2014-2024 COMPREHENSIVE REPORT

BREAKING DOWN THE TOP 100 DEFI HACKS

2025 UPDATE

HALBORN

TABLE OF CONTENTS

INTRODUCTION

DeFi hacks are increasingly prevalent, leading to significant financial losses amounting to millions of dollars.

In 2022, it was estimated that protocols incurred losses of $3.9 billion. While the total value stolen from DeFi platforms in 2023 decreased by over 50%, the number of protocols targeted in 2024 has risen slightly, though the total losses remain marginally lower than the previous year, totaling $1,282,061,959, $ 150,506,991 USD less than in the previous year. These incidents continue to pose a considerable risk to the community.

In this report, Halborn provides an exhaustive analysis of the top 100 most substantial losses in DeFi history, expanding upon our previous report, which covered up to the year 2023. Like the earlier edition, this review will explore the distribution over time, blockchain networks involved, causes, types of protocols and functions (where applicable), and whether each affected protocol had undergone prior audits. Additionally, we will offer remediation strategies and guidance to mitigate future risks. As key changes, we have broadened our research criteria and sources for this edition, ensuring a more thorough and expansive coverage across a greater span of years, from 2014 to 2024.

KEY FINDINGS

Some key findings from this study include:

- **DeFi hacks remain a concern, but they were slightly less severe in 2024**. The total funds lost in the top 100 largest DeFi hacks now stand at $10,773,130,910 USD. Whereas the period up to 2023 seemed to show a general increase in both the frequency and severity of hacks—followed by a decrease in 2023—this year's data indicates a 1% rise in the number of attacks compared to 2023. However, the average amount lost per attack in 2024 is $13 million USD lower than in the previous year, suggesting that while incidents still occur, their financial impact may be lessening.

- **Ethereum, BSC, Bitcoin, Polygon, and Arbitrum emerge as notable cases when comparing attack frequency and total value lost**. Ethereum and Binance Smart Chain, ranking among the top three chains by both Total Value Locked (TVL) and number of protocols, also occupy first and third places in terms of attack count and financial losses. Bitcoin, while third by number of attacks and second by losses, stands out for experiencing a disproportionately high number of hacks relative to its TVL and protocol count. Two newer chains, Polygon and Arbitrum, also warrant attention. Polygon is the fourth most frequently attacked chain, and Arbitrum ranks second among the most targeted networks last year, trailing only Ethereum. Both chains also display a higher-than-expected volume of hacks when considering their TVL and number of protocols, especially in the most recent year.

- **Off-chain attacks, particularly those involving compromised accounts, appear to be on the rise.** While on-chain exploits such as smart contract attacks, market manipulation, or governance breaches still account for most incidents overall, off-chain attacks now represent 44% of the total attacks and 55.6% of the total funds stolen. This trend becomes even more pronounced in 2024, where off-chain attacks make up 56.5% of all incidents and 80.5% of the stolen amount. Compromised accounts stand out as the most frequent and financially damaging type of attack, representing 42% of the overall attacks and 47% of the total losses. In 2024, compromised accounts are responsible for 55.6% of all incidents and an even greater share of the financial impact at 80.5%. These figures underscore the urgent need for robust security measures extending beyond smart contract audits, emphasizing comprehensive account protection strategies to safeguard user credentials and mitigate off-chain vulnerabilities.

- **Auditing both the code and the broader ecosystem is crucial for effective security**. Although most of the hacked protocols had not been audited, and while audited protocols account for only 20% of the total sample and 10.8% of the overall losses, certain attack vectors—such as market manipulation—can be difficult to detect if audits do not consider the full ecosystem and external interactions. Incorporating a more holistic assessment of how off-chain elements interface with on-chain components is equally important for identifying potential vulnerabilities and mitigating these advanced threats. Such comprehensive audits need to consider the protocol's interactions with external systems, including APIs, off-chain data feeds (like oracles), and the broader market context in which the protocol operates.

- **Lack of multi-signature or multi-party computation (MPC) solutions and insufficient use of cold wallets present significant security gaps**. Only 19% of the attacked protocols employed multi-sig or MPC schemes, which highlights the importance of careful private key management; if a multi-sig or MPC wallet is compromised, the potential losses can be substantial. Cold wallets add another layer of security, yet just 2.4% of the protocols used them, accounting for only 1% of total losses. This disparity suggests that increased adoption of cold wallets could considerably reduce the overall financial damage resulting from attacks.

- **A lack of—or faulty—input verification or validation stands as the leading cause of both hacks and losses in direct contract exploitation**. Moreover, it emerges as the predominant vulnerability, by both occurrence and total losses, across all smart-contract-related attacks. Notably, it was also the main vulnerability exploited in direct contract exploitation incidents throughout 2024.

- **Reentrancy attacks continue to pose a significant threat, maintaining their relevance years after they were first identified**. These attacks represent the second most frequent type of exploit in incidents involving smart contracts, accounting for 18.4% of such hacks. They are particularly damaging in scenarios of direct contract exploitation, where they constitute 23.1% of the incidents. Reentrancy attacks have consistently been a concern over the years, contributing to 20% of the hack instances last year and causing 21.7% of the financial losses observed. This persistence highlights the ongoing challenge they pose to blockchain security and the critical need for robust defensive mechanisms against them.

- **Be cautious of vulnerabilities related to faulty proof verification, particularly in bridge protocols.** These vulnerabilities are significant despite their infrequent occurrence; they constitute only 5.3% of smart contract attacks yet account for 26.8% of the total financial losses. This issue is crucial within the context of direct contract exploitation, where faulty proof verification contributes to 30.4% of the total losses. The substantial impact of such vulnerabilities, especially in bridges, which saw 50.9% of losses for this type of protocol, underscores their potential to cause major financial damage and highlights the need for rigorous security measures in these areas.

- **Be cautious with oracles.** A flawed oracle remains a significant vulnerability and the predominant reason for market manipulation attacks, responsible for 45.8% of such incidents. These flawed oracles are also the leading cause of financial losses in market manipulation, accounting for 59.3% of the damage. While there has been a notable reduction in the use and impact of flawed oracles over the past year—dropping from being implicated in 50% of market manipulation hacks and 71.6% of the associated financial losses in 2023 to 25% and 29.2%, respectively—they continue to represent a significant risk.

- **Flash loans can serve as a powerful attack vector.** Although most of the hacks studied did not involve them, they play a critical role in market manipulation and governance attacks. They account for 62.8% of the total funds lost in market manipulation incidents and are used in every governance attack in the dataset. Moreover, the use of flash loans has risen over time. In 2023, they were utilized in 50% of the attacks that could potentially involve them, increasing significantly from 15.4% in 2022. By 2024, that number rose further to 83.3%. This escalating trend demonstrates the growing importance of flash loans as a tool for malicious exploits. Projects should, therefore, be mindful of the risks associated with flash loan attacks, particularly if the protocol enables swapping and exchanging of assets or if token-based quorum power features in its governance processes.

- **Be wary of Ponzi and pyramid schemes, as well as protocols where owners have excessive privileges.** A privileged owner account is responsible for 50% of rug pulls and scams in the DeFi ecosystem, and these incidents lead to 42.8% of the financial losses from such schemes. While Ponzi and pyramid schemes constitute only 16.7% of all scams, they account for a disproportionate 48.9% of the losses. Notably, rug pulls and scams make up 12% of the hacks in this study and result in 15.6% of the total financial losses, ranking just behind compromised accounts and direct contract exploitation. Therefore, it's crucial to thoroughly research protocols before engaging with them to minimize risks.

- **There is a pressing need for increased transparency around off-chain attacks, especially those involving compromised accounts**. Over half (54.8%) of these incidents lack clarity regarding their origin and they account for 47.7% of the total financial losses. This highlights the importance of protocols being open and forthcoming with users about hacks and vulnerabilities, ensuring the community remains well-informed, fosters trust and is better protected.

- **Lending protocols, Bridges, and Centralized Exchanges (CEXs) consistently emerge as the most vulnerable types of blockchain protocols**. CEXs not only experience the highest frequency of attacks, accounting for 20.2% of all incidents, but also suffer the most significant financial damages, contributing to 29.4% of total losses. Lending protocols follow closely, being the second most frequently attacked, with 15.21% of incidents. Bridges, though fourth in terms of attack frequency at 10.1%, incur disproportionately high losses, representing 26.4% of the financial damages. Both Bridges and CEXs show a high ratio of attacks relative to their overall presence in the blockchain ecosystem. This pattern of vulnerability has persisted over time, with CEXs and Lending protocols remaining highly targeted in 2024 and CEXs alone accounting for 53.9% of the financial losses for that year. This ongoing trend underscores the critical need for enhanced security measures within these specific protocol categories.

- **Gaming protocols, a new threat and target?** Gaming protocols have emerged as a significant concern in the blockchain security landscape. While gaming protocols account for only a modest 3% of the total number of hacked protocols and represent 3.7% of the total financial losses across all types, their impact in 2024 highlights a growing trend. This year, they are responsible for a substantial 17.6% of the total value lost due to hacks, marking them as the second highest in terms of financial losses. This disproportionate impact suggests that gaming protocols might be becoming more attractive targets for hackers, possibly due to their increasing popularity and the substantial volumes of transactions they handle. Despite their relatively small representation in the overall blockchain ecosystem, the fact that they are experiencing more hacks than expected underscores the need for heightened security measures and vigilant monitoring within this sector. This trend points to the potential vulnerabilities inherent in gaming protocols, making them critical points of focus for future cybersecurity efforts in the blockchain industry.

- **Decentralized protocols exhibit a lower proportion of both hacks and total losses when compared to their centralized counterparts**. Decentralized protocols appear to exhibit a degree of resilience against hacking relative to their centralized counterparts, as evidenced by the proportion of hacks and associated financial losses. While decentralized protocols make up 38.4% of all hacked protocols, they are responsible for only 22.2% of the total monetary losses incurred from such incidents. This discrepancy suggests that decentralized protocols might inherently possess mechanisms or structures that mitigate the extent of damage from individual hacks. In the most recent year analyzed, the trend continues, with decentralized protocols representing 41.2% of the protocols subjected to attacks. Despite this significant representation, the financial impact of these hacks was relatively contained, accounting for just 31.4% of the total losses. This indicates a persistence of the trend where decentralized protocols suffer fewer losses relative to their occurrence in hacks.

- **Functions like "withdraw", "deposit", "transferOwnership", "verifyProof", and protocol-specific functions emerge as high-risk areas**. Withdraw-like and deposit functions represent a substantial portion of attack targets, accounting for 25.7% and 17.1% of incidents, respectively. This indicates a frequent focus on functions that directly manage asset flows, underscoring their allure to attackers due to the immediate financial gains they offer. However, functions involved in verifying proofs and transferring ownership of contracts have led to the most significant monetary damages, accumulating 27% and 18.1% of total losses, respectively. These functions are critical as they often control the broader permissions and integrity of the protocols, making their exploitation potentially devastating. In 2024, an emerging concern was protocol-specific functions, which, despite constituting only 20% of the attacks, led to the highest financial losses for the year at 33.2%. This highlights a trend towards attacks that exploit unique aspects of specific protocols, suggesting that these areas may require additional, tailored security measures and audit processes to mitigate risks effectively.

TIME DISTRIBUTION AND AMOUNT HACKED

The use and development of DeFi protocols have seen significant growth over the years.

However, the trend in losses incurred from hacks does not show a steady increase. As illustrated in Figures 1 and 2, these graphs represent the number of hacks per year, both as a percentage of total hacks and in absolute terms. The earliest recorded incident is the MtGox hack in February 2014.

From this starting point, the data indicates a trend where the number of hacks or similar attacks either increased or remained stable annually until 2021. Since then, there has been a decline in the frequency of these incidents through to 2023, with a slight increase observed in 2024 compared to the previous year, from 17 attacks in 2023 to 18 in 2024.

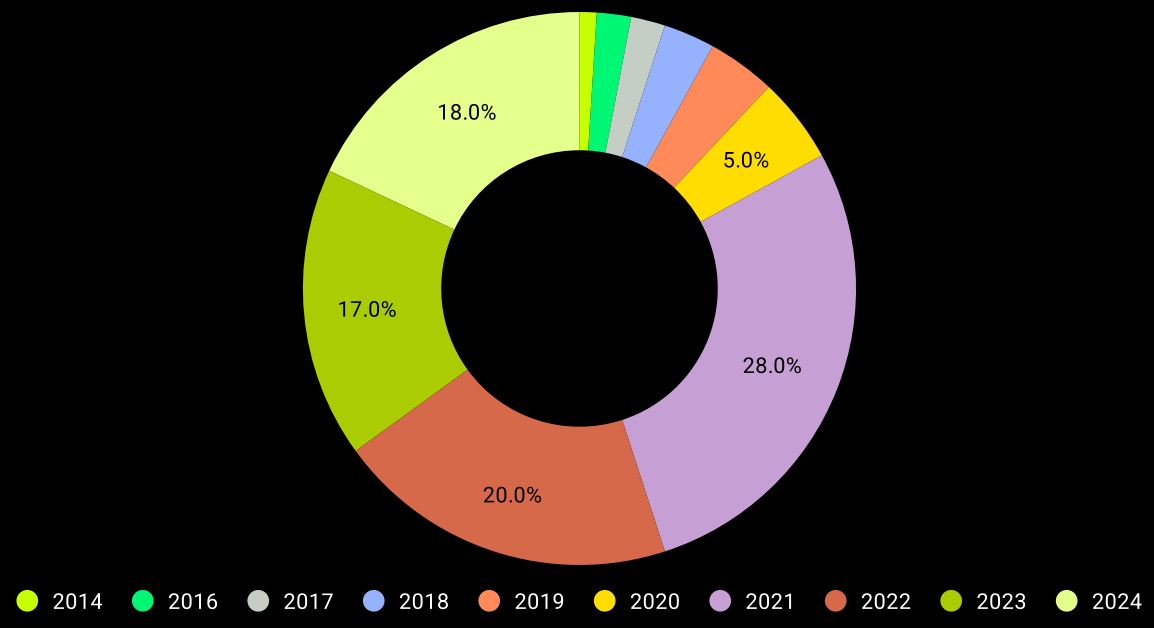

Figure 1: Number of hacks per year by percentage

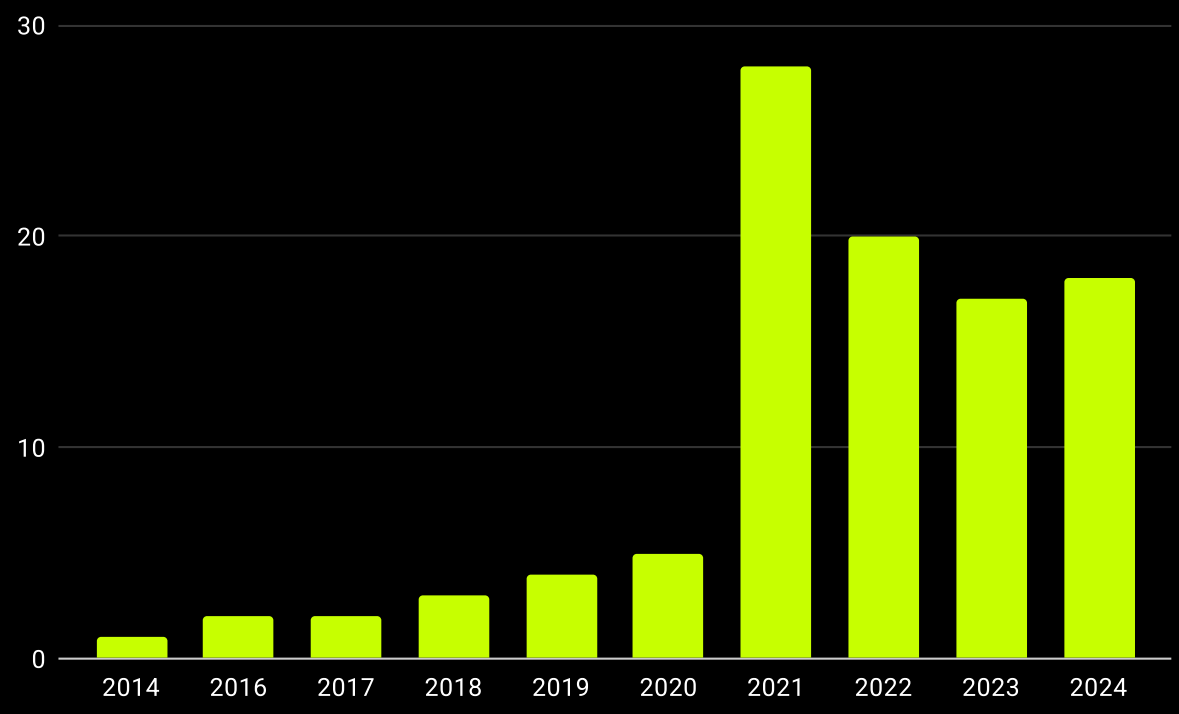

Figure 2: Number of hacks per year [count]

The cumulative hacked amount from these attacks is approximately $10,773,063,910 USD in total.

Analyzing the distribution of these losses by year reveals a spike in funds stolen in 2014. Subsequently, there was a noticeable decline in the amount lost, but from 2016 to 2019, there was a yearly increase in the volume of funds stolen. In 2020, there was a drastic reduction in losses. However, from then onwards until 2022, the losses escalated once again, only to decline through to 2024, resulting in a $1,282,061,959 USD loss for this year. This trend is detailed in Figures 3 and 4.

Important Note

It is important to note that, for the purposes of this report in this section and in sections following, we have considered the initial or potential amount hacked, even though this amount may later be reduced due to actions such as the protocol pausing its activities, freezing of funds, or even returns by the hacker. We consider that this approach ensures a comprehensive analysis of the full impact at the time of each incident.

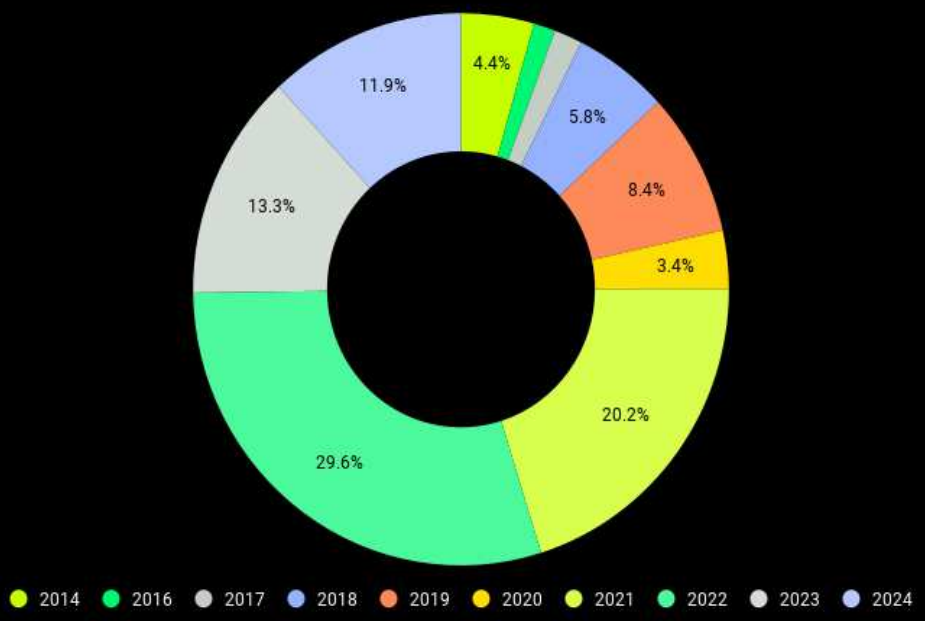

Figure 3: Loss caused by hacks per year by percentage

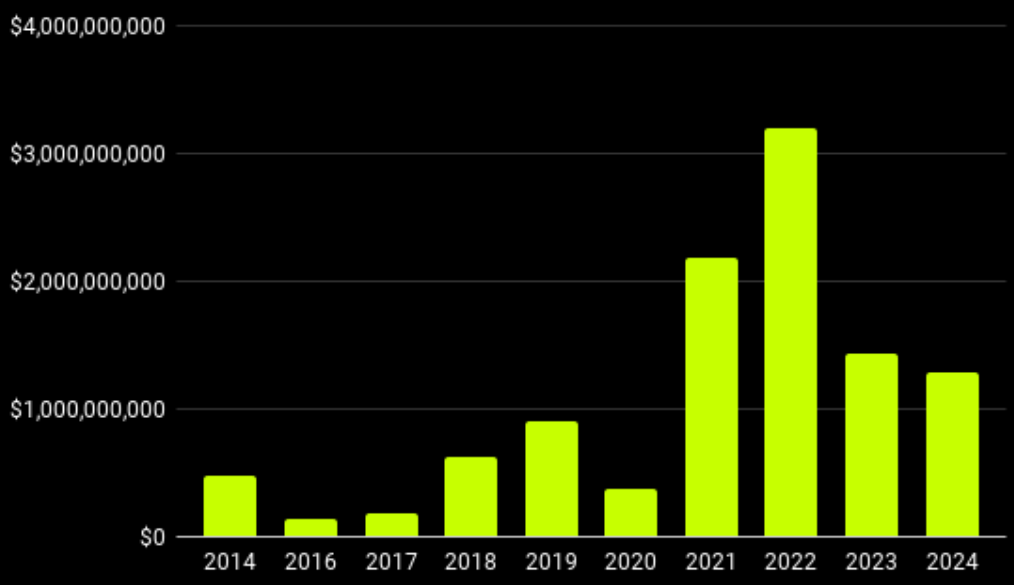

Figure 4: Loss caused by hacks per year [USD]

This trend can be explained by considering the severity of the attacks. While there were fewer attacks in 2022 than in 2021 (see **Figures 1** and **2**), the total amount of money lost was higher in 2022. As noted, the number of attacks dropped again in 2023, and so did the overall losses, falling to roughly half of the previous year's figure. In 2024, there was a slight increase in the number of hacks, yet the total amount lost went down again. This suggests that the attacks in 2023 were less severe financially than those in 2022, and the attacks in 2024 were less severe than those in 2023. **Figure 5** underscores this observation by showing that the average loss per attack in 2023 is lower by $75,386,238 than in 2022, and the average loss in 2024 is lower than in 2023 by $13,043,097.

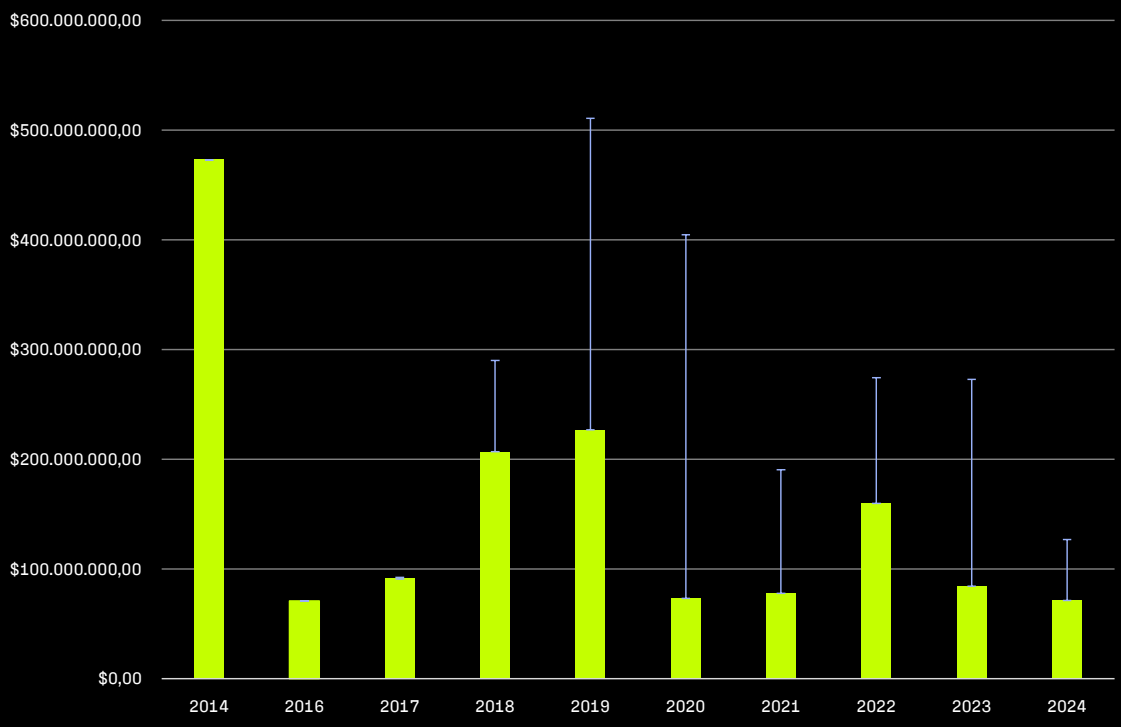

Figure 5: Average and standard deviation of the loss by year [USD]

The data presents a clear narrative of gradually decreasing attack severity, suggesting enhancements in protocol security and incident management over these last years or possibly a change in the types of targets or the value of assets being less lucrative or accessible.

As we can observe in **Figure 6**, Total value locked (TVL) saw a decline from the middle of 2022 into 2023, rebounded in 2024, though it still did not reach the peak levels observed in 2022. This fluctuation in TVL suggests changes in the economic attractiveness and possibly the vulnerability of blockchain assets. While the TVL was lower, the reduced number and scale of attacks could have been influenced by fewer lucrative targets. However, the increase in TVL in 2024 suggests that while assets might have become more attractive targets due to their increased value, the continued reduction in total amount hacked could likely be attributed to factors other than asset value alone.

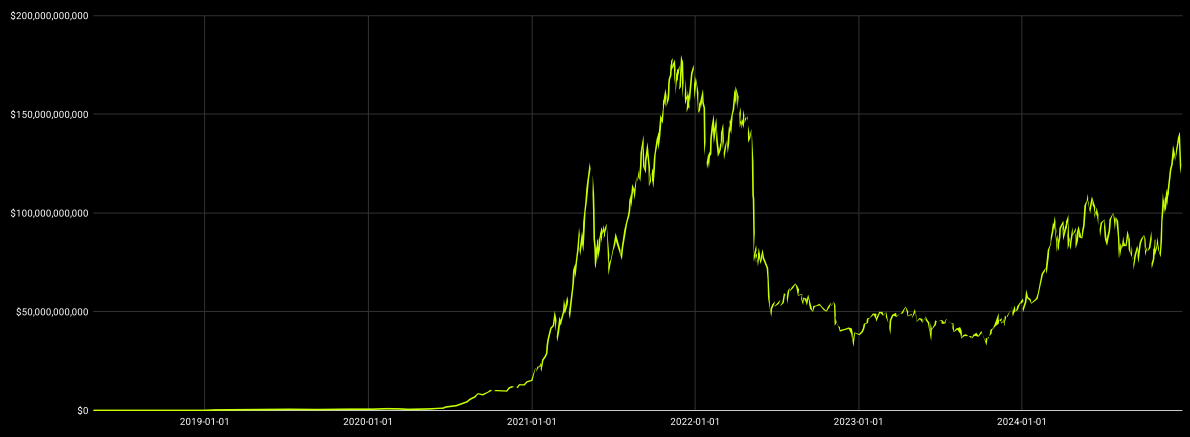

Figure 6: TVL in DeFi by year

DISTRIBUTION OF ATTACKS PER CHAIN

Figures 7 and 8 illustrate the distribution of different hacks across blockchain networks.

If an attack affects multiple chains, it is counted separately for each network involved. Notably, 38.2% of these attacks have occurred on the Ethereum network, which is recognized as the largest in terms of Total Value Locked (TVL) and the highest number of DeFi protocols. It is followed by the Binance Smart Chain (BSC), which accounts for approximately 12.5% of total hacks. Interestingly, BSC ranks fifth in TVL but second in the number of DeFi protocols, according to data from DefiLlama (source https://defillama.com/chains).

Bitcoin, ranking third in the frequency of attacks with 9% of them, is fourth by TVL and fourteenth by the number of protocols. Attacks categorized as "Multi" have impacted more than nine different chains or involve chains where the specifics have not been disclosed.

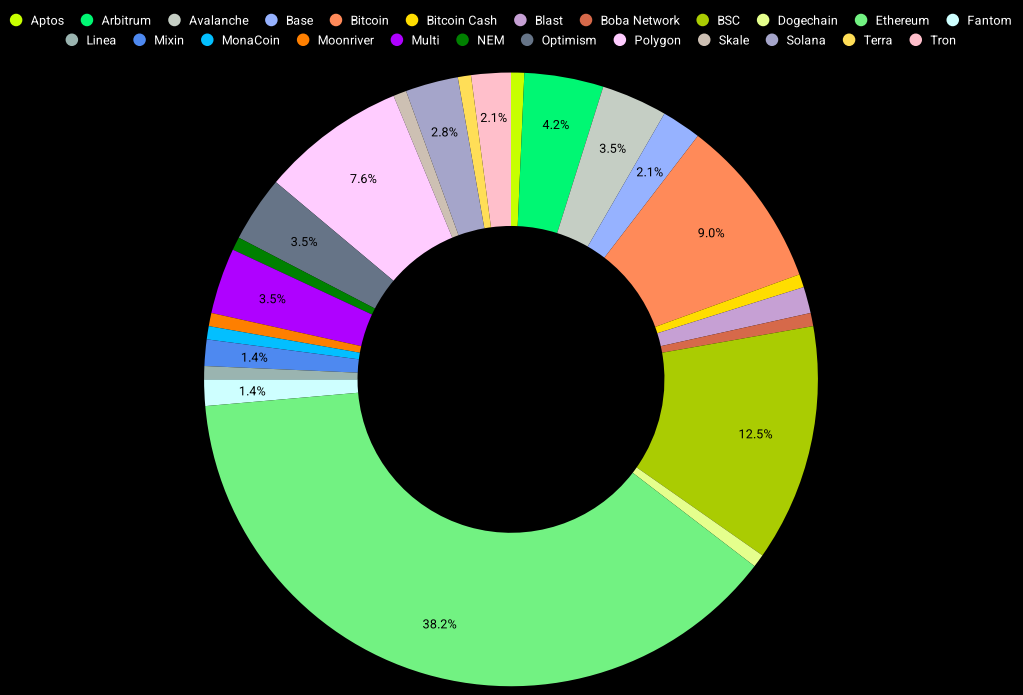

Figure 7: Number of attacks per chain [percentage]

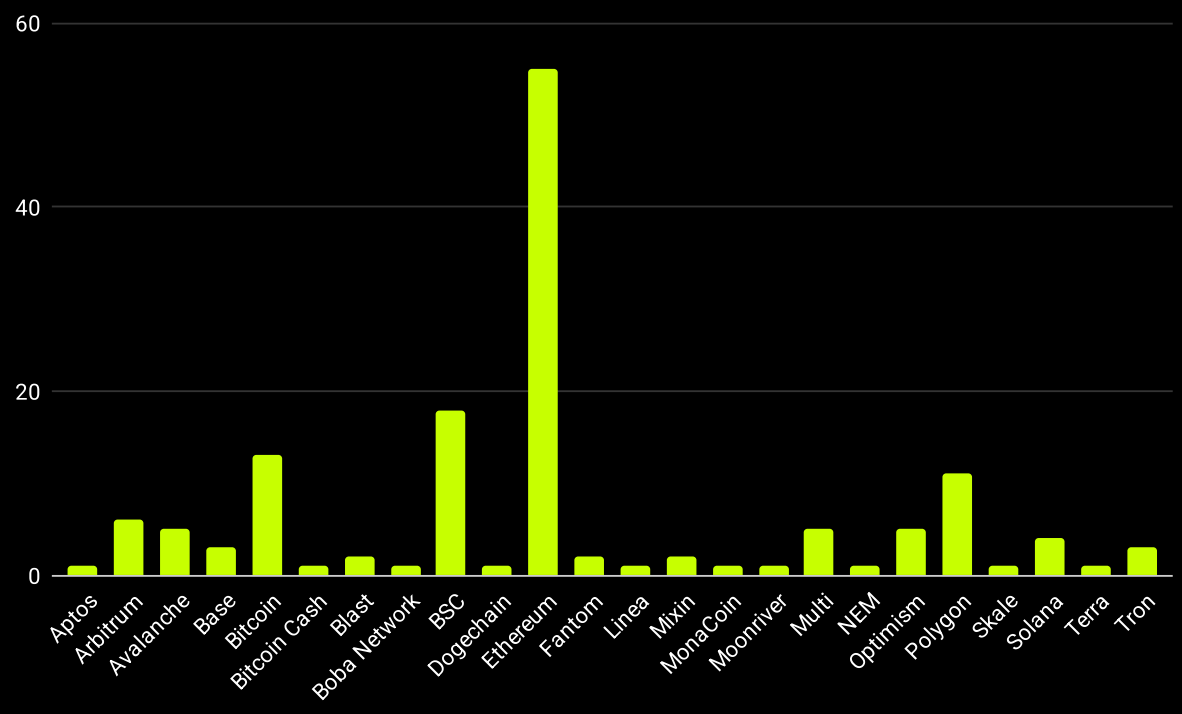

Figure 8: Number of attacks per chain [count]

Analyzing the financial impact of these attacks across different blockchain networks reveals critical insights into the distribution of stolen funds.

As depicted in Figures 9 and Figure 10, Ethereum accounts for a substantial 42.3% of the total funds stolen, amounting to approximately $ 4,561,704,053 USD. This is consistent with its status as the network with the highest Total Value Locked (TVL) and the largest number of DeFi protocols.

Bitcoin, ranking second in terms of losses, accounts for 17.1% of the hacked funds, totaling $1,845,050,000 USD. The Binance Smart Chain (BSC) follows, contributing to 12.5% of the total funds hacked, or roughly $ 1,345,375,403 USD. Notably, the percentage of losses for these chains, except for BSC, where it matches, exceeds their respective shares of attack occurrences. This suggests that attacks on these networks tend to result in higher financial damage compared to others.

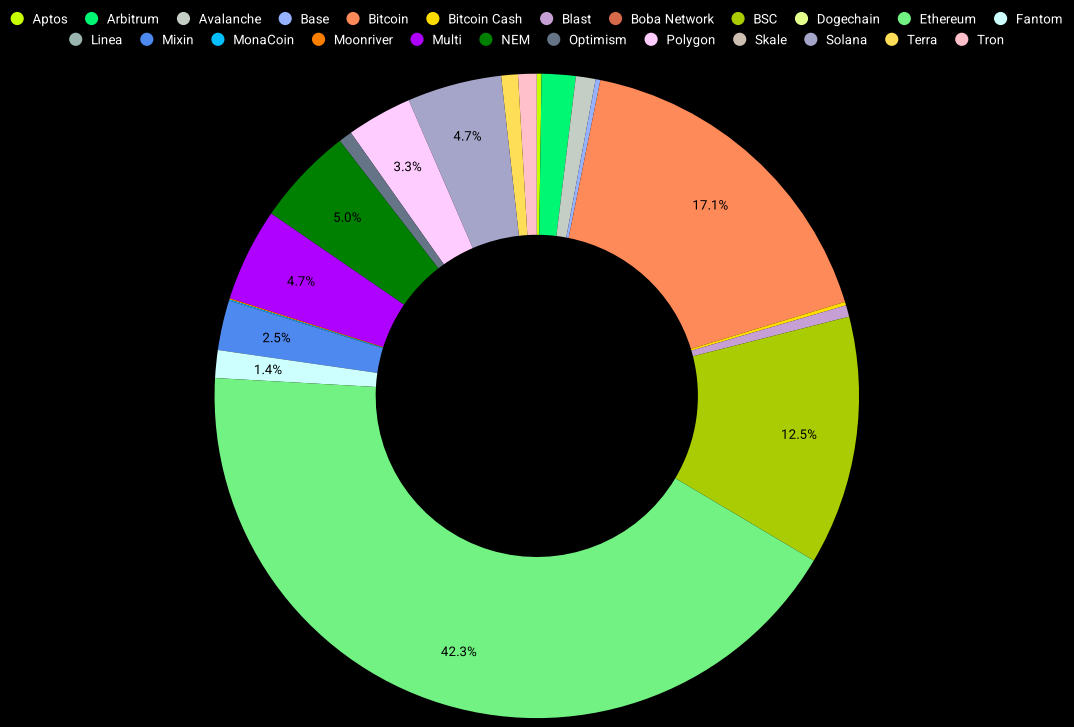

Figure 9: Loss by type of attacks per chain [percentage]

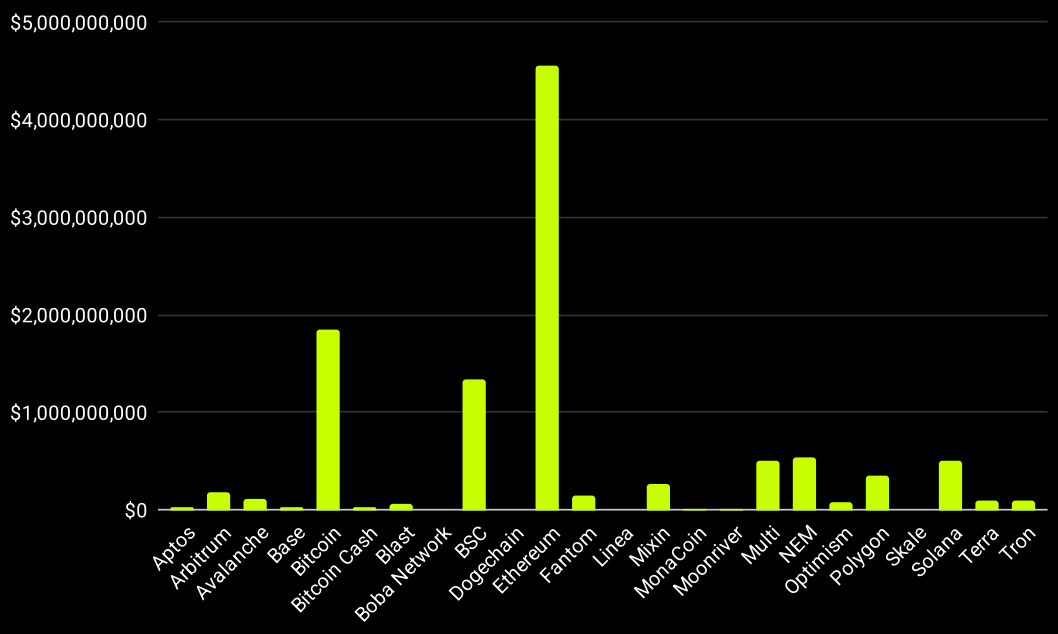

Figure 10: Loss by type of attacks per chain [count]

Observing Figure 11, which compares the ranking of blockchain chains based on the total value locked (TVL) and the number of hacks, provides an insightful look into whether the amount of value locked within a chain influences its susceptibility to attacks.

