



2024 Q3

GLOBAL WEB3 SECURITY REPORT, AML ANALYSIS

& Crypto Regulatory Landscape

SECURING BLOCKCHAIN ECOSYSTEM

CONTENTS

I. 2024 Q3 Global Web3 Security Statistics & AML Analysis 01

1. 2024 Q3 Web3 Security Overview	01
2. Loss by Project Type	02
3. Loss by Chain	03
4. Attack Type Analysis	03
5. Typical AML Security Incidents	04
6. Stolen Fund Flow Analysis	06
7. Audit Analysis	07
8. 2024 Q3 Web3 Security Summary	07

II. Key Regulatory and Compliance Events in Q3 2024 08

1. SEC Issues Notices of Effectiveness for Multiple Spot Ethereum ETF S-1 Applications	08
2. MiCA Legislation Imposes Regulations on Stablecoins	09
3. Hong Kong Monetary Authority Launches Project Ensemble Sandbox	10
4. Summary of Stablecoin Consultation Released in Hong Kong	11
5. Singapore Increases Risk Factor for Cryptocurrency Exchanges in AML/CFT Regulation Update	13
6. Turkey's Cryptocurrency Regulatory Policy: Amendments on Capital Markets Law	14

III. Securing Blockchain Ecosystem 15

1. Beosin Security Product	15
2. About Blockchain Security Alliance	16
3. CONTACT US	17

This research report, initiated by the Blockchain Security Alliance and co-authored by alliance members Beosin and Footprint Analytics, aims to comprehensively explore the global blockchain security landscape and key regulatory policies in the crypto industry for the third quarter of 2024. Through analysis and assessment of the current global blockchain security situation, the report will reveal the current security challenges and threats, and provide solutions and best practices. Additionally, the report will examine the positions and policy orientations of various governments and regulatory bodies regarding crypto industry regulation, to help readers understand the dynamic changes in the regulatory environment and their potential impacts.

I. 2024 H1 Q3 Web3 Security Statistics & AML Analysis

Data Source (As of Sept. 25):

<https://www.footprint.network/@Beosin/Footprint-Beosin-Q3-2024-Web3-Security-Report>

1. 2024 Q3 Web3 Security Overview

According to statistics from Beosin Alert, the total losses from hacks, phishing scams, and rug pulls in Web3 reached \$730 million in Q3 2024. Among them, 23 major attacks resulted in a total loss of approximately \$430 million; 3 rug pulls with total losses of around \$4.24 million; and total losses from phishing scams of approximately \$295 million.

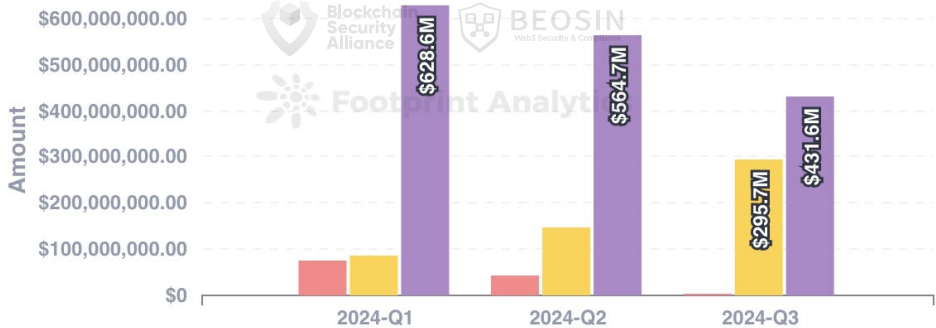
2024 Q3 Total Losses

Type	Amount (\$)
Total	731,550,000
Hacks	431,628,000
Phishing	295,682,000
Rug Pulls	4,240,000

Losses from phishing rose sharply in Q3 2024, with attacks and Rug Pull continuing to fall.

2024Q1-2024Q3 Losses by Type

● Rug Pulls ● Phishing ● Hacks



By project types, Centralized Exchanges (CEX) suffered the highest losses, with 4 attacks causing about \$297 million in losses, accounting for 40.6% of all attack losses.

Looking at losses by blockchain, Ethereum remained the chain with the highest losses and the most attack incidents. 21 attacks on Ethereum caused \$348 million in losses, accounting for 47.6% of the total losses.

In terms of attack types, Q3 2024 saw 5 incidents of private key compromises, causing \$305 million in losses, which represented 41.7% of total attack losses - the highest percentage among all attack types.

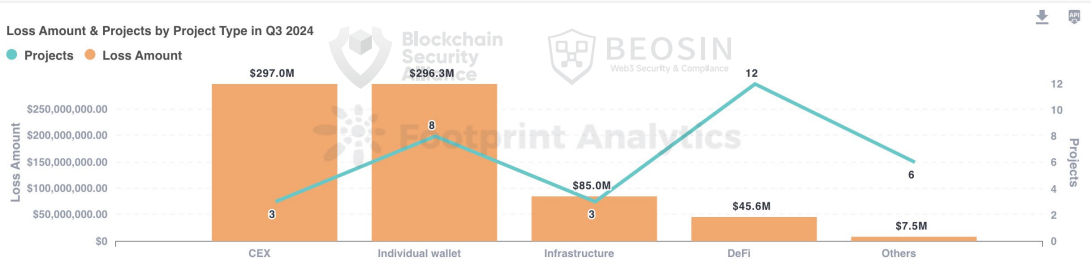
Regarding the fund flows, about \$16.9 million of stolen funds were frozen or recovered. The vast majority (approximately 78.9%) of the stolen funds are still held by attackers' addresses.

In terms of auditing status, the proportion of audited projects that suffered attacks have increased.

