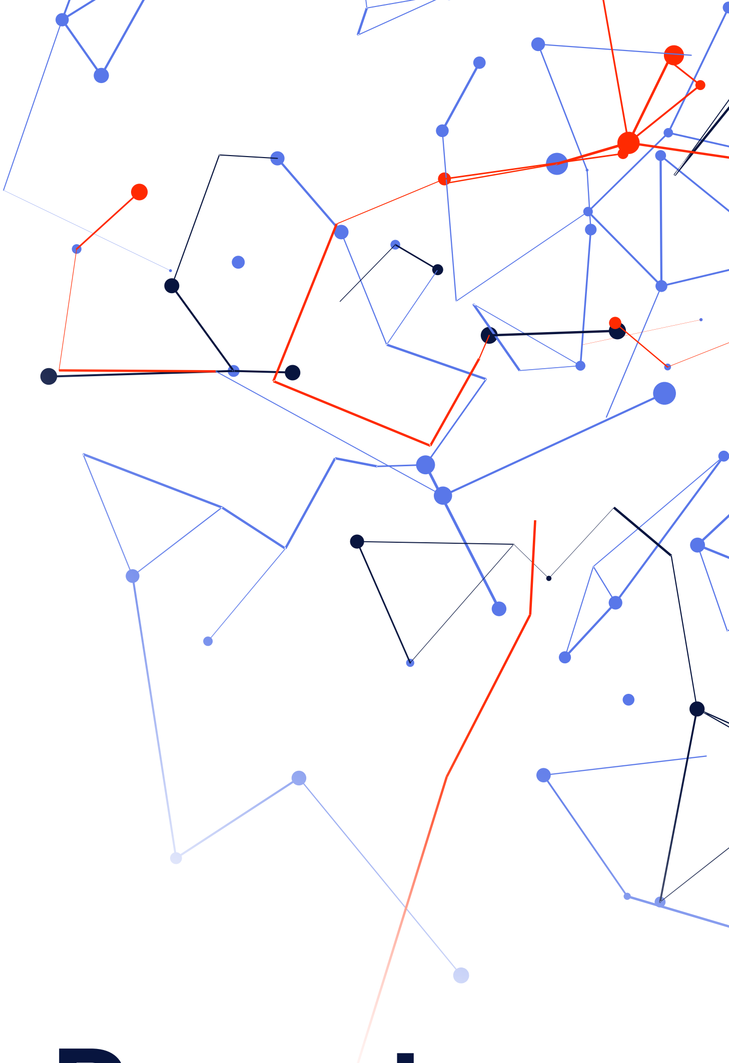
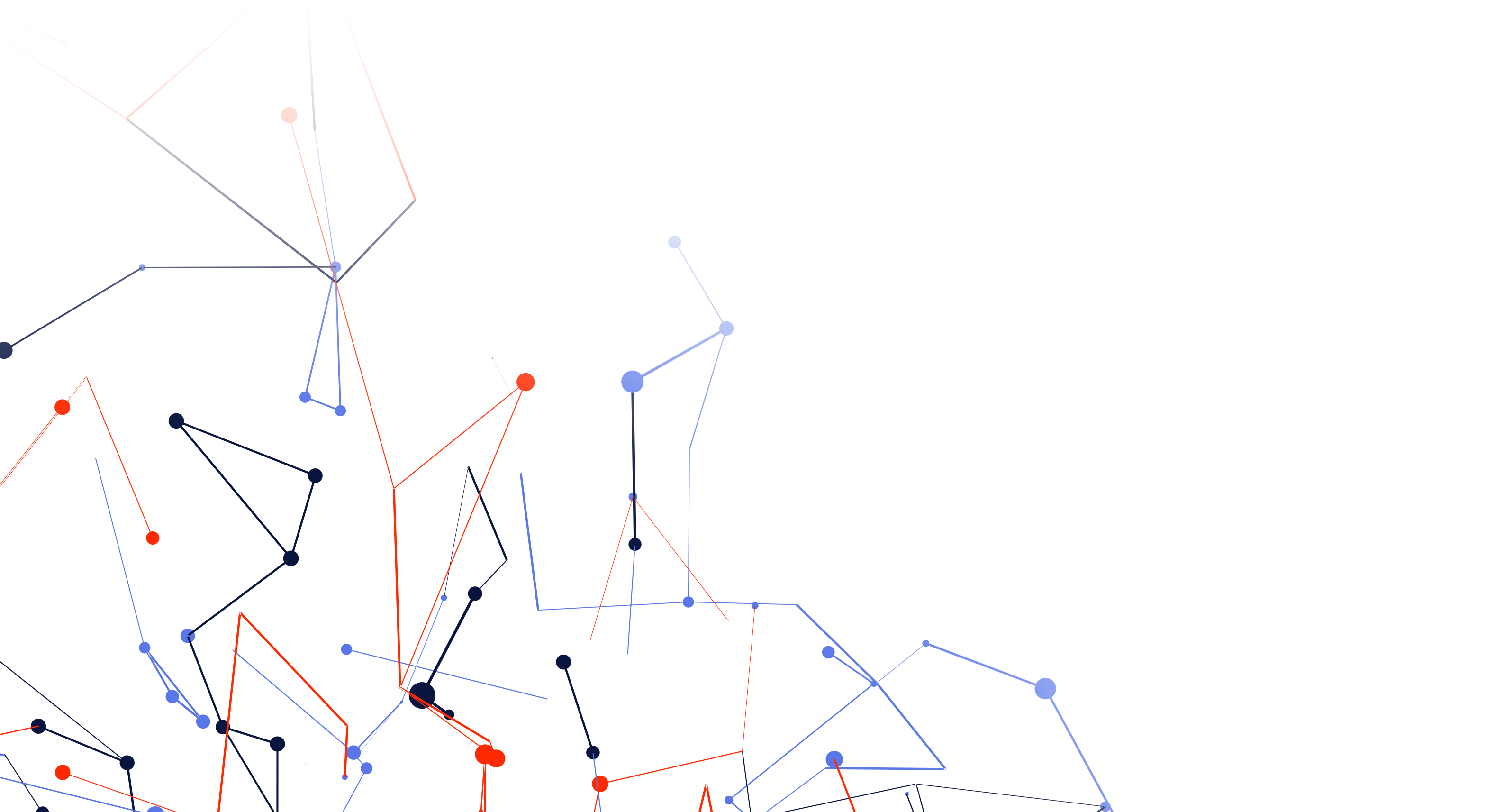
GLOBAL LEDGER



