CERTIK

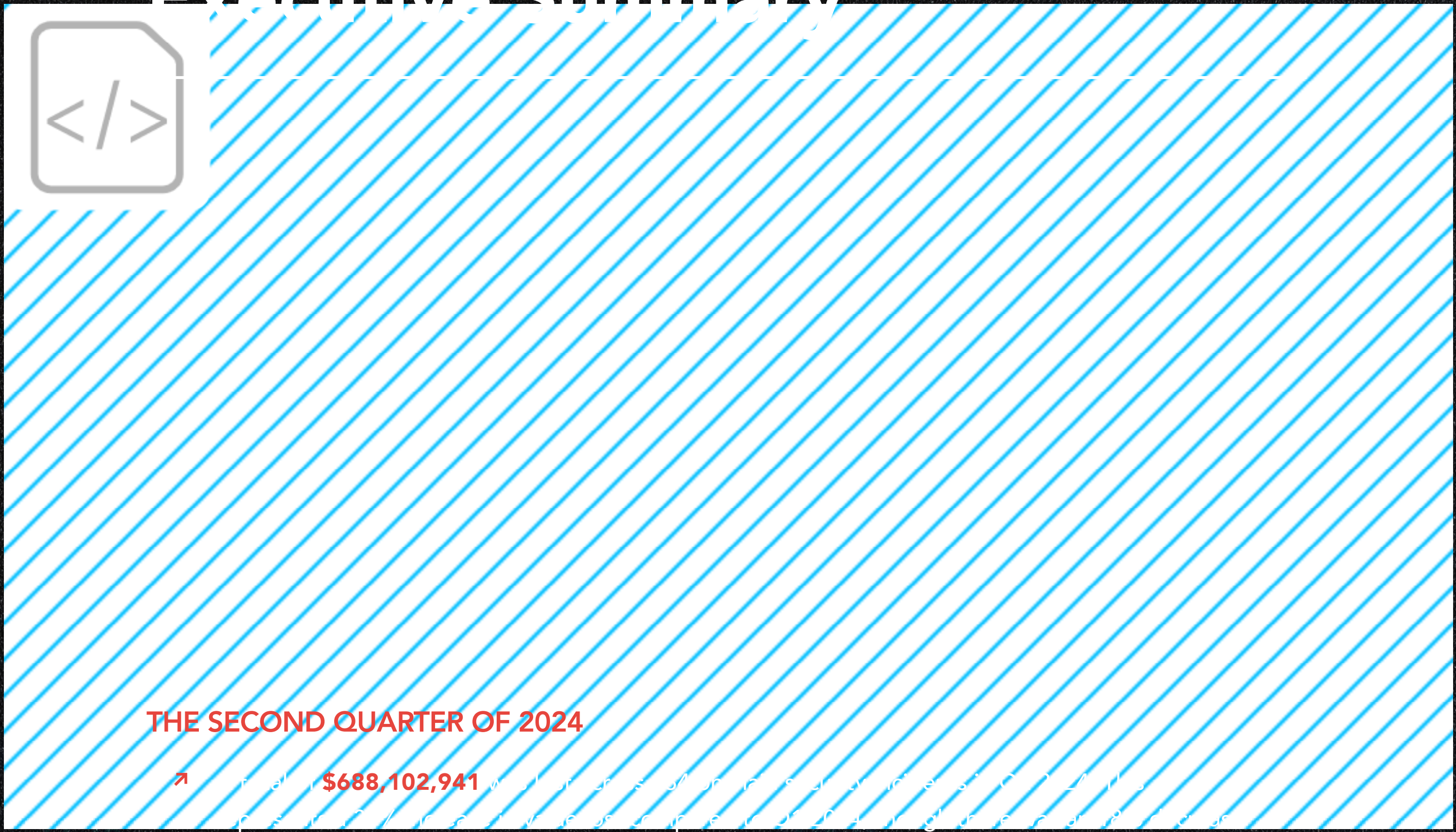
HACK3D

THE WEB3 SECURITY REPORT
Q2+H1 | 2024 EDITION

Securing the **Web3** World

Table of Contents

Executive Summary



THE SECOND QUARTER OF 2024

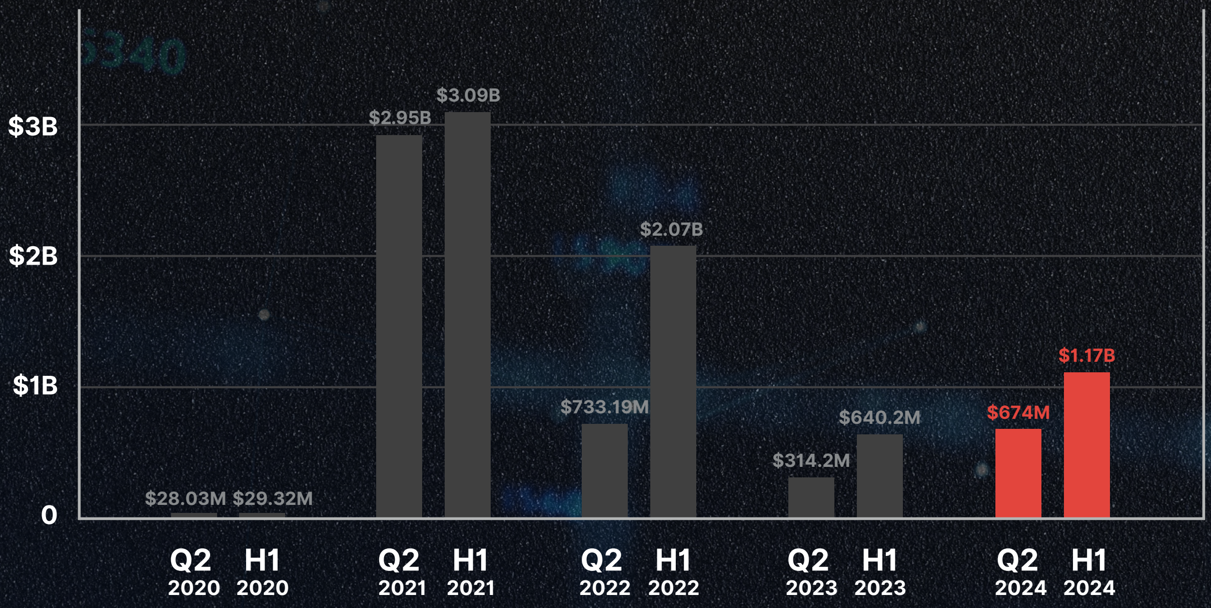
- [illegible] **$688,102,941** [illegible] in the number of incidents quarter-over-quarter.
- Phishing was the most costly attack vector in Q2 2024, with **$433,688,871** lost across 67 incidents, accounting for a large majority of total financial losses.
- Private key compromises followed, with **$170,064,635** lost in 16 major incidents.
- Ethereum experienced the highest number of security incidents, with a total of 83 hacks, scams, and exploits leading to **$170,636,798** in losses.
- The total dollar value of funds returned was $99,328,507 across 7 separate incidents, leading to adjusted total losses of **$588,774,434** for the quarter.