In this visualization, the chains are ranked from largest to smallest based on TVL and the number of hacks experienced. This allows for a nuanced analysis of how the economic significance of a chain correlates with its attractiveness as a target for hackers.

A key aspect of this figure is the inclusion of a blue line that acts as a benchmark for comparing the two rankings. If a chain's marker (representing its rank based on the number of attacks) is located below this blue line, it indicates that the chain is ranked higher (i.e., it has experienced more attacks) compared to its rank based on TVL. This positioning suggests that chains with higher numbers of attacks than expected, relative to their TVL, might be perceived as more vulnerable or attractive targets due to factors beyond just the amount of value they secure.

The addition of the ranking for only 2024 provides a temporal snapshot that helps in understanding the latest trends in blockchain security and hacker focus.

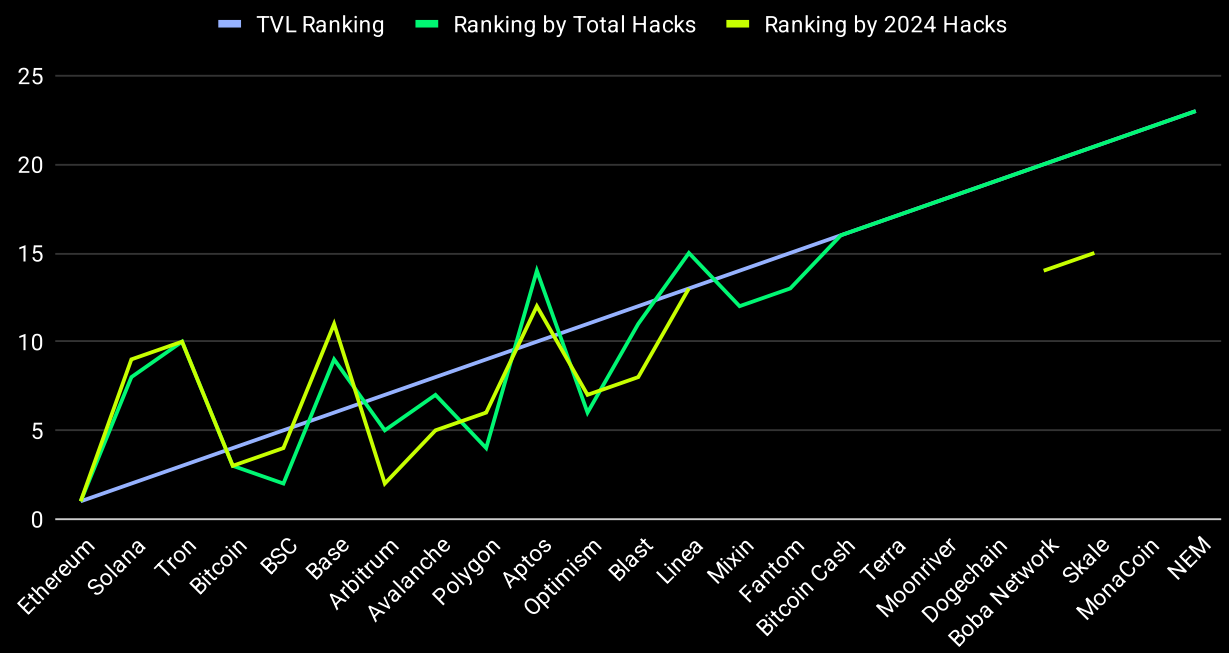

Figure 11: Order by TVL and number of attacks in total and only in 2024

In our analysis, a correlation generally exists between the frequency of attacks on blockchain chains and their Total Value Locked (TVL). However, certain chains warrant specific attention due to their unique patterns. Notably, Solana, Tron, and Base have substantial TVLs but have experienced relatively fewer attacks, suggesting a stronger security posture or possibly less exposure to common vulnerabilities.

On the other hand, there is a marked discrepancy in chains such as Binance Smart Chain (BSC), Polygon, and Optimism, where the frequency of attacks significantly exceeds what might be expected based on their TVL. This pattern suggests that these chains are especially appealing to attackers, possibly due to features such as lower transaction costs or faster block times.

In the year 2024, the disparity in attack frequency relative to TVL on the BSC and Polygon chains has become less pronounced, suggesting possible improvements in security measures or changes in attacker focus. However, Optimism continues to present a concern, maintaining a higher rate of attacks compared to its TVL. Additionally, new trends appear to be emerging with chains like Arbitrum and Blast, which are beginning to show similar patterns of higher attack frequencies.

It is also worth mentioning Boba Network and Skale, which have notably become targets for attackers over the past year.

Studying the frequency of attacks in relation to the number of protocols on various blockchain chains offers another insightful metric.

The underlying logic is straightforward: a higher number of protocols potentially provides more targets for hackers, thereby increasing opportunities for malicious activities and fund theft.

In Figure 12, we examine these metrics, showing the number of attacks relative to the number of protocols each chain hosts. For chains that experience an equal number of attacks, we prioritize them in the ranking based on the number of protocols they support. This approach allows for a nuanced understanding of how the density of protocols might correlate with the likelihood of being targeted by attackers.

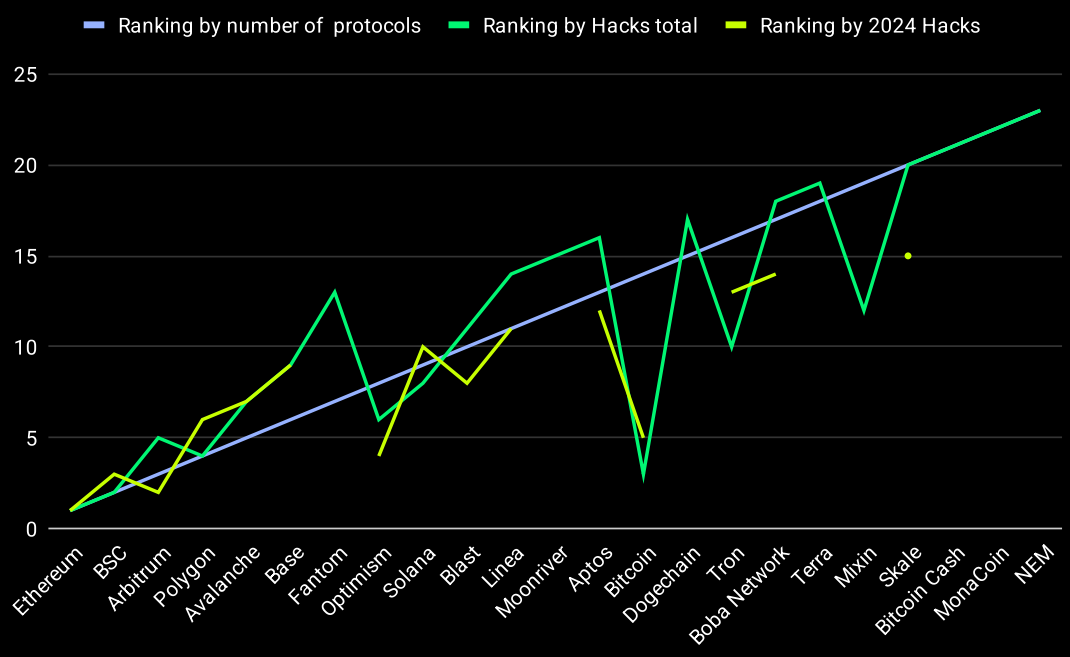

Figure 12: Order by number of protocols in chain and number of attacks in total and only in 2024

The relationship between the number of attacks and the number of protocols on various blockchain chains, as visualized in Figure 12, shows a somewhat less direct correlation compared to the earlier discussed correlation with TVL (Total Value Locked) in Figure 11. However, there still appears to be a discernible connection, indicating that chains with more protocols could be more vulnerable to attacks.

It's noteworthy that chains such as Arbitrum, Avalanche, Base, Fantom, Linea, Moonriver, Aptos, Dogechain, Terra, and Boba Network seem to experience fewer attacks than might be expected given the number of protocols they host. This could suggest either more robust security measures or possibly less lucrative targets for attackers.

On the other hand, Bitcoin, Tron, and Mixin exhibit a considerable disparity, with a notably high frequency of attacks relative to their number of protocols. This discrepancy is particularly pronounced in the case of Bitcoin, which remains a significant target for attacks despite hosting fewer protocols, likely due to its high profile and the large value processed on its network.

Focusing on the year 2024, Bitcoin continues to exhibit a higher-than-expected number of attacks relative to its number of protocols, indicating an ongoing vulnerability or attractiveness to attackers. Similarly, Optimism's discrepancy has also increased, suggesting a growing target profile over the recent period.

This analysis underscores the importance of not only the sheer number of protocols on a chain as a factor for security considerations but also the intrinsic qualities of the chain, such as user base, transaction volume, and inherent security features. Chains with fewer protocols but higher profile or transaction volumes, like Bitcoin, may need enhanced security strategies to mitigate this disproportionate risk of attacks.

Figures 13 and 14 illustrate the yearly distribution of hacks across various blockchain chains.

It's important to recognize that chains like BSC and Solana, which were introduced in 2020, would not appear in the data for earlier years.

Ethereum consistently registers the highest number of attacks among all chains, likely correlating with its status as the largest by both TVL and the number of protocols. This makes Ethereum a prime target for attackers due to the substantial assets and activities hosted on it. However, as newer chains like BSC and Solana have gained traction and usage, attacks appear to be more evenly distributed among these newer players, somewhat diminishing Ethereum's predominance in absolute numbers of attacks.

In 2023, the data shows new chains such as Algorand (released in 2017) and Moonriver (released in 2021) joining the list of chains targeted by attacks. In recent years, there have been notable inclusions of newer chains in the list of targeted networks. The year 2024 saw further diversification with the inclusion of newer chains like Blast (released in 2024), Aptos (released in 2022), Linea (released in 2023), Boba Network (released in 2021), and Skale (released in 2018). It indicates that as chains mature and accumulate value, they become more attractive targets for attackers and suggests a broadening landscape where attackers are continuously seeking vulnerabilities across a wider array of chains.

Bitcoin, notable for its high profile and significant transaction volume, was the most attacked network in 2014 and 2019, highlighting its perennial appeal to attackers. It also shared the lead with Ethereum in 2016 for the most attacks, underlining its ongoing vulnerability. In the latest year considered, 2024, Arbitrum has emerged as the second most attacked chain, pointing to its rising significance and perhaps vulnerabilities as it grows in usage.

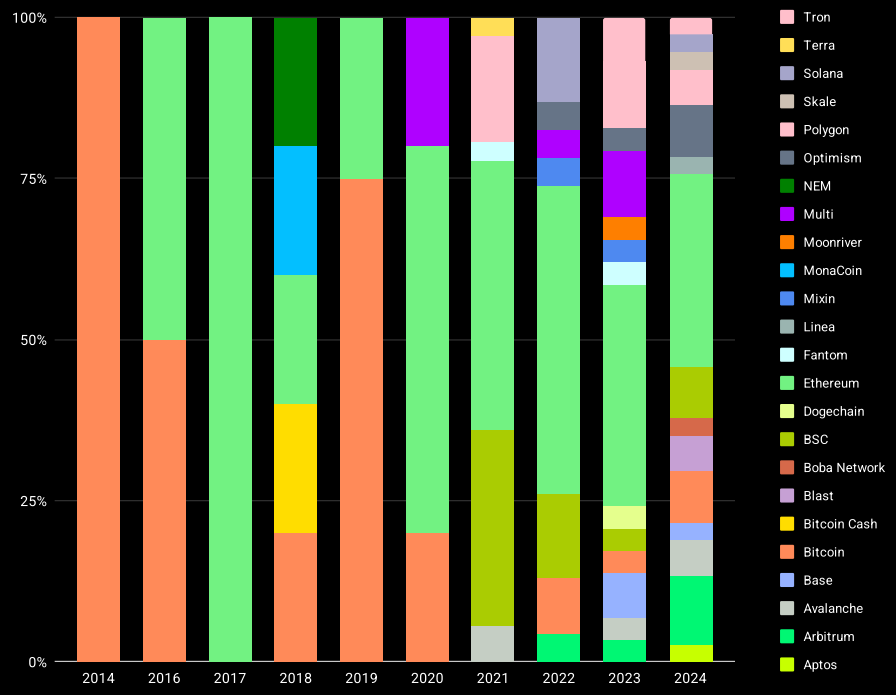

Figure 13: Number of attacks per year and chain [percentage]

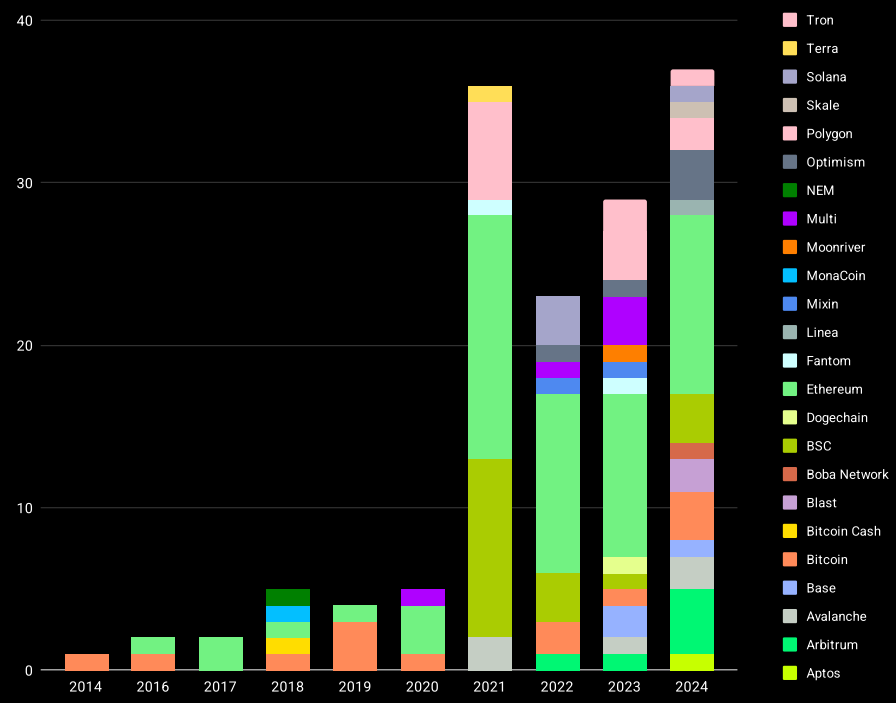

Figure 14: Number of attacks per year and chain [count]

The distribution of financial losses due to hacks across different blockchain chains over the years presents a revealing picture of the financial impact of these security breaches.

Ethereum, as the predominant platform, has consistently suffered the largest share of financial losses due to hacks, accounting for more than half of the total value lost almost every year since 2021. The exception was in 2023, where Ethereum's share of the total losses decreased to 41.1%. This sustained high level of financial loss underscores Ethereum's status as a lucrative target for hackers.

Bitcoin, which had previously seen a reduction in the proportion of losses, saw a resurgence in 2024, accumulating 25.5% of the amount hacked, totaling $326,650,000 USD. This resurgence might reflect increases in hacker activity targeting Bitcoin due to its high profile and significant transaction volume.

A notable instance of a massive single-event loss occurred with NEM in 2018, primarily due to the Coincheck hack. This event alone contributed to 86.1% of the total losses for that year while only representing 20% of the attacks for that period.

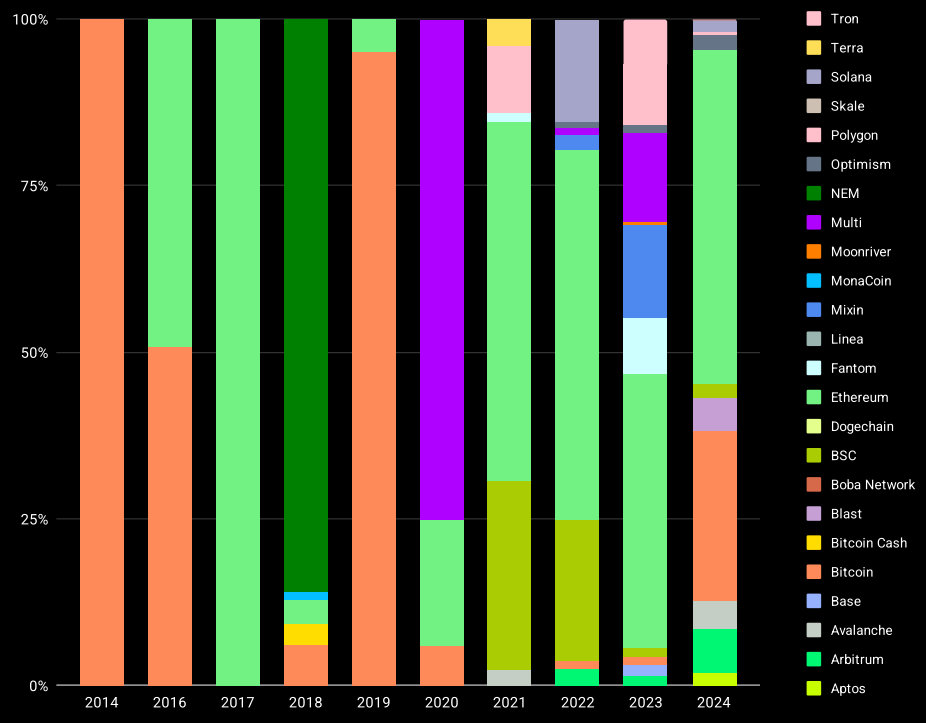

Figure 15: Loss caused by attacks per year and chain [percentage]

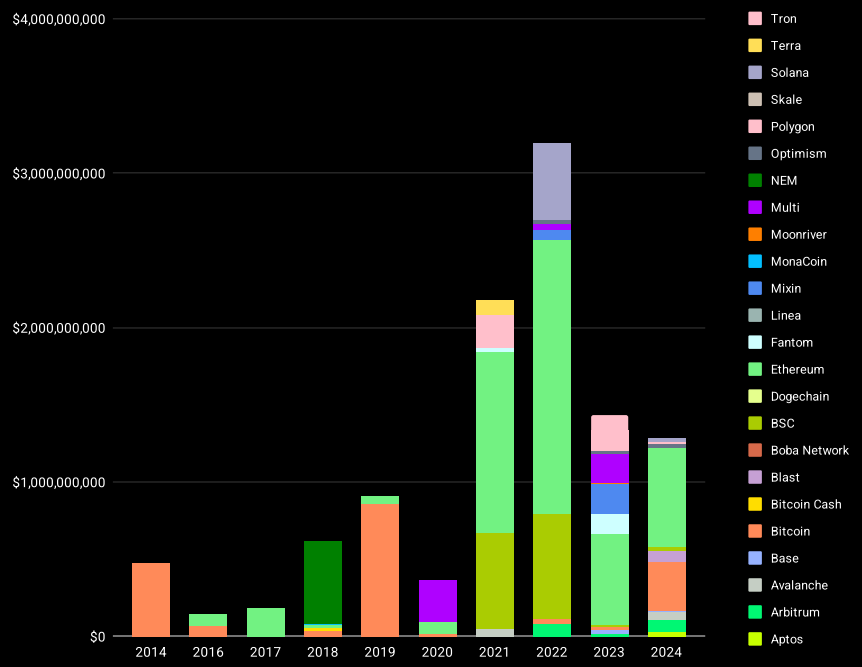

Figure 16: Loss caused by attacks per year and chain [USD]

TYPE OF DEFI ATTACKS

This section delineates two primary categories of attacks relevant to our analysis:

- **Off-chain attacks.** These are hacks where the principal attack vector occurs outside the blockchain, although the outcomes may be observable on-chain. Examples include compromised accounts or traditional cybersecurity breaches.
- **On-chain attacks.** This category includes attacks where the main vector occurs directly on the blockchain. Typical scenarios involve the exploitation of a contract or market manipulation attacks. Certain types of rug pulls and scams also fall under this category, specifically those that require a backdoor in a contract or rely on protocol design that allows certain accounts privileged access or control over the protocol's funds. When they are based on off-chain components (like Ponzi schemes), they are included in the first category.

These categories will have different sub-categories, namely:

Off-chain attacks:

- **Compromised account:** Called **compromised private key** in our previous report, this attack covers not only when a private key is stolen or leaked, commonly via phishing attacks or by compromising the system in which the private key is stored, but also when a signature or approval is compromised by any method. When an attacker is able to obtain the private key of an account by other methods (e.g., brute force on a weak cryptographic algorithm), it is also included in this category.

On-chain attacks:

- **Market manipulation attack:** Previously categorized as **price manipulation**, we have broadened the definition to encompass a wider range of attacks, now termed market manipulation. Market manipulation refers to any activities aimed at interfering with the normal operations of a market, which may include creating misleading or artificial conditions affecting prices, supply, or demand. **Price manipulation**, the term used before, is a subset of market manipulation that specifically targets the pricing mechanisms of assets within the DeFi ecosystem. It often exploits technical and systemic vulnerabilities related to how asset prices are determined and utilized. Market manipulation generally involves a series of operations, such as asset swaps, or the strategic supply and removal of liquidity, often encompassing multiple assets and a liquidity pool. It is particularly prevalent in scenarios where attackers can exploit low or empty liquidity pools, exploit contract vulnerabilities, or take advantage of inaccurate asset price data from flawed oracles.

- **Direct contract exploitation:** This form of attack grants the perpetrator access to various mechanisms of a protocol and allows for the unlawful acquisition of funds or tokens. While such attacks can involve multiple tokens and operations, they distinctly do not engage in pool manipulation or market manipulation. This focuses the attack on exploiting code vulnerabilities directly within the smart contract itself, bypassing the need for broader market tactics and instead leveraging flaws within the contract's design or implementation to extract value or disrupt the protocol's intended functions.

- **Governance attack:** When a perpetrator exploits a blockchain venture governed through decentralized means, it typically involves acquiring sufficient influence or voting power to execute a malicious proposal. This type of attack targets the decision-making processes within decentralized governance systems. The attacker manipulates these systems to gain control or enact changes that serve their interests, potentially leading to detrimental outcomes for the protocol, such as redirecting funds, altering critical protocol settings, or implementing unfavorable rules.

Both types of attacks:

- **Rug pull/Deceptive Practice (Scams):** It refers to scenarios where developers or project creators suddenly remove liquidity or funds from a DeFi protocol, leading to significant losses for investors or users. This typically occurs after enticing users to invest based on promises of high returns or other incentives. This category also includes situations where project leaders, such as CEOs, have been arrested and charged with fund withdrawal, as well as Ponzi schemes, insider jobs, and actions by rogue developers. When such deceptive practices are enabled by deliberate backdoors in the contract or using permissioned or centralized accounts that hold project funds on-chain—as dictated by the protocol's design—these actions are categorized as on-chain attacks. This is because the fraudulent activities leverage the technical and structural aspects of blockchain technology. However, when these practices occur without direct manipulation of blockchain components, such as through social engineering or external financial maneuvers, they are classified as off-chain attacks.

In the main categories, Figures 17 and 18 indicate that most attacks are on-chain, accounting for 56% of the total, compared to 44% which are off-chain.

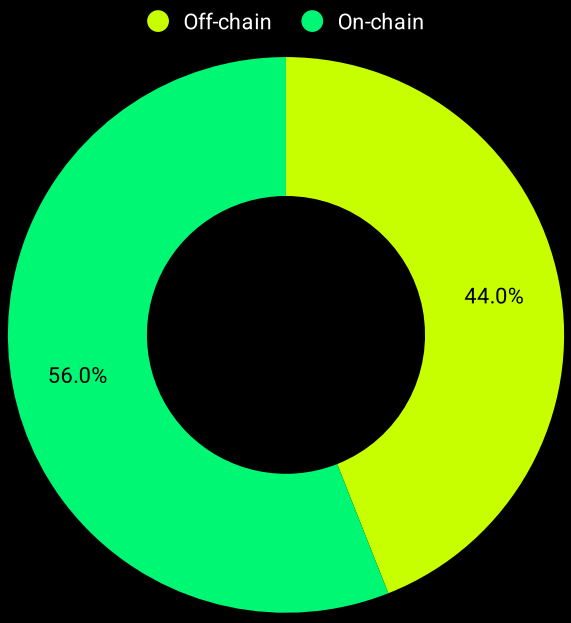

Figure 17: Number of off-chain and on-chain attacks [percentage]

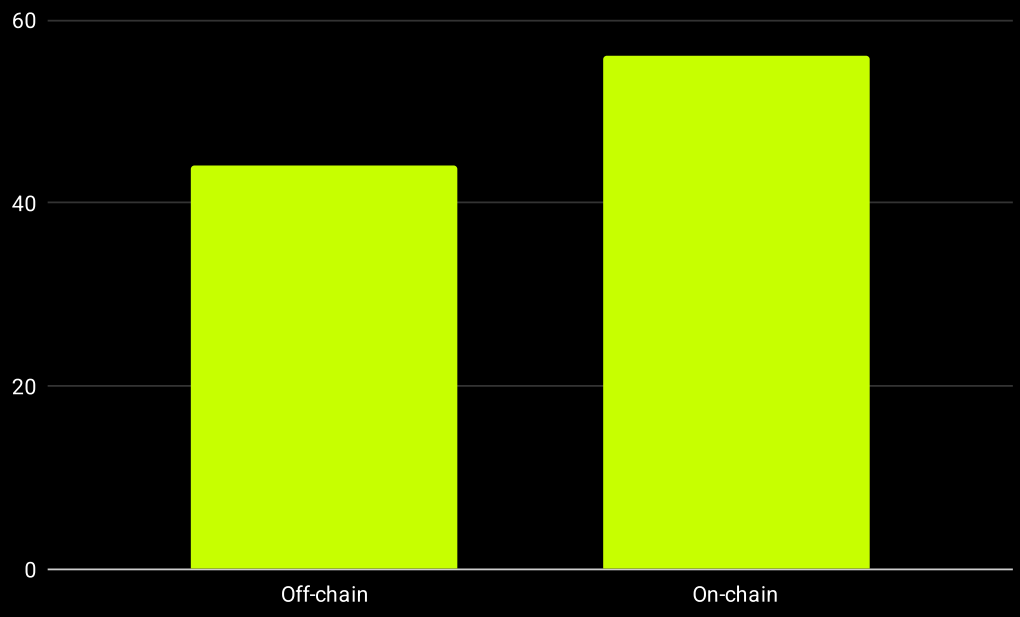

Figure 18: Number of off-chain and on-chain attacks [count]

However, when examining the financial impact caused by each type of attack (as shown in Figures 19 and 20), we observe that off-chain attacks are responsible for a higher total in financial losses, accounting for approximately 54.6% of the amount hacked, despite comprising only 44% of the attacks.

Specifically, losses due to off-chain attacks amount to around $5,883,144,839 USD, while on-chain attacks have resulted in approximately $4,889,919,071 USD in losses. This disparity highlights that while on-chain attacks are more frequent, off-chain attacks tend to result in larger financial damages.

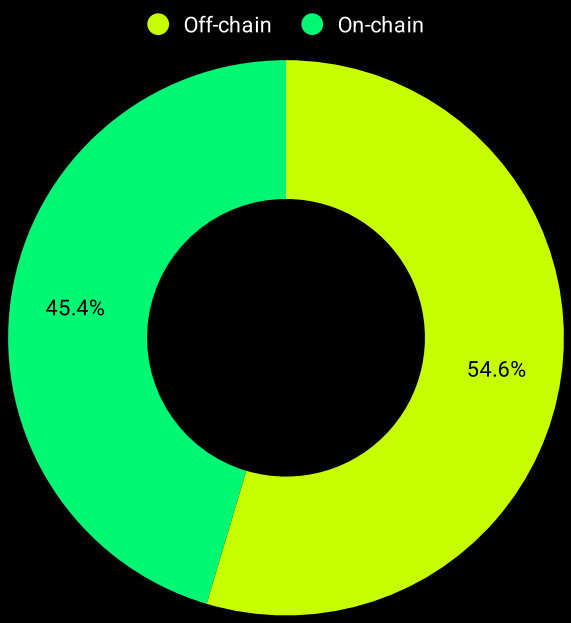

Figure 19: Loss caused by off-chain and on-chain attacks [percentage]

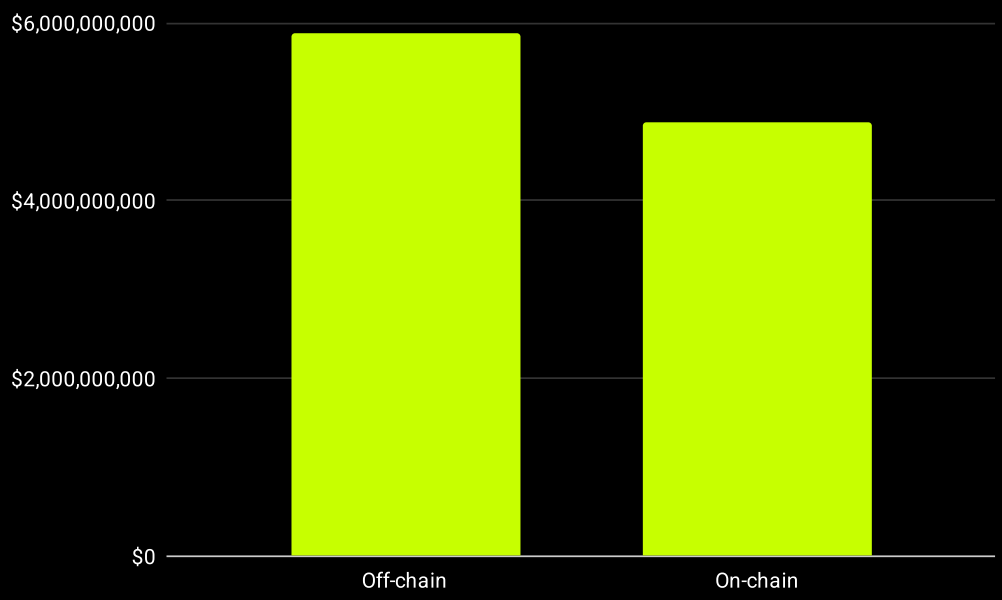

Figure 20: Loss caused by off-chain and on-chain attacks [USD]

By examining the data year by year, we observe that the number of hacks attributable to off-chain elements has generally increased since 2021.

However, there has been a slight decrease in 2024, where off-chain attacks accounted for approximately 55.6% of the hacks, compared to 64.7% in 2023 (as illustrated in Figures 21 and 22).

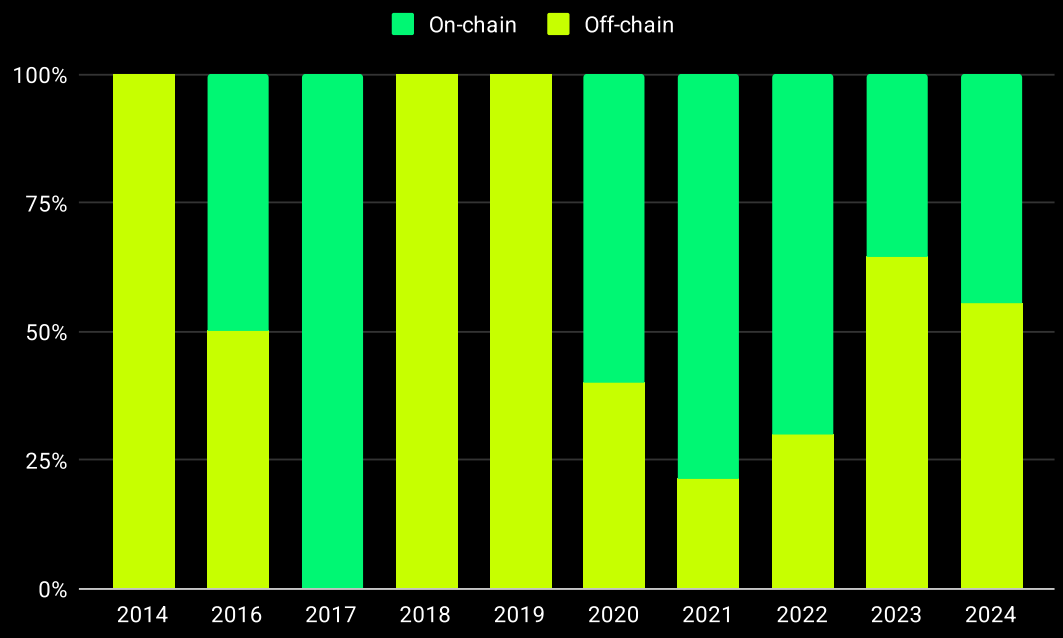

Figure 21: Number of off-chain and on-chain attacks per year [percentage]

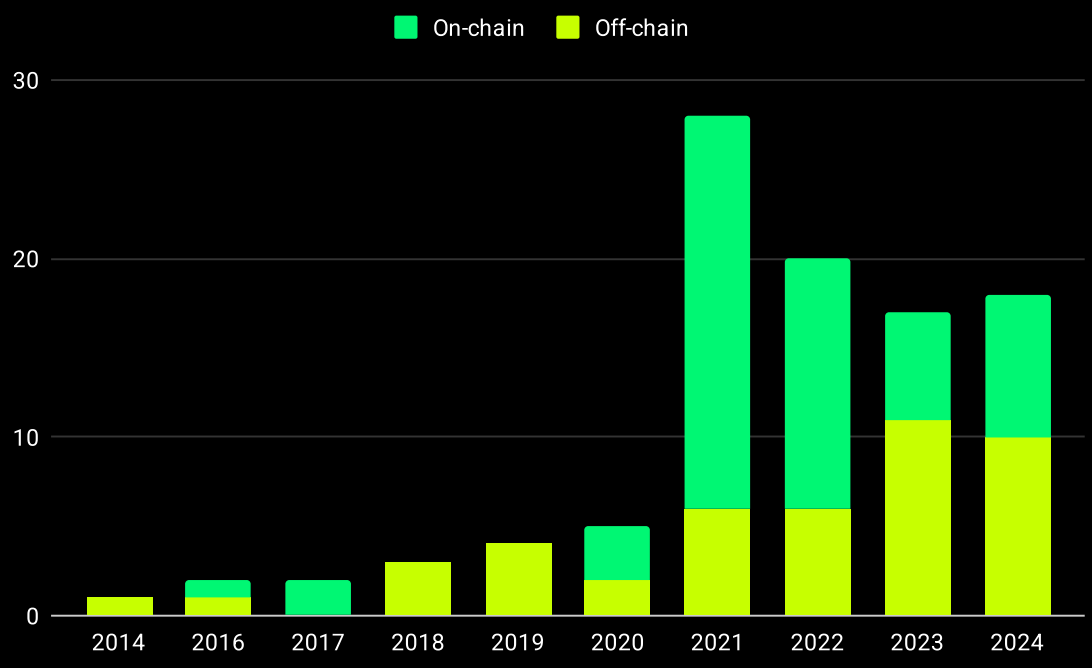

Figure 22: Number of off-chain and on-chain attacks per year [count]

By amount hacked, we can see a similar tendency in Figures 22 and 23. The percentage of funds lost by off-chain attack vectors increases each year since 2021, even in 2024.

The percentage in 2024 is higher in this case, reaching around 80.5% of total losses (around $1,032,664,888.26USD).