Crypto Hacks Report

Analytical Insight



Principal Takeaways

Total losses

2024: $1.94B

2 months of 2025: $1.89B

Most damaging attack method

Private key compromises: $930.08M, 48.03%

Most common attack type

Contract exploits: 116 incidents, 48%

Most targeted sectors

CEXs: $795M, 41.05%

DeFi platforms: $491.1M, 25.36%

Other: $650.4M, 33.59%

Laundering strategies

Mixers & privacy protocols: $763M, 39.4%

Wallets on CEXs & DEXs: $206.66M, 10.7%

Cross-chain protocols: $84.7M, 4.3%

CeFi vs. DeFi Losses

CeFi: $886.4M, 61.25% DeFi: $560.7M, 38.75%

Recovered

$155.53M, 8%

Foreword: Crypto Security in 2024 and the Turbulent Start of 2025

The cryptocurrency landscape in 2024 was marked by persistent security threats, with cybercriminals continuously adapting their methods to exploit vulnerabilities. From multi-million-dollar breaches of centralized exchanges to highly targeted attacks on DeFi platforms, the year underscored the evolving sophistication of blockchain-related crimes.

2025 started with an unprecedented security breach — the **$1.46 billion Bybit hack**, the largest in crypto history. This staggering incident, alongside a surge in early 2025 attacks, prompted us to reassess the state of blockchain security beyond the typical annual review.

This report presents a data-driven analysis of the most significant hacks in 2024, covering **265 recorded incidents** that resulted in total losses of **$1.94 billion**. Our analysis delves into key attack trends, targeted domains, laundering techniques, and recovery efforts. We employed **on-chain forensic tracking, transaction mapping, and entity clustering** to trace stolen assets and identify laundering pathways. Additionally, we examined . **cross-chain fund movements, mixer usage, and hacker wallet behaviours** to provide a comprehensive view of cybercriminal tactics.

Given the scale and impact of the Bybit breach, we extended our analysis to include a comparative perspective — contrasting the entirety of 2024 with the hacks of the first two months of 2025, where losses have already reached **$1.89 billion**.

By offering precise insights, we aim to empower industry stakeholders with actionable intelligence to bolster security measures and mitigate future risks.