- The average loss per incident was **$3,739,689** and the median loss per incident was **$204,614**.

Executive Summary

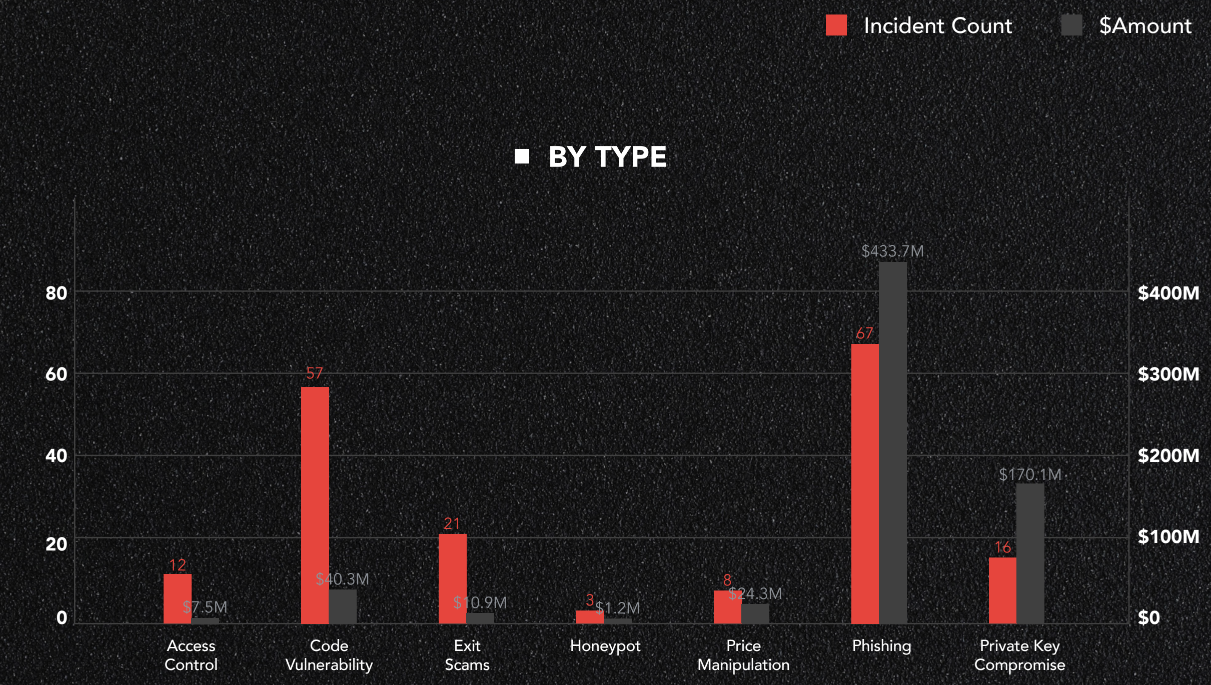
THE FIRST HALF OF 2024

- **$1,190,398,361** was lost across 408 onchain security incidents in H1 2024.
- Phishing accounted for **$497,735,904** lost across 150 incidents. Private key compromises followed, with **$408,949,115** lost in 42 incidents, highlighting persistent vulnerabilities in key management.
- Ethereum was the most affected chain, experiencing 235 incidents and **$397,405,773** in losses.
- The total value of funds returned in H1 2024 was **$177,791,389** across 18 incidents, leading to adjusted total losses of **$1,012,606,971** for the first half of 2024.
- The average loss per incident was **$2,932,729**, and the median loss per incident was **$230,784**.