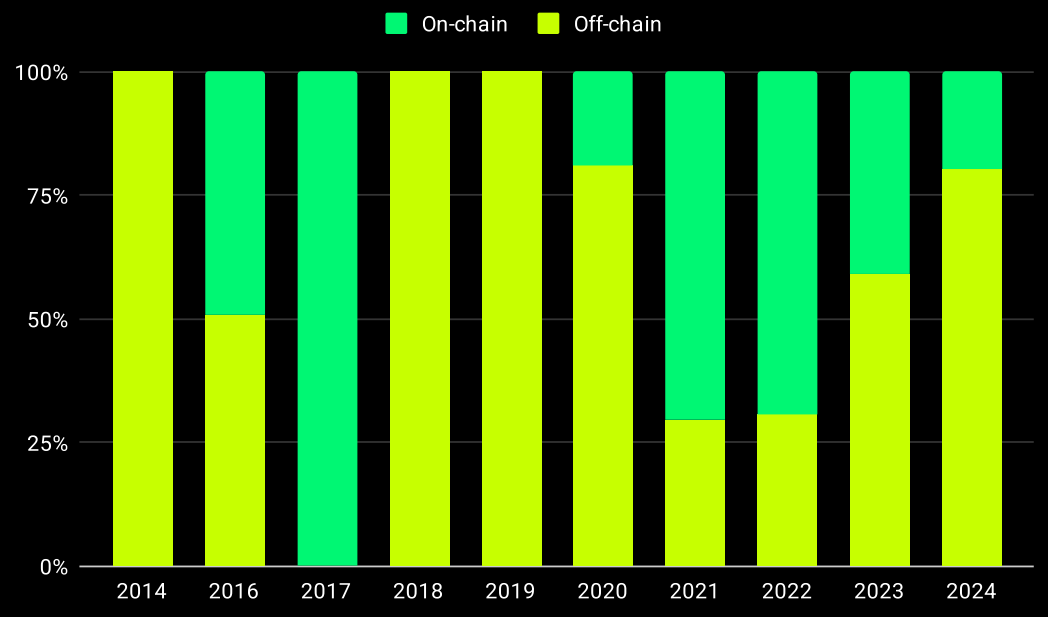

Figure 23: Loss caused by off-chain and on-chain attacks per year [percentage]

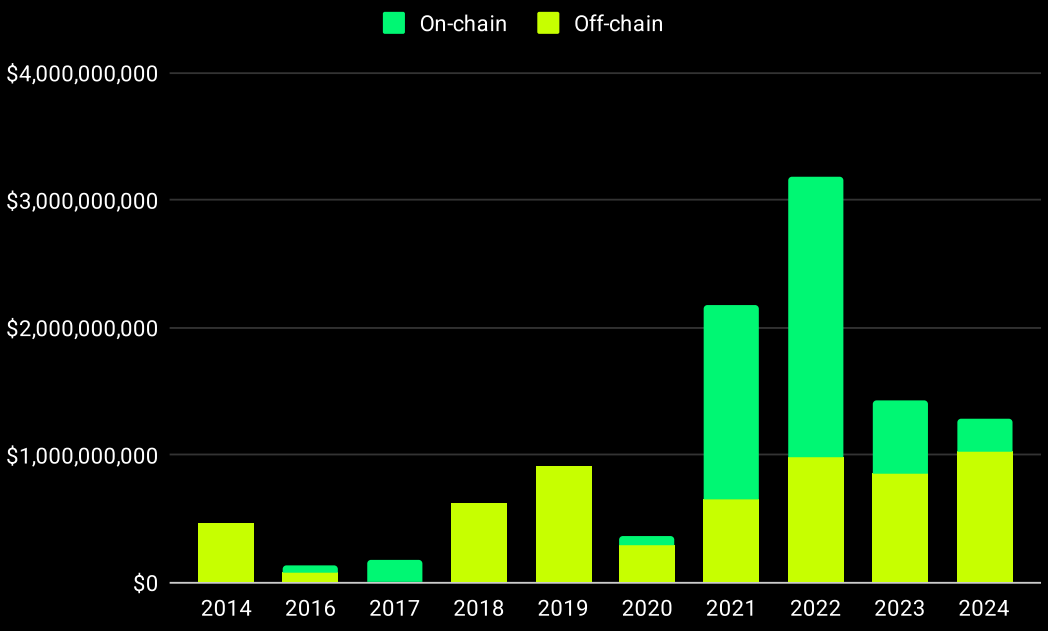

Figure 24: Loss caused by off-chain and on-chain attacks per year [USD]

Type of Attacks: Subcategories

As previously mentioned, the two main categories of attacks are further divided into several sub-categories.

According to Figures 25 and 26, which detail the division of these categories by occurrence, the most common cause of hacks is a compromised account, accounting for 42% of incidents. This is followed by attacks resulting from direct contract exploitation, which make up 26%, and market manipulation attacks, which represent 18% of the total.

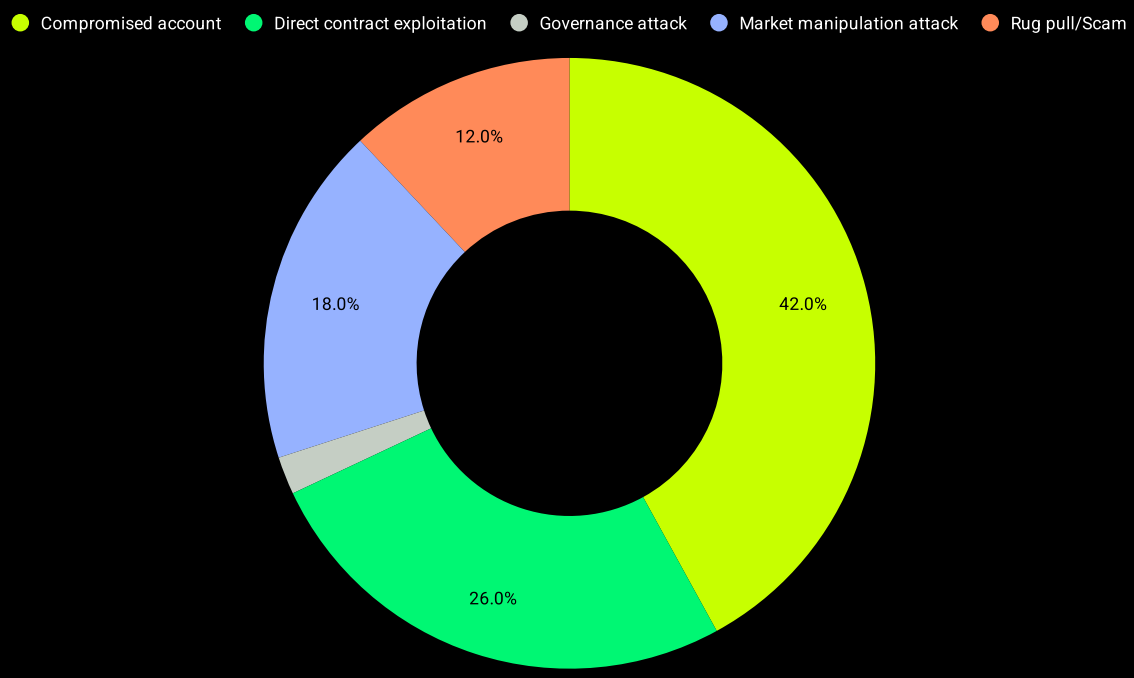

Figure 25: Number of attack sub-categories [percentage]

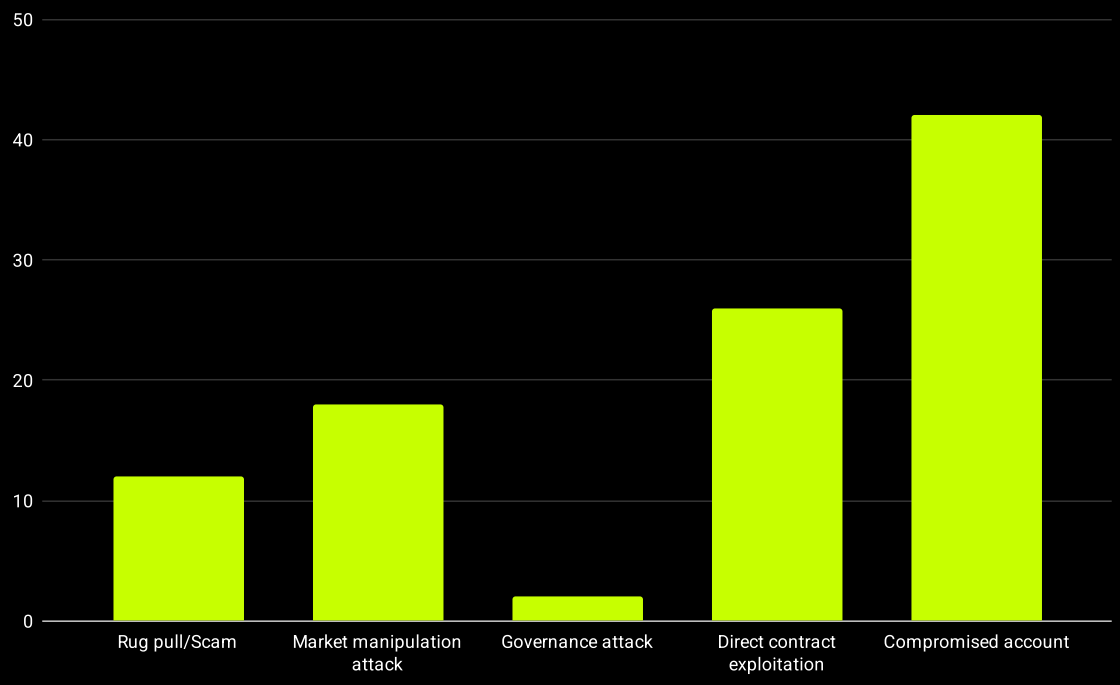

Figure 26: Number of attack sub-categories [count]

Analyzing the financial impact by type of attack reveals significant insights into the destructiveness of each attack vector, as depicted in Figures 27 and 28.

Compromised accounts are responsible for 47% of the total value hacked, totaling approximately $5,061,144,839 USD. This quantity is 5% higher than their occurrence rate, indicating that while these attacks are the most common, they are also very damaging in terms of financial losses. Direct contract exploitation, the second most common cause, accounts for 27.9% of the hacked value, amounting to $3,001,500,000 USD, which is slightly higher than its occurrence percentage.

It's noteworthy that while market manipulation attacks are the third most common by occurrence, they rank fourth in terms of the amount hacked, contributing to only 7.7% of the total losses ($830,123,000 USD). In contrast, rug pulls and other scams, although only representing 12% of the attacks, are responsible for a significant 15.6% of the total financial loss ($1,682,066,000 USD). This indicates that, although less frequent, these types of attacks can inflict substantial financial damage, underscoring their severe impact when they do occur.

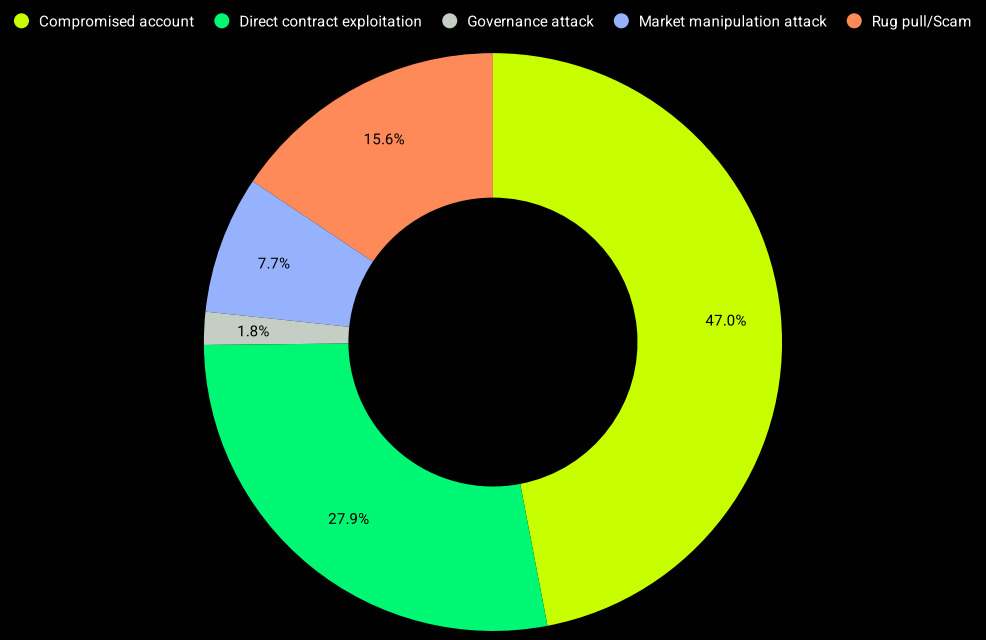

Figure 27: Loss caused by attack sub-categories [percentage]

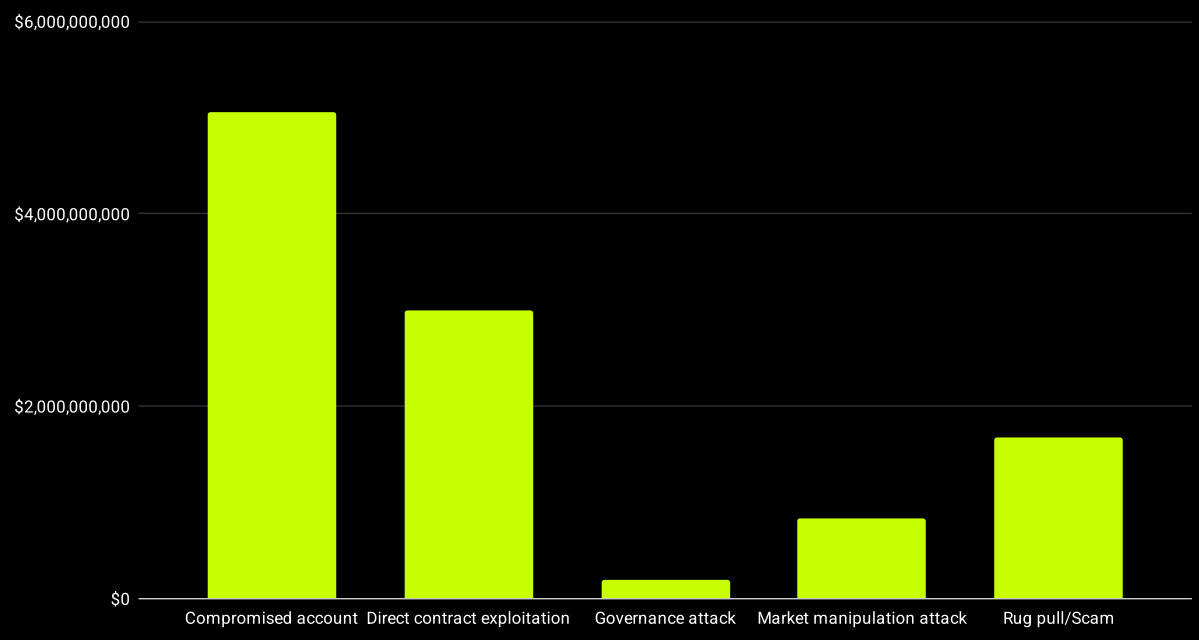

Figure 28: Loss caused by attack sub-categories [USD]

Analyzing the distribution of hacks by type over the years, as illustrated in Figures 29 and 30, reveals that compromised accounts have been a consistent and persistent threat within the DeFi ecosystem.

Compromised accounts have consistently been the predominant or one of the top attack vectors in almost every year, except for 2017, 2021 and 2022. Notably, in the last two years, they have accounted for more than half of all attacks, highlighting their ongoing relevance and danger.

Direct contract exploitation was the primary cause of hacks in 2017, accounting for 100% of the attacks that year, and again in 2022, where it was responsible for 45% of hacks. It also shared a significant proportion of attacks in 2020 and 2016, accounting for 40% and 50%, respectively, alongside compromised accounts.

Market manipulation was the leading cause of hacks in 2021, accounting for 32.1% of incidents, indicating a peak in this type of activity during that year.

Rug pulls and other scams had their most significant impact in 2019, where they accounted for 50% of the attacks, sharing the spotlight with compromised accounts.

Governance attacks are noted for their occurrence in 2022 and 2024, with each year witnessing a single instance of such an attack, making up 5% and 5.6% of the total attacks for those years, respectively.

This distribution suggests that while certain types of attacks may fluctuate in prevalence from year to year, compromised accounts remain a consistently significant risk, necessitating ongoing vigilance and improved security measures.

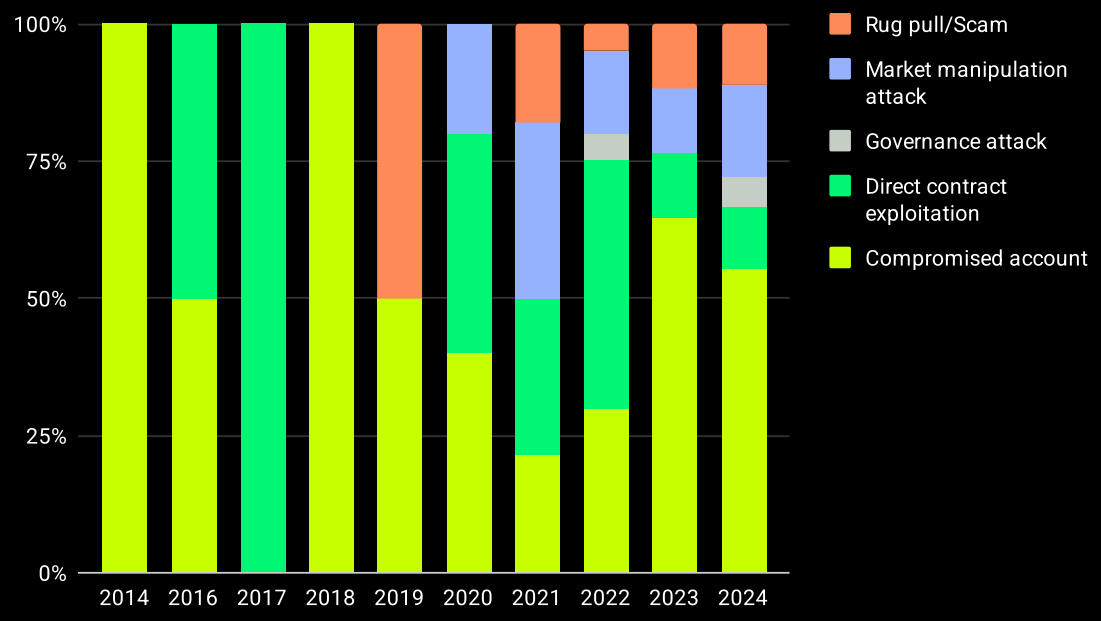

Figure 29: Number of attack sub-categories per year [percentage]

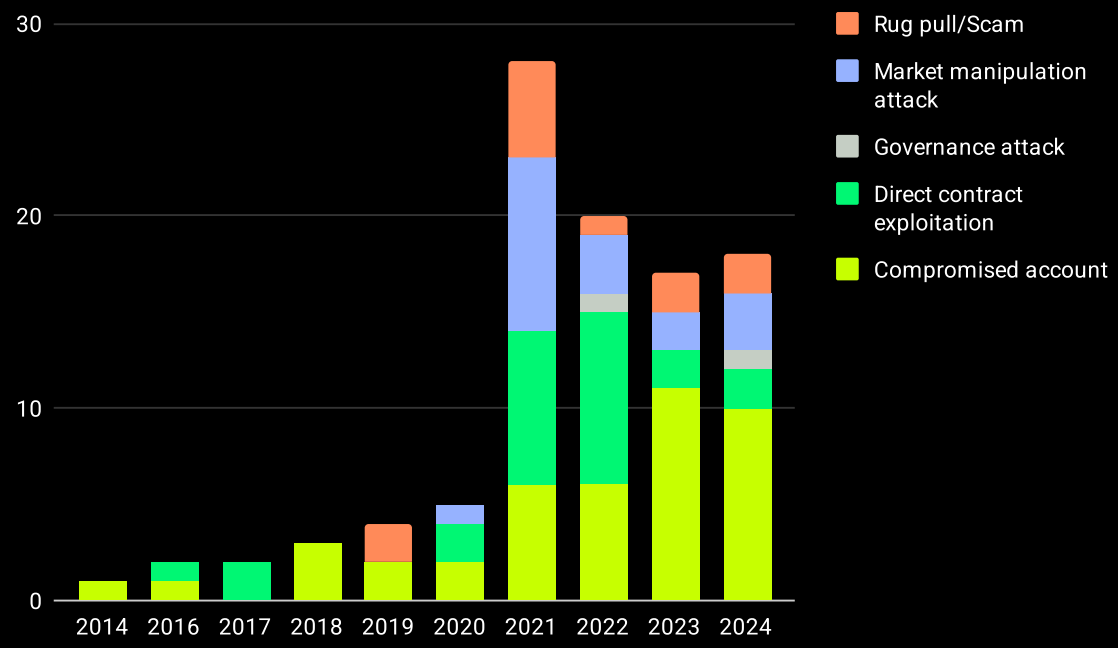

Figure 30: Number of attack sub-categories per year [count]

When analyzing the distribution of funds lost by type of attack each year, as depicted in Figures 31 and 32, we find some particularly alarming results concerning compromised accounts.

In 2024, this type of attack accounted for an overwhelming 80.5% of the total funds lost, amounting to $1,032,664,888 USD. This figure significantly exceeds their occurrence rate for the same year, which was only 55.6%. Similarly, in 2020, compromised accounts also led to disproportionate financial damages, constituting 81% ($297,000,000 USD) of the total amount hacked while only accounting for 40% of the attacks.

Attacks via direct contract exploitation have resulted in more financial loss compared to their frequency of occurrence in 2021 and 2023, representing 45.6% ($991,800,000 USD) and 18.6% ($266,300,000USD) of the total funds lost, against 28.6% and 11.8% of occurrences, respectively. However, for 2022 and 2024, the financial impact of these attacks was less pronounced compared to their occurrence rates, with losses of 43.1% ($1,376,500,000 USD) and 5.5% ($70,200,000 USD) versus occurrence rates of 45% and 11.1%.

Market manipulation attacks generally result in less severe financial impacts, accounting for fewer losses than their occurrences suggest. This indicates that while these attacks are frequent and generally sophisticated, they may not always translate into high financial losses.

Rug pulls and scams show varied economic impacts depending on the year. Notably, in 2019, these types of attacks were particularly devastating, accounting for 90.6% of the total funds lost in that year, which amounted to $822,000,000 USD.

On the other hand, governance attacks showed a slight increase in the financial losses in 2022, accounting for 5.7% ($181,000,000 USD) of the amount hacked but only 5% of the hacks, but they were less significant in 2024, constituting only 1.3% or $17,230,071 USD of the total losses against a rate of occurrence of 5.6%.

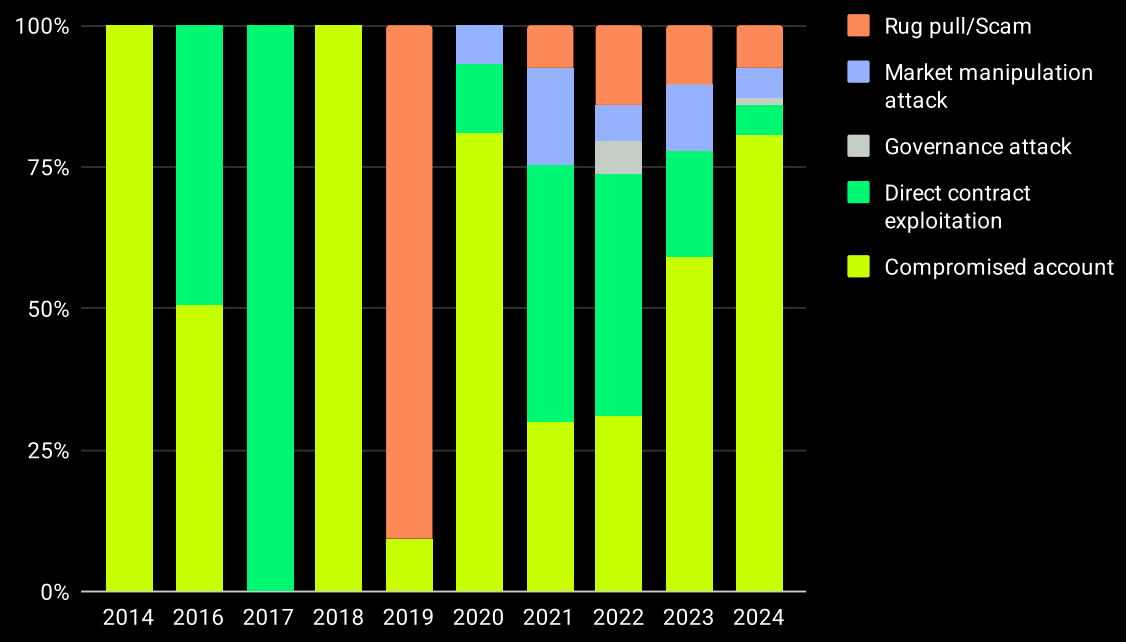

Figure 31: Loss caused by attack sub-categories per year [percentage]

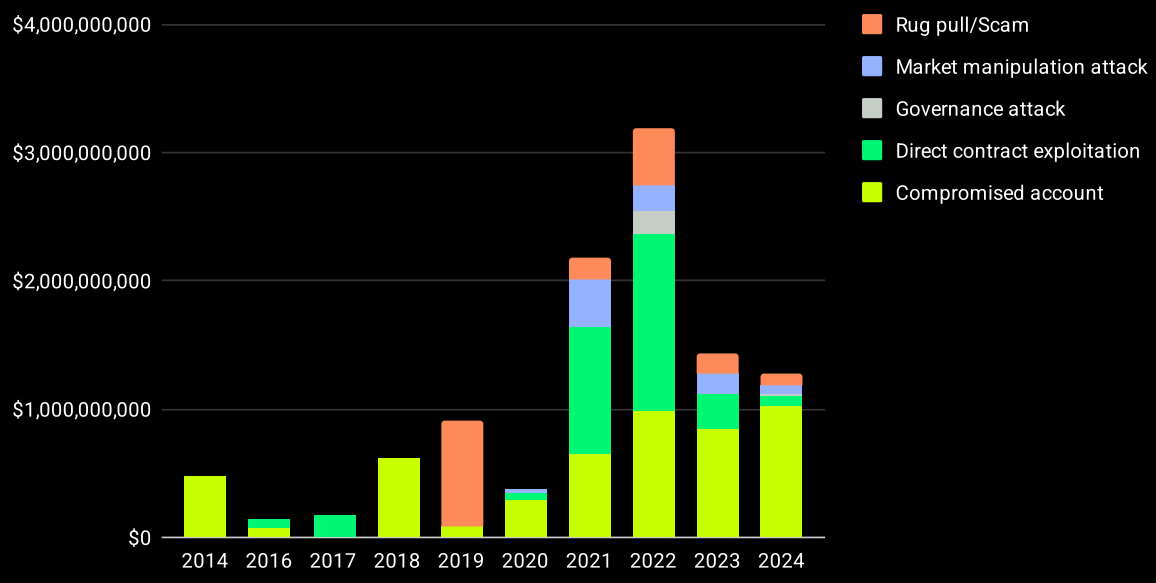

Figure 32: Loss caused by attack sub-categories per year [USD]

Signature Scheme and Wallet Protection

In the previous section, it was highlighted that the second most common cause of DeFi attacks involves the compromise of a project's account, which then allows attackers to exploit the protocol.

To deepen our understanding of how these vulnerabilities might occur, this analysis considers two key factors. First, we assess whether the vulnerable account was part of a multi-signature (multi-sig) or a multi-computation wallet or scheme. These security measures require that transactions must be authorized by two or more parties or involve all parts of a distributed signature, respectively.

Multi-sig setups offer enhanced security compared to single-signature transactions because they necessitate compromising more than one key or account to effect damage to the protocol. Similarly, in multi-computation wallets or schemes, the key is fragmented into several encrypted shares, which are then distributed among multiple stakeholders.

Our research indicates that only 19% of the attacks involving compromised accounts were associated with either a multi-signature or multi-computation wallet or scheme. There is one instance categorized as 'Unknown' due to the absence of publicly available information regarding the type of account that was attacked, as detailed in Figures 33 and 34.

This data underscores the relative rarity of breaches involving these more secure types of accounts, pointing to their effectiveness in mitigating risks associated with account compromises in the DeFi sector.

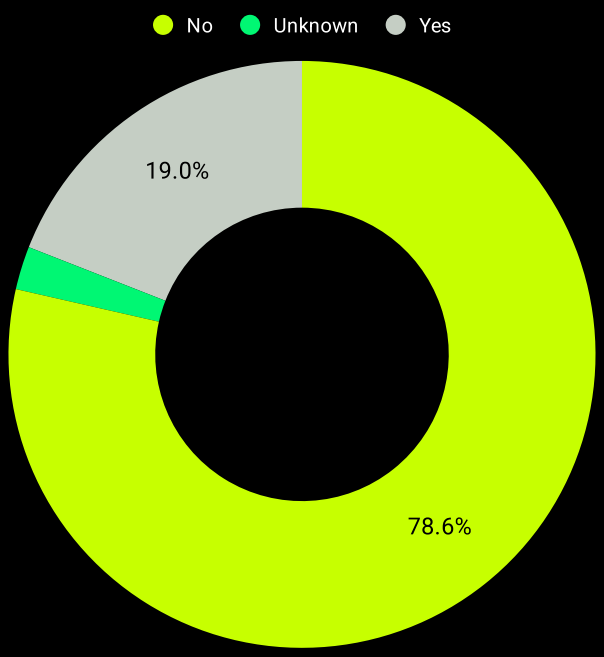

Figure 33: Number of wallets/schemes using multi-signature or MPC [percentage]

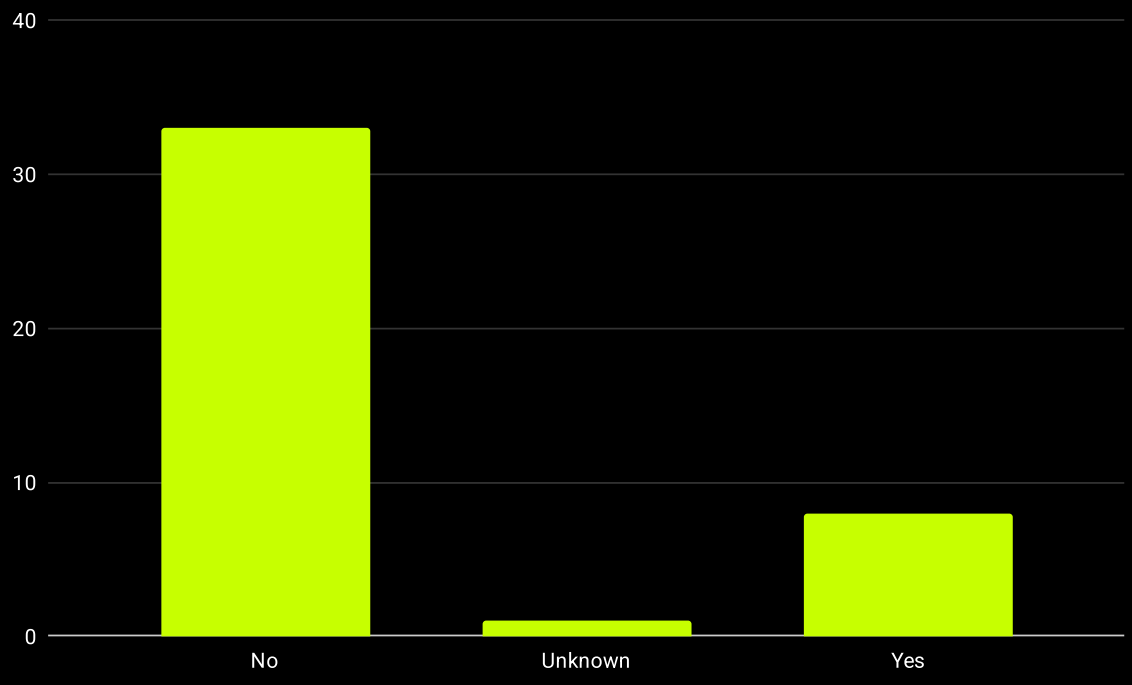

Figure 34: Number of wallets/Schemes using multi-signature or MPC [count]

While 78.6% of the protocols that were attacked did not employ multi-signature or multi-party computation (MPC) wallets or schemes, highlighting a higher risk associated with simpler security arrangements, it's important to note that these advanced security measures do not completely prevent financial losses from attacks.

In fact, even when such enhanced security features were in place, the attacks that successfully breached these protocols still led to significant financial repercussions, accounting for 29.5% of the total losses, or approximately $1,493,000,000 USD, as shown in Figures 35 and 36.

This data indicates that although breaching protocols secured with multi-sig or MPC wallets is more challenging, the high value of funds or the extensive management privileges these wallets often handle can result in substantial damages if compromised.

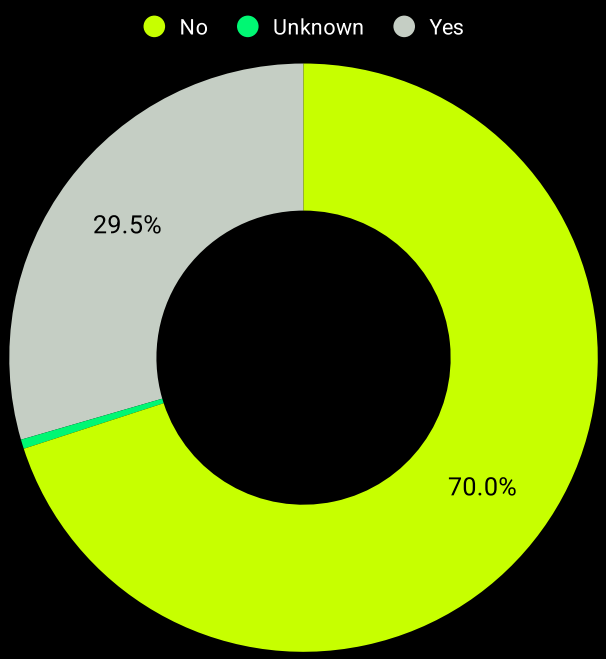

Figure 35: Loss caused by wallets using multi-signature or MPC [percentage]

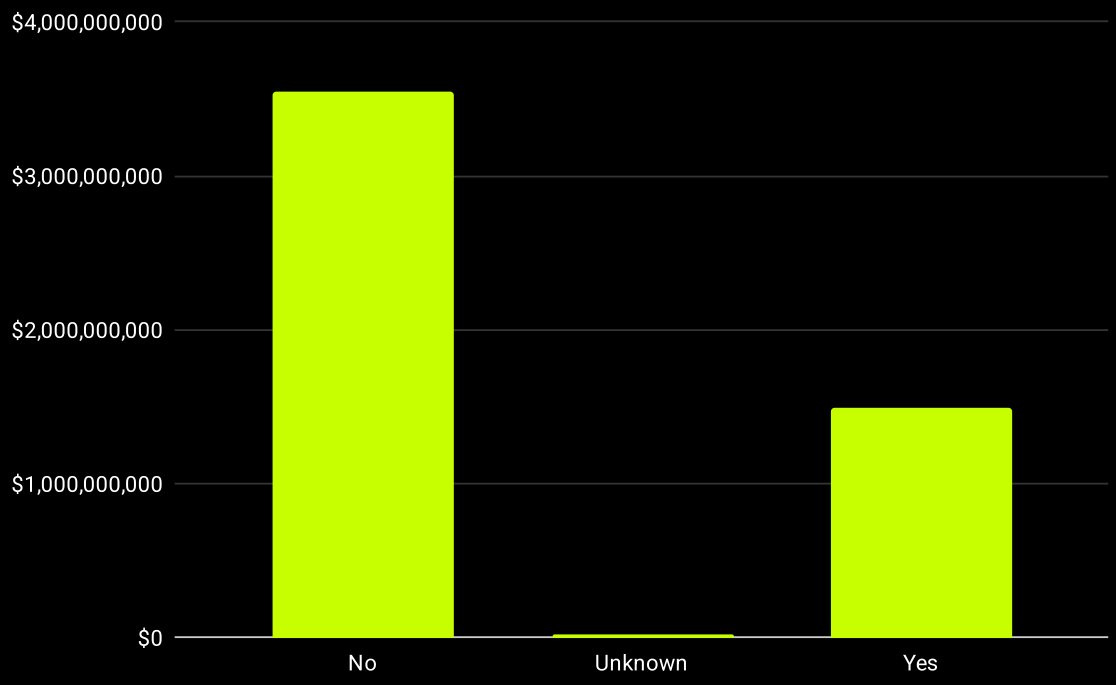

Figure 36: Loss caused by wallets using multi-signature or MPC [USD]

Over the years, the adoption of multi-signature or multi-party computation (MPC) wallets and schemes in the context of security breaches has shown some variation. For instance, this type of security measure was employed by Bitfinex during their 2016 hack.

Following this, approximately 30% of the attacks in 2018, 2022, and 2024 involved protocols using such wallets or schemes. In 2023, only one attack (9.1% of that year's total) featured this type of security technology. In other years, these enhanced security mechanisms were not utilized.

This pattern suggests an intermittent reliance on multi-signature and MPC technologies, reflecting either shifting security strategies among DeFi protocols or variations in how attackers target these systems.