Table of Contents

Principal Takeaways 2

Foreword: Crypto Security in 2024 and the Turbulent Start of 2025 3

1. Breakdown of 2024: Who Got Hit? 5

Sectors Most Targeted in 2024 5

Crypto Breach Breakdown: CeFi vs. DeFi Impact 6

2. Breakdown of 2024: How Were Victims Hacked? 7

Attack Methods Analysis 7

Key Lessons from 2024 Crypto Hacks 8

3. Largest Crypto Breaches of 2024: Top 25 by Losses 9

Breakdown of the 25 Largest Crypto Hacks 10

Biggest Crypto Heists Visualized 11

Which Tokens Were Hit the Hardest? 12

Where Did the Money Go? Tracing Laundered Funds 13

DMM Bitcoin. The Biggest Hack of 2024 Analysis 14

Q&A Overview 14

Money Laundering 15

4. Comparative Analysis of Hack Volumes in 2024 and 2025 16

Concluding Insights 17

Mitigation Strategies 17

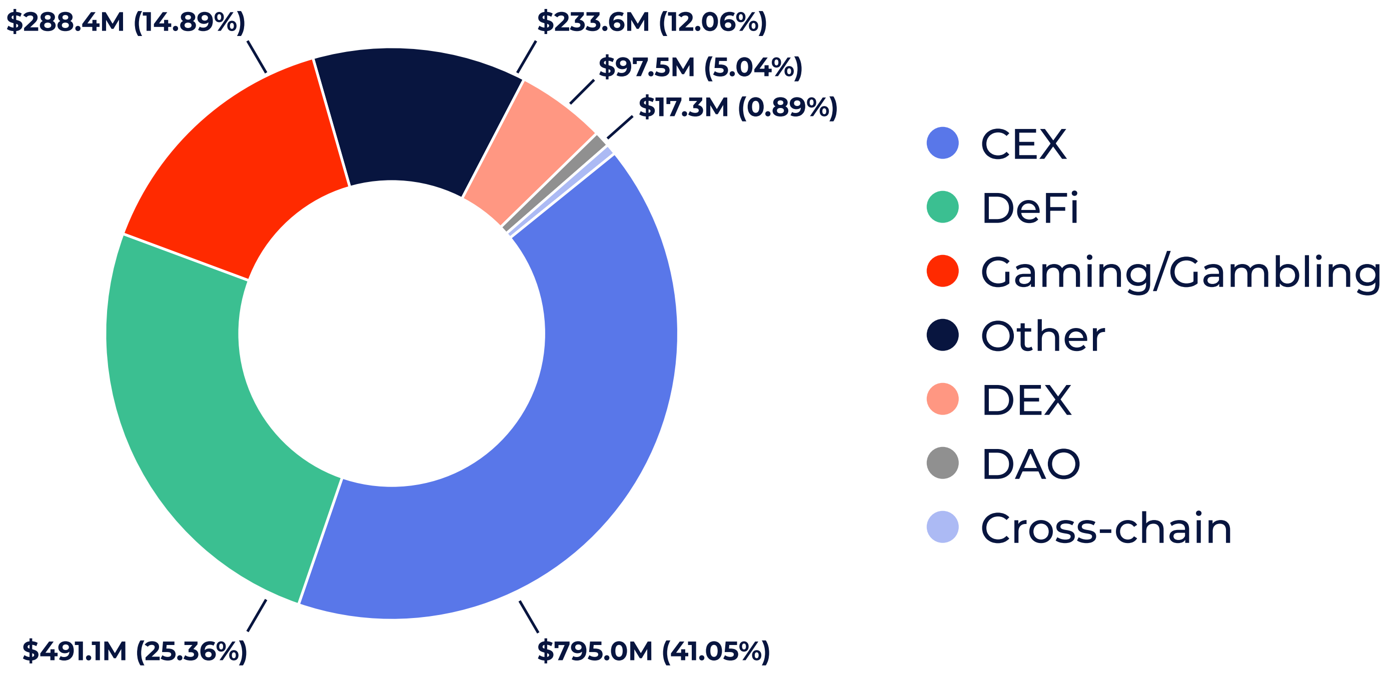
5. Conclusions 18

Breakdown of 2024. Who Got Hit?

Sectors Most Targeted in 2024

Let’s examine the most vulnerable sectors in 2024, uncovering where attacks were most concentrated and how various blockchain ecosystems were affected (Pic.1).

With $794.98 Million Stolen, CEXs Account for the Largest Share of Losses



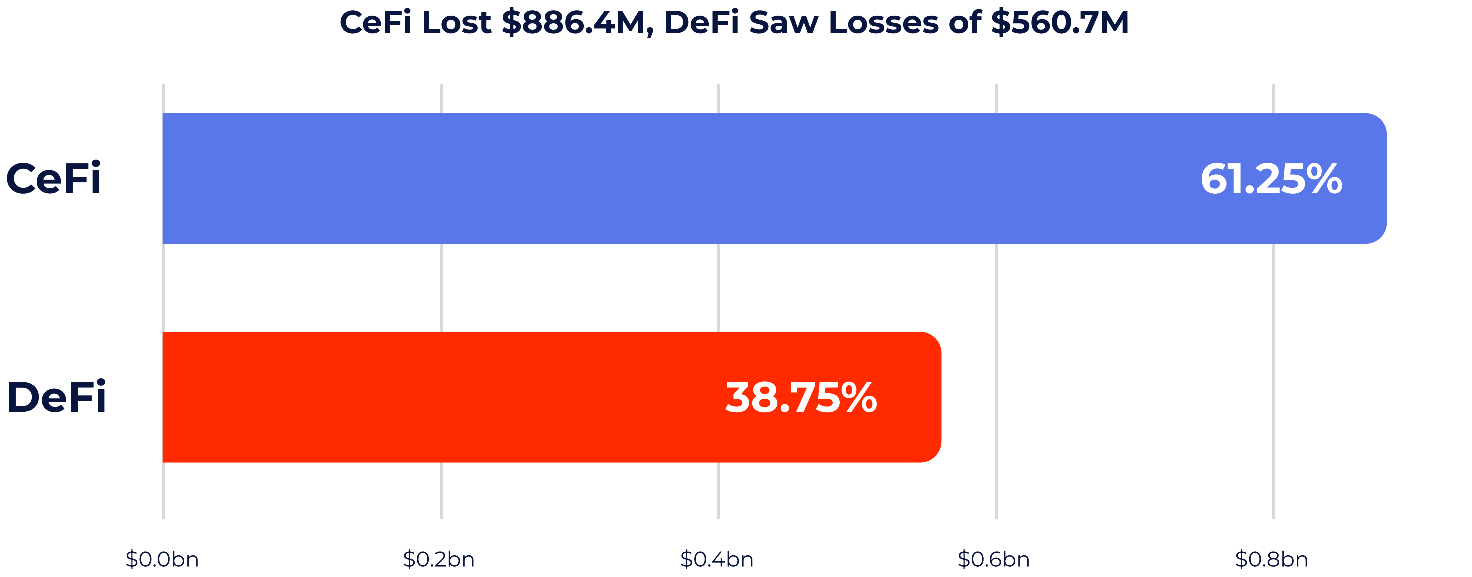
Pic.1. Visualisation of the most targeted sectors in 2024 hacks

- **Centralized Exchanges (CEXs):** With **$794.98 million (41.05%)** lost, CEX breaches accounted for the largest share, often involving hot wallet exploits.
- **DeFi Platforms:** Representing **$491 million (25.36% of total losses)**, DeFi projects remained a primary target due to vulnerabilities in smart contracts and decentralized structures.
- **Gaming/Gambling:** The sector incurred losses of **$288.37 million (14.89%)**, with attackers taking advantage of the increasing use of crypto in gaming environments.
- **Decentralized Exchanges (DEX):** Losses amounted to **$97.54 million (5.04%)**, with contract vulnerabilities as the primary attack vector.
- **DAOs:** Despite representing only **0.89%** of losses **($17.30 million)**, DAO exploits highlighted governance and operational vulnerabilities.

- **Cross-chain Protocols:** Incidents here targeted asset transfers between blockchains and led to **$13.59 million (0.70%)** in losses.
- **Other: $233.61 million (12.06%)** encompassed projects and incidents that do not fall under the other defined categories, including but not limited to blockchain solutions entities, incubators/launchpads, personal wallets, etc.

Crypto Breach Breakdown: CeFi vs. DeFi Impact

In crypto security, not all breaches are created equal. CeFi and DeFi operate on fundamentally different principles, which also means they face distinct security challenges. While CeFi hacks typically exploit centralized points of failure, DeFi attacks often target smart contract vulnerabilities and governance loopholes. Analysing their distribution helps refine security strategies, ensuring better protection for both sectors (Pic. 2).