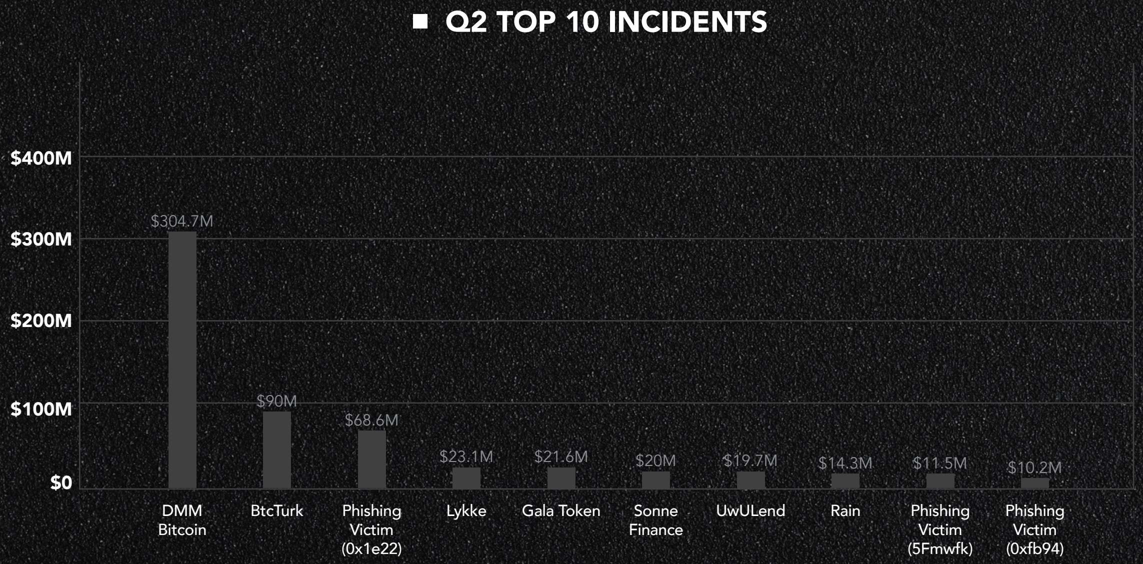
2020-2024 Stats Q2 vs H1



Q2 Statistics and Graphs

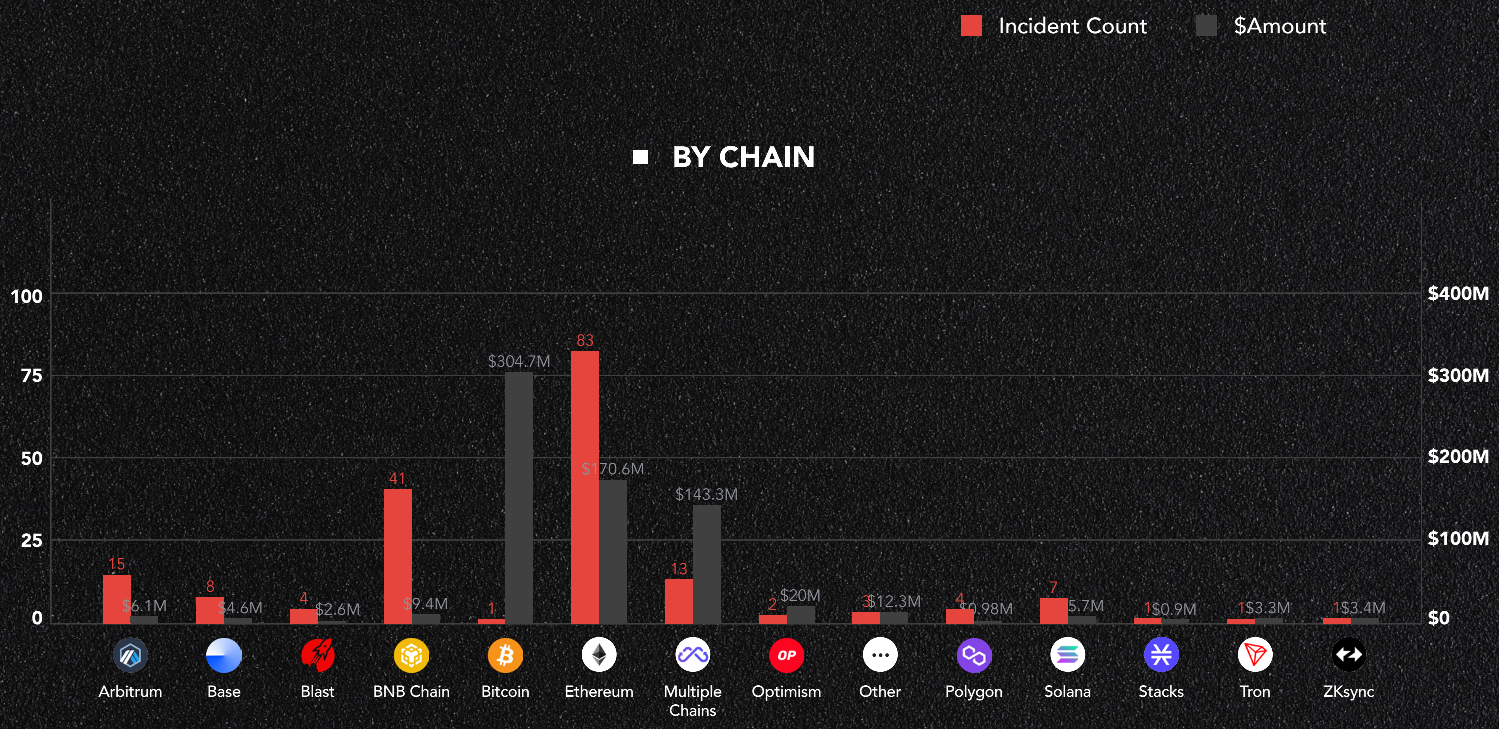


■ BY TYPE



■ Q2 TOP 10 INCIDENTS

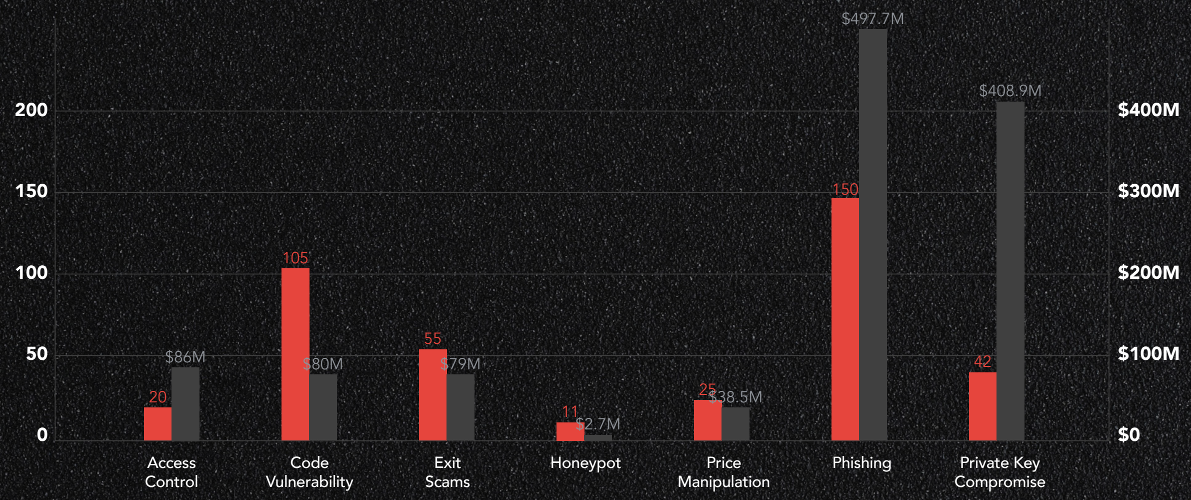
Q2 Statistics and Graphs



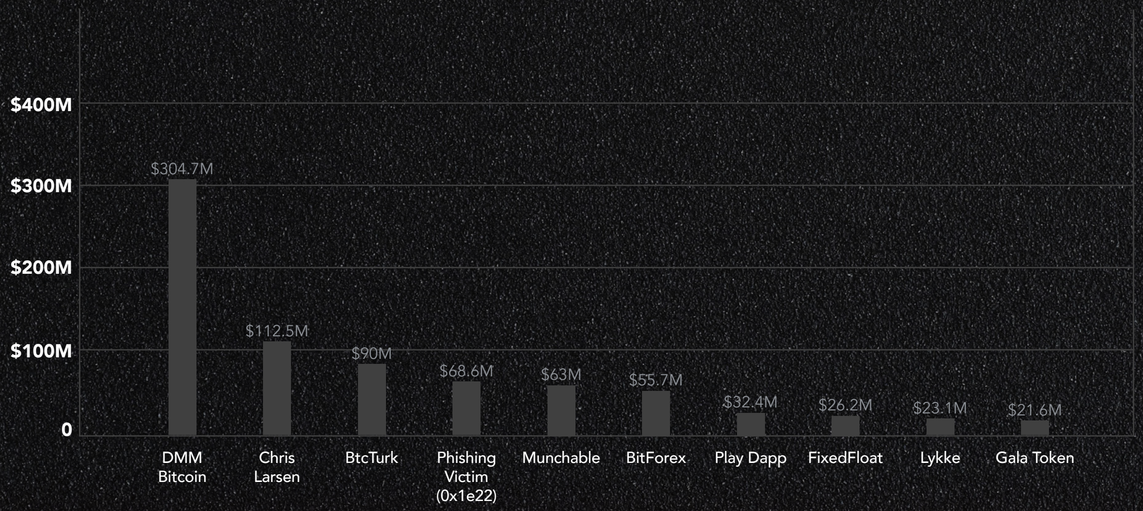
H1 Statistics and Graphs

🟥 Incident Count ⬛ $Amount

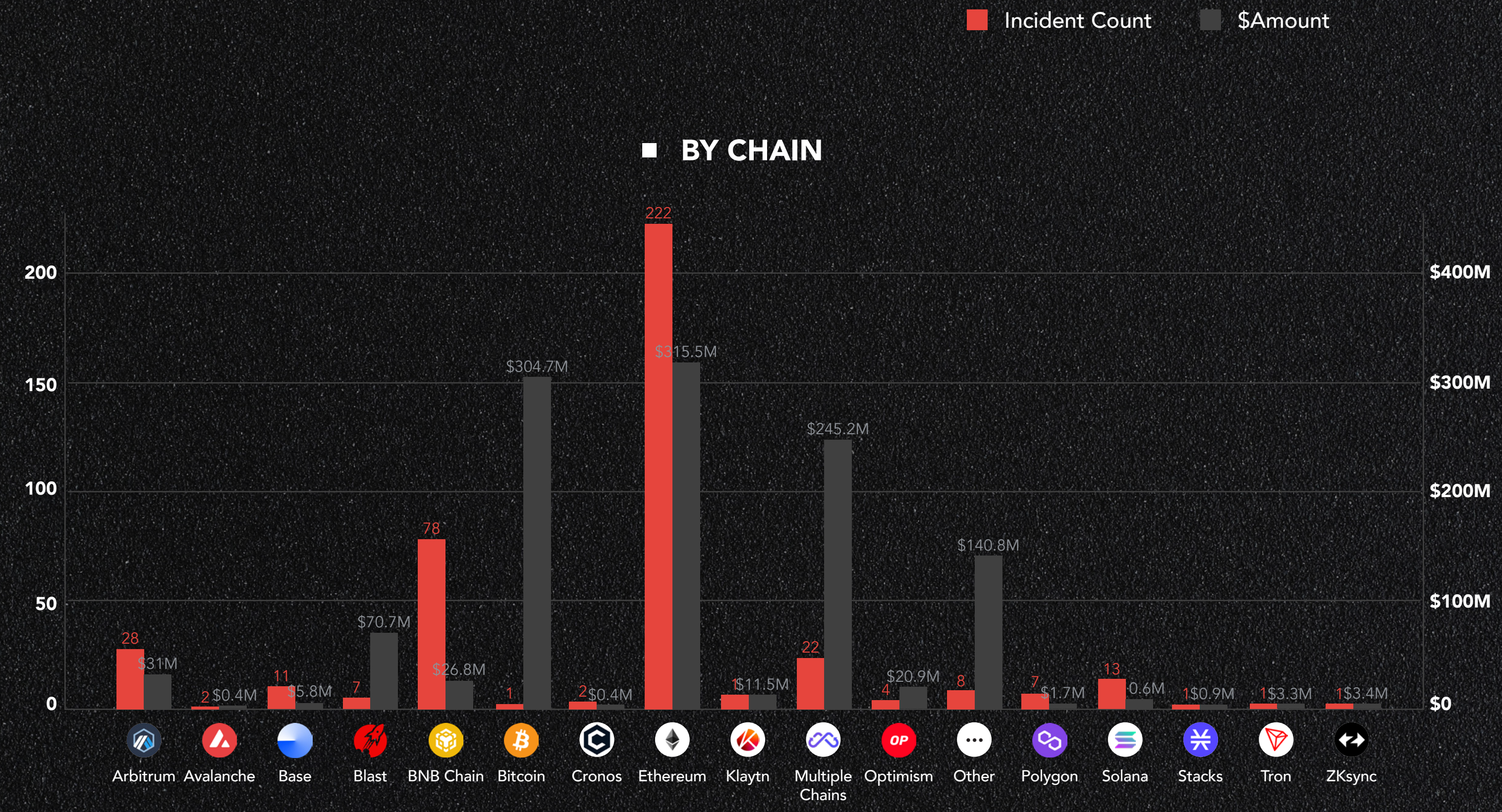
BY TYPE



Q2 TOP 10 INCIDENTS



H1 Statistics and Graphs



Statistics and Graphs

Q2

By Type:

Access Control: $7,543,696, 12 incidents

Code Vulnerability: $40,370,400, 57 incidents

Exit Scam: $10,882,389, 21 incidents

Honeypot: $1,245,668, 3 incidents

Price Manipulation/Flash Loan Attack: $24,307,282, 8 incidents

Phishing: $433,688,871, 67 incidents

Private Key Compromise: $170,064,635, 16 incidents

By Chain:

Arbitrum: $6,093,365, 15 incidents

Base: $4,627,015, 8 incidents

Blast: $2,622,362, 4 incidents

BNB Chain: $9,422,430, 41 incidents

Bitcoin: $304,700,000, 1 incident

Ethereum: $170,636,798, 83 incidents

Multiple Chains: $143,314,537, 13 incidents