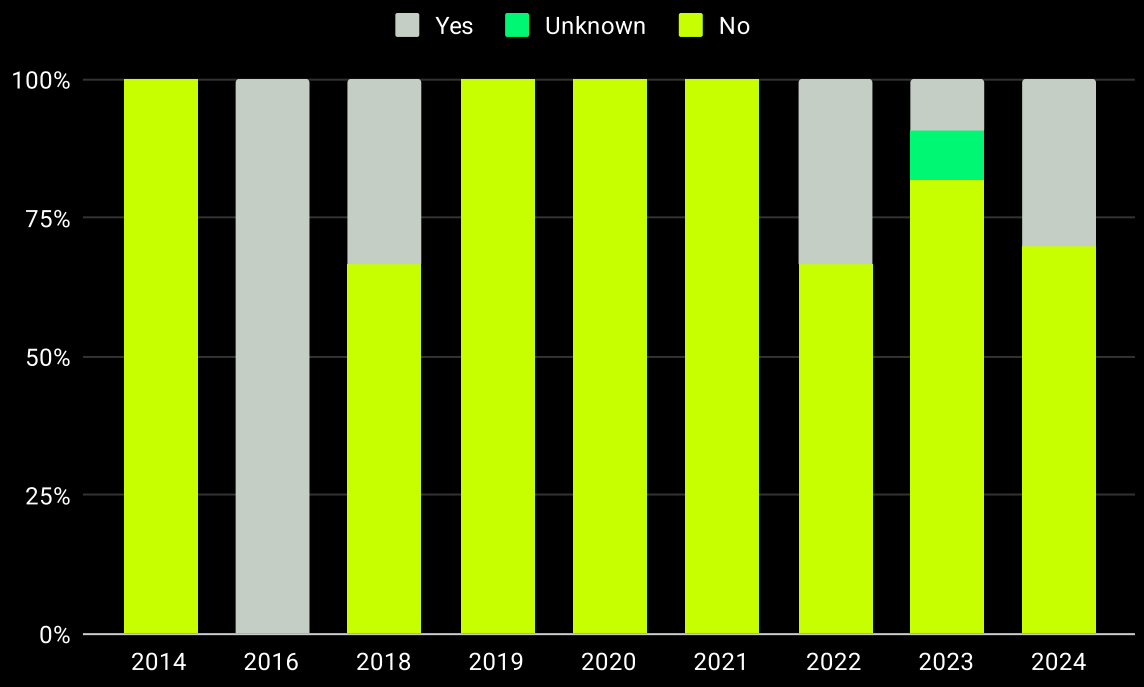

Figure 37: Number of wallets using multi-signature or MPC per year [percentage]

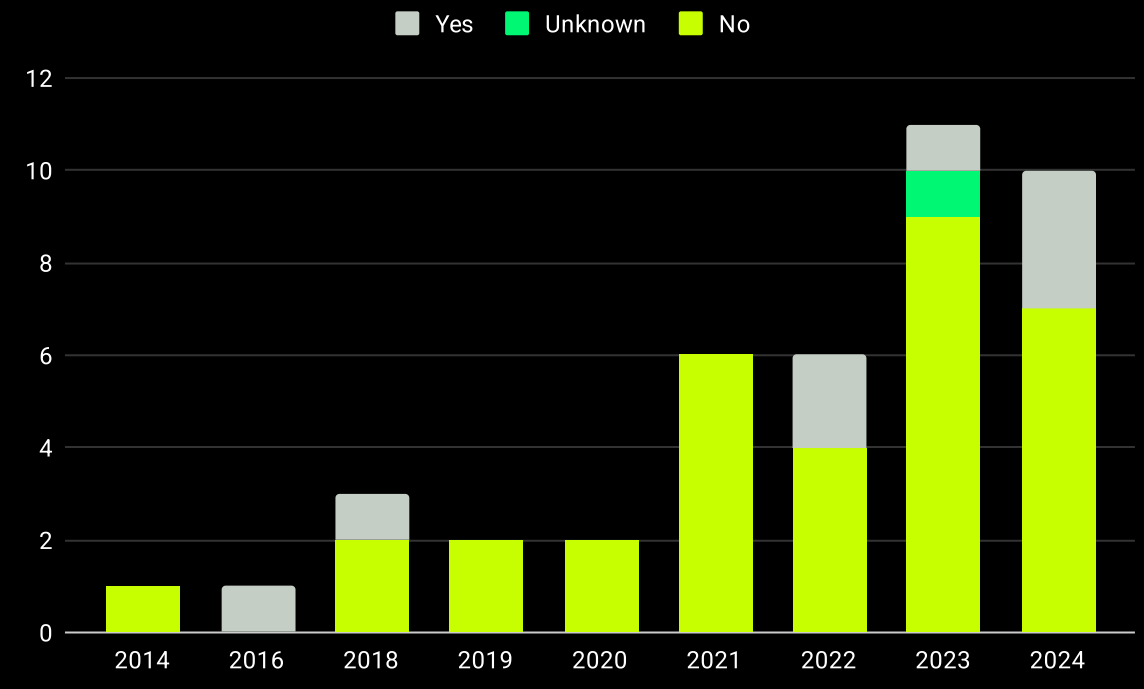

Figure 38: Number of wallets using multi-signature or MPC per year [count]

Examining the evolution of losses associated with multi-signature or multi-party computation (MPC) wallets and schemes, as depicted in Figures 39 and 40, reveals an inconsistent pattern across the years.

In 2018, these types of security measures experienced minimal financial losses, accounting for only 3.8% of the total, equivalent to $23,500,000 USD. This relatively low figure indicates that attacks on these secured mechanisms were less severe during this year.

However, a significant increase in losses is observed in later years, particularly in 2022 and 2024, where the quantity hacked amounted to 73.5% ($724,000,000 USD) and 57.3% ($592,000,000 USD), respectively. In 2023, the losses were proportionate to the occurrence rate of attacks on these wallets or schemes, making up 9.6% of the total or $81,500,000 USD.

The substantial increase in 2022 can be largely attributed to the Ronin Bridge hack, where attackers exploited vulnerabilities in the platform's multi-signature security, resulting in a loss of $624,000,000 USD.

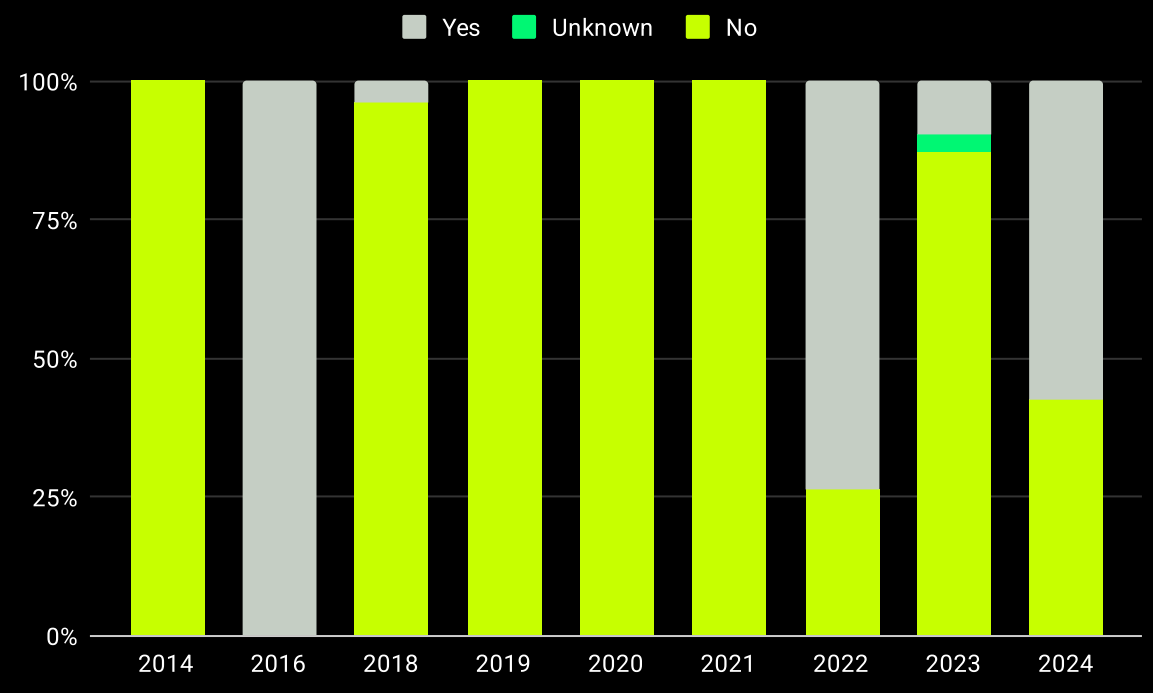

Figure 39: Loss caused by wallets using multi-signature or MPC per year [percentage]

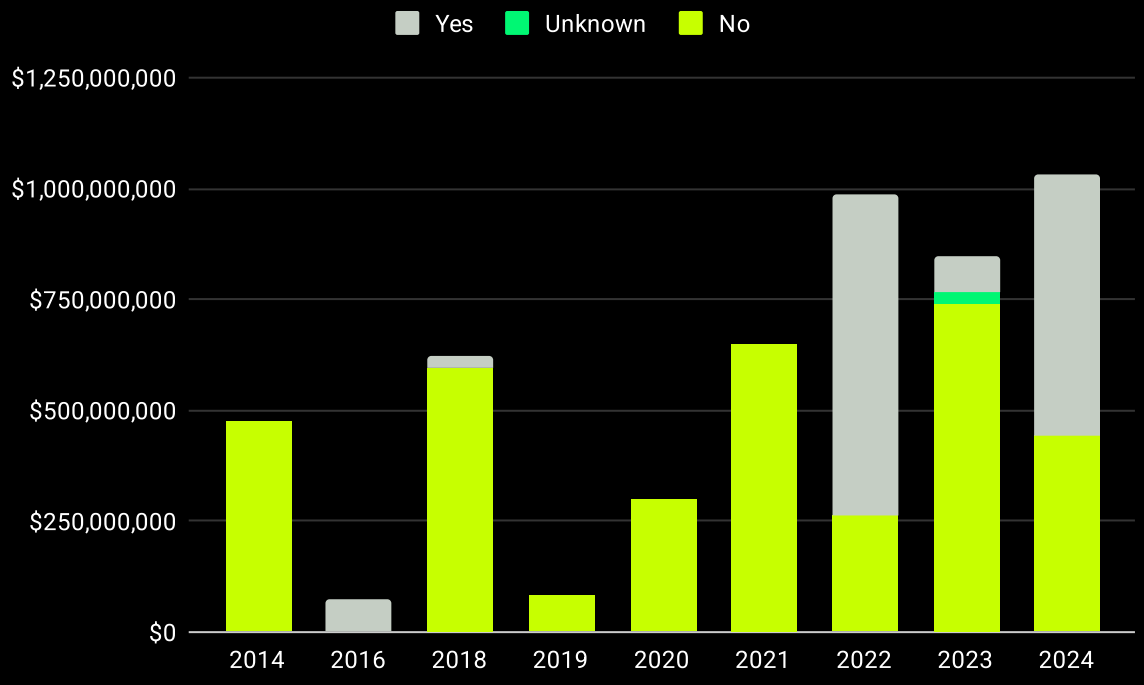

Figure 40: Loss caused by wallets using multi-signature or MPC per year [USD]

Another crucial aspect of securing digital assets involves the choice between using hot wallets, which are connected to the Internet, and cold wallets, which store private keys offline.

Hot wallets provide ease of use due to their constant internet connectivity, making them highly suitable for frequent transactions. However, this accessibility also makes them more vulnerable to cyberattacks since they can be targeted remotely by hackers. On the other hand, cold wallets offer enhanced security by keeping private keys offline, significantly reducing the risk of unauthorized remote access. To compromise a cold wallet, an attacker typically needs physical access to it, along with any necessary passwords or other security measures required to unlock access to the funds.

In the sample analyzed, as shown in **Figures 41** and **42**, a significant majority of the compromised accounts, 88.1%, were stored in hot wallets. This underscores the heightened risk associated with their use. Additionally, two cases are marked as N/A because they involved signature or approval compromises via phishing to individual users, where the distinction between hot and cold wallets does not impact the nature of the attack. There are also a couple of protocols where insufficient information is available about the type of account compromised. Notably, only one project, Radiant Capital, experienced a security breach involving their hardware wallets, which are a form of cold storage.

This instance highlights that while cold wallets are generally more secure, they are not entirely invulnerable to attacks, especially if physical security measures are compromised.

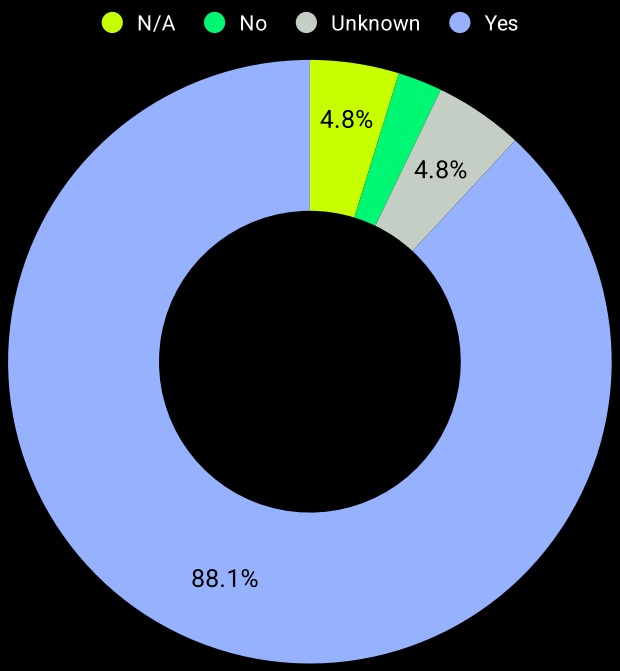

Figure 41: Usage of hot wallets [percentage]

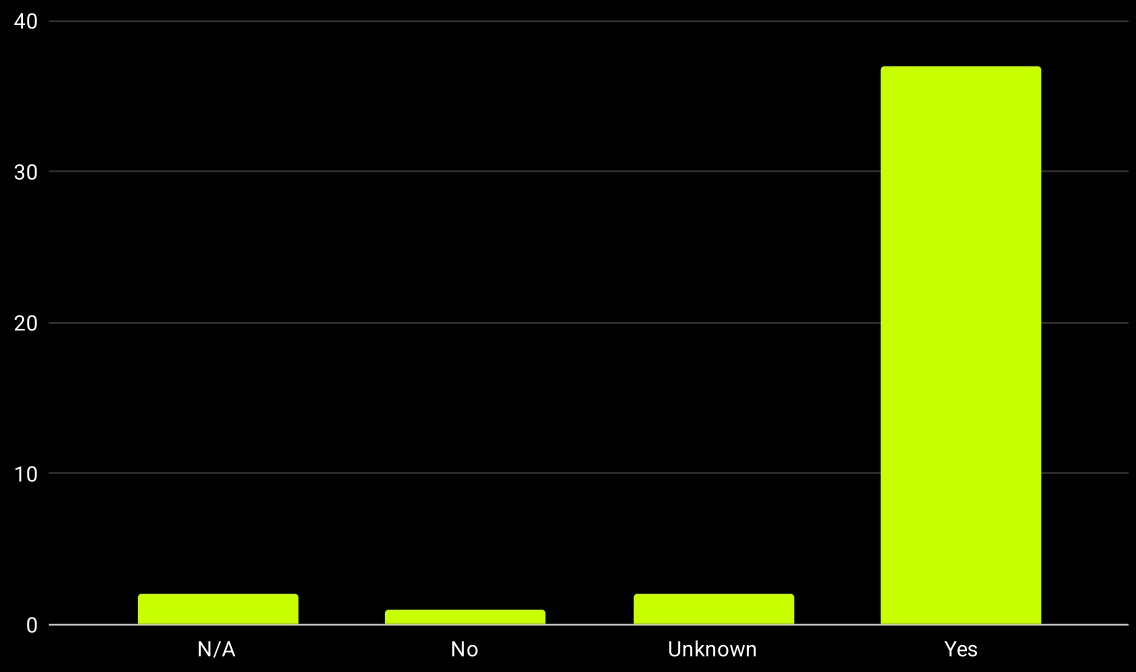

Figure 42: Usage of hot wallets [count]

Figures 43 and 44 provide a comparative analysis of the financial losses associated with different types of wallets, revealing that a substantial 90.7% of the total value lost, amounting to $4,590,674,839 USD, is attributed to compromises involving hot wallets.

This data underscores the high risk and frequent targeting of hot wallets due to their internet connectivity and easier accessibility for cybercriminals.

On the other hand, the losses from cold wallets constitute a lower proportion than their occurrence rate—only 1% of the total losses compared to 2.4% of the attacks. This discrepancy suggests that attacks on cold wallets might be less profitable, potentially due to the compromised keys being less critical or controlling fewer funds. However, it's important to note that the sample size for cold wallet attacks is relatively small, which limits the conclusiveness of this observation and could mean the results are influenced by other factors, such as the specific security protocols of the compromised accounts.

Furthermore, the category marked as N/A, involving cases where the wallet type does not significantly impact the nature of the compromise (such as signature or approval compromises through phishing), shows a similar trend of lower financial impact compared to occurrence, with 3.5% ($175,470,000 USD) of the losses versus 4.8% of the attacks.

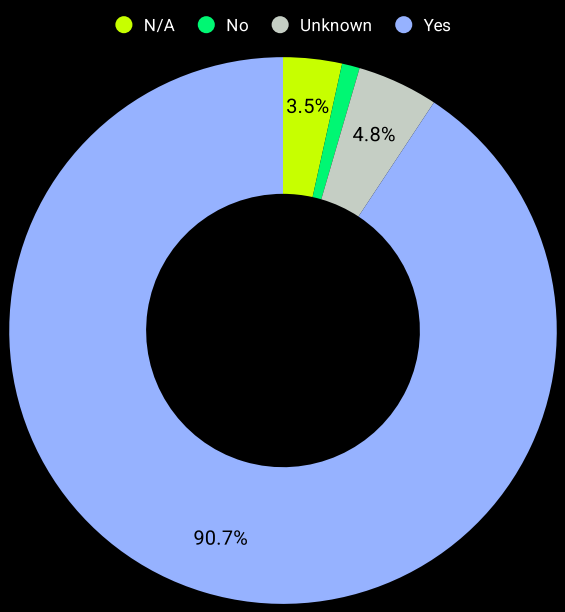

Figure 43: Loss caused by the usage of hot wallets [percentage]

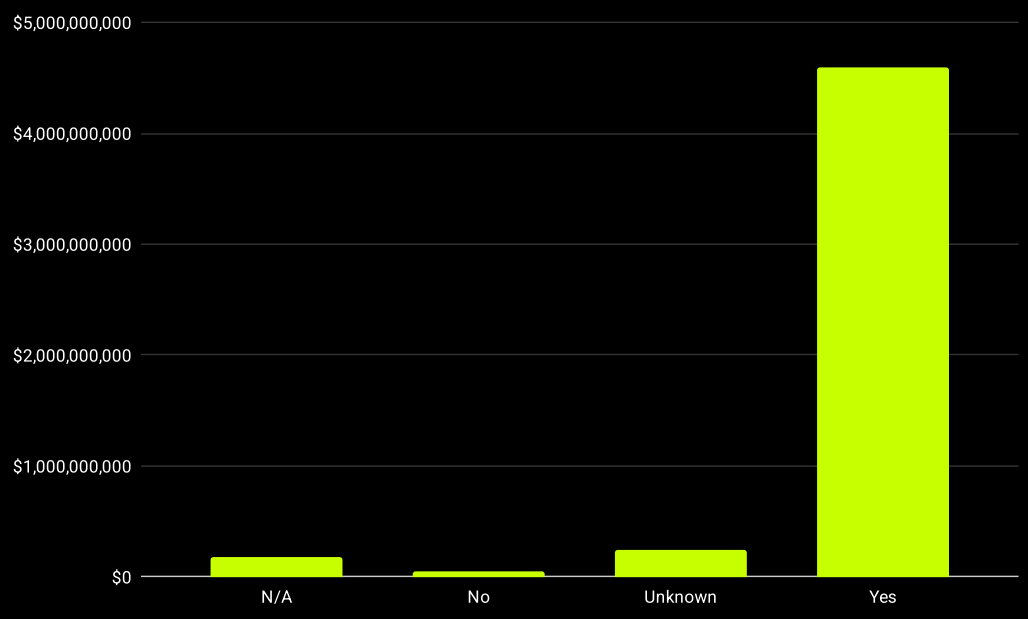

Figure 44: Loss caused by the usage of hot wallets [USD]

Analyzing the distribution of attacks by wallet type over the years, as shown in Figures 45 and 46, reveals specific patterns in the occurrence of security breaches based on the storage method used.

In 2024, there was only one recorded attack involving a private key stored in a cold wallet.

The N/A category, on the other hand, is spread between 2021 and 2024. This suggests a trend of security breaches that exploit human factors rather than technological vulnerabilities in more recent years.

Furthermore, cases where the type of compromised wallet remains unclear are documented in 2023 and 2024. This could indicate a lack of detailed reporting on the incidents that makes it difficult to ascertain the exact type of wallet or account compromised.

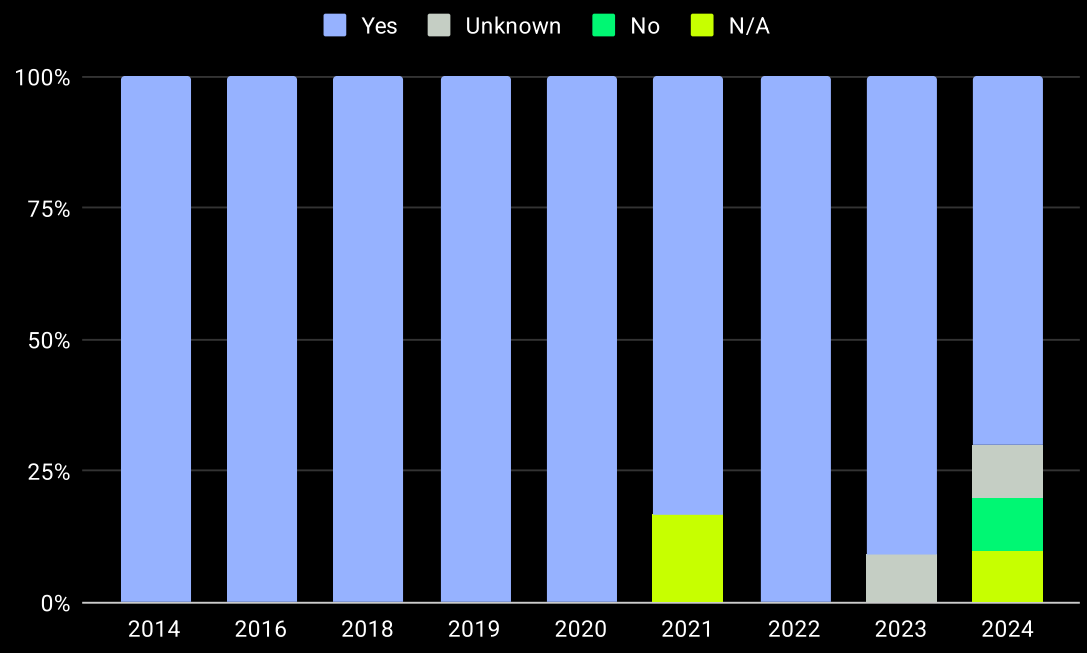

Figure 45: Usage of hot wallets by year [percentage]

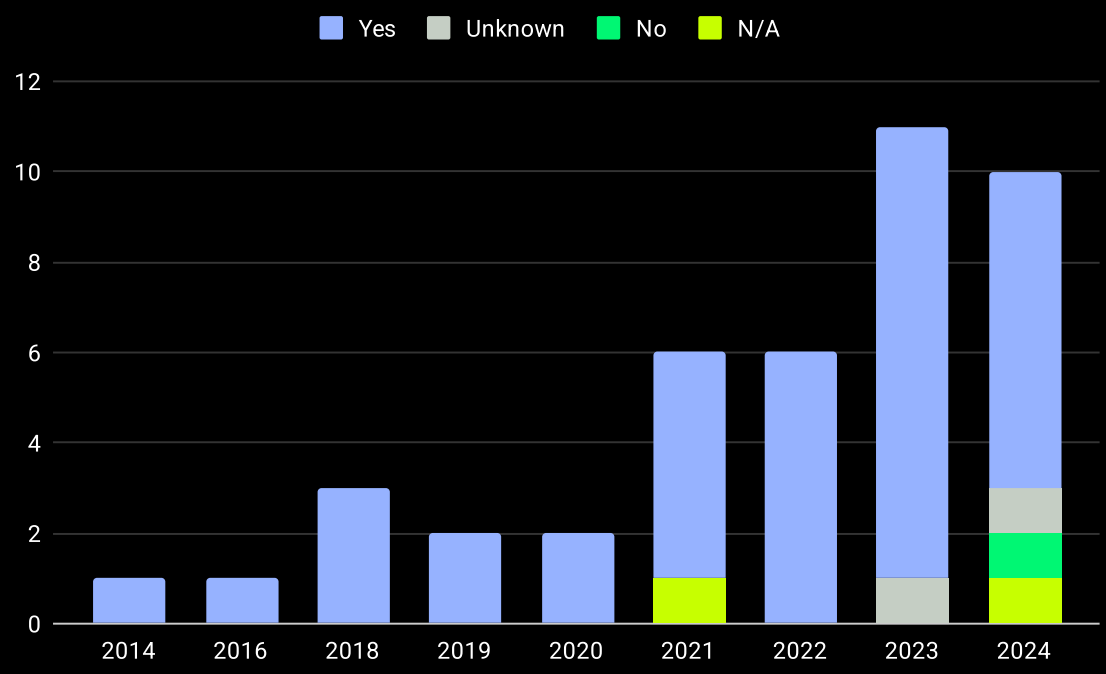

Figure 46: Usage of hot wallets by year [count]

Reviewing the losses by year, as depicted in Figures 47 and 48, reinforces previously observed trend: it confirms that the financial damage resulting from attacks on cold wallets tends to be smaller compared to those involving hot wallets.

However, as noted, the sample size for cold wallet attacks is quite small, which could mean that the apparent lesser damage might be influenced by factors such as the amount of funds stored or the specific security practices employed.

In terms of the N/A category, there is a notable discrepancy in the relative amount of funds lost. In 2021, the loss from an N/A attack accounted for 18.5% ($120,000,000 USD) of the total, which is slightly higher than its occurrence rate of 16.7%. Conversely, in 2024, the loss was lower at 5.4% ($55,470,000 USD) compared to its occurrence rate of 10%.

For attacks marked as unknown, the amount of funds lost also varies. In 2023, these attacks resulted in losses amounting to only 3.1% ($26,000,000 USD) of the total, against an occurrence rate of 9.1%, suggesting a lower impact per incident. However, in 2024, the loss from unknown attacks increased significantly to 20.9% ($216,000,000 USD) against an occurrence rate of 10%, indicating a higher financial impact.

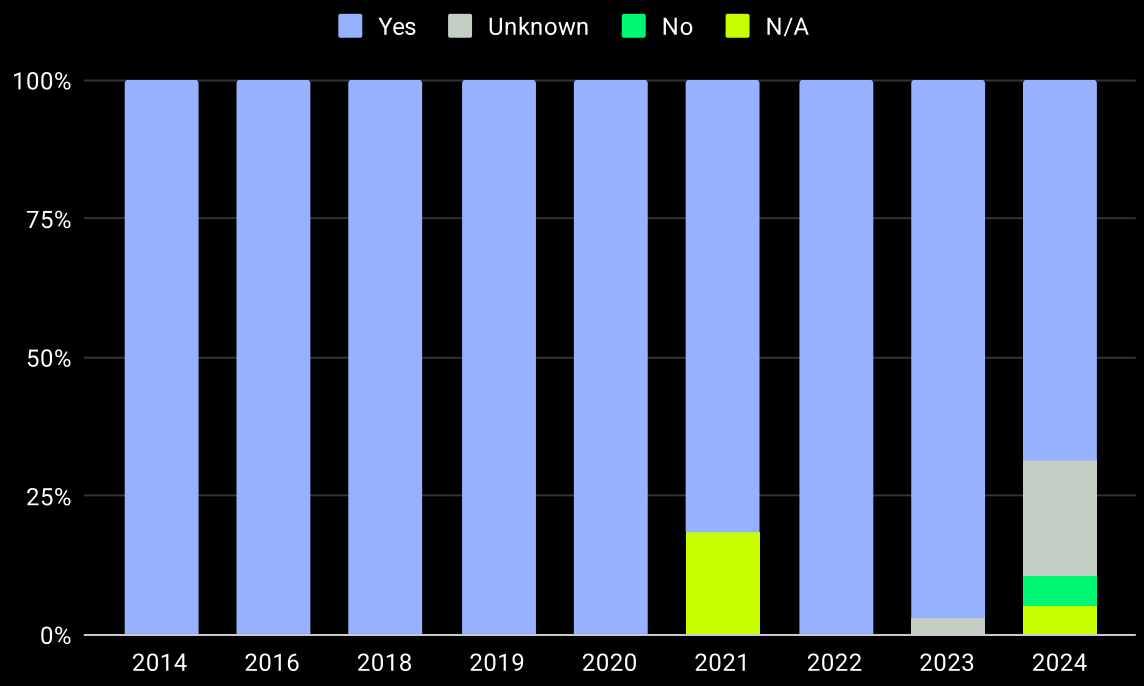

Figure 47: Loss caused by the usage of hot wallets by year [percentage]

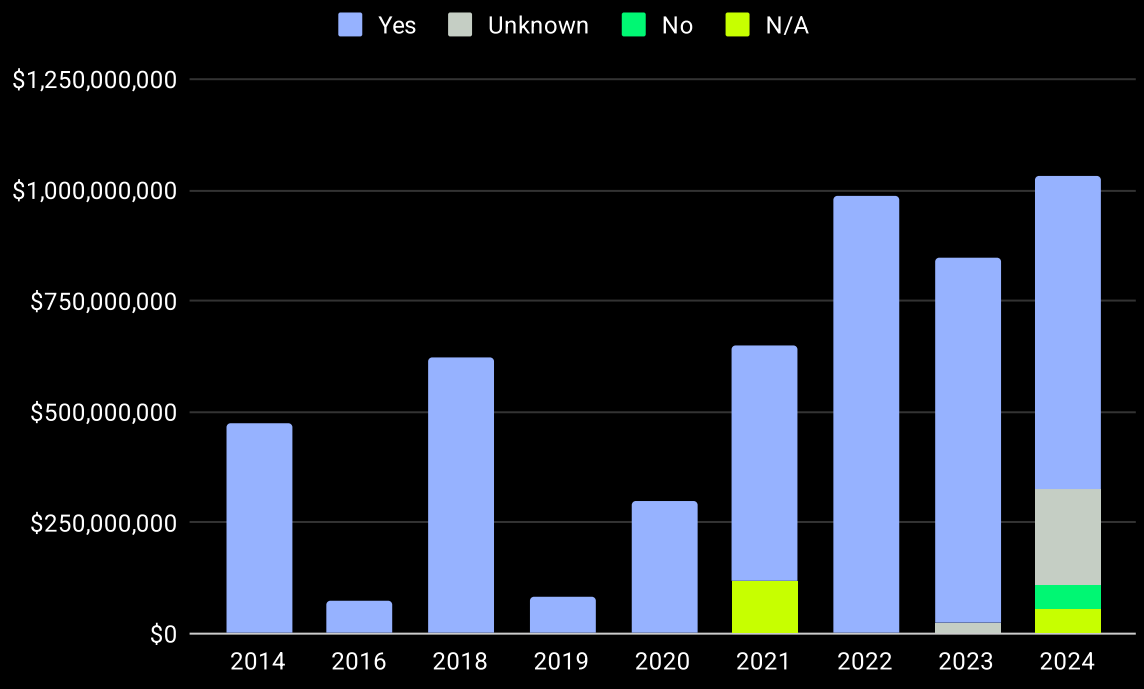

Figure 48: Loss caused by the usage of hot wallets by year [USD]

Use of Flash Loans

Flash loans allow users to borrow assets without upfront collateral, with the condition that the loan must be repaid within the same blockchain transaction.

While these loans offer legitimate opportunities for arbitrage and other financial strategies, they also present potential avenues for exploitation.

According to the data presented in Figures 49 and 50, a significant portion of attacks interacting with smart contracts utilize flash loans, though the majority do not. Specifically, 58.7% of such attacks do not involve the use of flash loans, while 41.3% do make use of them.

This indicates that while flash loans seem to be a notable vector for attacks, they are not overwhelmingly predominant in this context.

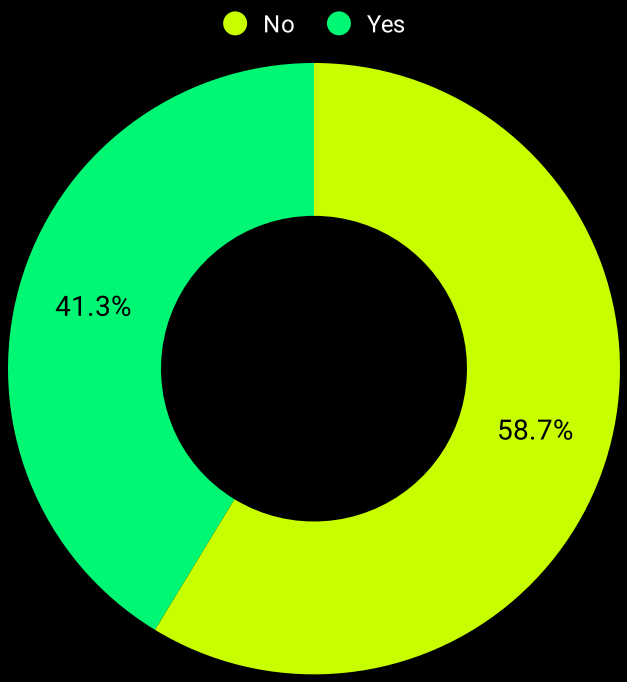

Figure 49: Usage of flash loans [percentage]

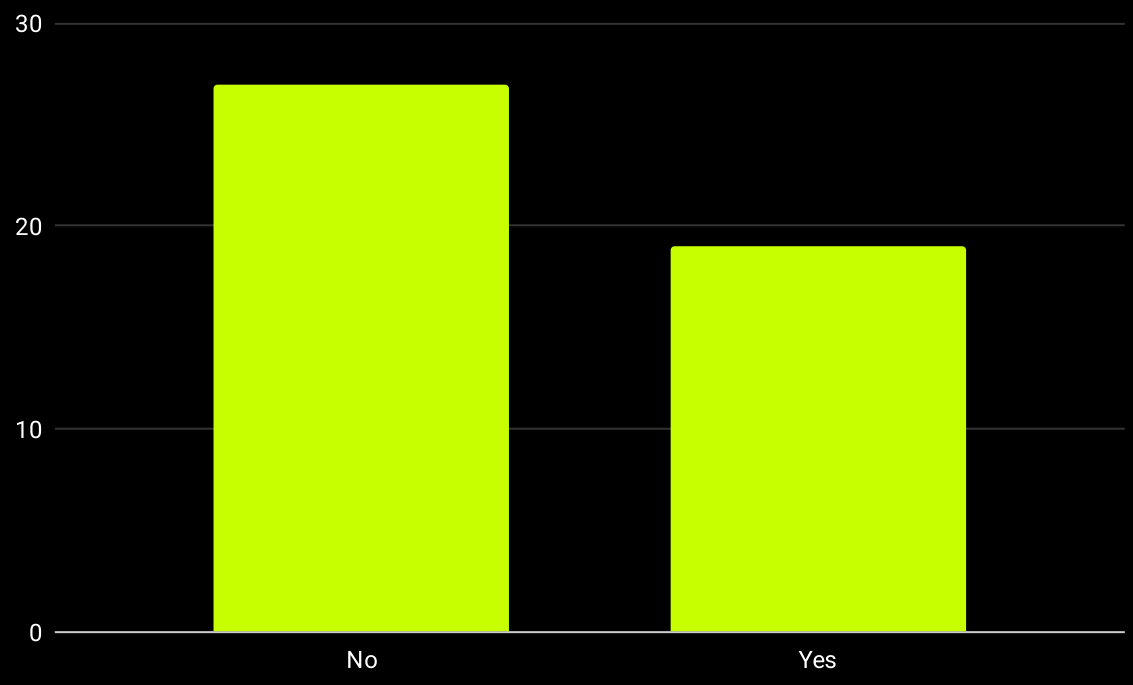

Figure 50: Usage of flash loans [count]

The analysis of whether flash loans result in higher financial losses during attacks is addressed in Figures 51 and 52.

Interestingly, the data suggests that although flash loans are employed in 41.3% of the attacks, they do not necessarily lead to proportionally larger losses. In fact, attacks involving flash loans account for only 25.5% of the total financial damage, approximately $1,028,353,071 USD.

This discrepancy indicates that while flash loans are a notable mechanism within the spectrum of attack vectors, their use does not inherently correlate with more significant financial damage compared to other types of attacks. It suggests that the impact of flash loans may be more related to the specific vulnerabilities they exploit rather than their intrinsic nature as a financial tool.

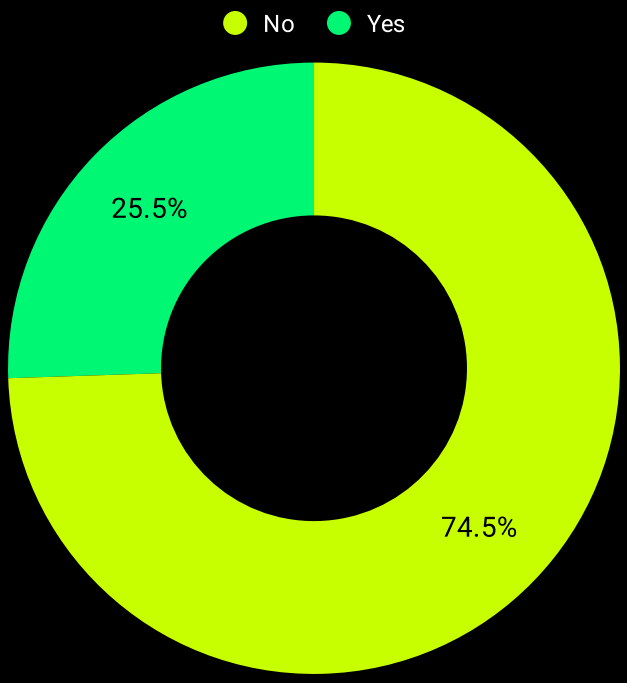

Figure 51: Loss caused by the usage of flash loans [percentage]

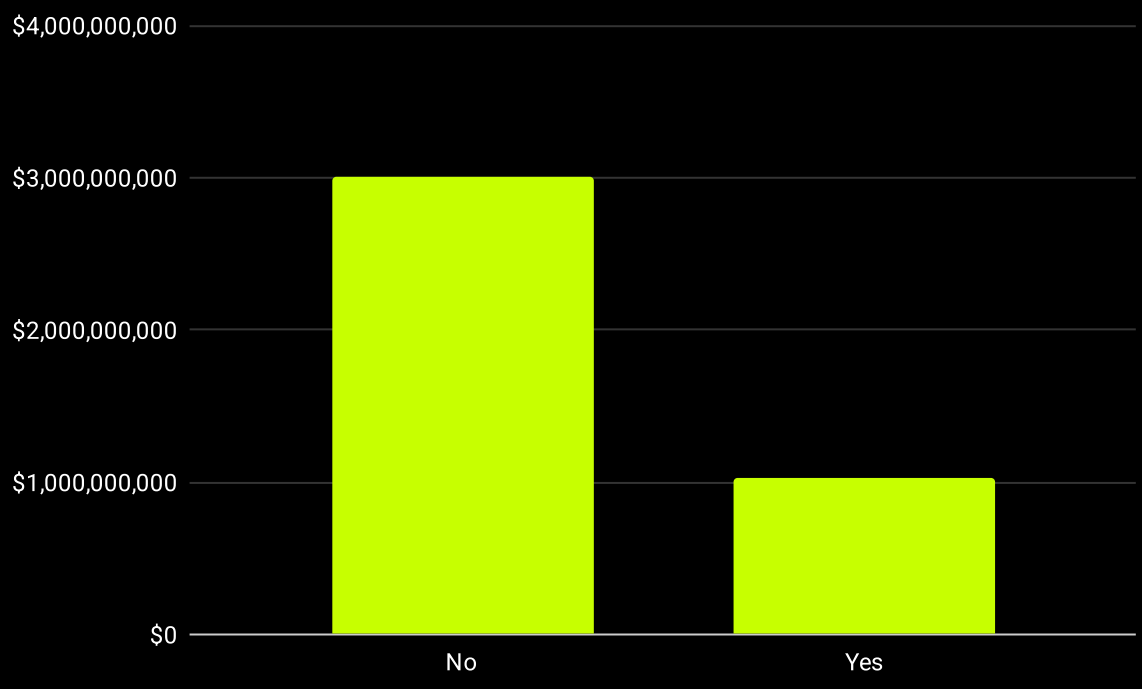

Figure 52: Loss caused by the usage of flash loans [USD]

The evolution of flash loan usage in attacks over recent years shows a dynamic trend, as depicted in Figures 53 and 54.