2. Loss by Project Type

CEX suffered the highest losses

In 2024 Q3, Centralized Exchanges (CEX) suffered the highest losses. Three attacks targeting CEXs resulted in a total loss of approximately \$297 million, accounting for 40.6% of all attack losses. Although CEX security incidents were few in number, each theft involved a massive amount, posing a severe challenge to the security of the exchange ecosystem.

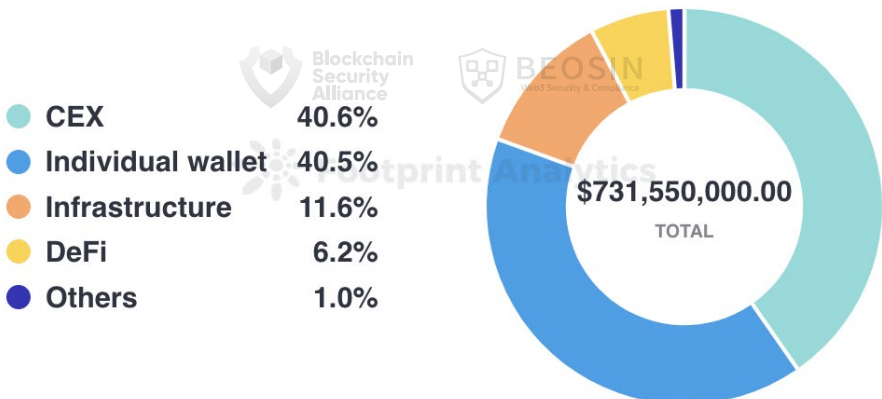


The second largest loss was user wallets. 8 phishing and social engineering attacks on user wallets caused approximately \$295 million (about 40.3%) in losses to regular users. Compared to the first half of 2024, Q3 saw a significant increase in attacks and losses against regular users.

A total of 12 of the 23 hacking incidents occurred in the DeFi space, which was the project type with the highest number of attacks, and these 12 DeFi attacks resulted in a total of more than \$45.6 million in losses, which was the fourth highest of all project types.

Other project types attacked included infrastructure, tokens, and others. Attacks against public chains and cross-chain bridges caused \$85 million in losses, ranking third among all project types.

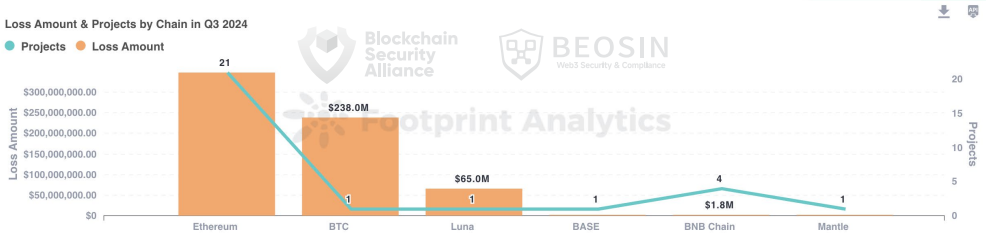
Market Share of Loss Amount by Project Type in Q3 2024



3. Loss by Chain

Ethereum saw the highest losses and the most attacks

Similar to 2024 H1, Ethereum remained the blockchain with the highest loss amount in 2024 Q3. A total of 21 attack incidents on Ethereum caused \$348 million in losses, accounting for 47.6% of the total losses.



BTC ranked second in terms of loss amount, with a total loss of \$238 million, accounting for 32.5% of the total losses. The BTC loss amount came from a social engineering attack on a whale address.

The third largest public chain in terms of losses was Luna (\$65 million), where attackers exploited a reentrancy vulnerability in the ibc-hooks timeout callback against Luna.

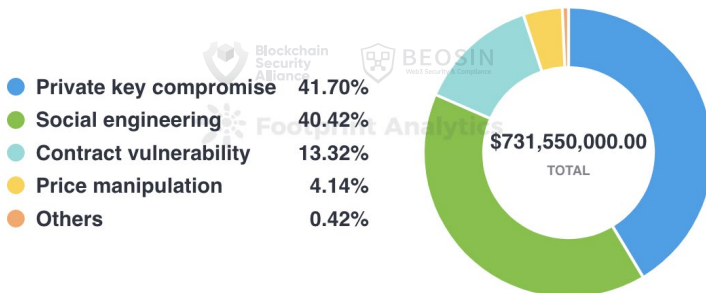
Ranking by the number of security incidents, the top two were Ethereum (21 incidents) and BNB Chain (4 incidents). The number of security incidents on different chains decreased compared to 2024 H1.

4. Attack Type Analysis

About 41.7% of losses came from private key compromises

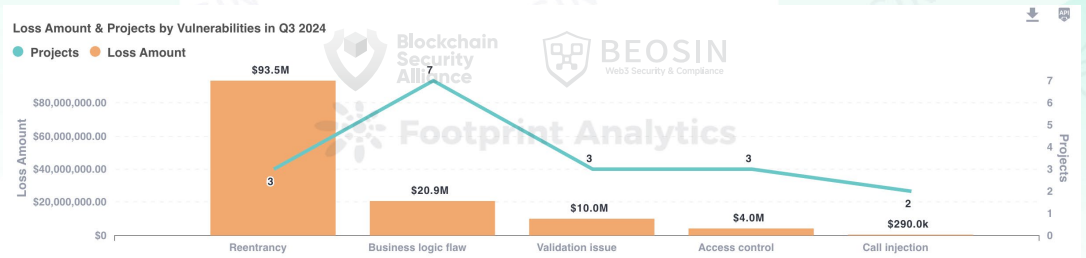
2024 Q3 saw 5 incidents of private key compromise, resulting in losses of \$305 million, accounting for 41.7% of total losses from attacks. Similar to the first half year, losses caused by private key compromise remained the highest among all attack types. Major private key compromise incidents with significant losses included: WazirX (\$230 million), BingX (\$45 million), and Indodax (\$22 million).