Optimism: $20,020,500, 2 incidents

Other: $12,336,053, 3 incidents

Polygon: $983,667, 4 incidents

Solana: $5,724,740, 7 incidents

Stacks: $900,000, 1 incident

Tron: $3,334,128, 1 incident

ZKsync: $3,387,346, 1 incident

Q2 Top 10 Incidents:

DMM Bitcoin: $304,700,000

BtcTurk: $90,000,000

Phishing Victim (0x1e22): $68,597,540

Lykke: $23,052,860

Gala Token: $21,613,470

Sonne Finance: $20,000,000

UwULend: $19,700,000

Rain: $14,277,950

Phishing Victim (5Fmwfk): $11,522,660

Phishing Victim (0x2154): $10,167,780

The total dollar value of funds returned was **$99,328,507** across 7 separate incidents.

For Q2 2024, average loss per incident was **$3,739,689** and the median loss per incident was **$204,614**.

Statistics and Graphs

H1

By Type:

Access Control: $85,986,347, 20 incidents

Code Vulnerability: $80,038,332, 105 incidents

Exit Scam: $79,072,016, 55 incidents

Honeypot: $2,659,400, 11 incidents

Price Manipulation/Flash Loan Attack: $38,474,257, 25 incidents

Phishing: $497,735,904, 150 incidents