After observing a decline in the use of flash loans from 2021 to 2022, there has been a notable resurgence in the following years. In 2023, flash loans were utilized in 50% of the attacks, and this figure increased dramatically in 2024, where 83.3% of attacks employed this mechanism.

This upward trend suggests that attackers are increasingly leveraging flash loans as a tool for exploitation within the DeFi ecosystem. The sharp increase in 2024 indicates a growing familiarity and sophistication among attackers in using flash loans to execute their strategies. This could be attributed to the unique capabilities of flash loans that allow for large, rapid movements of capital without upfront collateral, presenting opportunities for exploiting price differentials or vulnerabilities within DeFi protocols more effectively.

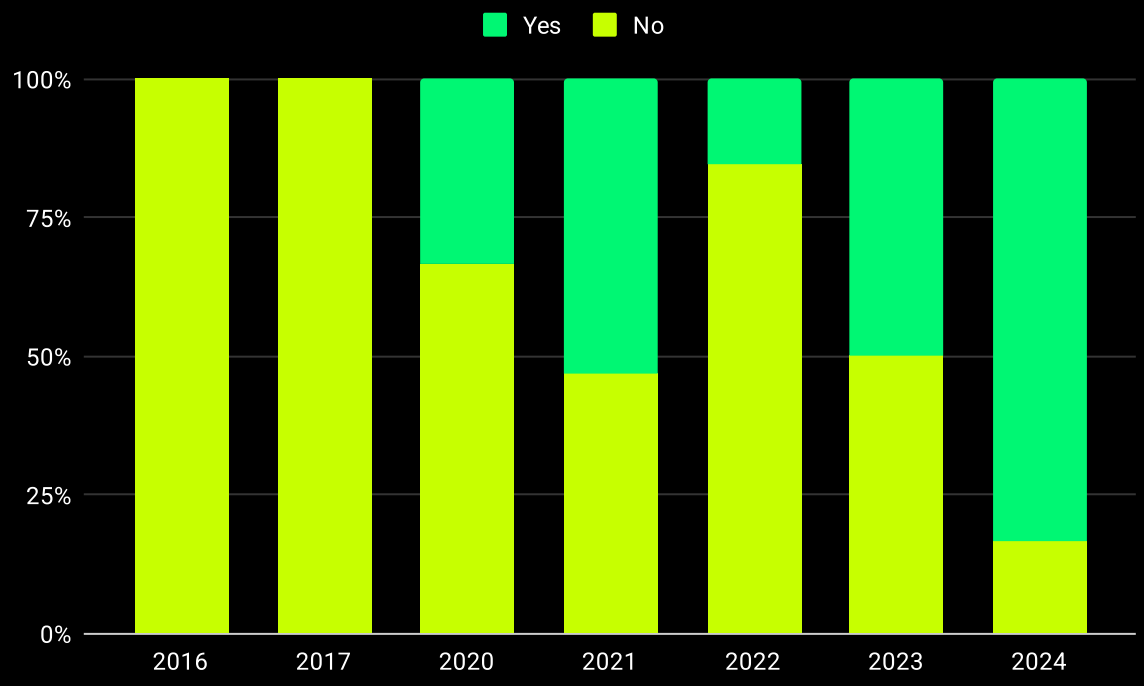

Figure 53: Usage of flash loans per year [percentage

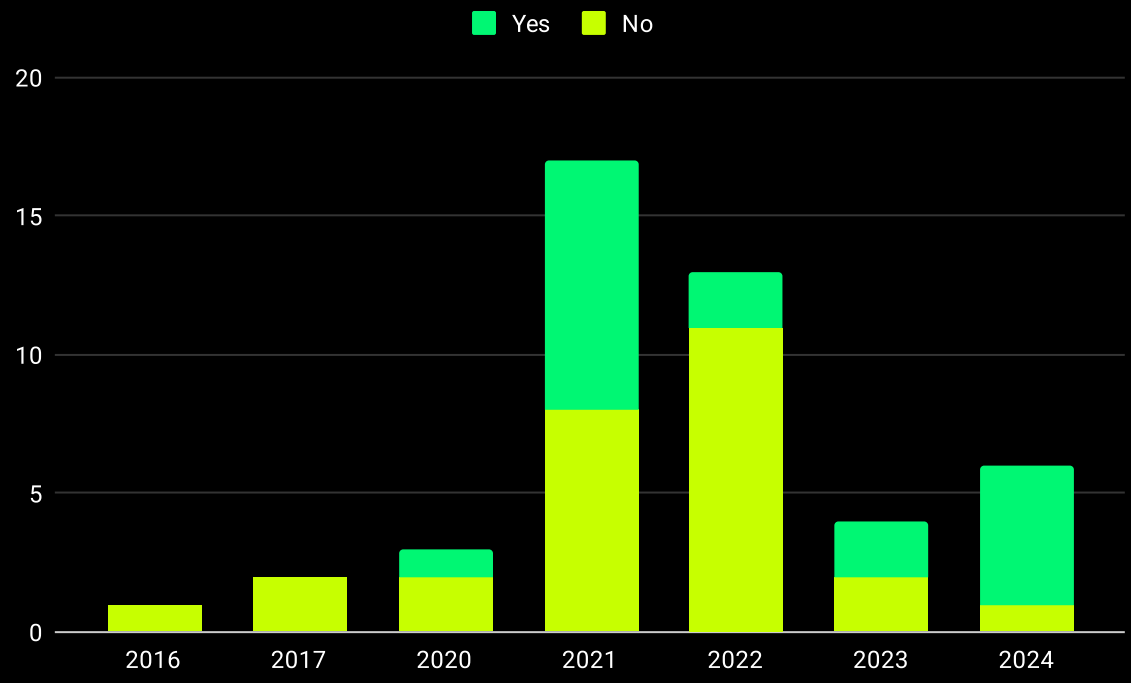

Figure 54: Usage of flash loans per year [count]

The financial impact of using flash loans in attacks, as shown in Figures 55 and 56, aligns mostly with their usage trends over the years, presenting a decline until 2022, followed by a significant increase in 2023 and 2024.

In 2023, flash loans accounted for 51.9% of the total financial losses, totaling $233,300,000 USD. This proportion rose even further in 2024, where flash loans were responsible for 76.9% of the losses, amounting to $85,109,071 USD.

The relationship between the rate of flash loan usage in attacks and the corresponding financial impact varies by year. For example, in 2020, 2022 and 2023, the financial losses from flash loan attacks were higher relative to their occurrence rate. On the other hand, in 2021 and 2024, particularly in the former year, the impact was less severe relative to their frequency; in 2021, flash loans constituted 52.9% of attack occurrences but only 33% of the financial losses, which was about $334,500,000 USD.

These fluctuations highlight that while flash loans can enable substantial financial manipulation, their actual impact on financial losses can vary greatly depending on the specific circumstances and vulnerabilities exploited in each attack.

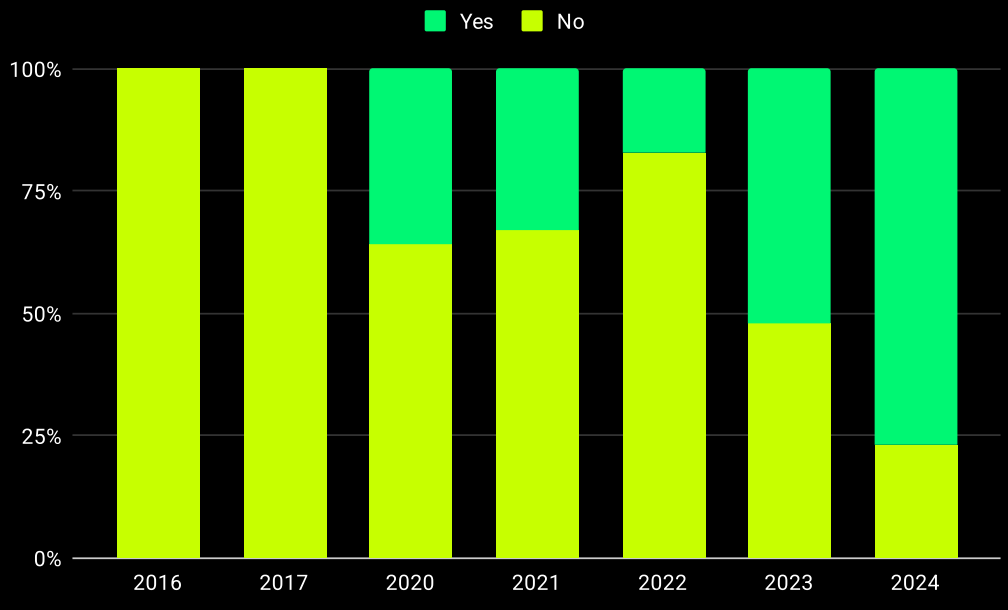

Figure 55: Loss caused by the usage of flash loans per year [percentage]

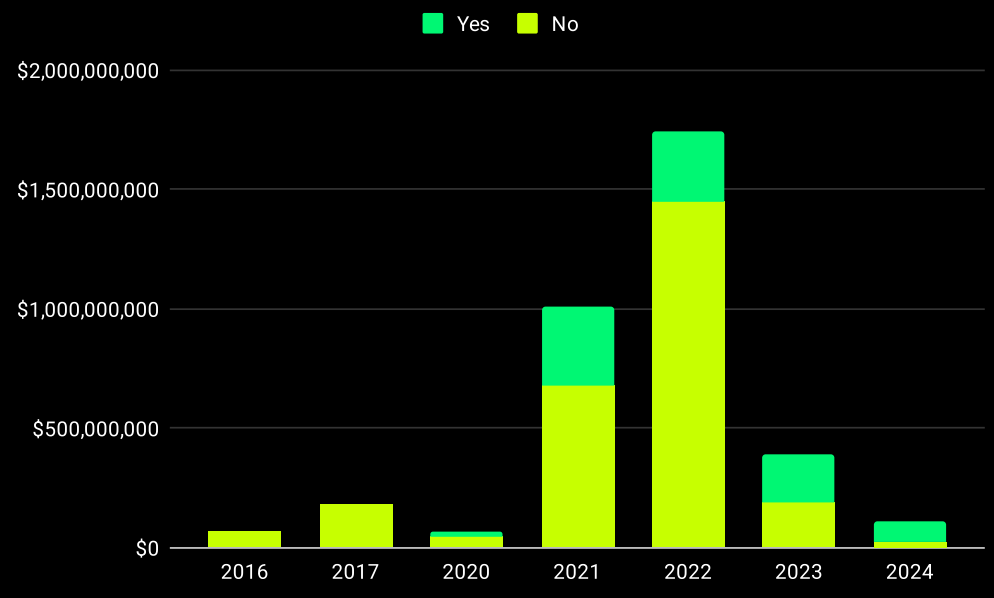

Figure 56: Loss caused by the usage of flash loans per year [USD]

Figures 57 and 58 provide a detailed breakdown of the use of flash loans across different sub-categories of attacks.

The data indicates that flash loans are not used in attacks involving compromised accounts or rug pulls. This is logical, as these types of attacks generally rely more on off-chain attack vectors or privileged permissions rather than the exploitation of financial mechanisms within the blockchain.

In the case of direct contract exploitation, only 19.2% of these attacks involve the use of flash loans. This suggests that while flash loans can be a tool in these attacks, they are not the primary method exploited by attackers targeting the direct exploitation of contract vulnerabilities.

On the other hand, most market manipulation attacks, at 66.7%, utilize flash loans. This high percentage underscores the utility of flash loans in scenarios where rapid, large-scale trades can significantly impact asset prices within a short time frame, which is characteristic of market manipulation schemes.

All the governance attacks in the sample also involve the use of flash loans, although it's important to note that this category only includes two examples. While this 100% usage rate in governance attacks might suggest a strong preference for flash loans in these scenarios, the small sample size means this finding may not be indicative of a broader trend and should be interpreted with caution.

These insights highlight that while flash loans are a powerful tool within certain types of DeFi attacks, their applicability varies significantly across different attack vectors.

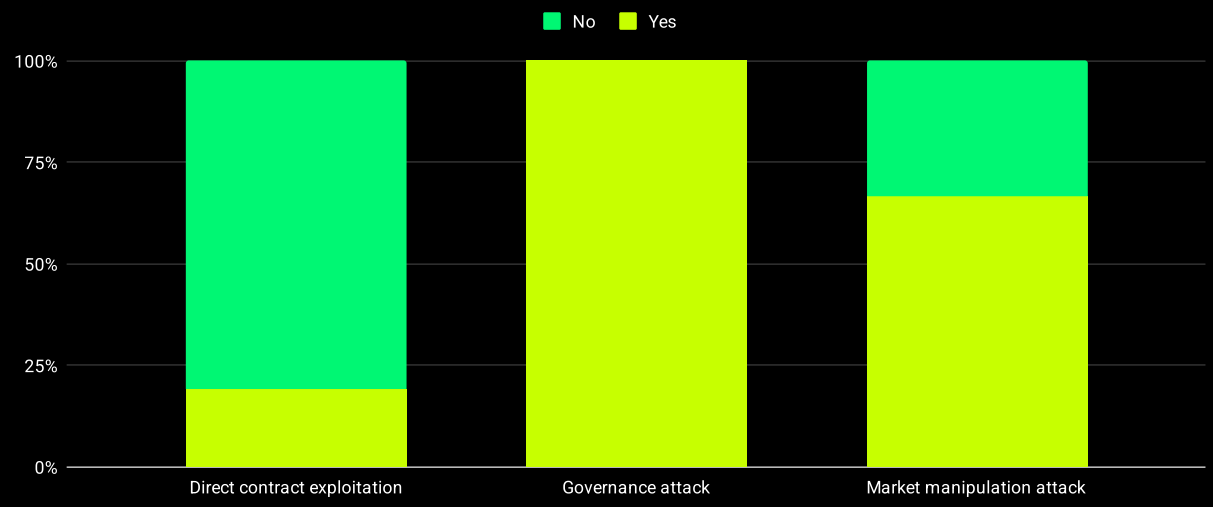

Figure 57: Usage of flash loans per type of attack sub-categories [percentage]

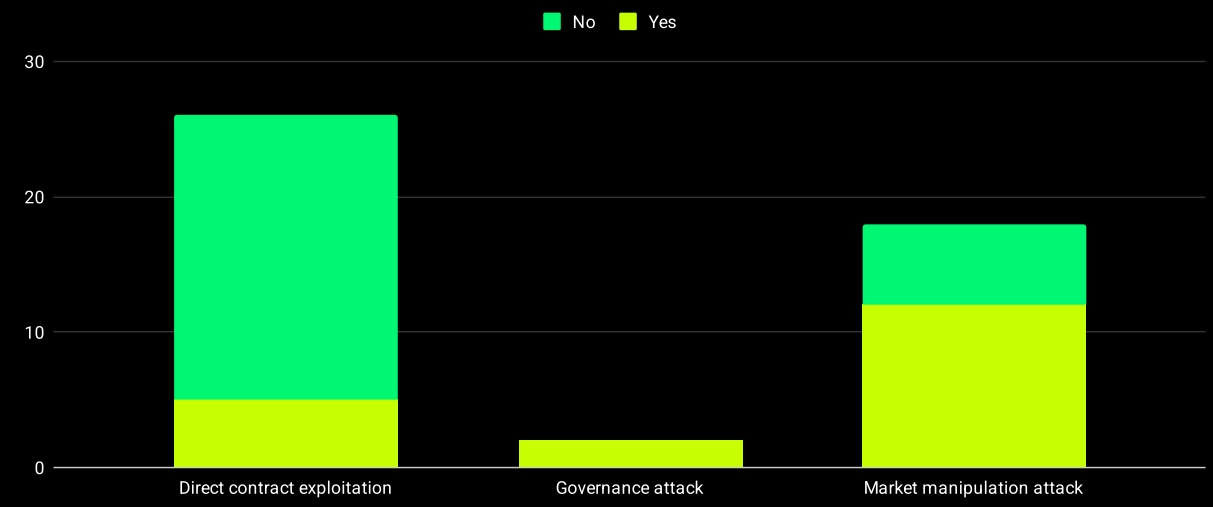

Figure 58: Usage of flash loans per type of attack sub-categories [count]

Figures 59 and 60 offer a comparative analysis of the financial losses associated with attacks that utilize flash loans.

In direct contract exploitation attacks, the utilization of flash loans accounts for only 10.3% of the total financial losses, amounting to $308,500,000 USD. This figure is notably lower than the percentage of these attacks that use flash loans (19.2%). This discrepancy suggests that while flash loans are employed in a notable fraction of direct contract exploitations, they do not necessarily result in proportionally higher financial damages compared to other methods used in such attacks.

Conversely, for market manipulation attacks, flash loans are responsible for a significant 62.8% of the financial losses, which totals approximately $521,623,000 USD. This percentage is slightly lower than the proportion of market manipulation attacks that utilize flash loans (66.7%), as indicated in previous charts (Figures 57 and 58). Despite this slight discrepancy, the data still highlights that flash loans play a major role in the financial impact of market manipulation attacks.

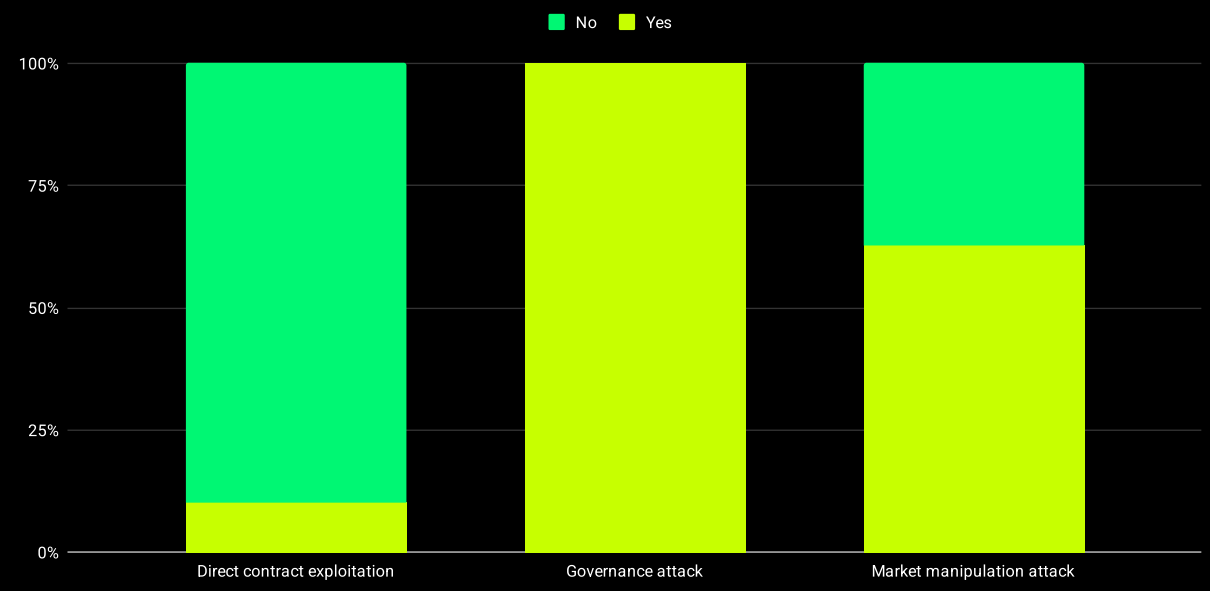

Figure 59: Loss caused by the usage of flash loans per type of attack sub-categories [percentage]

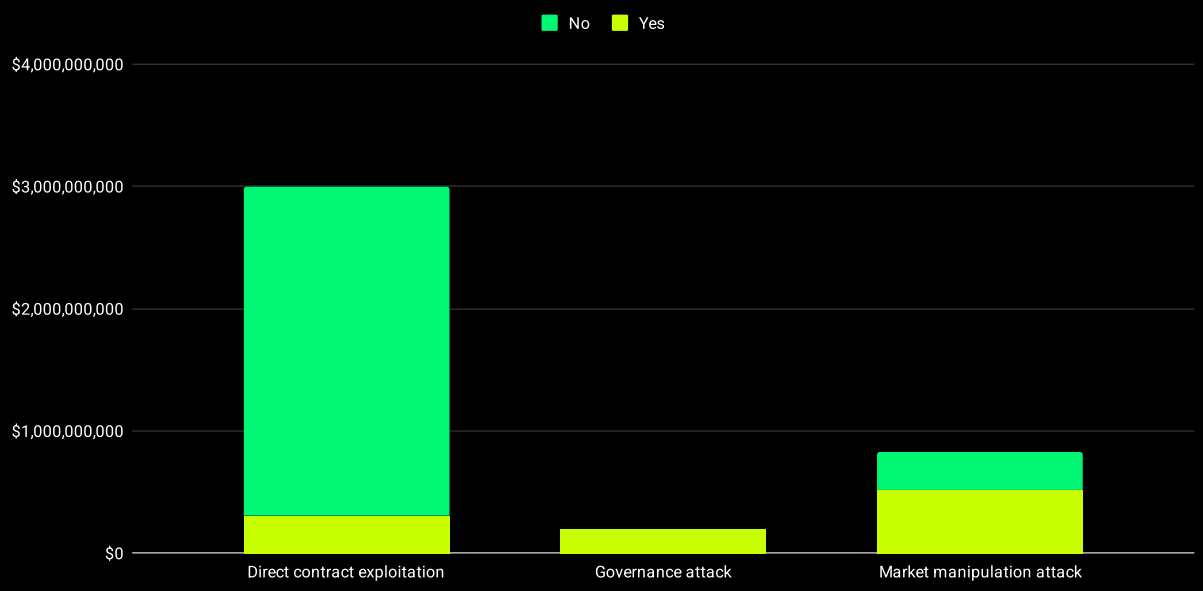

Figure 60: Loss caused by the usage of flash loans per type of attack sub-categories [USD]

The trend in the usage of flash loans in DeFi attacks over recent years, as illustrated in Figures 61 and 62, shows a noticeable fluctuation.

After their introduction in 2020, there was a decline in their usage until 2022, suggesting an initial reduction in their appeal or effectiveness for attackers or potentially increased countermeasures by DeFi platforms.

However, a significant resurgence in the use of flash loans is evident in 2023 and 2024. Specifically, flash loans were employed in 50% of the direct contract exploitation attacks in both years. This resurgence is even more pronounced in market manipulation attacks, where 50% of the attacks in 2023 and a remarkable 100% of the attacks in 2024 involved flash loans. This sharp increase highlights a growing reliance on flash loans for executing these types of cyber threats, especially in market manipulation, where their capacity to swiftly mobilize large volumes of assets can be particularly disruptive.

This trend suggests not only a renewed preference for flash loans among attackers but also highlights their continued potential to exploit vulnerabilities within the DeFi sector. The increased usage in recent years may reflect evolving strategies and innovations in attack methods, especially in the case of market manipulation attacks.

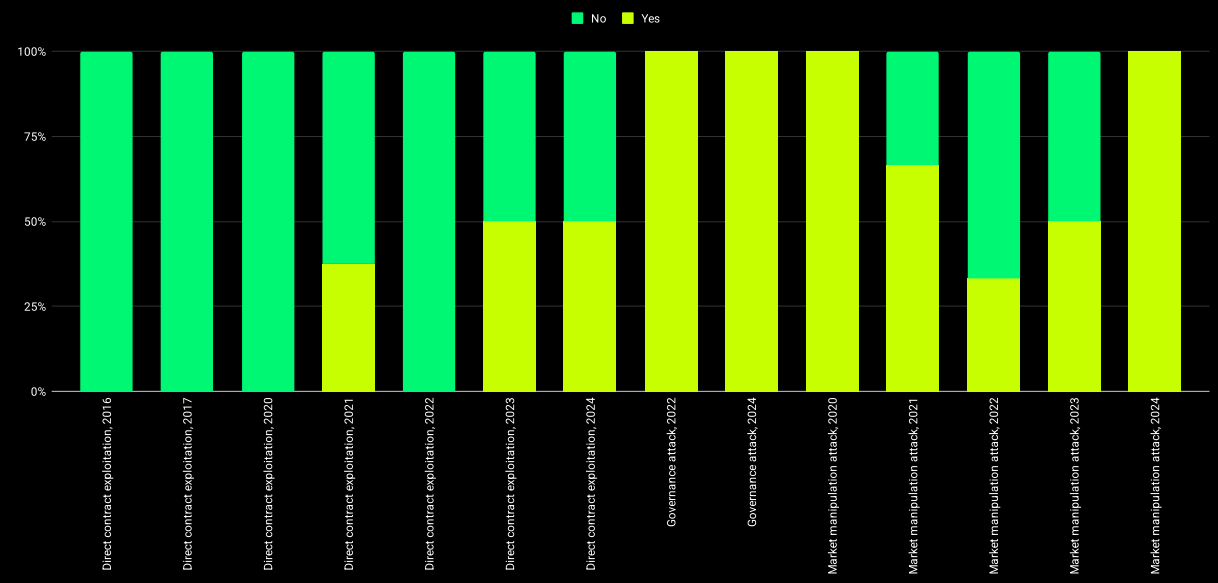

Figure 61: Usage of flash loans per type of attack sub-categories and year [percentage]

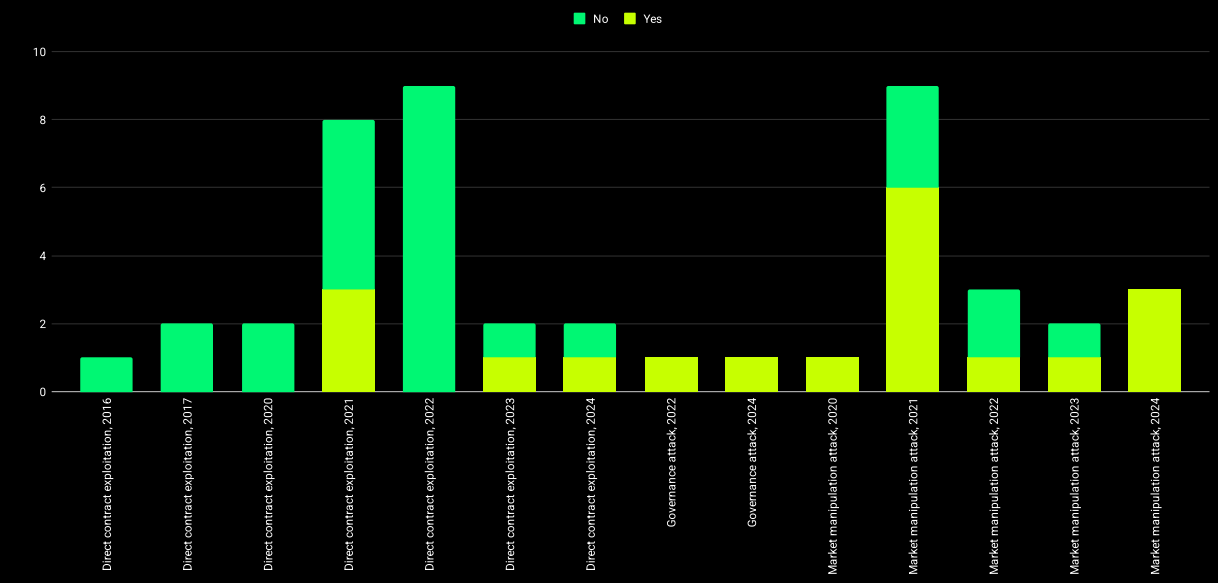

Figure 62: Usage of flash loans per type of attack sub-categories and year [count]

Observing the evolution of financial losses for each sub-type of attacks involving flash loans, as depicted in Figures 63 and 64, reveals a shifting pattern, particularly in the context of market manipulation.

Historically, market manipulation attacks have accrued substantial losses due to flash loan exploitation. However, the trend has fluctuated over the years. In 2020, flash loans were used in 100% of market manipulation attacks, resulting in $40,000,000 USD in losses. This percentage decreased to 72.2% in 2021, with losses totaling $267,700,000 USD, and again in 2022, accumulating 57.3% of the hacked value or $ 115,000,000 USD. A significant drop to 28.4% occurred in 2023, with $47,523,000 USD in losses, only to spike again to 100% in 2024, accounting for $66,400,000 USD in losses. This variation indicates changing dynamics in how flash loans are utilized and defended against in market manipulation attacks, with significant volatility in their impact from year to year.

The trend for direct contract exploitation attacks shows a consistently high financial impact relative to their occurrence. In the last two reported years, the losses from these attacks significantly exceeded their occurrence rates: 74% ($197,000,000 USD) and 63.7% ($44,700,000 USD) versus an occurrence rate of 50% in both years. This indicates that while flash loans are employed in half of these attacks, their financial impact can be disproportionately high, especially in later years.

For market manipulation in 2023, however, the financial impact was notably less than the occurrence rate, with losses accounting for only 28.4% of the total compared to 50% occurrence.

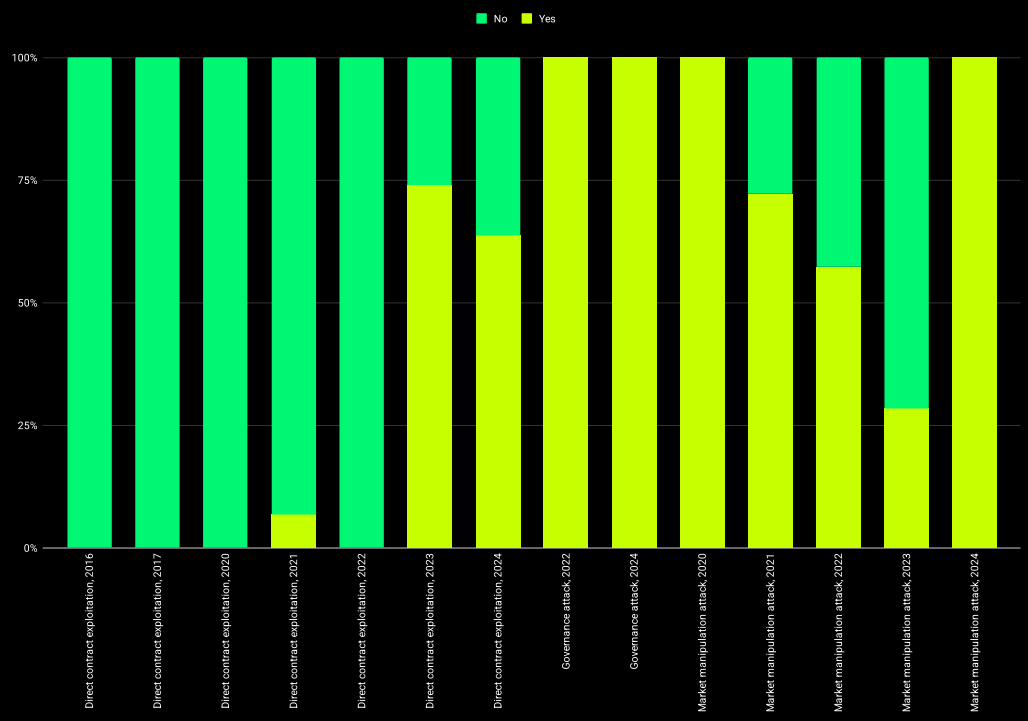

Figure 63: Loss caused by the usage of flash loans per type of attack sub-categories and year [percentage]

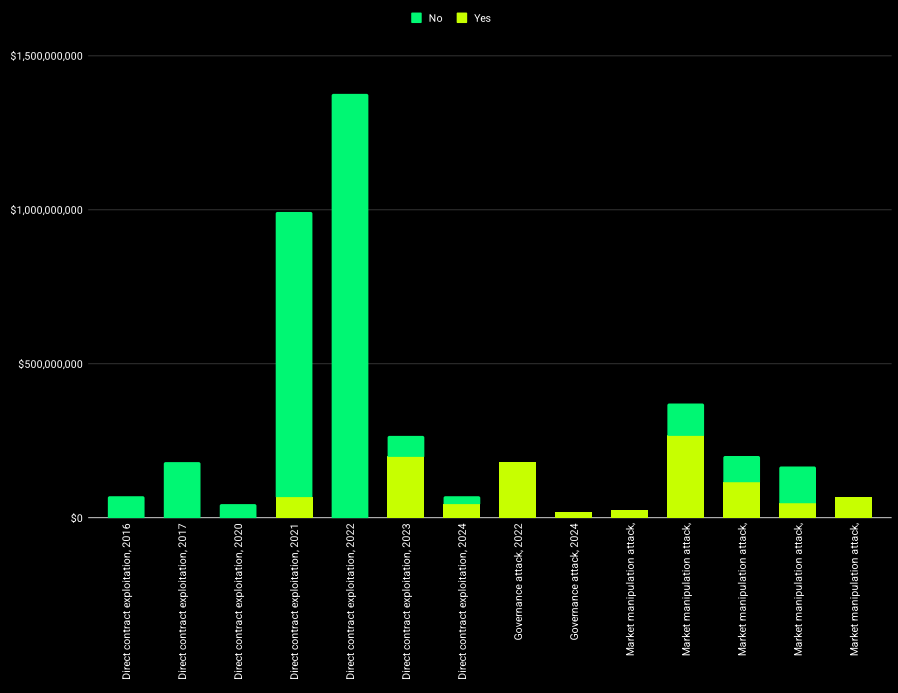

Figure 64: Loss caused by the usage of flash loans per type of attack sub-categories and year [USD]

Root Cause Analysis

To understand the vulnerabilities that enable various types of attacks on DeFi, it's essential to categorize and explain the root causes.

First, we want to explain those causes related to exploiting a smart contract vulnerability. These causes lead to direct contract exploitation, governance-related attacks, and some forms of market manipulation.

We will consider the following:

- **Math error:** This occurs when there's an error in the implementation of a mathematical formula or during the calculation process, such as rounding errors.
- **Lack of/faulty input verification/validation:** This category of vulnerability is exploited when a contract does not adequately verify or validate input arguments. Common examples include not checking for the uniqueness of two assets supplied or neglecting to verify that addresses are not zero addresses.
- **Reentrancy:** This is a common attack where an attacker calls a function recursively before the first instance of the call is finished, often aiming to withdraw funds repeatedly. It exploits the contract's state before it updates from the initial function call.
- **Faulty proof verification:** Critical in cross-chain interactions, such as bridges, where incorrect implementation of verification processes (like signature verification algorithms) can allow attackers to falsify actions on a connected chain.
- **Faulty initialization:** Particularly important for proxy contracts, this occurs when a contract remains uninitialized or is initialized with incorrect parameters.
- **EVM-based:** This category includes exploits that leverage specific behaviors of the Ethereum Virtual Machine (EVM), such as manipulating contract deployment to predict or influence contract addresses or exploiting nuances in how the ABI decoder interprets data.
- **Lack of/faulty access control:** Occurs when a function within a smart contract does not have proper restrictions on who can execute it or if the existing restrictions are not adequately enforced, allowing unauthorized parties to perform actions meant for specific roles.

- **Flawed proposal execution mechanism:** In decentralized governance, flaws in how proposals are executed post-vote can lead to exploitation. For example, allowing attackers to execute malicious proposals directly without adequate review or oversight.
- **Flaw in voting power mechanism:** Vulnerabilities in how voting power is calculated or applied can lead to attacks. For example, allowing attackers with minimal governance tokens to disproportionately influence or control protocol decisions, potentially leading to privilege escalation.
- **Logic error:** This broad category encompasses any other programming errors that do not fit neatly into the other categories but still lead to unexpected or undesirable outcomes that can be exploited, often related to how the protocol works or is intended to work.

Figures 65 and 66 illustrate how different vulnerabilities are distributed among the various sub-categories of attacks.

The most prevalent cause of attacks is a lack of or faulty input verification or validation, which accounts for 31.6% of the incidents. Following this, reentrancy emerges as the second most frequent vulnerability, representing 18.4% of attacks. Math issues or errors also constitute a significant proportion, involved in 15.8% of cases. Other vulnerabilities, such as governance-related issues, EVM-based errors, and problems with access control, are less common, contributing to smaller percentages of the total attacks observed.