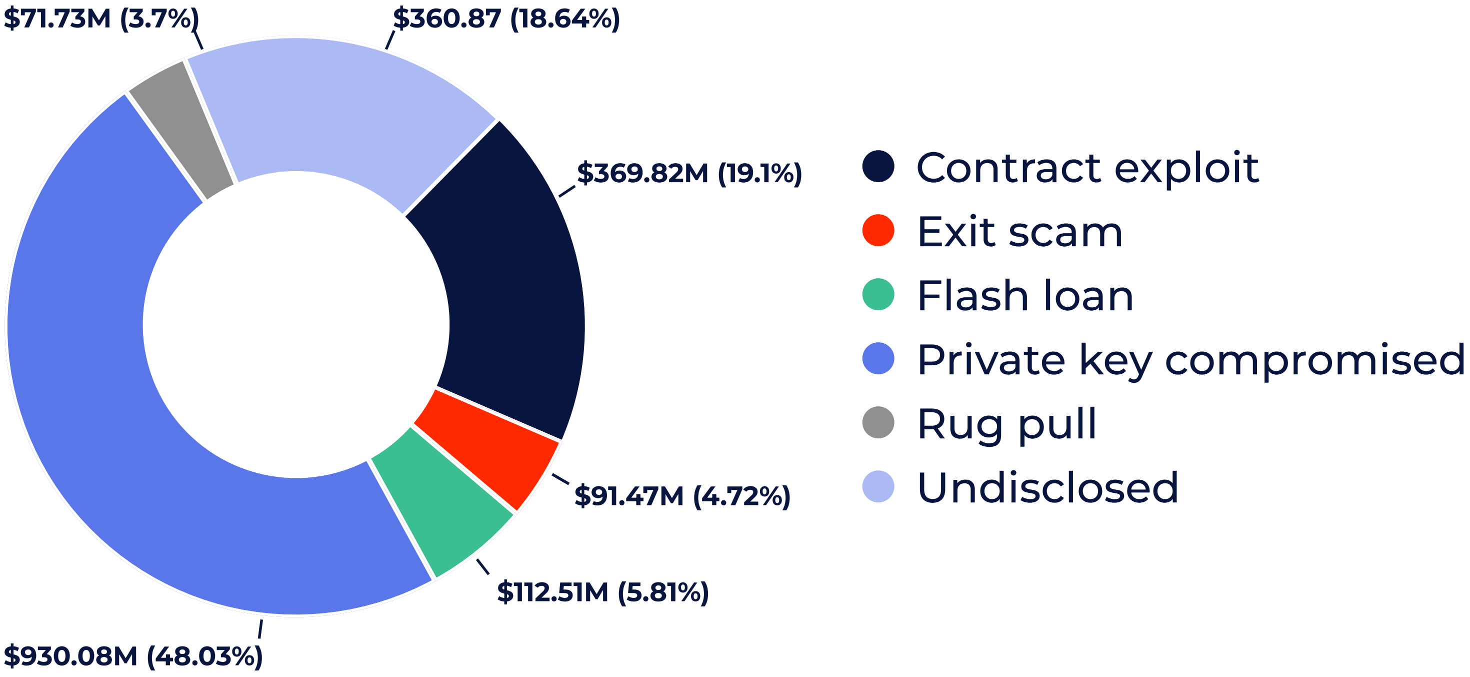
Pic. 2. Visualisation of stolen funds distribution between CeFi and DeFi in 2024 hacking incidents

Our data shows that CeFi continues to bear the brunt of crypto-related losses, accounting for **61.25% ($886.4M)** across **15 incidents**. In contrast, DeFi saw **111 hacks** totaling **$560.7M (38.75%)**, highlighting a significant disparity in security outcomes between the two sectors.

Breakdown of 2024. How Were Victims Hacked?

The methods employed by hackers in 2024 varied significantly, but certain attack vectors proved to be particularly damaging. The dominance of private key compromises, along with the high frequency of contract exploits, underscores the importance of securing both user credentials and smart contract infrastructure (Pic.3).

Private Key Compromises Caused the Biggest Losses: $930M



Pic. 3. Visualisation of the most popular hack types in 2024

Attack Methods Breakdown

- **Private key compromises (48.03%, $930M):** The largest cause of losses, where attackers gain unauthorized access to private keys, allowing them to drain funds from wallets or accounts.
- **Contract exploits (19.1%, $369.8M):** Vulnerabilities in smart contracts are exploited to manipulate or drain funds, often due to coding flaws.
- **Undisclosed reasons (18.64%, $360.8M):** Incidents where the exact method of attack remains unknown or unreported by the affected entities.

- **Flash loans (5.81%, $112.5M):** Attackers exploit uncollateralized loans to manipulate prices, drain liquidity, or execute complex arbitrage attacks.
- **Exit scams (4.72%, $91.5M):** Fraudulent projects or individuals abruptly disappear with users' funds, often after building trust.
- **Rug pulls (3.7%, $71.7M):** A form of exit scam where developers abandon a project and withdraw liquidity, leaving investors with worthless tokens.

Key Lessons from 2024 Crypto Hacks

- **Centralization Risks Persist** – despite the rise of decentralized solutions, **CeFi platforms lost nearly twice as much as DeFi**, showing that centralized services remain prime targets due to their hot wallet vulnerabilities and custody risks.
- **Hacks Are Becoming More Sophisticated, Not Just More Frequent** – While contract exploits were the most common, private key compromises caused the most damage. This suggests that attackers are **moving beyond technical vulnerabilities and targeting core security flaws in custody and key management.**
- **The Rise of Social Engineering in Crypto Heists** – Beyond technical exploits, attackers are increasingly leveraging social engineering tactics to gain access to private keys and critical infrastructure. This trend underscores the **need for heightened security awareness training** within organizations.
- **The Need for On-Chain Insurance and Incident Response** – With $1.94 billion lost, the lack of effective crypto-native insurance solutions is glaring. To mitigate future losses, the industry must invest in real-time security monitoring and on-chain recovery mechanisms.

Largest Crypto Breaches of 2024:
Top 25 by Losses

A few incidents accounted for the vast majority of losses in 2024. Despite 265 recorded hacks*, just 25 major breaches were responsible for over $1.45 billion in stolen funds — nearly 75% of the total $1.94 billion lost throughout the year. This highlights a critical pattern: high-impact attacks on centralized services and major DeFi protocols continue to dominate the landscape.