Private Key Compromise: $408,949,115, 42 incidents

By Chain:

Arbitrum: $30,951,358, 28 incidents

Avalanche: $443,700, 2 incidents

Base: $5,804,009, 11 incidents

Blast: $70,702,362, 7 incidents

BNB Chain: $26,770,097, 78 incidents

Bitcoin: $304,700,000, 1 incident

Cronos: $407,700, 2 incidents

Ethereum: $315,458,451, 222 incidents

Klaytn: $11,500,000, 1 incident

Multiple Chains: $245,170,194, 22 incidents

Optimism: $20,947,690, 4 incidents

Other: $140,848,393, 8 incidents

Polygon: $1,714,615, 7 incidents

Solana: $10,580,671, 13 incidents

Stacks: $900,000, 1 incident

Tron: $3,334,128, 1 incident

ZKsync: $3,387,346, 1 incident

H1 Top 10 Incidents:

DMM Bitcoin: $304,700,000

Chris Larsen: $112,500,000

BtcTurk: $90,000,000

Phishing Victim (0x1e22): $68,597,537

Munchable: $63,000,000

BitForex: $55,745,130

Play Dapp: $32,350,000

FixedFloat: $26,176,240 lost

Lykke: $23,052,860

Gala Token: $21,613,471

The average loss per incident in H1 was **$2,932,729**, and the median loss per incident was **$230,858**.