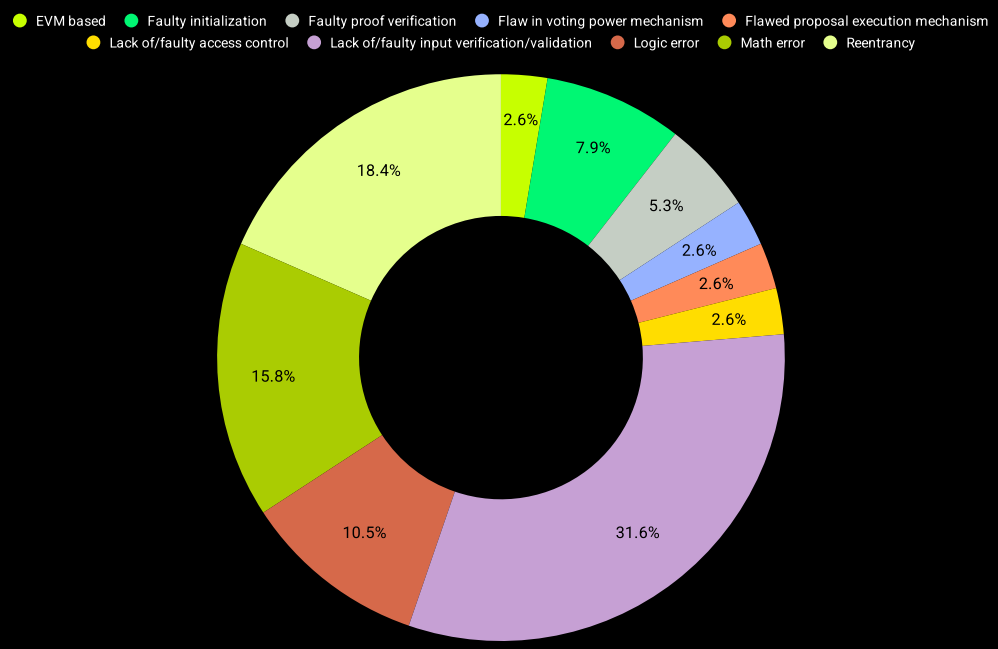

Figure 65: Number of type of vulnerabilities in contracts [percentage]

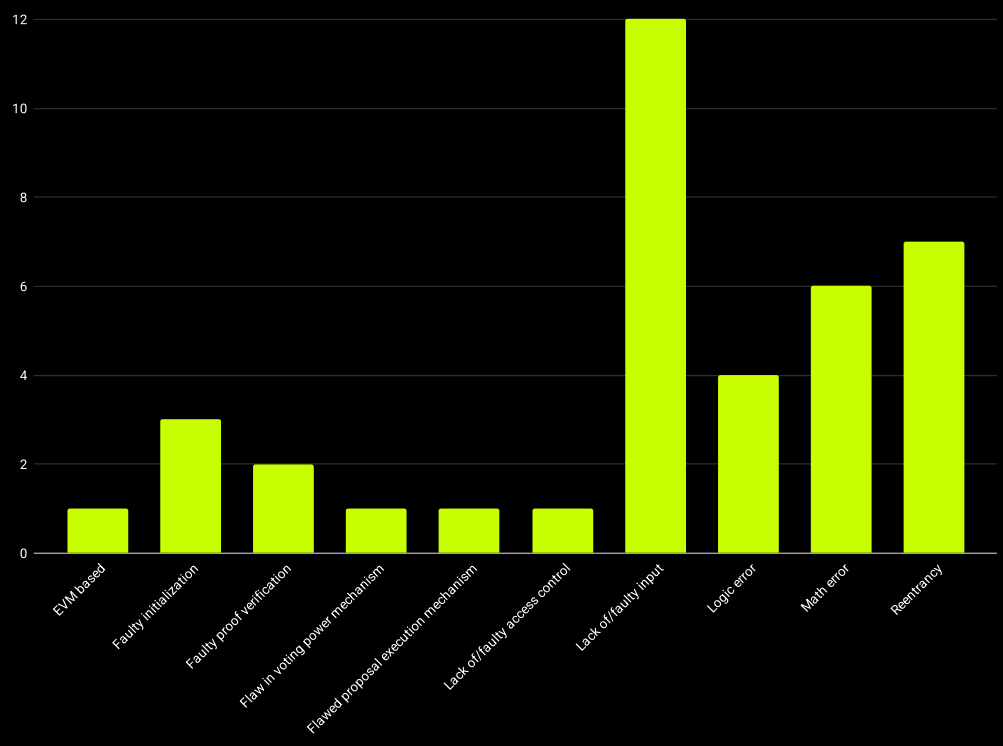

Figure 66: Number of type of vulnerabilities in contracts [count]

Figures 67 and 68 provide an analysis of how financial losses are distributed according to different types of vulnerabilities in smart contracts.

Calculating the precise impact of each type can be challenging, especially when multiple vulnerabilities are exploited in a single attack, as seen in complex cases like the Alpha Finance hack. In such instances, attackers employ a combination of vulnerabilities to execute their strategies, complicating the attribution of financial losses to any single cause.

To address this complexity and provide a clearer picture of how much each type of vulnerability contributes to the overall financial damage, losses have been divided equally among the various vulnerabilities involved in such multifaceted attacks in this section and in the rest of the report. This approach ensures that the financial impact is represented more accurately for each type of vulnerability.

The most significant losses are caused by issues related to a lack of or faulty input verification or validation, which accounts for 29.6% of total financial losses, amounting to approximately $ 1,007,675,000 USD.

Interestingly, faulty proof verification, while only accounting for 5.3% of occurrences, leads to 26.8% of the financial losses, totaling $912,000,000 USD. This disparity suggests that exploits targeting proof verification are particularly severe, often resulting in large losses relative to their frequency.

Faulty initialization is the third most costly vulnerability, responsible for 10.9% of the losses, or $372,000,000 USD, with its occurrence a bit lower at 7.9%.

In contrast, reentrancy and math errors, despite being the second and third most common vulnerabilities by occurrence, result in relatively lower losses than might be expected based on their frequency. Reentrancy leads to 9.4% of the losses ($320,100,000 USD) against an occurrence rate of 18.4%, and math errors lead to 8.5% of the losses ($287,898,000.00USD) versus a 15.8% occurrence rate. These figures indicate that while these vulnerabilities are common, their individual financial impact per incident may be less severe compared to vulnerabilities like faulty proof verification.

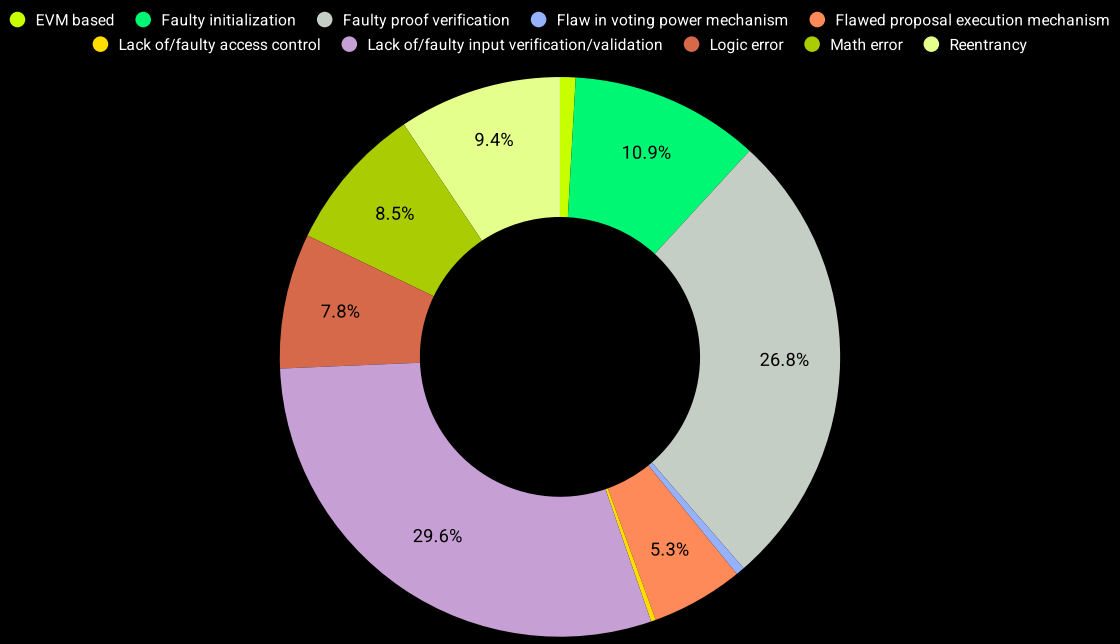

Figure 67: Loss caused by type of vulnerabilities in contracts [percentage]

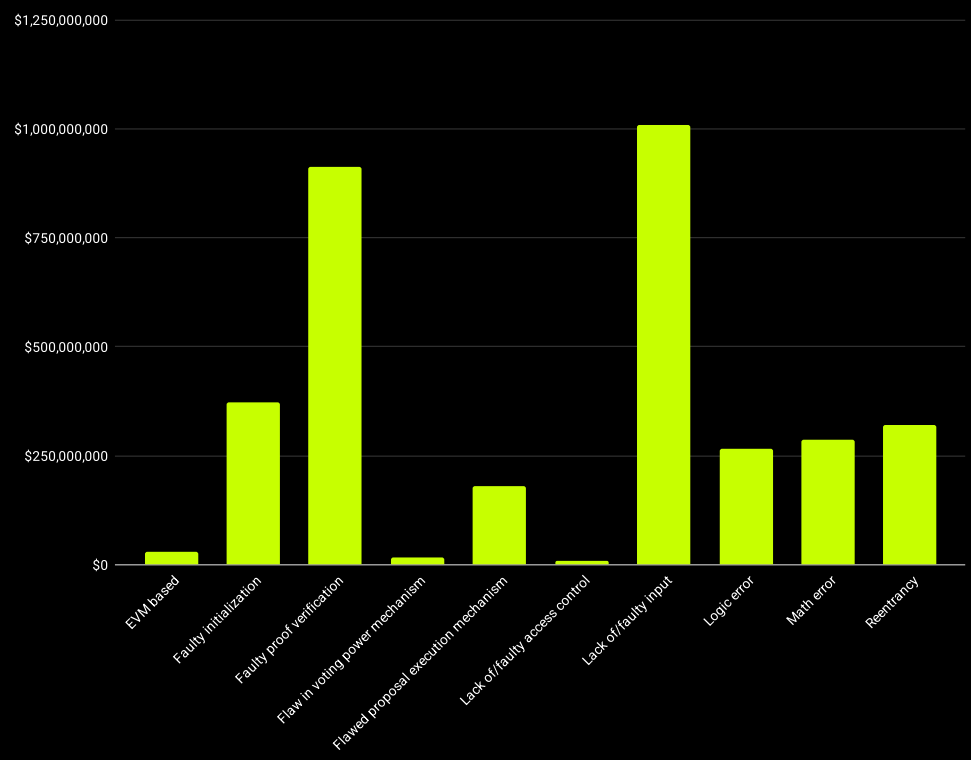

Figure 68: Loss caused by type of vulnerabilities in contracts [USD]

Over the years, the primary causes of attacks related to smart contracts have evolved significantly, as illustrated in Figures 69 and 70.

Initially, the dominant cause was the reentrancy attack on The DAO, which highlighted vulnerabilities in Ethereum's early smart contract implementations. This was followed by the faulty initialization issues that led to the Parity multi-sig wallet hacks in 2017.

From 2021 onward, the causes of attacks diversify further, although lack of/faulty input verification/validation continues to dominate as the primary vulnerability until 2023. In 2023, the landscape shifts slightly, with logic errors, reentrancy, and math errors emerging as the predominant causes.

In 2024, lack of/faulty input verification/validation resurged as the primary cause of hacks, suggesting either a resurgence in this type of vulnerability being exploited or perhaps lapses in secure coding practices among new or evolving projects.

It is notable that reentrancy attacks were consistently present in all years except for 2017, with their impact varying from 50% to as low as 10%. This persistent presence underscores the ongoing challenge of securing contracts against this well-known yet still effective attack vector.

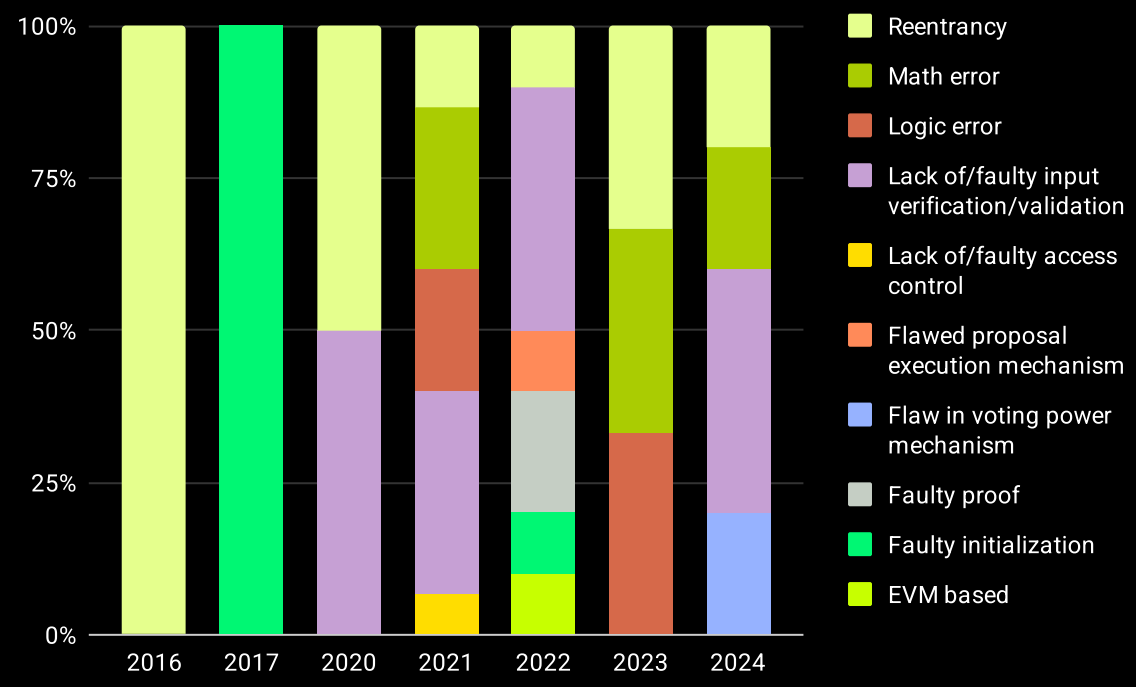

Figure 69: Number of type of vulnerabilities in contracts per year [percentage]

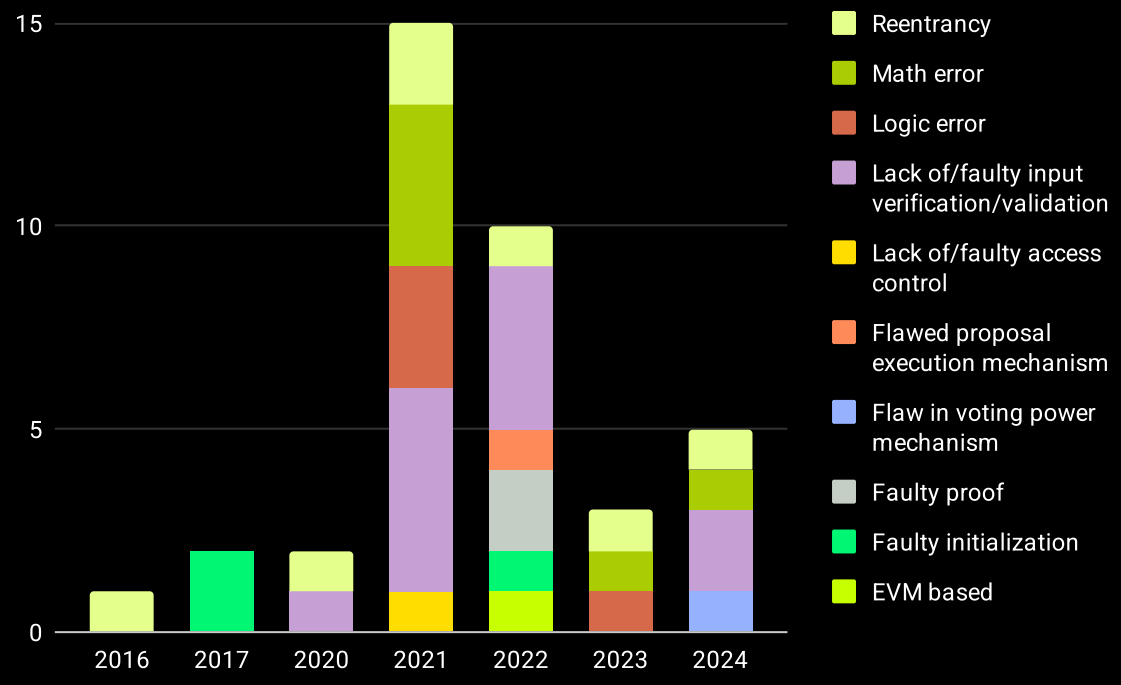

Figure 70: Number of type of vulnerabilities in contracts per year [count]

Figures 71 and 72 provide a detailed year-by-year breakdown of the financial losses attributed to each type of vulnerability in smart contracts.

Until 2020, the distribution of financial losses was relatively proportional to the rates of occurrence for each vulnerability type. However, from 2021 onwards, certain vulnerabilities began causing disproportionately high losses compared to their occurrence rates, indicating their potential for severe impact when exploited.

In 2021, vulnerabilities related to lack of/faulty input verification/validation were responsible for a substantial 67.9% of the total losses for the year, amounting to $753,775,000 USD, despite constituting only 33.3% of the attacks. This suggests that when these vulnerabilities are exploited, they can lead to significant financial damage.

2022 saw a similar pattern with faulty proof verification vulnerabilities, which accounted for 58.6% of the financial losses (approximately $912,000,000 USD) yet were present in only 20% of the attacks. This underscores the severe impact these vulnerabilities can have, particularly in environments like cross-chain operations, where a single flaw in proof verification can lead to extensive losses.

In 2023, logic errors followed this trend, causing more losses than their occurrence rate would suggest, with 62.8% of the losses ($197,000,000 USD) compared to an occurrence rate of 33.3%. This highlights the critical nature of ensuring robust logical constructs within smart contracts to prevent costly exploits.

By 2024, the pattern persists with lack of/faulty input verification/validation vulnerabilities again, leading to a disproportionate amount of financial damage, representing 56.4% of the total losses ($70,200,000 USD) versus an occurrence rate of 40%.

Reentrancy attacks show a more variable impact over the years. In 2020 and 2024, reentrancy led to more losses relative to other years, while in 2021, 2022, and 2023, the losses from reentrancy attacks were less pronounced compared to their occurrence rates.

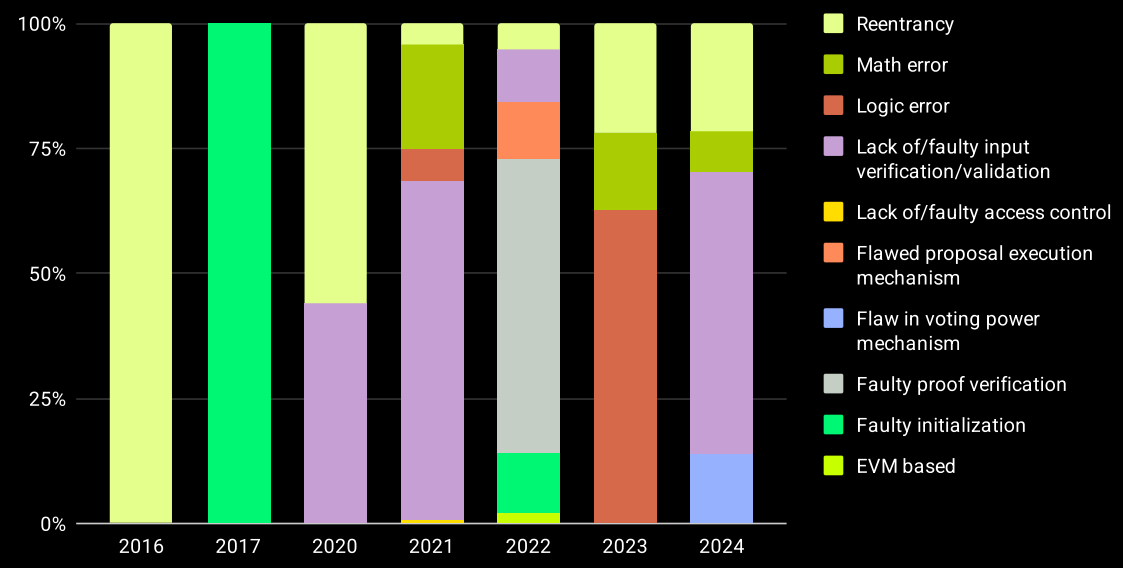

Figure 71: Loss caused by type of vulnerabilities in contracts per year [percentage]

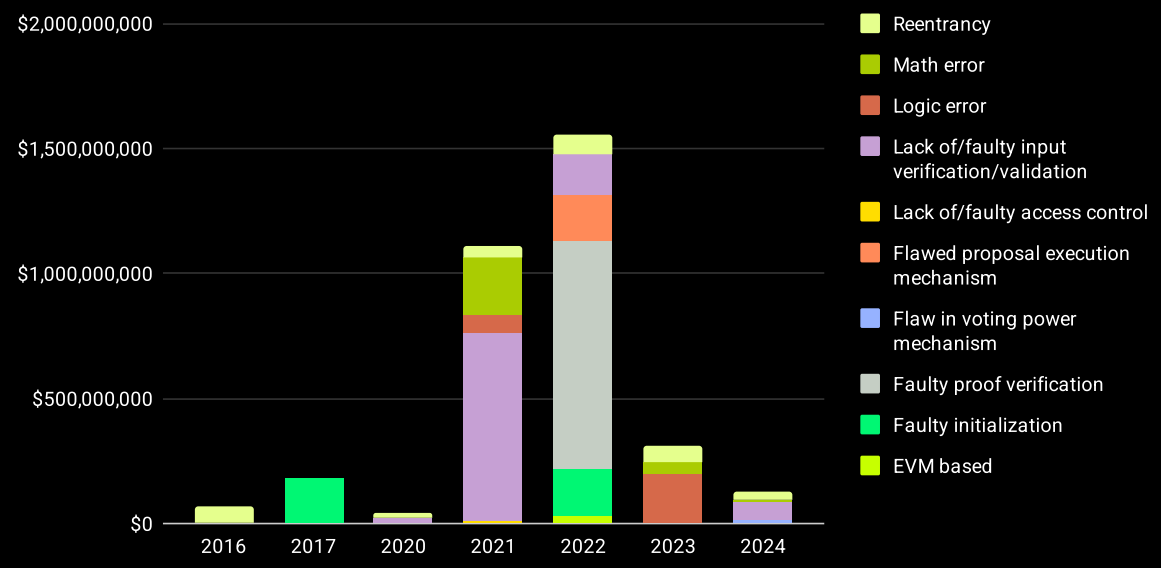

Figure 72: Loss caused by type of vulnerabilities in contracts per year [USD]

Once we have established these common causes, each sub-category will be studied separately.

Direct Contract Exploitation

In the context of direct contract exploitation, the data presented in Figures 73 and 74 highlights the prevalence of the previously discussed vulnerabilities that attackers frequently exploit.

Among these, the most common vulnerability leading to direct contract exploitation is a lack of or faulty input verification/validation, which accounts for 34.6% of the cases. This underscores the importance of rigorous checking and validation processes in smart contract development, as failures in this area continue to be a major avenue for attackers.

Reentrancy follows as the second most common vulnerability used in these attacks, making up 23.1% of the total. This highlights the ongoing relevance of reentrancy as a serious concern in smart contract security despite widespread awareness and the development of best practices to mitigate such attacks.

On the other hand, logic errors and faulty initializations each account for 11.5% of the direct contract exploitations. These vulnerabilities point to deeper issues in the design and initial setup of smart contracts, where fundamental mistakes can leave contracts open to exploitation.

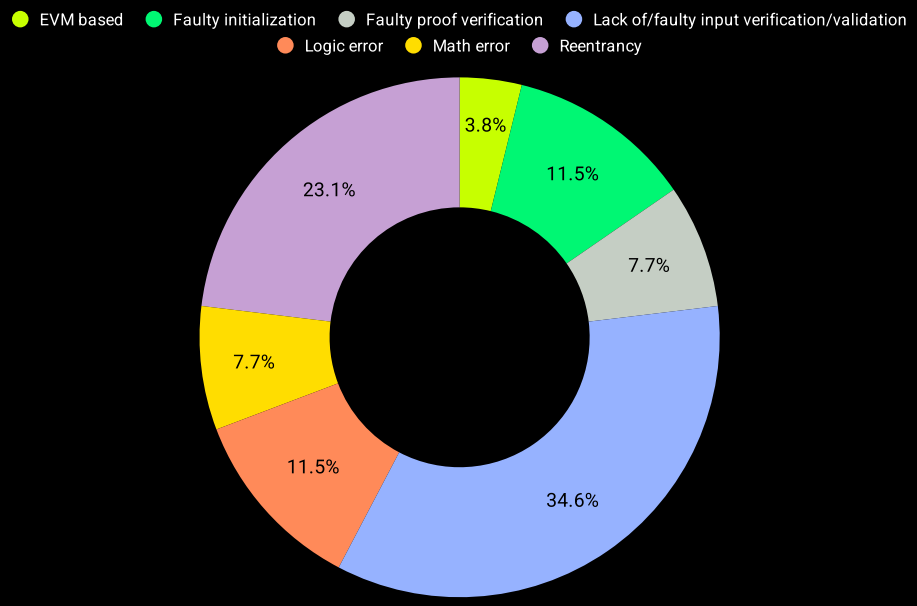

Figure 73: Number of type of vulnerabilities in direct contract exploitation [percentage]

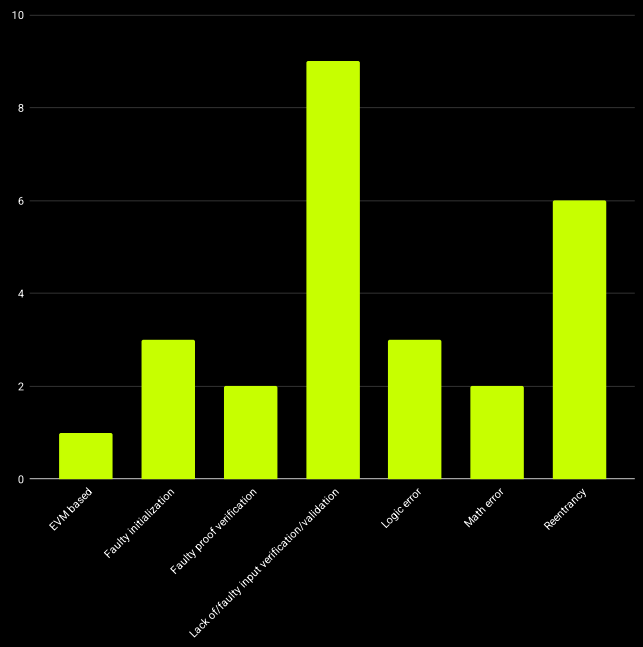

Figure 74: Number of type of vulnerabilities in direct contract exploitation [count]

The analysis of financial losses associated with specific vulnerabilities in direct contract exploitation, as shown in Figures 75 and 76, reveals significant insights into the financial impact relative to the frequency of these vulnerabilities.

The most significant financial losses come from a lack of or faulty input verification or validation, which accounts for 31.8% of the total amount hacked, accumulating approximately $954,900,000 USD. This figure is slightly less than its rate of occurrence, which is 34.6%. This discrepancy suggests that while this vulnerability is the most common, the individual incidents may not always result in the highest losses relative to other vulnerabilities.

Faulty proof verification stands out significantly in terms of financial impact. It accounts for 30.4% of the total amount lost ($912,000,000 USD) despite only occurring in 7.7% of the cases. This highlights the severity and potential for large-scale financial damage when faulty proof verification is exploited.

Faulty initialization is the third most significant vulnerability by financial impact, contributing to 12.4% of the losses, amounting to $372,000,000 USD. This figure is relatively close to its occurrence rate of 11.5%, indicating a more proportional relationship between frequency and financial impact for this type of vulnerability.

On the other hand, despite reentrancy being the second most common vulnerability by occurrence at 23.1%, it accounts for a comparatively lower percentage of the total financial losses at only 9.8% ($293,100,000 USD). This suggests that while reentrancy attacks are frequent, they often result in less financial damage per incident compared to more severe vulnerabilities like faulty proof verification.

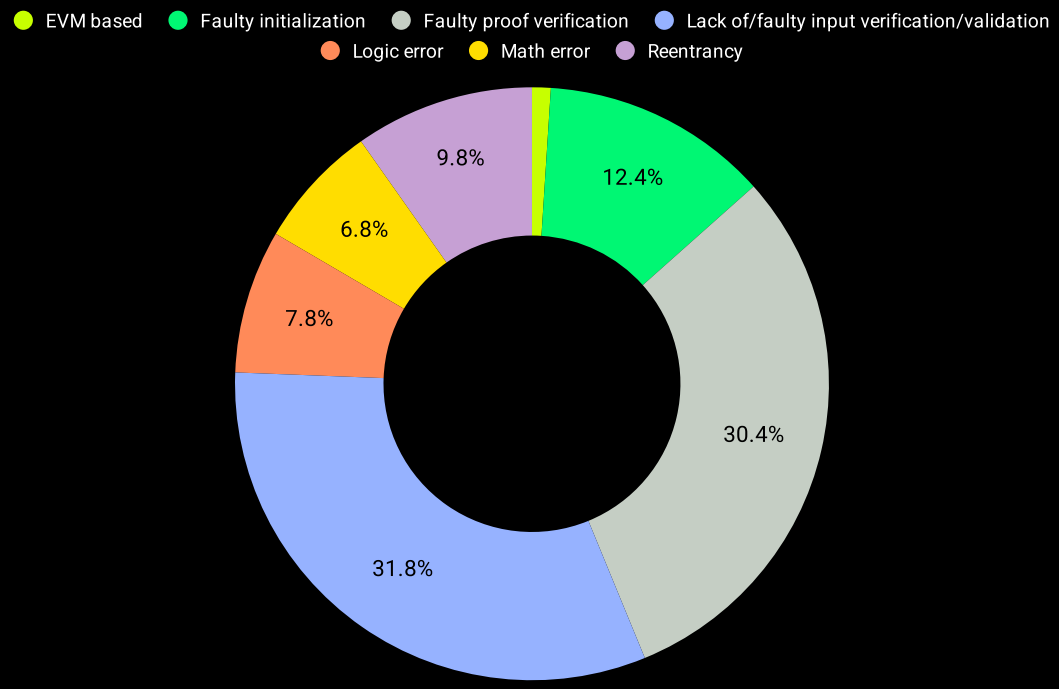

Figure 75: Loss caused by type of vulnerabilities in direct contract exploitation [percentage]

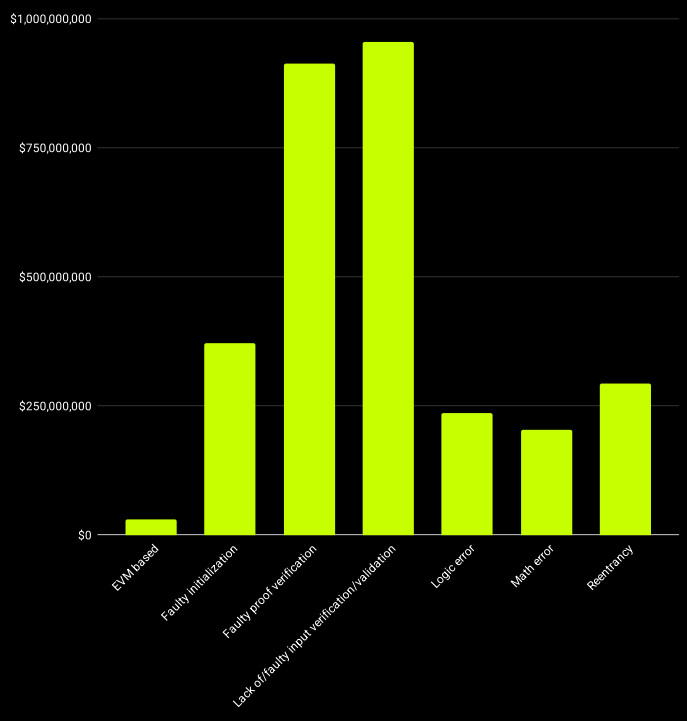

Figure 76: Loss caused by type of vulnerabilities in direct contract exploitation [USD]

The data from Figures 77 and 78 illustrates the shifting dynamics and prevalence of different vulnerabilities in smart contract attacks over the years.

While reentrancy was initially a dominant vulnerability, its prominence has varied significantly over the years. After decreasing to 11.1% of attacks in 2022, it increased again in 2023, accounting for half of all attacks during that year. However, it appears that in 2024, reentrancy has not been a prevalent method of attack, indicating possible improvements in contract design or mitigation techniques that specifically target this vulnerability.

Regarding lack of/Faulty Input Verification/Validation, this type of vulnerability has shown significant fluctuations. It was particularly threatening in 2020 and 2022. The year 2021 saw a more distributed scenario, with attacks evenly split among reentrancy, math errors, logic errors, and faulty input verification/validation. However, by 2024, this vulnerability accounted for all reported hacks, underscoring its continued relevance.

Logic errors and math errors also saw varied influence, with logic errors notably sharing prominence with reentrancy in 2023. The fluctuation in these vulnerabilities highlights the complexity and evolving nature of smart contract programming, where different types of logical and mathematical oversights can become significant in different years.

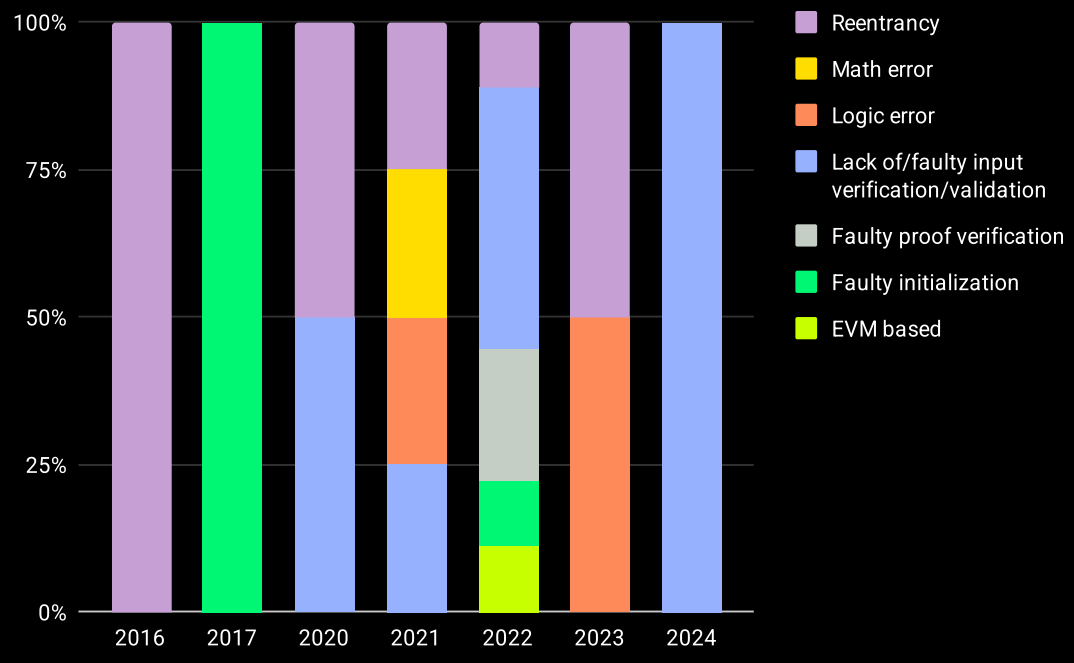

Figure 77: Number of type of vulnerabilities in direct contract exploitation per year [percentage]

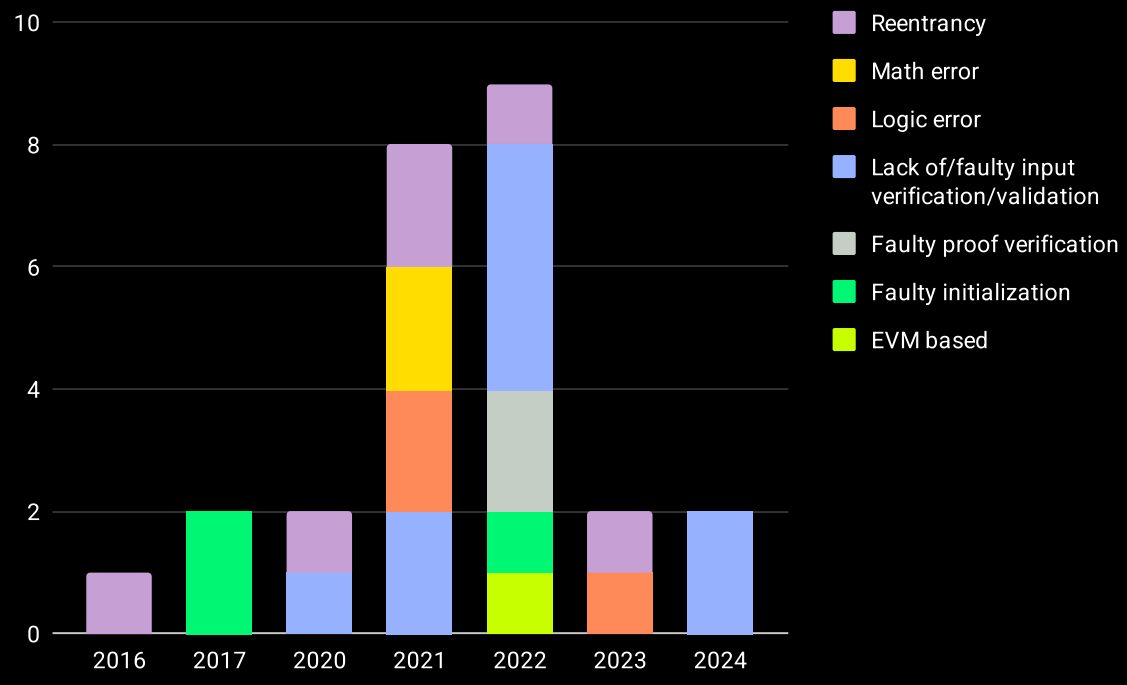

Figure 78: Number of type of vulnerabilities in direct contract exploitation per year [count]

Figures 79 and 80 illustrate the evolving financial impact of specific vulnerabilities in smart contracts over recent years.

Up to 2020, the financial losses due to various vulnerabilities closely mirrored their rates of occurrence. This alignment suggests that during this period, the financial impact of each type of vulnerability was relatively predictable based on its frequency.

In 2021, the pattern shifts notably with lack of/faulty input verification/validation causing a disproportionate amount of the losses. This vulnerability was responsible for 70.7% of the financial losses for the year, totaling $701,000,000 USD, despite only occurring in 25% of incidents.

In 2022, a similar trend is observed with faulty proof verification, which led to 66.3% of the total losses, approximately $912,000,000 USD, against only 22.2% of occurrences. This again underscores the potential for great losses when such vulnerabilities are not adequately addressed.