Market Share of Loss Amount by Attack Type in Q3 2024



Social engineering attacks ranked second in terms of loss amount, with 1 such attack causing losses of about \$238 million.

Among the 23 attack incidents, 18 were due to contract vulnerability exploits, accounting for about 78%. The total loss from contract vulnerability exploits reached \$128 million, ranking third.



Breaking down by vulnerability types, the top three vulnerabilities causing losses were: reentrancy vulnerabilities (\$93.46 million), business logic flaws (about \$20.9 million), and validation issues (\$10 million). Business logic flaws were also the most frequent vulnerability, accounting for 7 out of 18 contract vulnerability attacks.

5. Typical AML Security Incidents

5.1 Beosin Trace's analysis of LI.FI incident

On July 16, according to Beosin Alert, an attack on LI.FI, a cross-chain protocol, was detected, in which attackers exploited a call injection vulnerability in the project's contract to steal assets from users who authorized the contract.

There is a function named `depositToGasZipERC20` that can convert specified tokens into platform tokens and deposits them into the GasZip contract, but the code of the conversion logic does not limit the call data, which allows an attacker to use this function to perform a call injection attack and withdraw assets from authorized users of the contract.

```

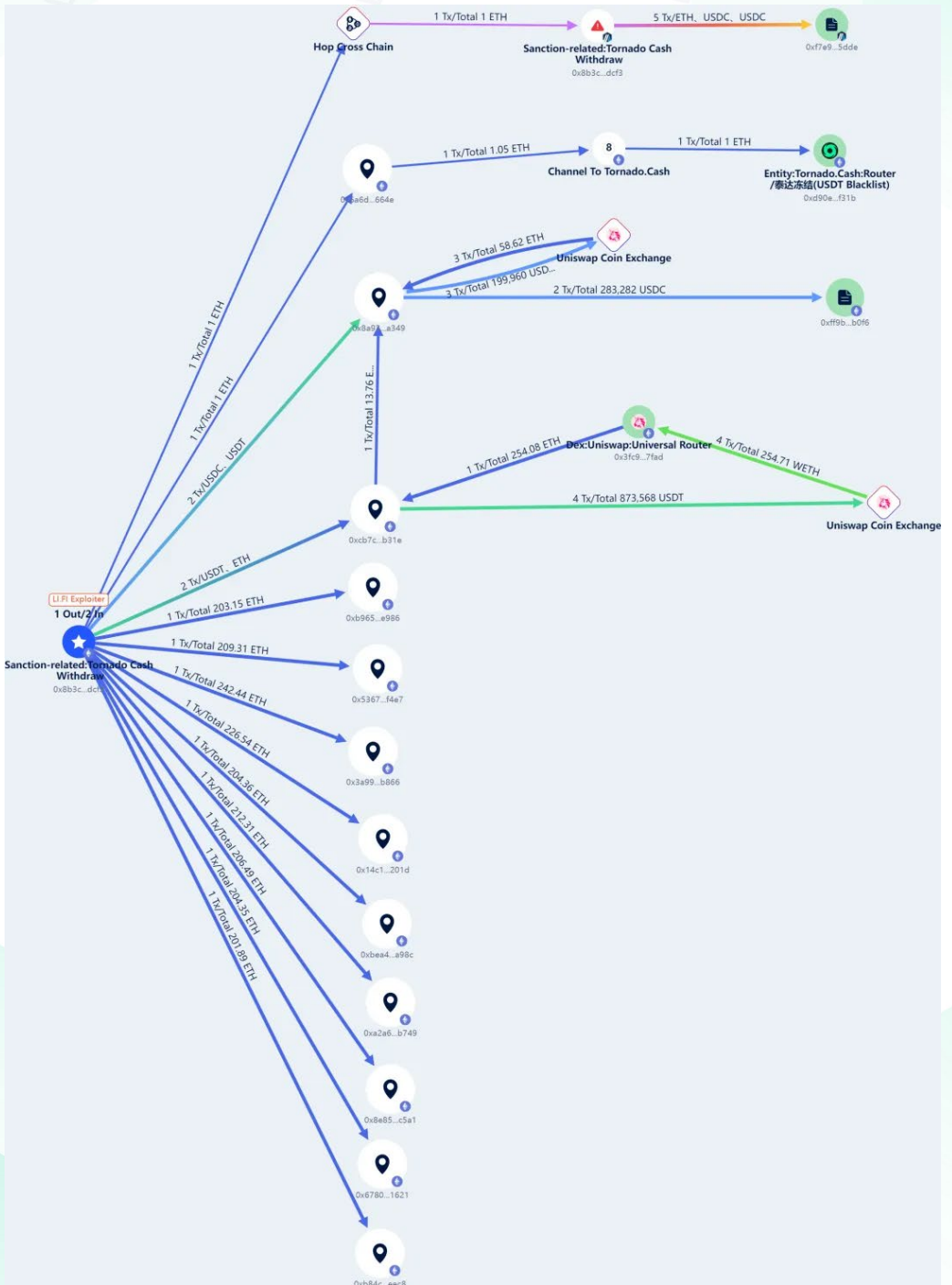
51
52     if (initialSendingAssetBalance < _swap.fromAmount) {
53         revert InsufficientBalance(
54             _swap.fromAmount,
55             initialSendingAssetBalance
56         );
57     }
58
59     // solhint-disable-next-line avoid-low-level-calls
60     (bool success, bytes memory res) = _swap.callTo.call{
61         value: nativeValue
62     }(_swap.callData);
63     if (!success) {
64         LibUtil.revertWith(res);
65     }
66
67     uint256 newBalance = LibAsset.getOwnBalance(_swap.receivingAssetId);
68

```

In addition to the call injection contract vulnerability, this incident is also noteworthy for the configuration of the Facet contract in Diamond mode. Further analysis revealed that the GasZipFacet contract was deployed 5 days before the attack and registered in the LI.FI contract by the project's multi-signing administrator ten hours before the attack.