The total value of funds returned in H1 was **$177,728,142** across 17 incidents.

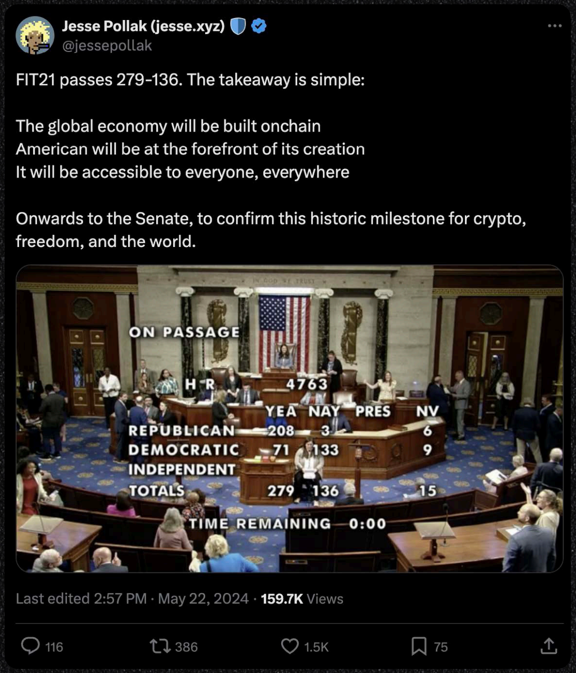
Overview

Q2 2024 saw the most losses since Q3 of last year, despite a relatively quiet quarter during which the markets mostly consolidated Q1's gains.

Bitcoin ranged within 20% of the new $73,737 all time high it put in on March 14, though only crossed the $72,000 threshold once in the quarter. The network's fourth halving proceeded without a hitch in April, and saw the block reward cut from 6.25 BTC to 3.125 BTC.

Big news came for Ethereum, with spot ETFs in the United States getting the green light from the SEC. These funds are all but guaranteed to start trading within the coming weeks, and analysts will have a close eye on how inflows stack up to those that the Bitcoin ETFs saw after they launched in January.

The passage of the FIT21 bill in the U.S. offers a better-defined future for digital assets in the United States. It received bipartisan support from Democrats and Republicans, and seemed to have been influenced by a late about-face from the executive branch. While certain sections of the bill received some criticism (notably its definition of "investment contract asset"), its passing was mostly welcomed in the crypto community.



Jesse Pollak (jesse.xyz)
@jessepollak

FIT21 passes 279-136. The takeaway is simple:

The global economy will be built onchain
American will be at the forefront of its creation
It will be accessible to everyone, everywhere

Onwards to the Senate, to confirm this historic milestone for crypto, freedom, and the world.

Last edited 2:57 PM · May 22, 2024 · 159.7K Views

116 386 1.5K 75

Source: @jessepollak

Still, the U.S. is playing catchup to some parts of the world, where the onchain industry is less bogged down in regulation. And the effects are being felt. According to a Coinbase report:

> The US continues to lose developer share, down 14 points in the past five years; only 26% of crypto developers are US-based today.
>
> – Coinbase, The Fortune 500 Moving Onchain

Both Bitcoin and Ether ETFs are currently trading in Hong Kong, and Dubai regulators recently eased certain restrictions that were deemed too stringent by market participants. While things are moving at a pace many in crypto are not used to, the direction is clear: with regulation comes institutional capital flows.

Platforms that want to take advantage of these flows will need to demonstrate their security and functionality under pressure. $674 million of losses across Q2 – and $1.17 billion in H1 – is not the most encouraging sign. Phishing incidents represented the majority of Q2 losses, which highlights the pain points still involved in safely transacting on public networks.

Other notable types of incidents in Q2 include code vulnerabilities, access control issues, and exit scams. Code vulnerabilities accounted for $37.37 million across 57 incidents, emphasizing the persistent challenge of securing smart contracts and decentralized applications. Access control failures, while fewer in number (11 incidents), still resulted in significant losses of $7.51 million. Exit scams, where project creators abscond with investor funds, led to $10.31 million in losses across 20 incidents, underscoring the ongoing risks in the DeFi space.

Price manipulation and flash loan attacks were particularly damaging, causing $44 million in losses over 13 incidents. These attacks exploit vulnerabilities in the DeFi ecosystem, manipulating token prices and draining liquidity pools. Private key compromises, another critical issue, resulted in $174 million in losses across 17 incidents, reflecting the importance of robust key management practices.

By chain, Ethereum remains the most targeted network, with 86 incidents resulting in $172 million in losses. BNB Chain followed, with 44 incidents totaling $12 million. Other chains, like Arbitrum and Avalanche, also saw significant losses, highlighting that security challenges are not confined to any single blockchain. Multi-chain incidents accounted for $143 million across 13 events, indicating the interconnected nature of the crypto ecosystem and the potential for cross-chain vulnerabilities.

In terms of individual incidents, the top 10 losses in Q2 were dominated by phishing attacks and platform breaches. The largest single incident was an attack on Japanese exchange DMM Bitcoin, resulting in a $304 million loss. Other significant breaches included BtcTurk ($90 million) and multiple high-value phishing victims.