By examining these incidents, we can better understand:

- **Where attackers struck the hardest**
- **Which platforms suffered the biggest losses**
- **What security flaws led to the most devastating breaches**

That's why we decided to take a closer look at these 25 hacks. By analyzing the most significant breaches in detail, we can better understand attack patterns, common vulnerabilities, and the shifting tactics of cybercriminals.

Let's take a look at the full breakdown.

*For clarity, we excluded scams like phishing, Ponzi schemes, fake investment platforms, etc., concentrating solely on direct asset compromises that impact blockchain networks.

Breakdown of the 25 Largest Crypto Hacks

This section provides an in-depth look at the top 25 hacks of 2024, detailing affected entities, their types, and financial losses (Table 1).

Hacked Entity	Public Report	Entity Type	Total Loss, USD	Date
DMM Bitcoin	Link	CEX	305,000,000	31/05/2024
WazirX	Link	CEX	230,000,000	18/07/2024
Gala Games	Link	Gaming	215,500,000	20/05/2024
Ripple Co-Founder Chris Larsen	Link	Personal Wallet	108,670,167	30/01/2024
Munchables	Link	DeFi	62,500,000	27/03/2024
Radiant Capital	Link	DeFi	58,000,000	16/10/2024
Crypto Whale	Link	Personal Wallet	55,473,618	21/08/2024
BtcTurk	Link	CEX	55,000,000	22/06/2024
BingX	Link	CEX	44,715,733	20/09/2024
Penpie	Link	DeFi	30,000,000	03/09/2024
DEXX	Link	DEX	30,000,000	16/11/2024
FixedFloat	Link	CEX	26,105,134	16/02/2024
Thala	Link	DEX	25,500,000	15/11/2024
Indodax	Link	CEX	22,000,000	11/09/2024
Lykke	Link	CEX	22,000,000	04/06/2024
Sonne Finance	Link	DeFi	20,868,543	15/05/2024
U.S. Government-Controlled Wallet	Link	Government	20,587,241	25/10/2024
Curio Ecosystem	Link	DeFi	16,967,000	23/03/2024
Gamee	Link	Gaming	16,308,000	22/01/2024
Rain	Link	CEX	14,800,000	29/04/2024

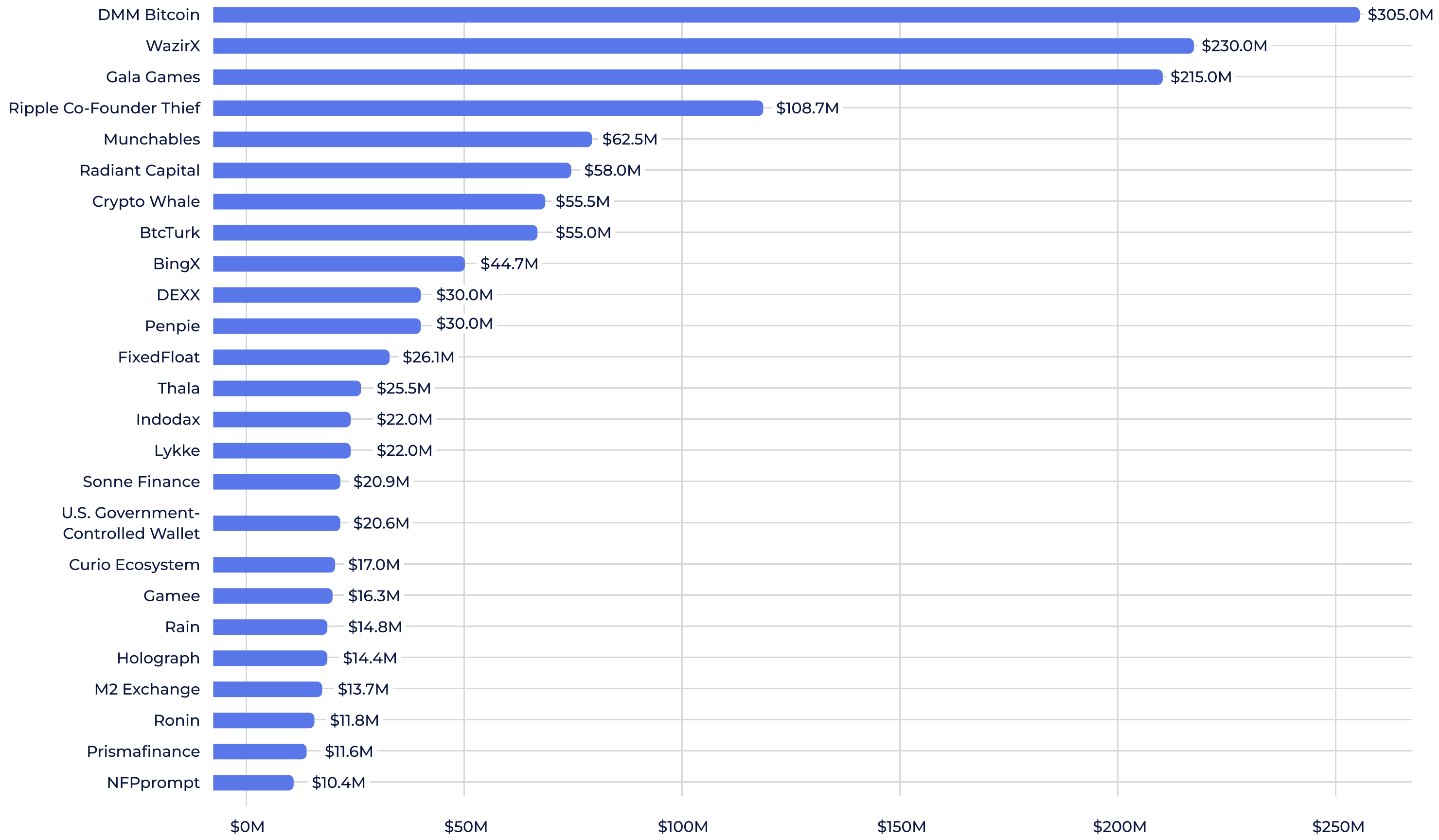
Hacked Entity	Public Report	Entity Type	Total Loss, USD	Date
Holograph	Link	DeFi	14,400,000	13/06/2024
M2	Link	CEX	13,667,846	31/10/2024
Ronin	Link	Cross-chain protocol	11,794,313	06/08/2024
Prismafinance	Link	DeFi	11,600,000	28/03/2024
NFPrompt	Link	NFT project	10,400,000	15/03/2024

Table 1. Key details of the 25 largest hacks of 2024

Biggest Crypto Heists Visualized

The graph below offers a **concise breakdown of the largest hacks**, highlighting stolen amounts and affected entities. While centralized exchanges remained prime targets, DeFi platforms, gaming projects, and even government-controlled wallets were also heavily impacted (Pic. 4).