Therefore, through this incident, it can be found that for upgradeable models such as Diamond, the security of the new function contract also needs to be given high priority.

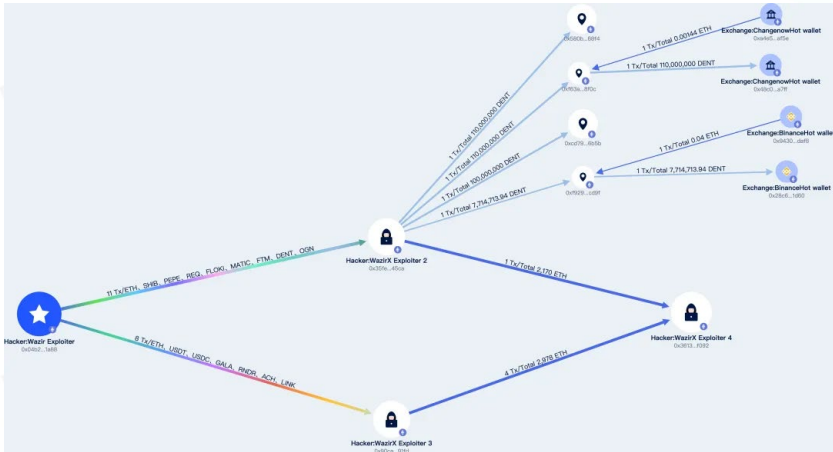
Beosin Trace's tracking of the stolen funds found that the losses included 6,335,900 USDT, 3,191,900 USDC, and 169,500 DAI, a total loss of about \$10 million.



5.2 Analysis of WazirX incident with a loss of \$235 million

On July 18, according to Beosin Alert, WazirX was attacked, and the attackers obtained the signature data of the exchange's multi-signature wallet administrator, modified the logical contract of the wallet, and made the wallet execute the wrong logic to steal assets, involving more than \$230 million.

Beosin Trace tracks the flow of the stolen funds. So far, the hackers have transferred some of the funds into Changenow and Binance. 0xf92949ab576ac2f8dc9e4650e73db083f1f9cd9f is a Binance deposit address of the hackers.



On the other hand, the hacker sent 801 billion SHIB tokens to the address 0x35fe... 745CA with a total value of \$14.02 million.

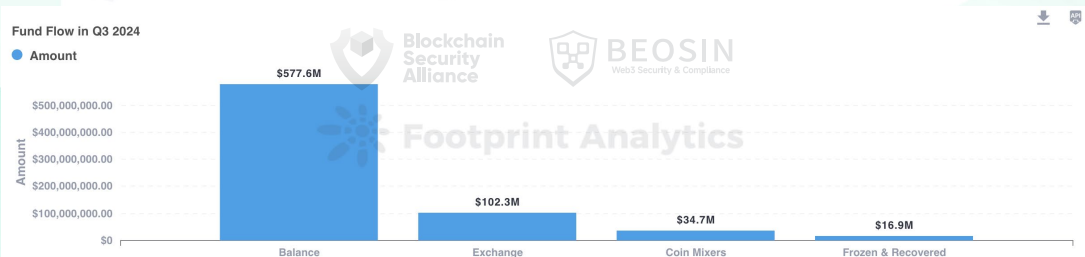
6. Stolen Fund Flow Analysis

According to analysis from the Beosin KYT anti-money laundering platform, of the funds stolen in Q3 2024, \$16.9 million were frozen or recovered. This percentage has significantly decreased compared to 2024 H1.

About \$577 million (78.9%) of the stolen funds are held at hacker addresses. As global regulatory agencies intensify their anti-money laundering efforts, it has become more difficult for hackers to launder their stolen funds. As a result, a considerable number of hackers have chosen to temporarily keep the stolen funds at on-chain addresses.

Approximately \$102 million of the stolen funds were transferred to various exchanges, accounting for about 13.9%, which is higher than in 2024 H1.

A total of \$34.71 million (5.4%) were transferred to mixers. Compared to H1, the amount of stolen funds laundered through mixers in Q3 2024 has significantly decreased.

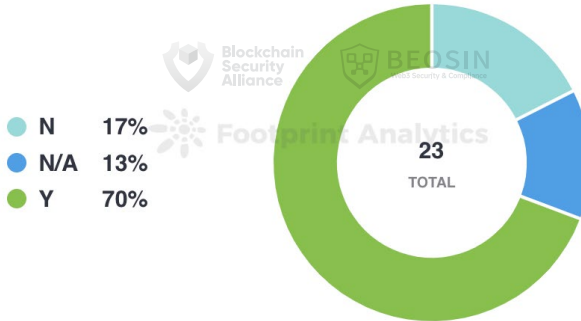


7. Audit Analysis

The proportion of audited projects have increased

In Q3 2024, out of 23 attack incidents, 4 involved projects that had not been audited, while 16 involved projects that had been audited. The proportion of audited projects is higher than in 2024 H1, indicating that the Web3 industry as a whole is placing greater importance on security.

Whether Audited - Projects in Q3 2024



Among the 4 unaudited projects, 3 incidents (75%) involved contract vulnerabilities. Of the 16 audited projects, 11 incidents (68.75%) involved contract vulnerabilities. The overall proportions are roughly equivalent. Compared to H1, the overall quality of security audits in 2024 has somewhat declined.

8. 2024 Q3 Web3 Security Summary

Compared to the same period in 2023, total losses caused by hacks, phishing scams, and rug pulls in Q3 2024 decreased to \$730 million (this figure was \$889 million in Q3 2023). While fallen cryptocurrency prices had some impact on the decrease in total amount, the overall security situation in the Web3 space remains far from optimistic.