Overall, Q2 2024 was marked by significant financial losses due to security breaches, emphasizing the ongoing challenges in the cryptocurrency and DeFi sectors. Phishing attacks and code vulnerabilities remain prevalent, with substantial losses impacting both individual users and large platforms.

The introduction of regulatory frameworks like the FIT21 bill in the U.S. and the approval of spot ETFs for Bitcoin and Ethereum indicate a maturing market, poised for increased institutional participation. However, the substantial losses experienced in Q2

Top 3 Incident Analyses

1. DMM BITCOIN: $304 MILLION

On May 31, 2024, DMM Bitcoin, a Japanese cryptocurrency exchange, confirmed it had been hacked, resulting in the theft of 4,502.9 BTC, valued at approximately $304 million. DMM Bitcoin detected the breach and took steps to prevent further thefts, including restricting certain services such as new account openings, cryptocurrency withdrawals, and new leveraged trading positions. The exchange assured customers that all Bitcoin deposits would be fully guaranteed, with support from its group companies to procure the equivalent amount of BTC lost.

2. BTCTURK: $90 MILLION

On June 22, 2024, BtcTurk, one of Turkey's largest cryptocurrency exchanges, experienced a major cyberattack targeting hot wallets containing ten different cryptocurrencies. The exchange halted all cryptocurrency deposits and withdrawals to mitigate the impact. BtcTurk assured users that cold wallets, where the majority of assets are stored, remain secure, and users' assets would not be affected. The attack caused a 10% drop in AVAX prices, as significant amounts of AVAX were moved to Coinbase and THORChain and sold off for Bitcoin. Binance is assisting with the investigation and has frozen over $5.3 million in stolen funds.

Binance CEO Richard Teng stated that their security teams are working around the clock to protect the ecosystem from bad actors and will provide further updates as more information becomes available.

3. PHISHING VICTIM (0X1E22): $68 MILLION

Private key compromises were the most damaging attack vector throughout 2023, resulting in nearly 48% of all losses despite representing just 6.3% of total security incidents. However, so far in 2024 we've seen phishing take over as the number one attack vector.

$484 million was lost to phishing attacks in H1 2024, compared to the $413 million lost to private key compromises. While there have been nearly three times more phishing attacks than private key compromises, this leapfrogging deserves closer attention.

Phishing Victim (0x1e22) represented the third-largest loss of Q2, when they fell prey to an address poisoning attack, resulting in the loss of approximately $68,597,540 in Wrapped Bitcoin (WBTC). The sequence began when the victim sent a small test transaction to a new wallet. Unbeknownst to them, an attacker known for address poisoning planted a similar-looking address in their wallet.

Consequently, the victim mistakenly transferred a substantial sum of 1,155.28802767 WBTC, equivalent to about $68 million, to the fraudulent address, believing it was their intended recipient.

In a surprising twist, the attacker returned the entire amount to the victim's address. The likely motivation behind this unexpected act of restitution was the attacker's IP address being leaked, possibly through a vulnerability in MetaMask's RPC.

In another unusual incident, phishing victim 0x2154 lost approximately 1,806 EtherFi (LQIDETH) tokens, worth $7,097,896. The attack was executed through address poisoning, leading the victim to send tokens to the wrong address. After the attack, the victim received 1,445 tokens back, reduced by Inferno's tax. Surprisingly, the attacker returned the entire amount to the victim's address, though the exact reason for this return remains unclear. The attacker’s identity might have been compromised, prompting the restitution.

Note that in our coverage of security incidents we prioritize counting the total amount lost, though we also provide statistics on the amounts returned. You can’t rely on an attacker returning your funds, and an incident where this happens still deserves to be included in the overall figures pertaining to value lost.

Others are not so lucky. These two incidents were the only two cases we identified of phishing victims seeing their lost funds returned, leaving $346,387,700 in the hands of scammers.

Further Reading

Below is a selection of the educational blogs and incident analyses we've put out over the course of Q2 as part of our mission to raise the standard of security, transparency, and education across the onchain ecosystem.

Blogs

↗ **FIT21 For Purpose: What the U.S. Congress's New Bill Means for Crypto Compliance**

The Financial Innovation and Technology for the 21st Century Act (FIT21) establishes a comprehensive regulatory framework for digital assets, distinguishing between securities, commodities, and other digital properties. The article highlights the bill's focus on enhancing consumer protections and supporting innovation in the U.S. cryptocurrency sector, providing readers with insights into the legislative changes and their implications for the industry

↗ **Advanced Formal Verification of ZKP: A Tale of Two Bugs**

Here we discuss the importance of formal verification (FV) in identifying and fixing vulnerabilities in zero-knowledge proofs (ZKP) systems. It highlights two specific bugs found during the audit of zkWasm, illustrating the challenges and methodologies involved in ensuring the security and correctness of ZK systems through both code and design verification.

↗ **Enhancing Stablecoin Operations with SkyInsights**

SkyInsights enhances stablecoin operations by offering advanced compliance and monitoring solutions. SkyInsights helps issuers tackle security, regulatory, and operational challenges, ensuring transparency and building trust among users and investors by integrating real-time transaction monitoring, risk assessment, and automated reporting features.

↗ **Advanced Sanctions Screening With SkyInsights**

SkyInsights' new Advanced Sanctions Screening Tool provides comprehensive, real-time compliance by integrating with global sanctions lists and offering broad blockchain coverage. This user-friendly tool features automated alerts, detailed reporting, and seamless integration with existing systems to help financial institutions, crypto exchanges, and compliance teams stay ahead of potential threats and maintain international regulatory compliance.