In 2023, logic errors emerge as a costly vulnerability, causing 74% of the financial losses ($197,000,000 USD), despite constituting 50% of the vulnerabilities exploited.

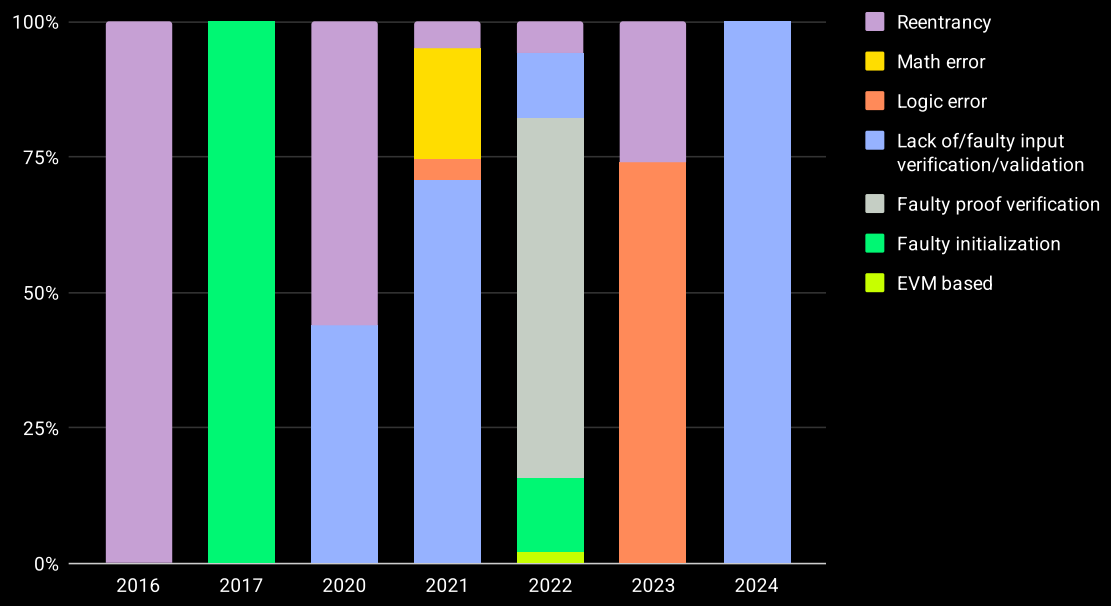

Figure 79: Loss caused by type of vulnerabilities in direct contract exploitation per year [percentage]

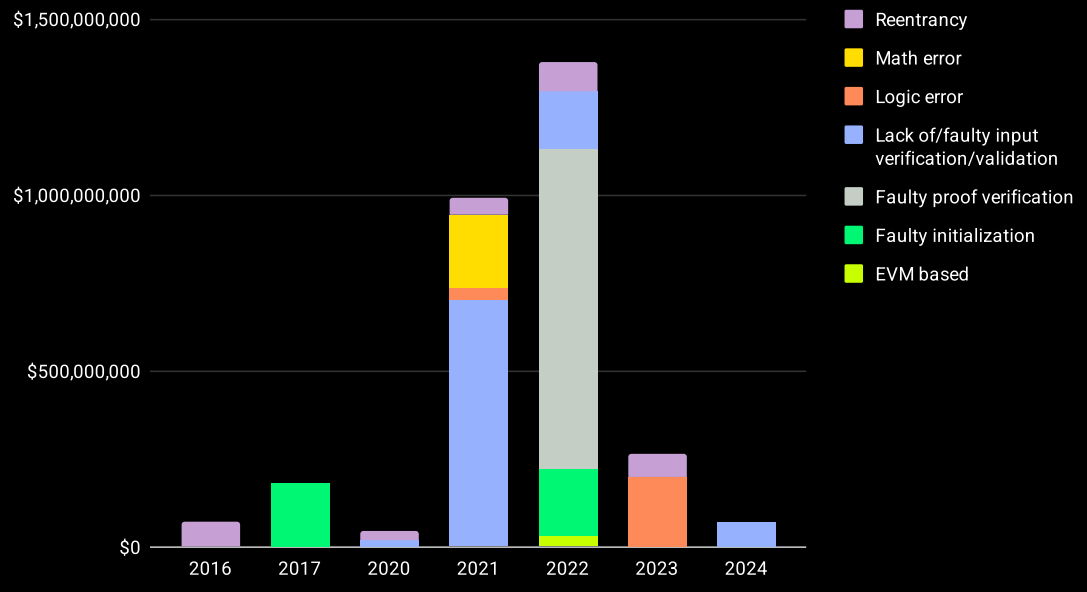

Figure 80: Loss caused by type of vulnerabilities in direct contract exploitation per year [USD]

Market Manipulation Attacks

Market manipulation attacks can arise from various vulnerabilities, not only in smart contracts but also from other critical components of the blockchain ecosystem.

In our research, we will focus on two primary sources that facilitate this type of attack:

- **Flawed oracle:** Oracles are crucial for blockchain networks as they provide external data that smart contracts cannot directly access. A flawed oracle can result from the data source being compromised, whether through negligence, malicious actions, or susceptibility to manipulation. The integrity of an oracle is vital; therefore, utilizing multiple, diverse data sources can enhance security by reducing the likelihood of a simultaneous compromise across all sources. An effectively designed oracle system also incorporates mechanisms to guard against external tampering and eliminates single points of failure through decentralization. Additionally, it should offer incentives for users to report data accurately and reliably.
- **Low liquidity in pool:** This vulnerability is particularly prevalent in DeFi ecosystems where liquidity pools play a fundamental role. Pools with low liquidity are especially susceptible to market manipulation attacks. In such scenarios, even a modest amount of capital can disproportionately influence the price of assets within the pool, leading to significant market distortions.

Figures 81 and 82 present the primary causes of market manipulation attacks within the DeFi ecosystem.

A significant majority of these incidents, approximately 45.8%, are facilitated by flawed oracles. These oracles, which provide critical price data for decentralized applications, when compromised, enable attackers to manipulate market prices maliciously.

Following flawed oracles, the exploitation of contract vulnerabilities, particularly mathematical errors, represents the second most common cause, accounting for 16.7% of such attacks.

Lastly, low liquidity in pools is another notable factor, responsible for 12.5% of the market manipulation attacks. This condition makes it easier for attackers to significantly alter asset prices with relatively small amounts of capital.

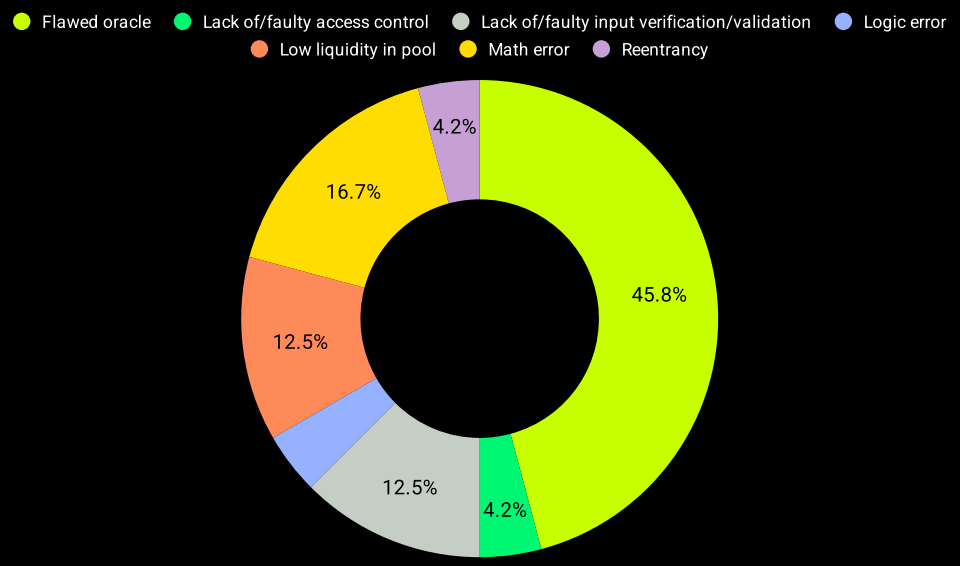

Figure 81: Number of type of vulnerabilities in market manipulation attacks [percentage]

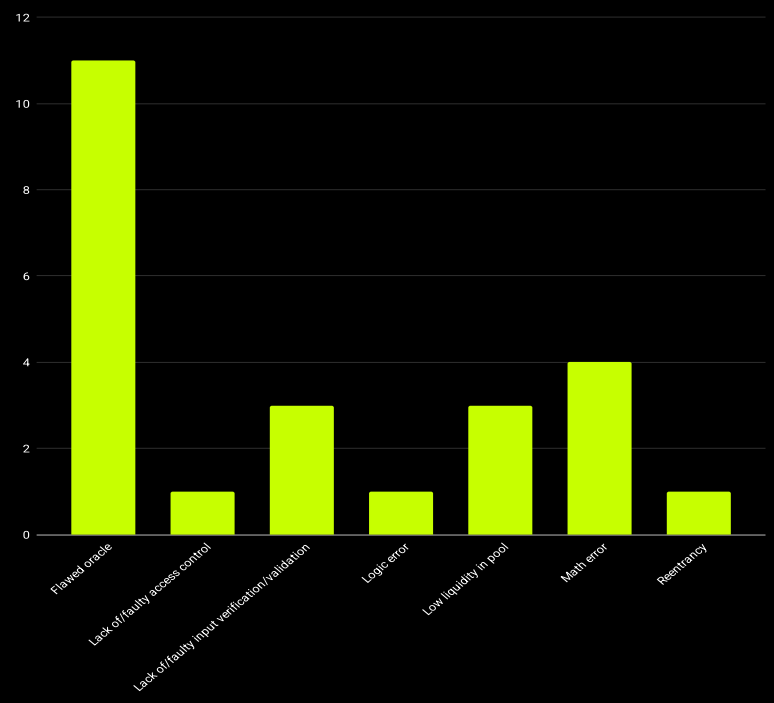

Figure 82: Number of type of vulnerabilities in market manipulation attacks [count]

When examining the distribution of losses by cause, as depicted in Figures 83 and 84, it is evident that the most frequent cause of market manipulation also results in the highest financial losses.

Flawed oracles lead this category, accounting for 59.3% of the total value lost, which amounts to approximately $ 492,200,000 USD. This correlation between frequency and impact underscores the critical vulnerabilities introduced by compromised price data sources.

Interestingly, while low liquidity in a pool or an empty market ranks second in terms of financial impact—representing 16.2% of the losses, or $ 134,375,000 USD—it only accounts for 12.5% of occurrences. This discrepancy highlights the significant damage that can be inflicted even by less frequent events when market conditions are vulnerable.

Math errors come in third, causing 10.1% of the financial losses, totaling $ 83,898,000 USD, slightly less than their occurrence rate of 16.7%. This alignment suggests math error incidents could lead to relatively high financial repercussions.

The remaining types of attacks contribute to smaller proportions of financial losses relative to their occurrences, indicating that while they may happen with some frequency, their financial impact tends to be less severe compared to the top causes.

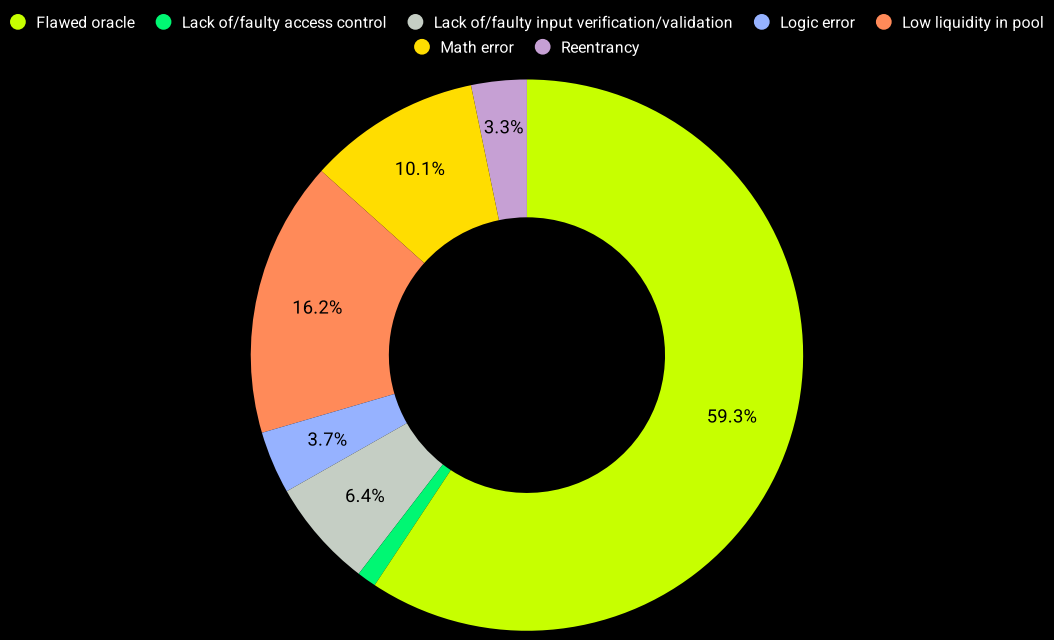

Figure 83: Loss caused by type of vulnerabilities in market manipulation attacks [percentage]

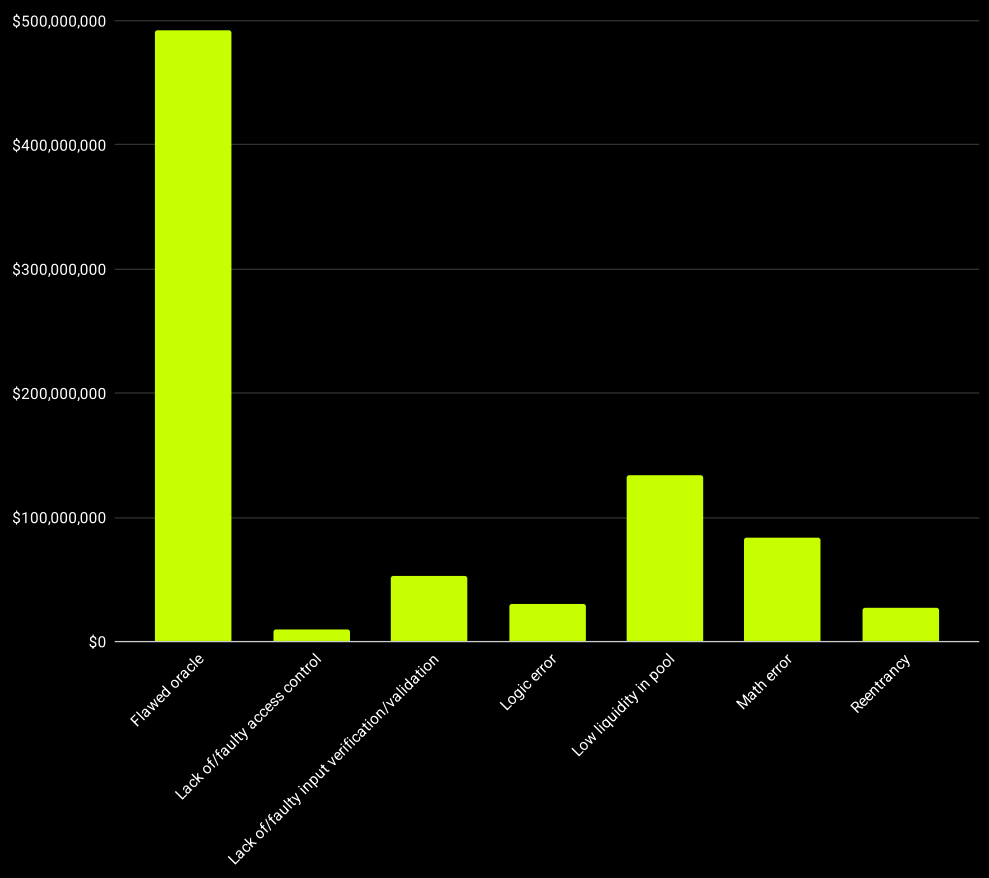

Figure 84: Loss caused by type of vulnerabilities in market manipulation attacks [USD]

As detailed in Figures 85 and 86, the historical data shows a significant trend in the causes of market manipulation attacks in the DeFi sector up to 2023.

Until that year, the predominant cause was the use of flawed oracles by protocols. However, in 2023, the distribution of causes shifted, with flawed oracles and math errors contributing equally to the incidence of attacks.

In 2024, the landscape of vulnerabilities leading to market manipulation attacks has further diversified. This year, the causes of hacks are evenly split among several factors: reentrancy vulnerabilities, math errors, low liquidity in pools, and flawed oracles.

This equal distribution could indicate a broadening of vulnerabilities and attack vectors within the DeFi sector, indicating that attackers are exploiting a wider array of technical weaknesses.

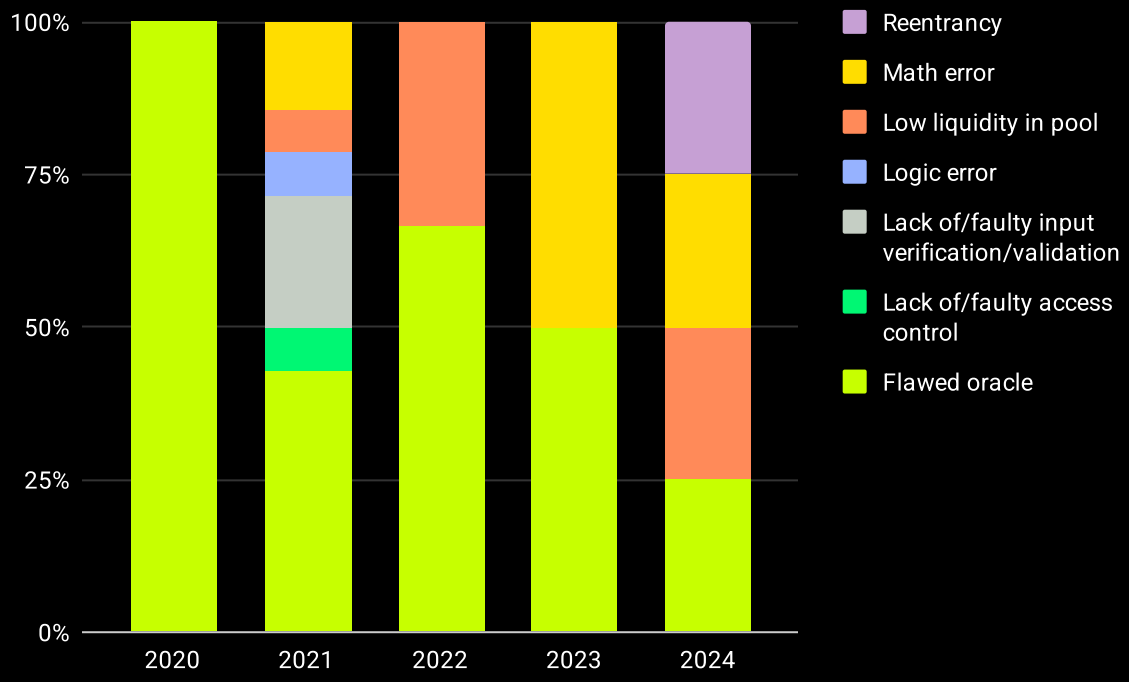

Figure 85: Number of type of vulnerabilities in market manipulation attacks per year [percentage]

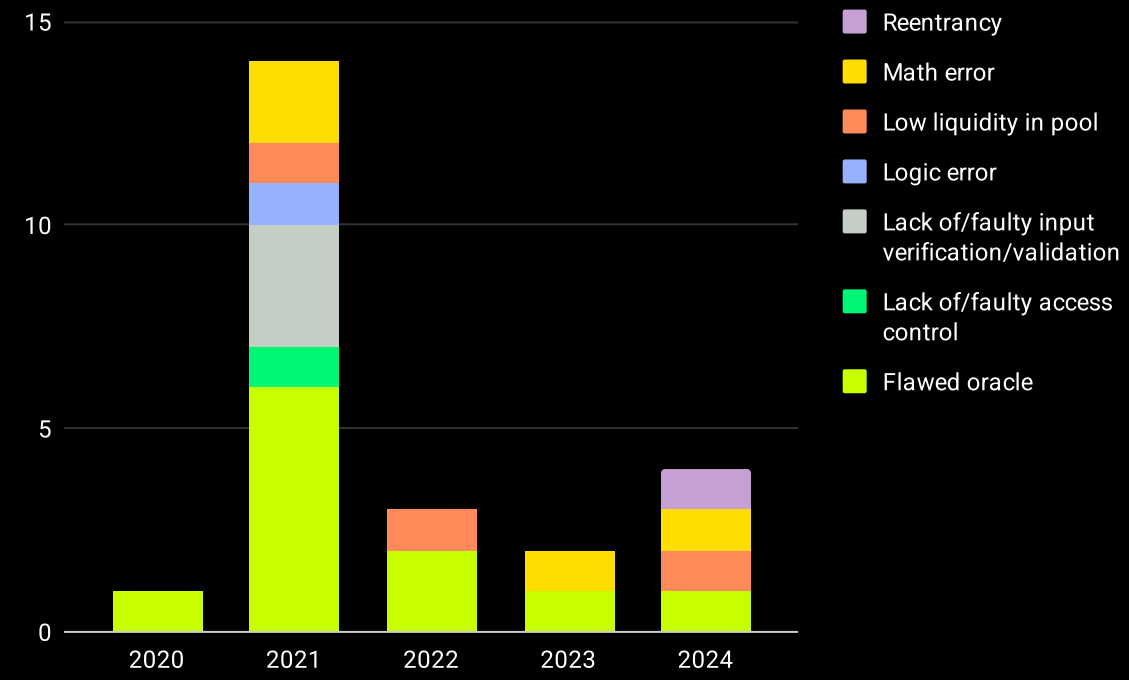

Figure 86: Types of vulnerabilities in market manipulation attacks per year [count]

Figures 87 and 88 provide a detailed view of the distribution of financial losses due to market manipulation attacks by year.

In 2021, flawed oracles were a significant vulnerability, accounting for 65.4% of the total amount hacked, which equaled $ 242,200,000 USD, despite representing only 42.9% of the occurrences that year.

In 2022, the trend shifts towards attacks that exploit empty markets or low liquidity in pools. These attacks accounted for a substantial 57.3% of the financial losses, amounting to $115,000,000 USD, while only occurring 33.3% of the time. This indicates a high financial damage relative to their frequency.

For 2023 there is an increase in losses attributed to flawed oracles, which accounted for 71.6%, or $120,000,000 USD of the losses, compared to a 50% occurrence rate, also indicating a substantial financial damage in relation to its rate of occurrence.

In 2024, reentrancy attacks have emerged as a significant concern, responsible for 40.7% of the financial losses, totaling $27,000,000 USD, against a 25% occurrence rate. Similarly, flawed oracles continue to cause more loss than their rate of occurrence, with these attacks responsible for 29.2% of the financial losses, or $19,400,000 USD, which is about 4% more than their occurrence rate.

This data, together with the rate of occurrence for each type of attack suggests a continuing trend where flawed oracles remain a critical risk point.

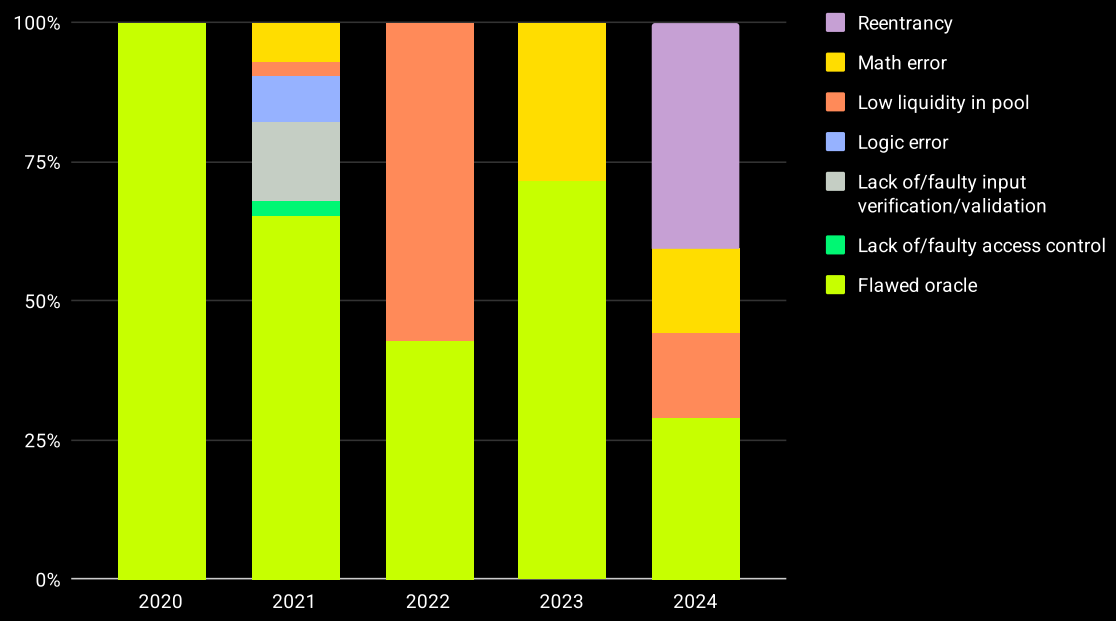

Figure 87: Loss caused by type of vulnerabilities in market manipulation attacks per year [percentage]

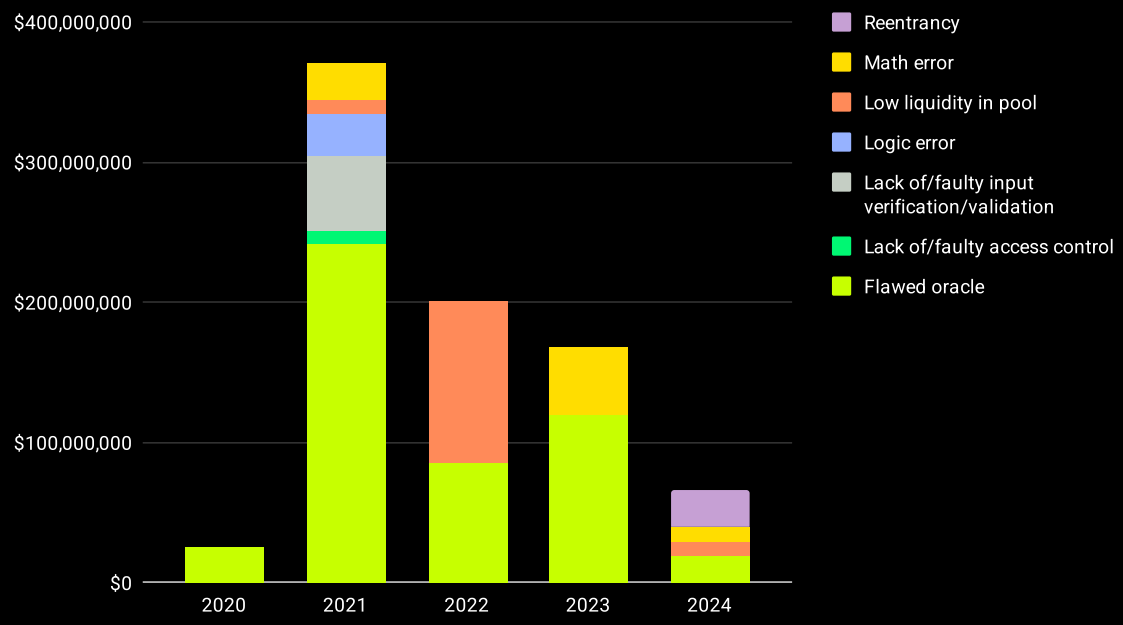

Figure 88: Loss caused by type of vulnerabilities in market manipulation attacks per year [USD]

Governance Attacks

In our sample, we only have two protocols whose hack was possible because of a governance attack. The attacks method by occurrence, are, therefore, divided equally.

The data presented in Figures 89 and 90 highlights the distribution of financial losses associated with governance attacks.

A significant majority of these losses, amounting to 91.3% or approximately $181,000,000 USD, are attributed to flaws in the proposal execution mechanisms. This substantial portion of the losses underscores the critical vulnerabilities that can arise when execution mechanisms are not robustly designed or securely implemented.

In comparison, flaws in the voting power mechanisms account for a smaller fraction of the financial impact, representing 8.7% or about $17,163,071 USD of the total losses. While less significant in terms of financial volume compared to proposal execution flaws, vulnerabilities in voting mechanisms still represent a serious security concern, as they can lead to the misallocation of funds or the passing of malicious proposals.

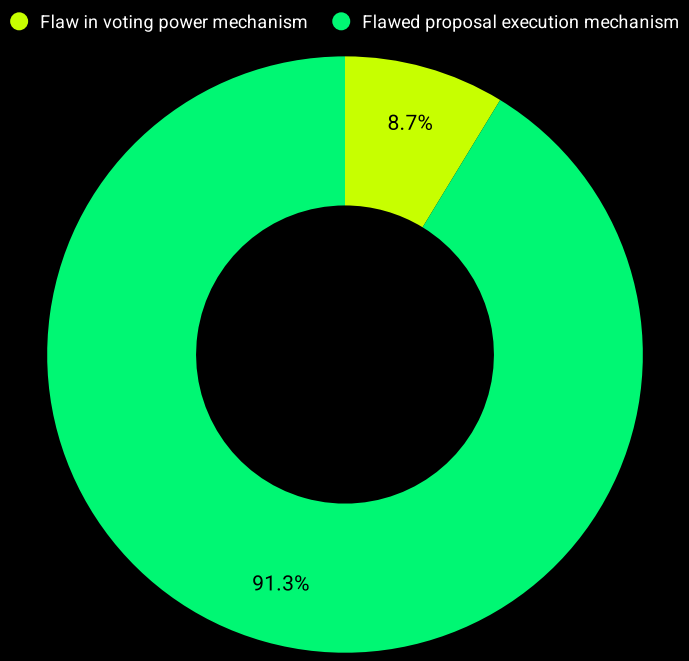

Figure 89: Loss caused by methods used in governance attacks [percentage]

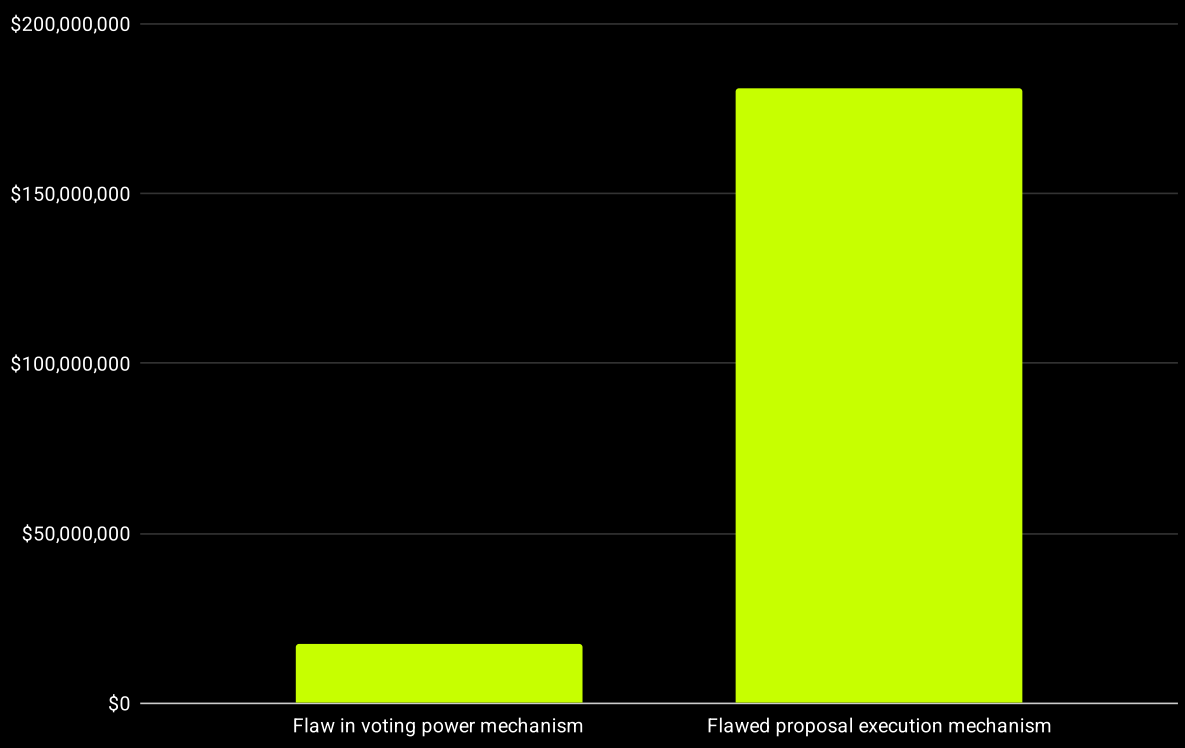

Figure 90: Loss caused by methods used in governance attacks [USD]

Figures 91 and 92 illustrate the distribution of governance attacks by year, highlighting specific incidents and their underlying causes.

In 2022, the governance attack executed through a flawed proposal execution mechanism represents a critical instance where vulnerabilities within the execution process were exploited.

The other significant incident, occurring in 2024, was caused by a flaw in the voting power mechanism.

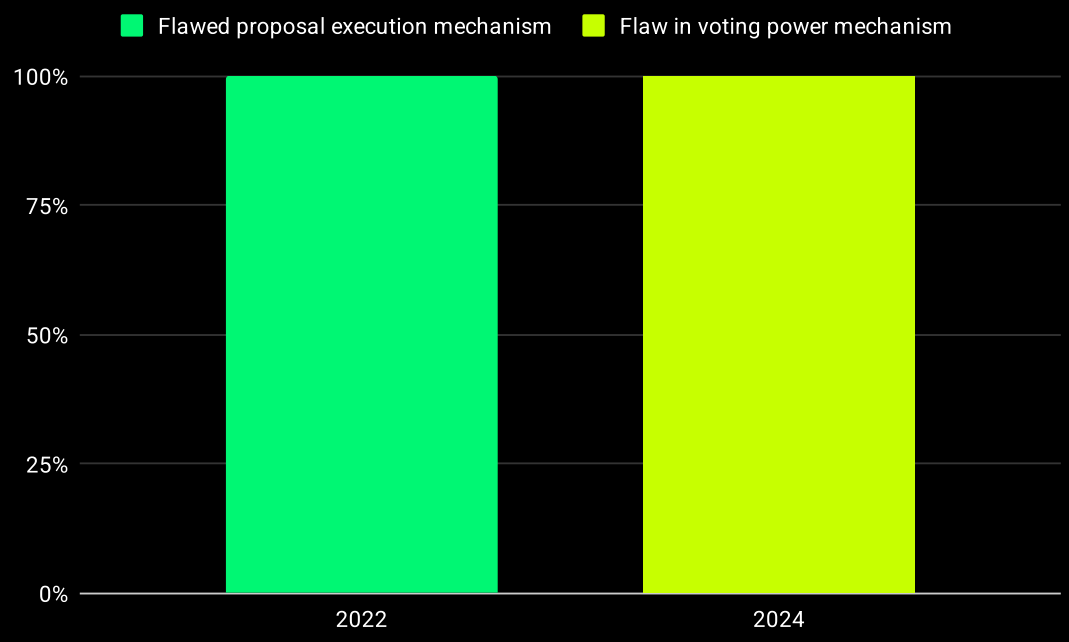

Figure 91: Number of methods used in governance attacks per year [percentage]

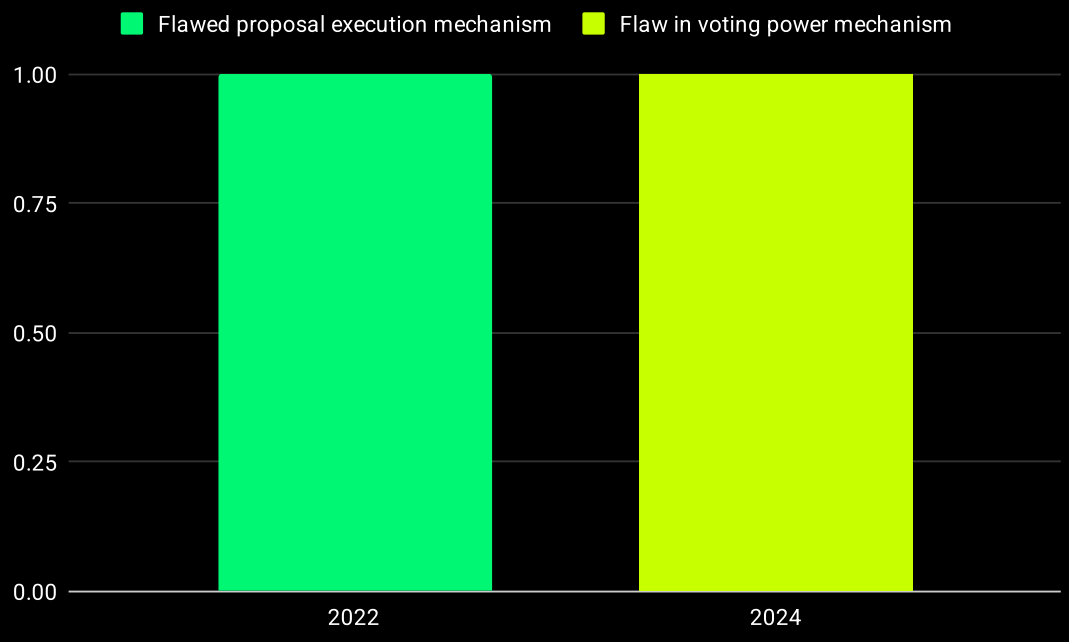

Figure 92: Number of methods used in governance attacks per year [count]

Figures 93 and 94 provide an overview of the financial losses attributed to governance attacks across different years.