As in 2024 H1, private key compromises remained the most damaging type of attack in 2024 Q3. About 41.7% of the loss amount came from private key leak compromises. In terms of project types, private key compromise incidents spanned various Web3 domains: gaming platforms, token contracts, individual wallets, infrastructure, exchanges, etc. All Web3 project teams and individual users need to be vigilant, storing private keys offline, using multi-signature wallets, being cautious with third-party services, and conducting regular security training for privileged employees.

In Q3, 5.4% of stolen assets were sent to mixers while 78.9% of assets remained at hacker addresses, further indicating the increasing difficulty for hackers to launder their stolen funds. Still, 13.9% of stolen funds were transferred to various exchanges, highlighting the need for exchanges to promptly identify hacker behavior and actively cooperate with law enforcement agencies and project teams to freeze funds and conduct investigations. Currently, cooperation between exchanges, law enforcement agencies, project teams, and security teams has shown notable results, and it's expected that more stolen funds will be recovered in the future.

Among the 23 attack incidents this quarter, 18 still involved contract vulnerability exploits. It is recommended that project teams seek professional security companies for audits before launch. Beosin, as a globally leading blockchain security company committed to the secure development of the Web3 ecosystem, has audited over 3,000 smart contracts and public blockchains. As a trusted blockchain security company, Beosin can provide excellent security audit services for project teams.

The background features a light green gradient with vertical columns of binary code (0s and 1s) in a slightly darker shade. In the lower half, there are large, overlapping, curved green shapes that resemble stylized waves or abstract architectural elements, creating a sense of depth and movement.

II. Key Regulatory and Compliance Events in Q3 2024

This report will explore key regulatory and compliance events in Q3 2024 in the United States, Dubai, Singapore, and Hong Kong, providing insights into the evolving regulatory landscape for digital assets.

1. SEC Issues Notices of Effectiveness for Multiple Spot Ethereum ETF S-1 Applications



On July 23, according to official information from the SEC, it has formally approved the S-1 applications of several ETF issuers, officially allowing for the listing of spot Ethereum ETFs. The notice indicates that the SEC has notified at least two of the eight companies applying to launch the first spot Ethereum ETFs in the U.S. that their products can begin trading on Tuesday. Products from BlackRock, VanEck, and six other companies will start trading on Tuesday morning on three different exchanges: the Chicago Board Options Exchange (CBOE), the Nasdaq, and the New York Stock Exchange, all of which have confirmed they are ready to begin trading.

Another significant impact of the approval of spot Ethereum ETFs is the shift in the attitude of U.S. regulators towards crypto policy. With the U.S. elections underway, the differing inclinations of the Democratic and Republican parties towards the crypto industry are noteworthy.

Previously, the former House Speaker Nancy Pelosi was considering supporting the Republican crypto legislation, FIT21, during a vote this week in the House. Additionally, a resolution on the cryptocurrency accounting standards bill, SAB121, was also expected soon.

After the approval of spot Ethereum ETFs, mainstream market opinions suggest that this positively impacts the regulatory environment for cryptocurrencies. Earlier, Alex Thorn, head of research at Galaxy Digital, indicated that the SEC's regulatory stance on Ethereum would seek to find a balance between the views that "ETH" itself is not a security, while "staked ETH" (or, more tenuously, "staked ETH as a service") is a security.

This is very similar to the demands of the FIT21 bill, which aims to clarify which digital assets are regulated by the Commodity Futures Trading Commission (CFTC) and which are regulated by the Securities and Exchange Commission (SEC). This distinction is crucial, as there are significant differences between the definitions of "commodity" and "security," which will impact how they are regulated. In summary, as a category of crypto assets with smart contracts, the passage of the spot ETF will undoubtedly have a profound effect on the crypto industry.

2. MiCA Legislation Imposes Regulations on Stablecoins

With the implementation of the EU MiCA (Markets in Crypto-Assets) regulation, 2024 will mark a significant milestone for the crypto industry in the EU and beyond. This groundbreaking regulatory framework is regarded as the most comprehensive in the world and will fundamentally change the landscape of the crypto industry, with key implementation dates of June 30 for stablecoins and December 30 for Crypto Asset Service Providers (CASPs).

As previously mentioned, MiCA (1) imposes stringent requirements on the reserves backing stablecoins; (2) mandates detailed disclosure of information related to collateral, operations, and risk management processes; and (3) requires authorization from the competent authority in the EU member state to offer stablecoins within the EU.

Exchanges operating in the EU may delist non-compliant stablecoins. Whether local or global, stablecoin issuers must comply with regulations in the short to medium term, or they will ultimately vanish from the EU market, as evidenced by recent announcements from exchanges like Binance, Bitstamp, Kraken, and OKX regarding the delisting or gradual phasing out of non-compliant tokens. Over time, the EU will be a market with zero tolerance for regulatory loopholes regarding "Internet Funny Money."

According to Patrick Hansen, Circle's head of EU policy, the follow-up implications of MiCA include:

- Despite certain restrictions or excessive regulatory protectionism in the law, MiCA represents an opportunity to develop a unique European crypto asset market, with expectations for localization, institutionalization, specialization, and potential integration (across all ecosystems) in the EU's crypto market;
- In the short to medium term, local and global stablecoin issuers must comply with regulations or ultimately exit the EU market, as demonstrated by recent announcements from exchanges;
- Euro stablecoins are expected to grow and face local competition; foreign unregulated exchanges will encounter significant restrictions in the EU, making reverse solicitation operations extremely difficult, even impossible;
- A significant portion of the implementation work for MiCA remains to be completed, warranting further observation; while MiCA undoubtedly offers tremendous opportunities for the EU, it requires collaborative efforts from the industry, regulators, policymakers, and ultimately the nearly 450 million consumers to fully realize its potential;
- The longer the regulatory vacuum regarding cryptocurrencies persists in major jurisdictions like the U.S. and the U.K., the greater the potential global impact of MiCA standards.

