainable growth and providing investors with a more secure environment.

Author:Ember

References

1. https://hacked.slowmist.io/zh/statistics/?c=all&d=all
2. https://hacked.slowmist.io/zh/statistics/?c=all&d=2024
3. https://www.footprint.network/@Beosin/Footprint-Beosin-Q1-2024-Web3-Security-Report
4. https://www.footprint.network/@Beosin/Footprint-Beosin-Q3-2024-Web3-Security-Report
5. https://www.footprint.network/@Beosin/Footprint-Beosin-H1-2024-Web3-Security-Report
6. https://dune.com/queries/3446964/5791304
7. https://www.bbc.com/news/world-europe-66752785
8. https://www.gemini.com/cryptopedia/the-dao-hack-makerdao
9. https://www.pwc.tw/zh/news/press-release/press-20240131.html
10. https://www.deheheng.com/content/31030.html
11. https://cointelegraph.com/news/japanese-exchange-dmm-loses-bitcoin-private-key-hack
12. https://home.treasury.gov/news/press-releases/jy0916
13. https://beosin.com/resources/more-than-300-million-in-losses-analysis-of-45029-btc-abnormal-outflow-on-dmm-bitcoin-exchange
14. https://beosin.com/resources/over-100m-involved-and-127-suspects-detained-analysis-of-turkeys-crypto-ponzi-scheme

Links

Gate Research Official Website

Previous Research Reports

About Gate Research

Gate Research is a professional institute dedicated to blockchain industry analysis. We are committed to providing deep insights into the development trends of the blockchain sector. We aim to equip professionals and enthusiasts with forward-looking and expert industry insights. With a foundational commitment to democratizing blockchain knowledge, we strive to simplify complex technical concepts into understandable language. We present a comprehensive view of the blockchain industry by analyzing vast amounts of data and observing market trends, helping a wider audience understand and engage with this dynamic field.

research@gate.me