↗ **Tax-Free Fraud: Exposing the ZhongHua Scam**

We expose the ZhongHua scam, where attackers used complex tax function logic to hide transfer functions enabling a rug pull. By creating 9.99 trillion ZhongHua tokens, they drained the pool's liquidity, exploiting a balance check loophole in the token contract to facilitate fraudulent transfers.

↗ **SkyInsights: New Feature Releases Overview**

SkyInsights introduces a suite of new features designed to enhance blockchain security and compliance. The updates include an advanced compliance suite, sophisticated sanctions screening, and expanded blockchain support, providing users with comprehensive tools to ensure regulatory compliance and operational efficiency.

sCrypt: Nine Smart Contract Development Best Practices

We outline nine best practices for smart contract development, focusing on security and efficiency, covering essential tips like verifying transaction and data integrity, implementing proper authorization, and ensuring consistent token amounts to prevent double-spending. These practices help developers create robust and secure smart contracts on Bitcoin and other UTXO-based blockchains.

Advanced Formal Verification of Zero Knowledge Proof Blockchains

CertiK completed the first full formal verification of zkWasm circuits, ensuring that zero-knowledge proofs correspond correctly to smart contract executions. This formal verification process enhances the security and reliability of zkVMs, crucial for the next generation of blockchain applications.

Advanced Formal Verification of ZKP: Verifying a ZK Instruction

We discuss the formal verification of zero-knowledge proof (ZKP) virtual machines (zkVM), focusing on verifying the correctness of individual zk instructions. The detailed process ensures that each instruction, like the XOR operation, maintains the integrity of zkVM state transitions, thereby enhancing the security and reliability of zk-based smart contracts.

Beyond Chainalysis: Why VASPs Are Switching to SkyInsights for Crypto Compliance

SkyInsights offers a modern, cost-effective alternative to Chainalysis for crypto compliance, featuring advanced technology, broader blockchain coverage, and an intuitive interface. It provides superior data analysis and compliance tools, making it a strategic choice for businesses looking to reduce costs while enhancing security and regulatory adherence.

How to Build Trust and Demonstrate Integrity with KYC For Project Teams

Our KYC verification service helps Web3 projects build trust and demonstrate integrity by verifying the identities of core team members. This process includes comprehensive background checks, interviews, and ongoing assessments, ensuring transparency and security while protecting against insider threats and enhancing visibility.

Customized Formal Verification: The Five Step Process

Our custom formal verification service involves a five-step process to enhance the security of smart contracts by tailoring verification to each project's unique features. This process includes writing customized specifications, translating them into a verification language, interactive verification, triaging results, and continuous verification with each code revision.

Doubling Down on Security: Skynet Insight and Active Monitor

Skynet Insight and Active Monitor enhance security for crypto projects by providing accessible on-chain data analytics and real-time monitoring of critical assets like websites, smart contracts, and social media. These tools ensure continuous security assessment and transparency, enabling projects to monitor growth, detect threats, and maintain robust security post-audit.

↗ **What is FinCEN and Why Does It Matter?**

The Financial Crimes Enforcement Network (FinCEN) is a bureau of the U.S. Department of the Treasury that combats financial crimes, including money laundering and terrorism financing. FinCEN's recent proposal aims to regulate virtual currency mixing services, requiring crypto businesses to maintain detailed records and report suspicious transactions to enhance compliance and transparency in the financial system.

↗ **Crypto's Top Three Compliance Risks and How To Mitigate Them**

The top three compliance risks for the crypto industry include exposure to illicit activities, navigating international sanctions, and managing jurisdiction-dependent regulations. SkyInsights provides tools for real-time monitoring, risk scoring, and comprehensive compliance strategies to help businesses stay compliant and secure.

↗ **Decrypting MuskSwap: A Web of Scams and Tracking Funds Through Tornado Cash**

MuskSwap turned out to be an exit scam, resulting in significant financial losses for investors. After an initial surge, the token experienced massive drops, and subsequent delays and withdrawals indicated malicious intent. The scammers behind MuskSwap used a series of token launches and liquidity withdrawals to siphon funds, ultimately laundering approximately $3.5 million through Tornado Cash.

Incident Analyses

↗ **Normie Incident Analysis**

The Normie Incident involved a flash loan attack exploiting a vulnerability in the Normie contract on Base, causing a 99% drop in the token's value. The attacker gained 224 WETH (~$881,686) and has offered to return 90% under certain conditions. This highlights the risks of inheriting vulnerabilities from forked code and underscores the need for thorough audits and continuous monitoring.

↗ **Pike Finance Incident Analysis**

The Pike Finance incident involved two exploits resulting in a combined loss of nearly $2 million. The first exploit on April 26, 2024, leveraged a forged message, while the second exploit on April 30, 2024 exploited storage collisions in upgradeable contracts.

↗ **Alex Bridge Incident Analysis**

The Alex Bridge incident involved a $6.3 million loss due to a private key compromise, with assets transferred to malicious addresses on Binance Smart Chain and Stack BTC. A white hat rescue partially mitigated the impact, highlighting the risks of private key compromises and the importance of robust security measures.

↗ **Sonne Finance Incident Analysis**

The Sonne Finance incident involved a $20 million exploit due to a precision loss vulnerability. The attacker manipulated the exchange rate of the soVELO contract, allowing them to redeem large amounts of VELO tokens with minimal input.

↗ **Hedgey Finance Incident Analysis**

The Hedgey Finance incident resulted in a $2 million loss due to a vulnerability in the ClaimCampaigns contract. The attacker exploited the createLockedCampaign function to approve tokens and cancel campaigns without revoking approvals, allowing them to transfer tokens.

CertiK's Security Suite

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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