Circle has announced that USDC and EURC can now be used under the new EU stablecoin legislation and it is the first global stablecoin issuer to comply with MiCA standards. Starting July 1, Circle has begun to issue USDC and EURC to European customers.



3. Hong Kong Monetary Authority Launches Project Ensemble Sandbox

In August 2024, a significant milestone was reached in the Hong Kong financial market with the official launch of the Ensemble tokenization sandbox by the Hong Kong Monetary Authority (HKMA) and the Securities and Futures Commission (SFC). This innovative regulatory environment provides a testing platform for the tokenization of financial resources and has the potential to revolutionize the traditional financial system. Industry giants, including HSBC and the Global Shipping Business Network (GSBN), have begun proof-of-concept testing, with HashKey Group also planning to join the project. This sandbox initiative in Hong Kong is not just an experiment but may become a standard for future global financial markets.

The HKMA stated that the sandbox has been established to facilitate interbank settlement using experimental tokenized currencies and to focus on the trading of tokenized assets. Participating banks in the Ensemble project working group have connected their tokenized deposit platforms to the sandbox, preparing for future experiments in cross-bank payment synchronizations and cash settlements.

What is the Hong Kong Ensemble Sandbox?

The Ensemble sandbox is a platform created by the HKMA to allow financial institutions and technology companies to experiment with asset tokenization in a controlled environment. Tokenization refers to converting physical assets or rights into digital forms represented by tokens on a blockchain. This process not only enhances liquidity and transparency but also reduces transaction costs and improves market efficiency.

This initiative is part of Hong Kong's strategy to become a global leader in financial innovation. Ms Julia Leung, Chief Executive Officer (CEO) of the Securities and Futures Commission (SFC), emphasized that the project aims to prepare the financial system for the future, highlighting the importance of conducting experiments within a regulated environment to ensure that new technologies can be implemented safely and sustainably.

Leung also stated that the launch of the sandbox demonstrates how innovation and regulation can open new pathways for Hong Kong's financial market. As the two major architects of Hong Kong's financial market, the SFC and HKMA share the same vision and are committed to leading Hong Kong's financial system boldly into the future through innovative market infrastructure.

Key Participants

The launch of the Ensemble sandbox has attracted the attention of major financial and technological institutions. HSBC, as one of the largest banks in the world, was among the earliest participants. Its involvement reflects the growing interest of traditional banks in blockchain technology and tokenization, which are seen as tools for enhancing operational efficiency and providing new products and services to clients.

Another key participant is the Global Shipping Business Network (GSBN), an alliance of major shipping companies and logistics operators. GSBN views the sandbox as an opportunity to explore how tokenization can optimize shipping and global trade operations, reduce transaction times, and enhance supply chain transparency.

Finally, as a leader in the digital asset space, HashKey Group has announced plans to join the sandbox. Their participation underscores the importance of collaboration between traditional sectors and the cryptocurrency sector to build a robust and inclusive financial ecosystem.



Goals of the Ensemble Sandbox

The design goals of the Ensemble sandbox are clear: to test the feasibility of tokenization, identify and mitigate associated risks, and develop a regulatory framework suitable for widespread adoption. Participation from institutions like HSBC and GSNB ensures that the solutions developed are scalable and can be integrated into global markets.

One of the most interesting aspects of the sandbox is its ability to conduct experiments in a real but regulated environment. This approach allows for the identification of any technological, regulatory, or market issues before implementing solutions globally. Additionally, the sandbox provides Hong Kong regulators with a unique opportunity to work with companies to create flexible regulations that can quickly adapt to technological changes.

4. Summary of Stablecoin Consultation Released in Hong Kong

According to a consultation summary jointly initiated by the HKMA and the Financial Services and the Treasury Bureau, stablecoin issuers will now be regulated by the HKMA. Although the consultation summary has been completed, there are currently no clear legislative and regulatory guidelines available, and specific recommendations for anti-money laundering concerning stablecoins have yet to be provided.

Definition of Stablecoins

The definition of stablecoins excludes the following categories:

- Deposits (including tokenized or digital forms of deposits)
- Certain securities or futures contracts (primarily recognized collective investment schemes and recognized structured products)
- Any amount or instrument held in a stored value payment tool
- Digital forms of fiat currency issued by a central bank or on its behalf
- Certain limited-use digital forms of value

Stablecoins issued using decentralized distributed ledgers or similar technology, where the decentralized distributed ledger operates without any individual having unilateral control or the ability to materially change its ledger functionality or operation, such as TerraUSD (UST), Dai (DAI), and sUSD (Synthetix USD).

Fiat-backed Stablecoins

Regulators deem it necessary to include all fiat-backed stablecoins under the proposed regulatory framework since both single-currency and multi-currency fiat stablecoins are linked to the traditional financial system and could pose risks to financial stability. Given that fiat stablecoins could evolve into widely accepted payment methods, they pose higher and more urgent risks to monetary and financial stability.