DMM Bitcoin Hack Is The Largest in 2024, with $305M Stolen



Pic. 4.Visualization of the 25 largest 2024 hacks by USD losses

Targeted blockchains include (in alphabetical order): **APT, ARB, AVAX, BASE, BCH, BLAST, BNB, BOBA, BSC, BTC, ETH, FTM, LTC, OP, POLYGON, SKALE, SOL, TRON, and XRP.**

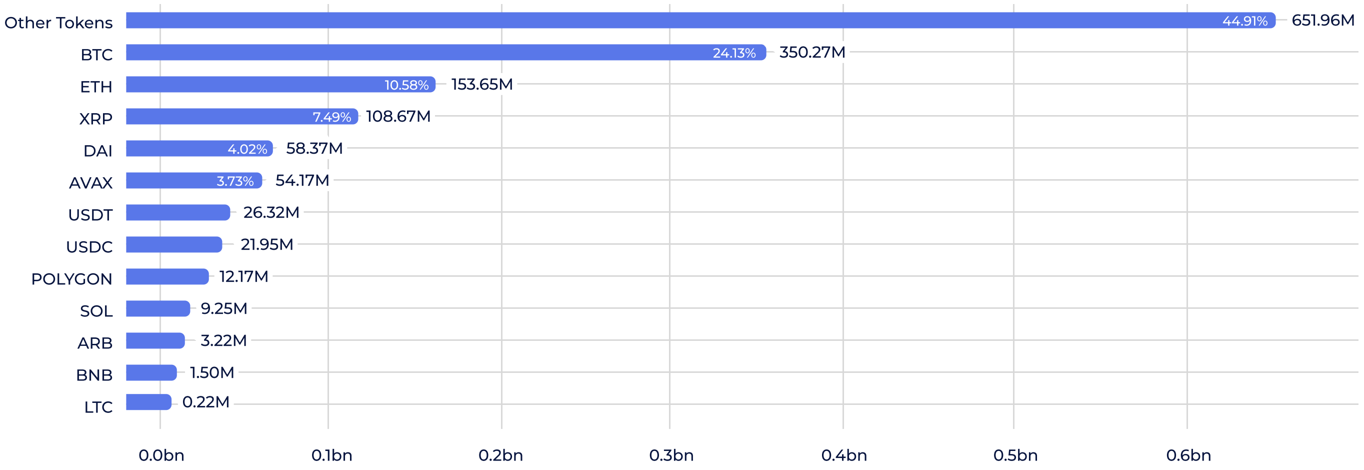
Which Tokens Were Hit the Hardest?

Bitcoin continues to play a dominant role in crypto crime, accounting for **$350.27M** or **24.13%** of total stolen value. However, **Ethereum** and stablecoins like **USDT, USDC,** and **DAI** are also major targets due to their widespread use in DeFi and cross-chain transactions.

Despite representing a smaller share of hacks, **stablecoins stay at the center of attention** — not just for regulators and users but also for hackers. Their liquidity and stability make them a preferred asset for laundering, and attackers often **swap stolen funds into stablecoins instantly** to mitigate volatility and facilitate cross-chain movement.

The following graph highlights the distribution of stolen funds across different tokens (Pic. 5).

BTC, ETH, XRP Among Top Hacked Assets



Pic. 5. Visualization of top tokens stolen in the 25 major hacks of 2024 by USD amount

Where Did the Money Go? Tracing Laundered Funds

Of all traced and identified funds these are the most common destinations:

Mixers & Privacy Protocols: $763.48M was funneled through services like Tornado Cash, Wasabi wallets, private mixers, coin joins, and platforms such as eXch and Railgun.

Transferred to Exchanges: $206.66M ended up in centralized and decentralized exchanges.

Cross-Chain Transfers: At least $84.7M was moved across chains using protocols like Across, Stargate Finance, Synapse, Hop, THORChain, Mayan Finance, Circle CCTP, Wormhole, Celer Network, and LayerZero.