Response to Guidelines and Conditions for Stablecoin Issuers

- Any promotion of unlicensed fiat-backed stablecoin issuance activities by any party (including issuers, agents, and intermediaries) is illegal.
- Issuers must establish independent accounts with licensed banks or custodians approved by the Monetary Authority to manage reserve assets.
- Issuers must separate reserve assets from their own assets and establish effective trust arrangements to provide users of fiat-backed stablecoins with statutory rights and priority claims to the reserve assets.
- Issuers must demonstrate that their reserve asset investment policies and liquidity management policies are commensurate with the scale and complexity of their business, ensuring they can meet redemption requests under normal and stressed conditions.
- Issuers must fulfill redemption requests within one business day of receiving the request.
- Issuers must have sound risk management procedures and internal controls to safeguard and manage reserve assets.
- Issuers must regularly disclose the total amount of circulating stablecoins, the market value of reserve assets, and their composition.
- Issuers must not pay interest to fiat users.
- Issuers must be incorporated in Hong Kong, and senior executives must reside in Hong Kong and effectively oversee their stablecoins.
- The minimum paid-up capital requirement for issuers is HKD 25 million or 1% of the face value of the circulating stablecoins, whichever is higher.
- Issuers must publish a stablecoin white paper, which should include general information about the issuer, the risks associated with using the fiat-backed stablecoin, the technology employed, the issuance, distribution, and redemption mechanisms and procedures, the rights of potential fiat-backed stablecoin users, and the applicable conditions and fees for redemption.
- Issuers must conduct a risk assessment at least once a year. Regulatory authorities will issue clear regulations regarding the qualifications of auditors and the scope of audits in the future.



5. Singapore Increases Risk Factor for Cryptocurrency Exchanges in AML/CFT Regulation Update


On July 1, Singapore's regulatory authorities released an updated version of the country's National Risk Assessment (NRA) on terrorist financing and the national strategy for combating terrorist financing.

This move aims to prevent terrorist organizations and groups from exploiting Singapore's openness as an international financial, business, and transportation hub to fund terrorism.

According to the latest update, the risk level for cryptocurrency trading platforms or Digital Payment Token (DPT) service providers has been elevated from medium-low to medium-high. Cross-border online payments remain categorized as high risk, as they have been identified as potential new channels for terrorist financing activities.

The latest challenges to crypto platforms comes weeks after a report labeled digital payment tokens as high risk. According to Singapore's latest Money Laundering National Risk Assessment (MLNRA), DPT service providers represent serious risks and vulnerabilities in the context of anti-money laundering (AML).

3.3 The key findings of the NRA are summarised in the table below.

KEY ML THREATS	
 Fraud , particularly cyber-enabled fraud	 Corruption , originating from abroad
 Organised Crime , especially illegal online gambling associated with foreign organised criminal groups	 Tax Crimes , originating from abroad
	 Trade-based money laundering
OTHER NOTABLE ML THREATS	
 Environmental Crime	 Drug-related offences
 Cyber-crime	
HIGHER ML RISK SECTORS	
<i>Inherent exposure to key ML threats, and cross-border transactions/customers, despite stronger controls</i>	
 Banks pose highest ML risks to Singapore	
 <i>Abused through their roles as professional / financial intermediaries, exposure to cross-border transactions, and/or placement in high value assets, while taking into account controls in place</i>	
<ul style="list-style-type: none"> • Corporate Services Providers • Real Estate • Casinos • Licensed Trust Companies • Precious stones and precious metal dealers 	<ul style="list-style-type: none"> • Digital Payment Token Services Providers • Payment Institutions, with cross border money transfer services • External Asset Managers

Major Findings from the MLNRA in Anti-Money Laundering. Source: MAS

The Monetary Authority of Singapore (MAS) has been actively involved in regulating the digital asset market. A few months ago, Singapore's regulators expanded the scope of regulated payment services to include digital token service providers, incorporating digital assets into user protection laws.

This law allows MAS to impose stricter requirements on DPT service providers concerning anti-money laundering, counter-terrorism financing, user protection, and financial stability. It also facilitates DPT providers in offering custody and crypto transfer services in the country.

Singapore is regarded as a supportive environment for cryptocurrencies, with a high adoption rate. While the global cryptocurrency ownership rate is approximately 4.2%, Singapore's adoption rate is as high as 11.2%. According to Singaporean regulations, digital currencies are referred to as digital payment tokens.

6. Turkey's Cryptocurrency Regulatory Policy: Amendments on Capital Markets Law

Since 2021, Turkey has been placed on the FATF grey list due to money laundering risks. To overcome this adverse situation and clarify the taxation policy for cryptocurrencies, Turkey has intensified its regulatory efforts in this area. Turkey has now successfully removed itself from the grey list, and a new regulatory framework has been established to pave the way for the normalization of the cryptocurrency market.

On July 2, 2024, the Capital Markets Board of Turkey (CMB) officially announced the Capital Markets Law Amendment No. 7518, incorporating regulations for crypto asset service providers (CASPs) into legislation. This marks a new phase in Turkey's cryptocurrency regulation, requiring all CASPs to obtain CMB approval and comply with standards set by TUBITAK. Additionally, activities related to banking must also receive approval from the Banking Regulation and Supervision Agency (BDDK). These regulations not only strengthen oversight but also ensure the healthy development of the crypto asset industry.

According to the new regulations, the establishment of crypto asset platforms must meet the following conditions:

- 1.The platform must be established as a joint-stock company, with a minimum paid-in capital of 50 million Turkish Lira.
- 2.All shares must be issued in cash and registered.
- 3FOUNDERS and managers must comply with the Capital Markets Law and other relevant regulations, demonstrating sufficient financial capability, honesty, and trustworthiness.
- 4.The scope of operations for the crypto asset platform must be clearly defined, covering activities such as purchasing, selling, initial issuance, distribution, clearing, transfer, and custody.

The new regulations require currently operating CASPs in Turkey to submit the necessary documents to the CMB within one month; companies failing to submit applications must make a decision to liquidate within the same timeframe. Platforms operating temporarily must apply for operational permits by November 8, 2024, or face expulsion.

During the transition period, a total of 76 exchanges have received temporary licenses to continue operations and must comply with the new regulations. Meanwhile, 8 exchanges that failed to meet the requirements have been ordered to liquidate.