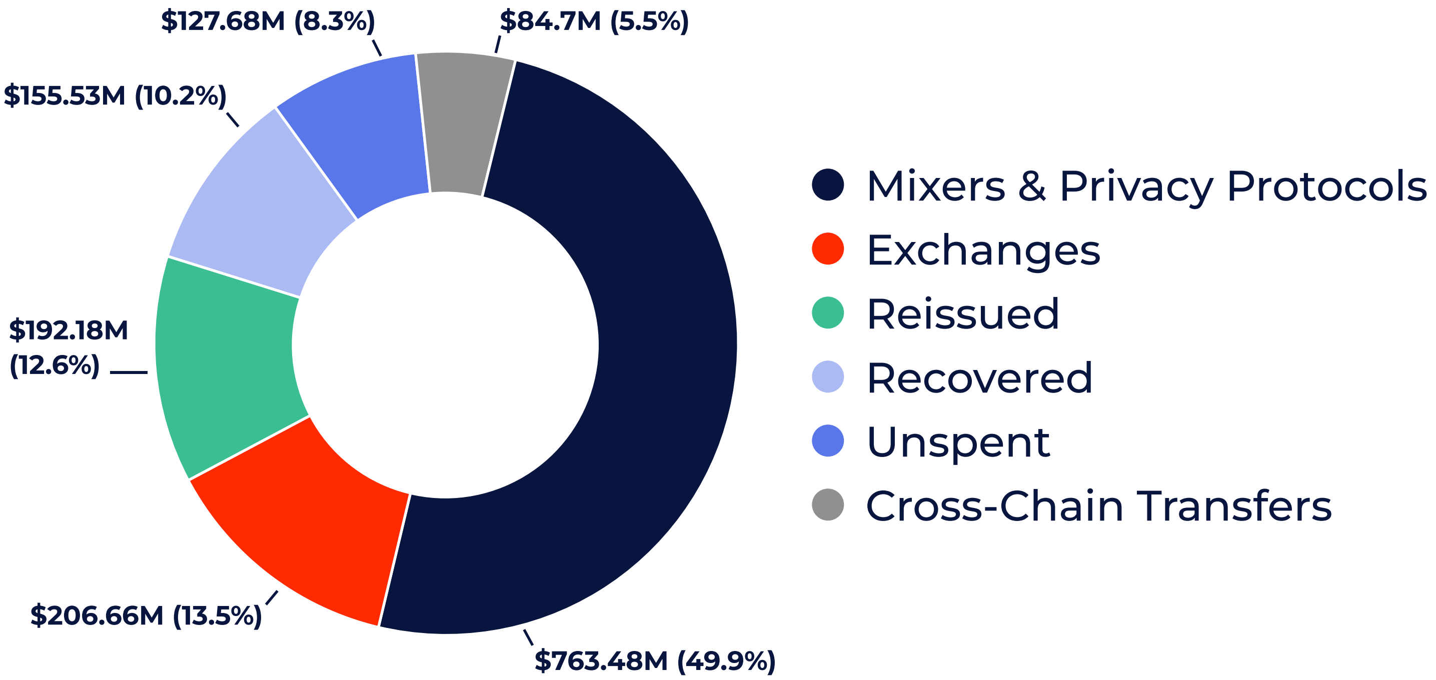
Reissued Funds: $192.18M was burned as part of Tether's contingency measures and subsequently reissued.

Recovered Funds: $155.53M was returned by hackers, either through negotiated bounties or in full. Notably, three hacks led to full restitution:

- **Munchables DeFi Draining Exploit (Mar 2024)**
- **Ronin Bridge Exploit (Aug 2024)**
- **Thala DEX Exploit (Nov 2024) with $300,000 bounty negotiated.**

Unspent Funds: $127.68M remained idle in hacker wallets at the time of research (Pic. 6).

~ 50% Stolen Funds Funnelled Trough Mixers and Privacy Protocols



Pic. 6. Top destinations of stolen funds from the 25 largest hacks of 2024

DMM Bitcoin. The Biggest Hack of 2024 Analysis

In 2024, the cryptocurrency sector witnessed its largest security breach with the DMM Bitcoin hack, resulting in significant financial losses and raising concerns about the industry's vulnerability to sophisticated cyber attacks.

Q&A Overview

When? The breach took place on May 31, 2024, at 05:12 UTC.

How much? The attackers successfully stole **4,502.9 BTC**, valued at approximately $305M at the time of the theft. The breach exclusively involved the Bitcoin blockchain.

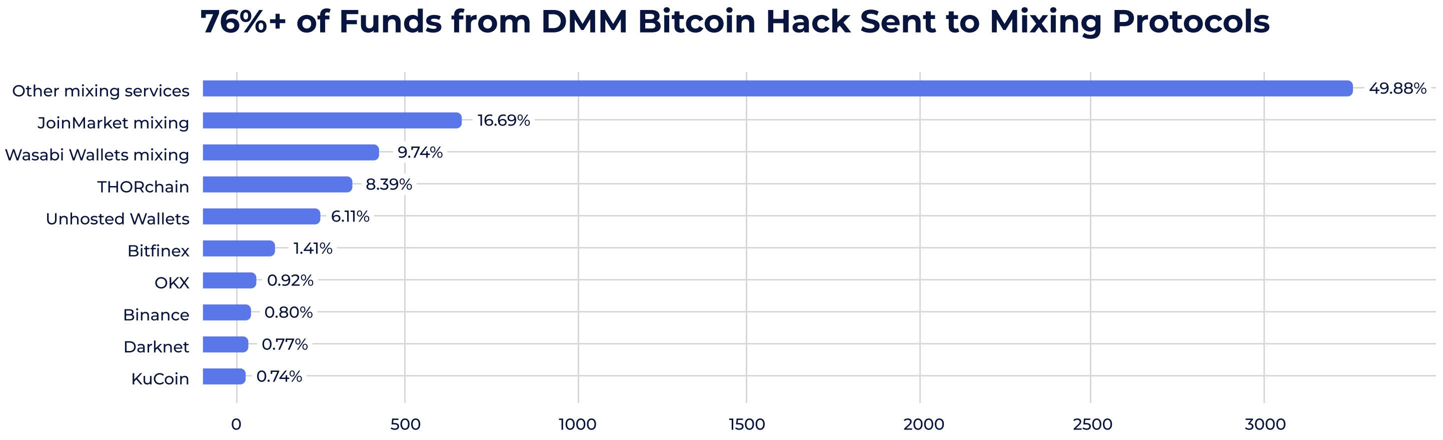
How? Although DMM confirmed the hack, it never disclosed specific details about the vulnerability that caused the security breach. As per FBI report: In March 2024, a North Korean hacker posing as a LinkedIn recruiter targeted a Ginco employee, sending a **malicious Python script disguised as a test**. The victim uploaded it to GitHub, leading to a breach. By May, attackers used session cookies to impersonate the employee, access Ginco’s communications, and later manipulate a DMM transaction.

Who? According to the same FBI report, the hack was attributed to the North Korean cyber group TraderTraitor, also known as Jade Sleet, UNC4899, and Slow Pisces. This group is notorious for employing targeted social engineering tactics to infiltrate cryptocurrency platforms.

Money Laundering

The stolen **4,502.9 BTC** was swiftly moved across various laundering channels to obscure its origins. Typically, such large sums are not directed towards mixing protocols all at once due to the natural processing limitations of mixing protocol pools and the higher risk of unwanted attention and possible blocks of funds.

Given this, we conducted our own detailed **counterparty analysis** to track where the funds were actually dispersed, uncovering additional laundering tactics beyond conventional mixing services (Pic. 7).



Pic. 7. Top 10 counterparties of the DMM Bitcoin hacker

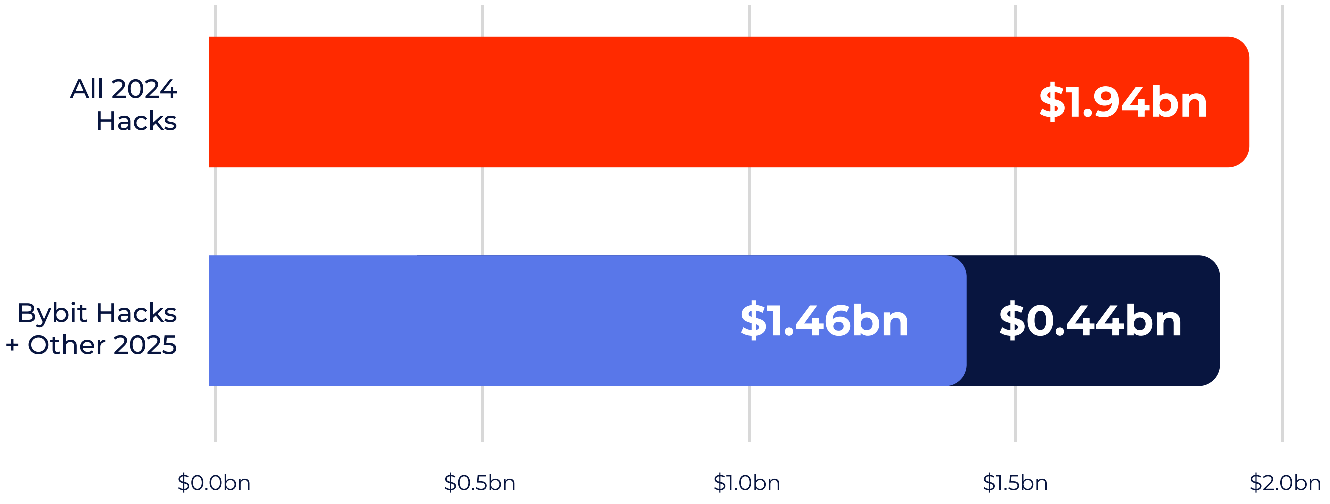
- At least **76.31% (~3437 BTC)** flowed into different **mixing protocols**, both private and public, to break transaction traces and hinder law enforcement tracking.
- **8.39% (~377 BTC**) was **cross-chained** via THORchain and a relatively smaller amount **(0.46% or ~21 BTC)** via Avalanche Bridge.
- **5.7% (~253 BTC)** of the identified stolen funds were eventually sent to regulated entities.
- Notably, laundering efforts **continue to this day,** over **10 months after the initial theft**, demonstrating the hackers’ calculated and patient approach to offloading illicit funds.

Comparative Analysis of Hack Volumes in 2024 and 2025

In 2024, $1.94 billion was stolen in cryptocurrency hacks. However, just the **first two months of 2025** have already seen $1.89 billion in stolen funds — nearly matching the total volume of 2024 (Pic. 8). This surge is largely due to the **$1.46 billion** Bybit hack, the largest in cryptocurrency industry history, believed to be orchestrated by Lazarus, a North Korean hacker group.

The graph compares the total stolen in 2024 with the Bybit hack and other recorded hacks in January and February 2025, highlighting the increased scale and concentration of cyberattacks. This trend points to a shift toward larger, more targeted attacks in 2025, particularly by groups like Lazarus.

Two Months of 2025 Crypto Thefts Already Exceed 97% of 2024 Total



Pic. 8. Visualization comparing total funds lost in 2024 and the first two months of 2025

Concluding insights

- **DPRK's State-supported Hacker Groups:** Believed to be responsible for at least $659.7M in stolen funds from just five major hacks, all ranked among the top 20 crypto incidents of 2024.
- **Mixing Services:** 18 of the 26 hacks (69%) involved mixing techniques, with 13 utilizing the notorious Tornado Cash service.
- **Cross-Chain Laundering:** 14 out of 26 hacks (54%) used cross-chain protocols to launder funds, including six incidents involving THORChain and five using Stargate Finance.
- **Stablecoin Targets:** USDT, USDC, and DAI collectively represented 7.34% of the total initial hacker targets.
- **Challenges for Hackers:** Issuers can **freeze or blacklist** stablecoins, making them riskier to hold. While hackers use them for quick laundering, they primarily target decentralized assets to avoid traceability.

Mitigation Strategies

To address these persistent threats, Global Ledger recommends:

- **Comprehensive Security Audits:** Regular and rigorous contract audits for DeFi platforms.
- **Enhanced Key Management:** Adoption of hardware security modules and multi-signature wallets.
- **Collaborative Efforts:** Industry-wide cooperation to track stolen funds and develop preventive measures.

Conclusions

Crypto hacks totaled **$1.94B** in **2024**, but just **two months into 2025**, losses have already reached **$1.89B** — driven by the record-breaking $1.46B Bybit hack. This marks a shift toward larger, more coordinated attacks, particularly from state-backed groups like Lazarus, reinforcing CeFi as the primary target.

Laundering methods such as **mixers and cross-chain protocols** remained prevalent in 2024, complicating asset recovery. While $155.53M (8%) of stolen funds were retrieved last year, large-scale breaches like Bybit present new challenges for tracking and enforcement.

As attacks escalate, strengthening security protocols, enhancing industry collaboration, and advancing threat intelligence are critical to mitigating future risks.

Global Ledger remains committed to providing actionable insights and supporting efforts to combat crypto-related crime.