The new regulations impose severe penalties on individuals and entities engaging in unauthorized crypto asset services. Violators will face 3 to 5 years of imprisonment and fines ranging from 5,000 to 10,000 days. Misappropriating entrusted funds or assets will result in even harsher penalties, with a maximum of 14 years in prison and substantial fines.

Those involved in fraudulent activities to cover up misappropriation will face 14 to 20 years in prison and fines of up to 20,000 days. Additionally, individuals illegally using resources from revoked licensed CASPs will face up to 22 years in prison and fines of up to 20,000 days.



REFERENCE:

<https://www.chaincatcher.com/article/2134773>
<https://cointelegraph.com/news/singapore-raises-crypto-exchange-risk>
<https://mp.weixin.qq.com/s/a9Y8yiNEBbR4NuBkMtoIXQ>

The background features a light green gradient with vertical columns of binary code (0s and 1s) in a slightly darker shade. In the lower half, there are several overlapping, semi-transparent green curved shapes that resemble stylized waves or abstract architectural elements.

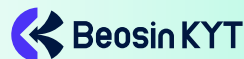
III. Securing Blockchain Ecosystem

1. Beosin Security Product

KYT

AML and crypto compliance platform

Relying on more than 1 billion address tags and malicious address database, Beosin KYT, the cryptocurrency AML and crypto compliance platform can help VASP (Virtual Asset Service Providers) build KYT (Know Your Transactions) and risk assessment capabilities. The system analyzes massive amounts of on-chain transactions to identify transactions and address types, and then uses the system's massive library of entity addresses and machine learning analytics to assess risky transactions. Beosin KYT are currently serving multiple clients around the world to comply with AML regulations.



Try Beosin KYT: <https://kyt.beosin.com/>

Trace

Cryptocurrency tracing and investigation platform

Beosin-Trace is a cryptocurrency fund tracing platform that combines big data, AI and other technologies. It is a personalized investigation tool for global clients in recovering their lost cryptocurrencies. It has successfully helped clients recover 100+ millions of stolen assets, including funds that flowed into mixers (such as Tornado Cash).



Try Beosin Trace: <https://beosin.com/service/tracing>

All-In-One Audit Solution

By utilizing Beosin's independently developed formal verification tools and comprehensive network security technologies, we offer security auditing services for Web3 projects. Over 3,000 smart contracts audited and 85,000+ vulnerabilities identified. With abundant smart contract security dataset, powered by AI Large Language Model, we trained an intelligent model that can deeply understand smart contract logic, further enhancing the Formal Verification Tool Vaa's ability to detect and verify security issues in complex business contracts.

Due Diligence

Offering comprehensive due diligence solutions, Beosin's professional team is dedicated to assisting you in evaluating potential risks and compliance, providing accurate and reliable due diligence reports to aid you in making informed decisions.

2. About Blockchain Security Alliance



The Blockchain Security Alliance was initiated by Beosin in joint collaboration with several units from diverse industry backgrounds, including university institutions, blockchain security companies, industry associations, fintech service providers, etc. The first batch of alliance council include Beosin, SUSS NiFT, NUS AIDF, BAS, FOMO Pay, Onchain Custodian, Semisand, Coinhako, ParityBit, and Huawei Cloud. The current members include: Huobi University, Moledao, Least Authority, PlanckX, Coding Girls, Coinlive, Footprint Analytics, Web3Drive, and Digital Treasures Center.

The members of the Security Alliance will work and cooperate together to continuously secure the global blockchain ecosystem with their own technical strengths. The Alliance Council also welcomes more people in blockchain-related fields to join and jointly defend the security of the blockchain ecosystem.

Alliance Registration: <https://forms.gle/pb3NaUgS3a2Sswnc8> market@beosin.com

About Beosin

As one of the first blockchain security companies in the world to engage in formal verification, Beosin focuses on the "security + compliance" solution. It has offices in 10+ countries and regions and provides "All-in-One" blockchain compliance products + security services covering Smart Contract Audit, On-chain Risk Monitoring & Blocking, Crypto Tracing, Virtual Asset Anti-money Laundering (AML), and Compliance Assessments to meet local regulatory requirements. With 60+ technical patents and software copyrights, 100+ top security experts, 20 years of network security experience, and 85,000+ identified vulnerabilities, Beosin is committed to the secure development of Web3 ecosystem. It has cooperated with 200+ Web3 enterprises and regulatory agencies around the world including HashKey Group, Monetary Authority of Singapore, and Hong Kong Police Force and has audited 3,000+ smart contracts and blockchain mainnets, including PancakeSwap, Ronin Network, and SyncSwap.



About Footprint Analytics

Footprint Analytics is a blockchain data solutions provider. We leverage cutting-edge AI technology to help analysts, builders, and investors turn blockchain data and combine web2 data into insights with accessible visualization tools and a powerful multi-chain API across 30+ chains for NFTs, GameFi, wallet profile, and money flow data.

About SUSS NiFT

The SUSS Node for Inclusive Fintech (NiFT) is the "Centre of Excellence" spearheading all Fintech initiatives at the university. It is a multi-disciplinary centre drawing on expertise from faculty members across SUSS' five schools, their collective publications and programmes. Established in 2021, SUSS NiFT is essentially a re-launch of SUSS' endeavor in the Fintech and blockchain domain since 2016. NiFT serves to deliver high-quality research, public education, and policy advocacy for inclusivity in the Financial Technology sector for the benefit of society.





2024 Q3

GLOBAL WEB3 SECURITY REPORT, AML ANALYSIS

& Crypto Regulatory Landscape

SECURING BLOCKCHAIN ECOSYSTEM

CONTACT US



market@beosin.com

Email



t.me/beosin

Telegram



[@Beosin_com](https://twitter.com/Beosin_com)

Official Twitter



[@BeosinAlert](https://twitter.com/BeosinAlert)

Alert Twitter