Consistent with the breakdown shown in Figures 89 and 90, most of these losses—approximately $181,000,000—occurred in 2022 due to a flaw in the proposal execution mechanism. The remaining $17,163,071 in losses took place in 2024 and can be traced back to a vulnerability in the voting mechanism.

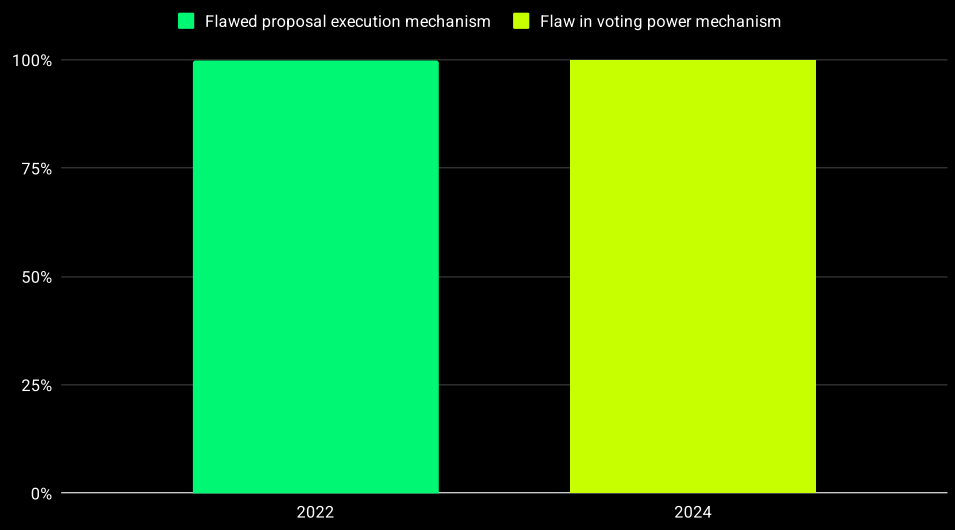

Figure 93: Loss caused by methods used in governance attacks per year [percentage]

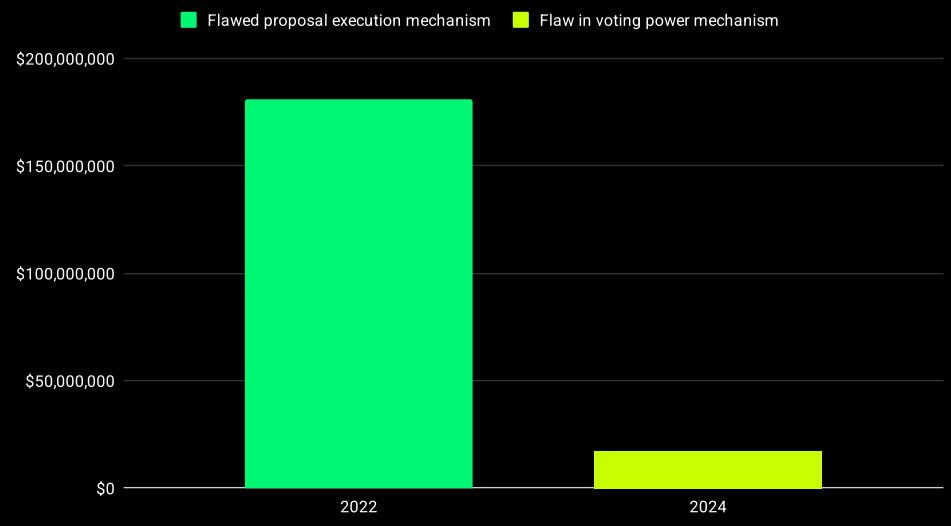

Figure 94: Loss caused by methods used in governance attacks per year [USD]

Rug pull/scams

Rug pulls and scams within projects can manifest through various methods, significantly undermining user trust and financial security. We have identified the primary tactics employed to achieve that goal:

- **Privileged owner account:** Some projects facilitate rug pulls or scams by maintaining control over accounts with elevated permissions, such as admin rights or access to a project's hot wallet. These privileged accounts enable them to execute transactions on already deployed contracts or withdraw funds **directly** without requiring anything else.

- **Malicious upgradable contract:** Some projects are structured to allow contract upgrades, which can be exploited by deploying a malicious contract either initially or during the operation phase. The malicious contract can perform unauthorized actions or manipulate the state. Subsequently, the contract may be switched to a benign version to obscure the malicious activities and deceive users.

- **Malicious library:** This method involves incorporating a malicious library within the project’s codebase. The library, often unverified, contains hidden functions or exploits that can be triggered to divert funds or manipulate the protocol's operations.

- **Challenge key knowledge:** This technique relies on the project developers having exclusive knowledge of a secret key or a piece of critical information required by the contract's code. This exclusive knowledge enables them to access or redirect funds in a manner not intended by the users or other stakeholders.

- **Ponzi/Pyramid Scheme**: This category includes fraudulent investment strategies using the blockchain where returns for older investors are paid out from the contributions of new investors rather than from profit earned by the operation of a legitimate business. Ponzi schemes promise high returns that are not achievable through conventional investments and use incoming funds from new investors to pay returns to earlier investors. Pyramid schemes operate on a similar principle but primarily make money through the recruitment of an ever-increasing number of investors. Each participant attempts to recruit others to invest under them in a hierarchical structure resembling a pyramid. Both types of schemes are

unsustainable and eventually collapse when it becomes impossible to recruit new participants, leading to significant financial losses for most involved, except those at the top of the structure.

Figures 95 and 96 provide a detailed breakdown of the methods used in rug pulls and scams, showing the distribution of these categories by occurrence.

The most common method by which projects execute rug pulls involves the control of privileged owner accounts, which accounts for 50% of all cases. This method highlights a significant risk associated with centralized control and insufficient checks on accounts with elevated permissions within DeFi projects.

Tied for the second most frequent method are Ponzi/pyramid schemes that use cryptocurrency and DeFi innovations to lure users and the exploitation of contract upgrade mechanisms through malicious upgradable contracts, each accounting for 16.7% of occurrences.

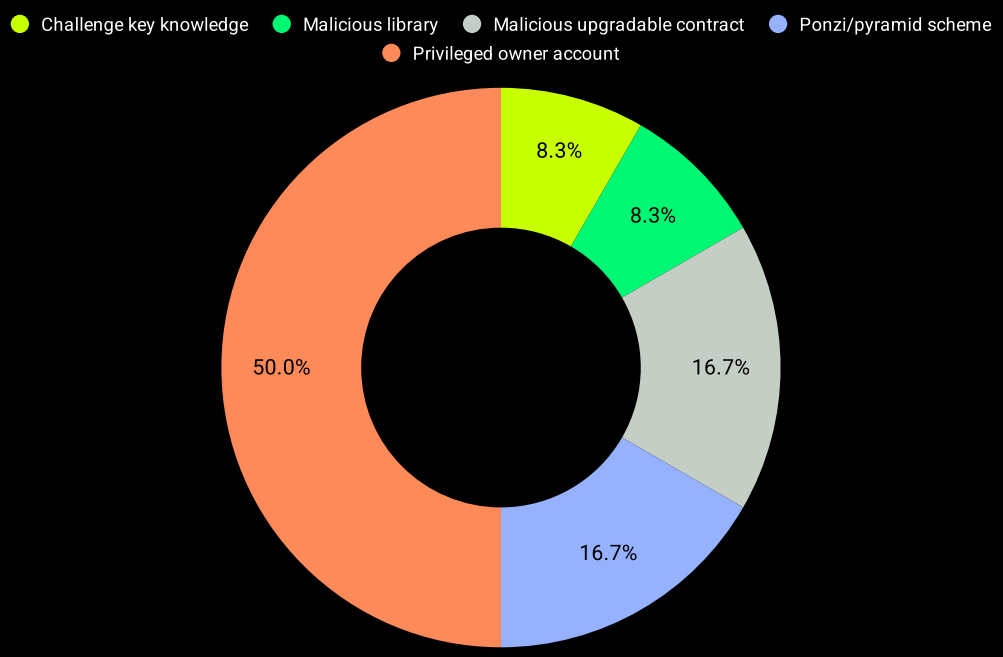

Figure 95: Number of methods used in rug pulls/scams [percentage]

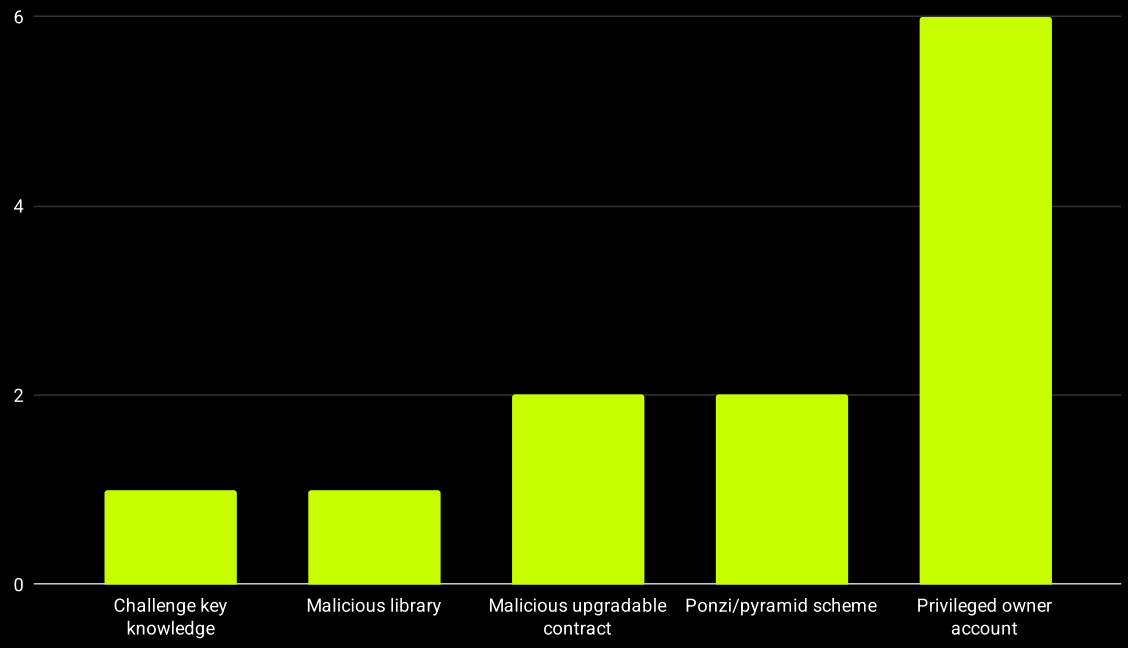

Figure 96: Number of methods used in rug pulls/scams [count]

In Figures 97 and 98, the distribution of financial losses from various types of rug pull and scam attacks is shown, providing insights into the effectiveness and financial impact of each method.

While privileged owner accounts are still a significant source of losses, accounting for 42.8% of the total funds scammed or approximately $720,466,000 USD, they no longer represent the most losses compared to their 50% occurrence rate. This indicates that while common, the average financial impact per incident may be lower than some other methods.

In contrast, Ponzi and pyramid schemes, despite their lower occurrence rate of 16.7%, account for a staggering 48.9% of the total funds scammed, amounting to $822,000,000 USD. This disproportionate impact suggests that these schemes are not only prevalent but also exceedingly profitable, exploiting large numbers of participants before their collapse.

The rest of the methods lead to less amount loss than their rate of occurrence. Notably, the use of malicious upgradable contracts, despite being a technologically sophisticated method, accounted for only 5.6% of the total funds scammed, amounting to $94,500,000 USD, a significant decrease from their 16.7% rate of occurrence. This discrepancy may indicate that while technologically clever and relatively common, the actual execution or the conditions under which these contracts are exploited might not always lead to high financial losses.

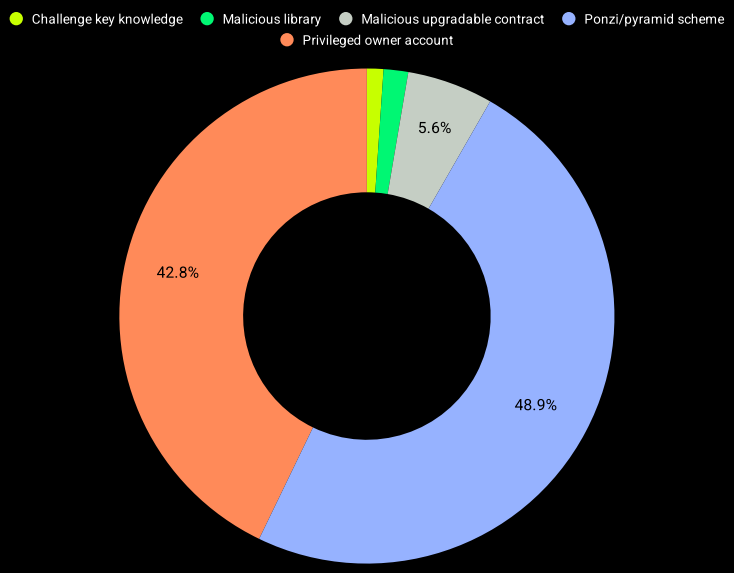

Figure 97: Loss caused by methods used in rug pulls/scams [percentage]

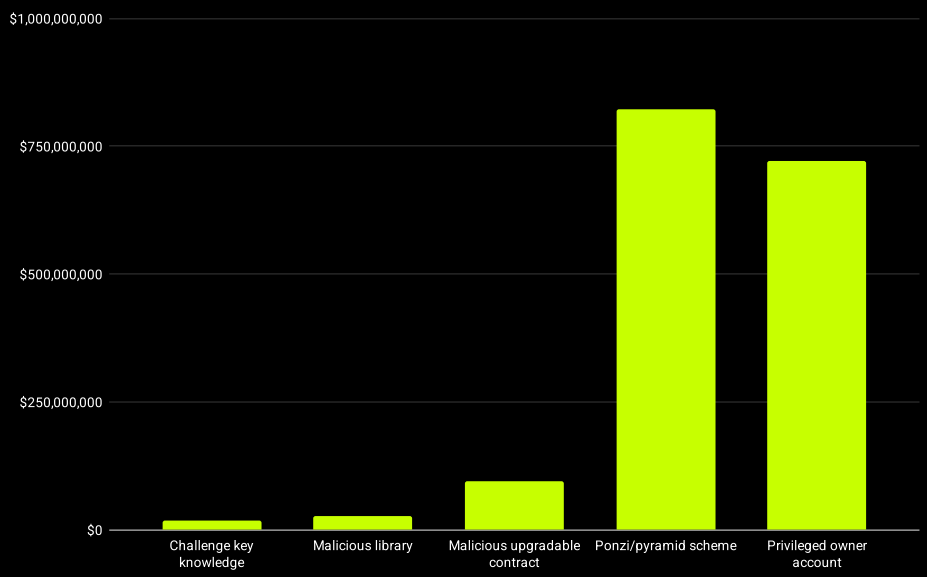

Figure 98: Loss caused by methods used in rug pulls/scams [USD]

Figures 99 and 100 provide a year-by-year analysis of the distribution of rug pulls and scams within the DeFi ecosystem, highlighting how these fraudulent activities have evolved over time.

Starting from 2019, rug pulls and scams began to register significantly enough amount lost to be included in this analysis. There was a notable spike in cases in 2021, with a total of 5 recorded instances, whereas other years typically averaged around 2 per year. This spike indicates a peak in fraudulent activity during this period.

Initially, these scams predominantly involved Ponzi and pyramid schemes. However, probably because awareness of these deceptive mechanisms has increased over time, there has been a diversification in the methods employed. Despite this diversification, privileged owner accounts have remained the predominant method through most years. In 2024, however, the use of privileged owner accounts was matched by the incidence of scams involving malicious contract upgrades.

The year 2021 stands out not only for its high number of cases but also for the variety of methods used. In this year, privileged owner accounts were involved in 40% of the occurrences, while malicious upgradable contracts, knowledge of a challenge key, and use of a malicious library each accounted for 20% of the cases.

This data seems to imply that, generally and over the years, attackers tend to favor less technologically advanced methods of deception that rely more on centralized control and ownership of protocols. Such methods exploit trust and administrative power rather than relying solely on sophisticated technological mechanisms, suggesting that the human and governance aspects of protocols are critical vulnerabilities exploited by attackers.

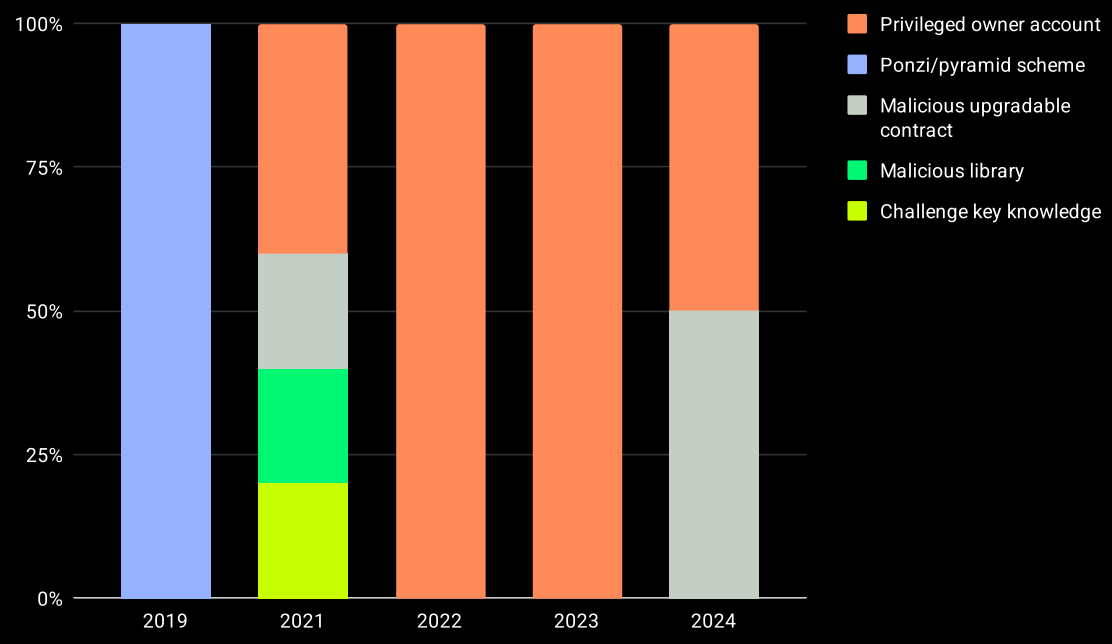

Figure 99: Number of methods used in rug pulls/scams per year [percentage]

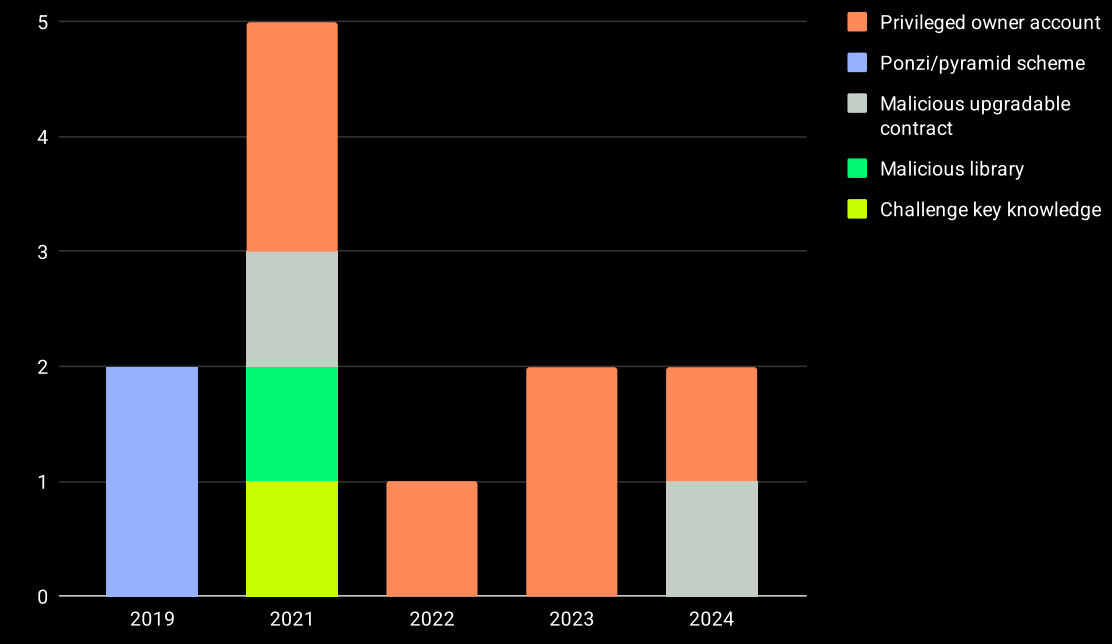

Figure 100: Number of methods used in rug pulls/scams per year [count]

Figures 101 and 102 detail the distribution of financial losses due to rug pulls and scams over the years.

A significant spike in losses occurred in 2019, totaling $822,000,000 USD, predominantly due to Ponzi and pyramid schemes. This year marked the highest financial impact from these types of scams, underscoring the substantial losses they can inflict.

2022 saw another notable spike, with losses amounting to $450,000,000 USD. In contrast, other years typically recorded losses below the $250,000,000 USD threshold, indicating less severe financial impacts during those periods.

For the years 2019, 2022, and 2023, the distribution of losses aligns precisely with their rate of occurrence since they are attributed to a single root cause each year.

In 2021, however, the landscape shifts slightly. Privileged owner accounts were responsible for most of the financial damage, accounting for 53% of the losses or $87,000,000 USD, despite representing only 40% of occurrences.

2024 sees malicious upgradable contracts as the leading cause of losses, responsible for 65.4% of the financial impact, totaling $62,500,000 USD, even though these only occurred in 50% of the cases. This illustrates that, although less favored by occurrence, sophisticated scams can lead to substantial losses, especially in later years.

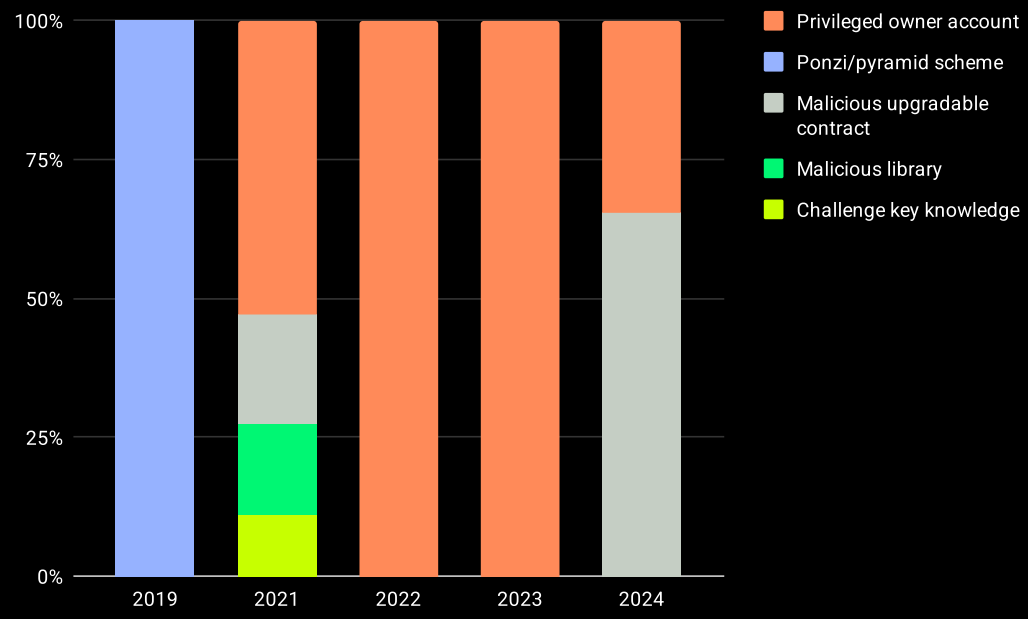

Figure 101: Loss caused by methods used in rug pulls/scams per year [percentage]

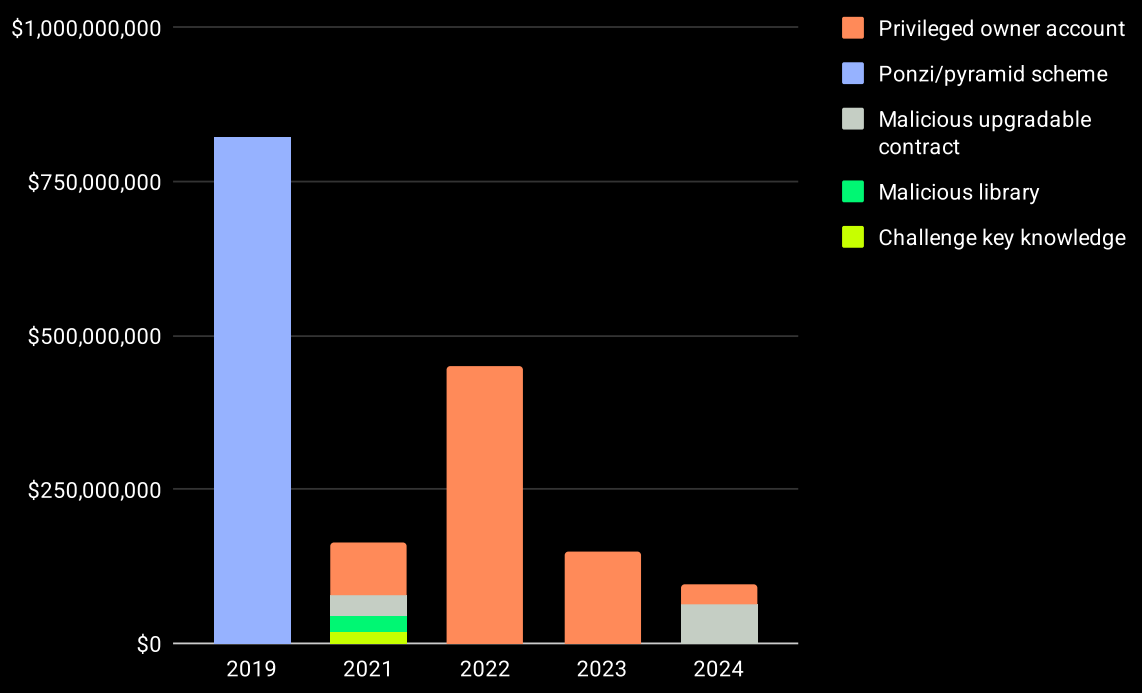

Figure 102: Loss caused by methods used in rug pulls/scams per year [USD]

Compromised Account

Accounts can be compromised through various methods, each with unique vulnerabilities and attack vectors:

- **2FA bypass:** This method involves circumventing a protocol's two-factor authentication system to gain unauthorized access to sensitive keys or the account.
- **Flawed key generation:** Poor implementation of the algorithm used for generating private keys can simplify unauthorized access, making the keys easier to predict or intercept.
- **Compromised server/infrastructure:** In cases where a project's server or infrastructure is breached (not due to social engineering or phishing), critical data such as keys, mnemonics, or other sensitive information can be stolen directly by attackers

- **Security management flaw:** Errors in configuring or managing the security settings of third-party tools or protocols can lead to private key leakage or account compromise.
- **Compromised API keys:** Attackers obtain API keys for the protocol, enabling them to perform actions—such as withdrawing funds—under the guise of legitimate access.
- **Social engineering attack/Phishing:** Social Engineering Attack/Phishing: This attack is possible using social engineering or phishing techniques. An example includes disguising a malicious email as a legitimate one to deceive a project's developer or tricking users into approving transactions by presenting visually misleading or confusing information. This type of attack may also employ malware to facilitate the deception.
- **Third-party hack:** A data breach at a third party, outside the direct control of the project or users, results in the theft of keys or compromise of accounts. An example would be the hacking of a database maintained by a service provider.
- **Unknown:** In some instances, the exact method used for compromising accounts or stealing keys remains undisclosed or unknown.

Figures 103 and 104 provide a detailed breakdown of how accounts or private keys are compromised.

A significant majority, 54.8%, of these incidents fall under the category where the method of compromise is either unknown or not disclosed by the affected protocol. This high percentage highlights a lack of transparency or possibly the complexity and stealthiness of the attack methods used, making detection and diagnosis challenging.

Following this, social engineering or phishing attacks are the most common identifiable methods, accounting for 26.2% of cases. These techniques exploit human errors and are effective in bypassing even the most robust technical safeguards by deceiving individuals into providing access or sensitive information directly to attackers.

Both compromised server or infrastructure and third-party hacks are tied for third place, each responsible for 4.8% of the incidents. These breaches indicate vulnerabilities either within the project's own hardware and software environments or within external systems that they rely upon, showing the broad range of attack surfaces that need to be secured in the DeFi ecosystem.

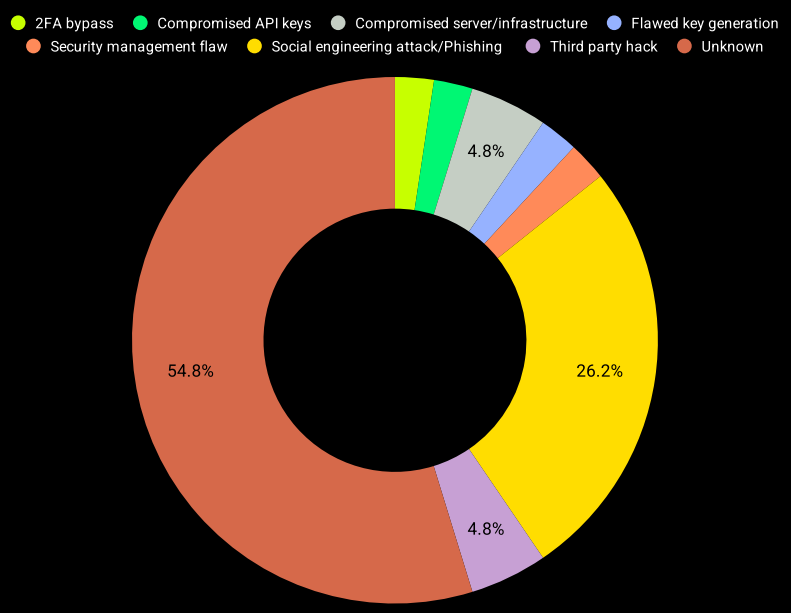

Figure 103: Number of reasons causing a compromised private key [percentage]

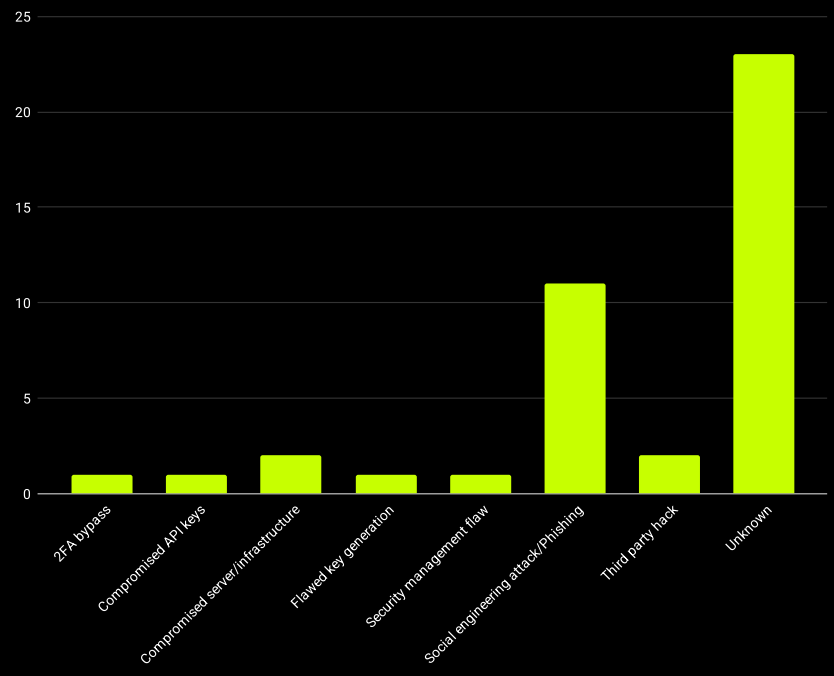

Figure 104: Number of reasons causing a compromised private key [count]

Figures 105 and 106 present the distribution of lost funds by root cause

Most financial losses, amounting to 47.7% or approximately $2,416,574,839 USD, come from causes that are unknown or not disclosed. While this is slightly lower than might be expected given their high rate of occurrence, it still represents the largest portion of the total financial damage, underscoring the significant impact of incidents where the breach method remains unclear or secret.

Social engineering and phishing attacks result in substantial financial damage, constituting 41.1% of the losses or about $2,079,770,000 USD. This is considerably higher relative to their occurrence rate of 26.2%, indicating that when these attacks occur, they tend to result in significant financial detriment.

Third-party hacks, where external services or partners are compromised, account for 4.7% of the total financial losses, amounting to around $237,000,000 USD. This is slightly lower than their occurrence rate of 4.8% but still significant, placing them third in terms of financial impact.

Other causes contribute even less financially relative to their frequency, suggesting these methods tend to be less costly compared to the dominant attack vectors.

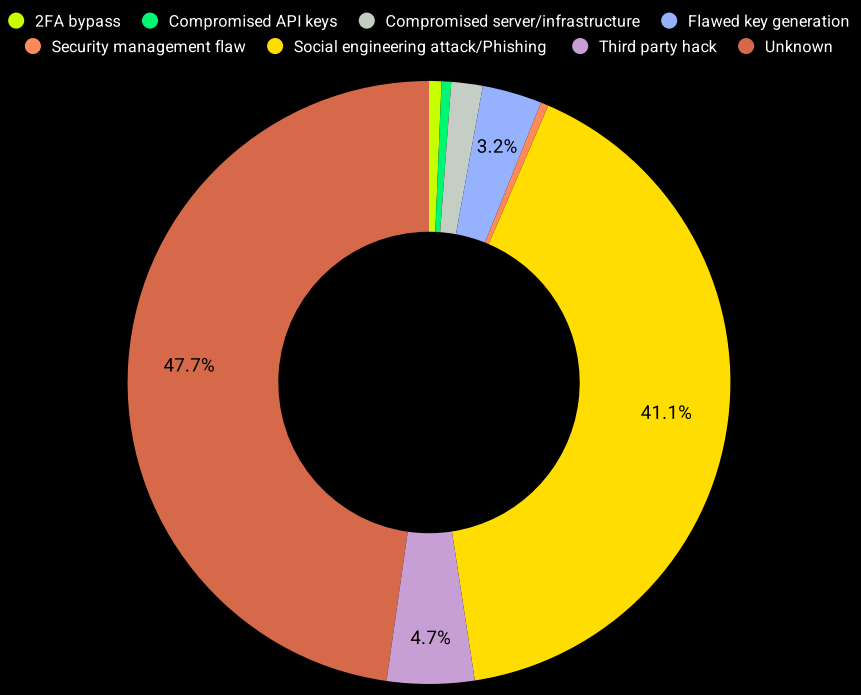

Figure 105: Loss caused by reasons leading to a compromised private key [percentage]

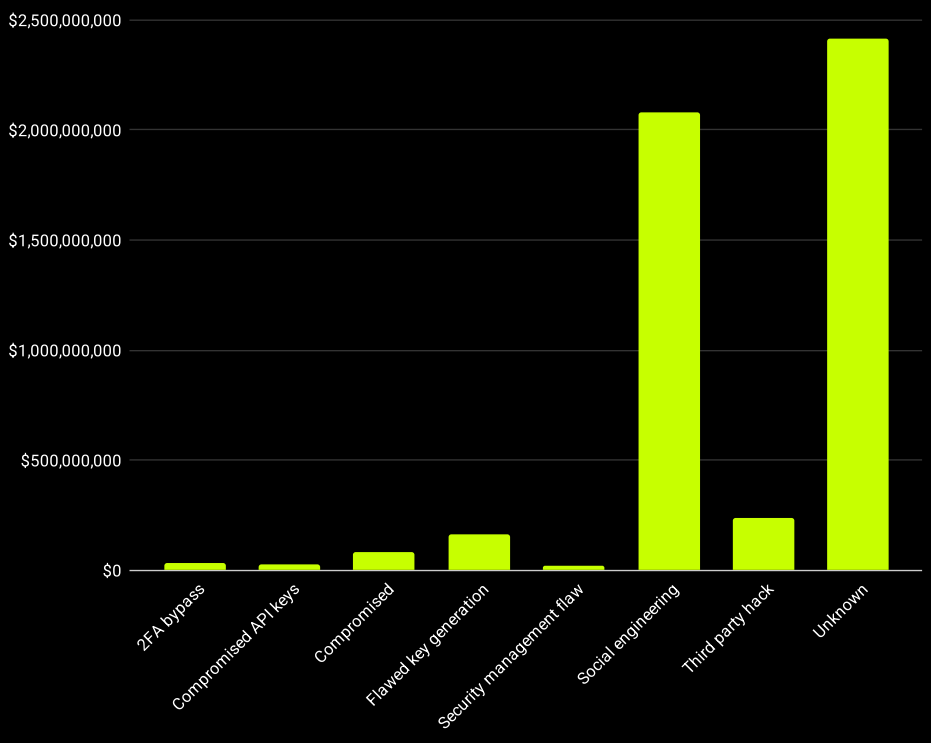

Figure 106: Loss caused by reasons leading to a compromised private key [USD]

Figures 107 and 108 provide an analysis of how accounts were compromised over various years.

Throughout most of the observed period, the predominant issue has been that the method of account or key compromise remains unknown. However, there are exceptions in 2019, 2020 and 2024, where social engineering or phishing attacks were as prevalent as the unknown causes.

From 2021 onwards, there has been a noticeable diversification in the causes of account compromises. Unlike earlier years, which typically saw dominance by one or two types of attacks, 2021 marked a shift with a broader array of vulnerabilities being exploited. In 2022, accounts were compromised through a variety of methods: third-party hacks, social engineering or phishing, flawed key generation, and 2FA bypass, each accounting for 16.7% of the incidents. The remaining percentage of cases continued to fall into the unknown category.

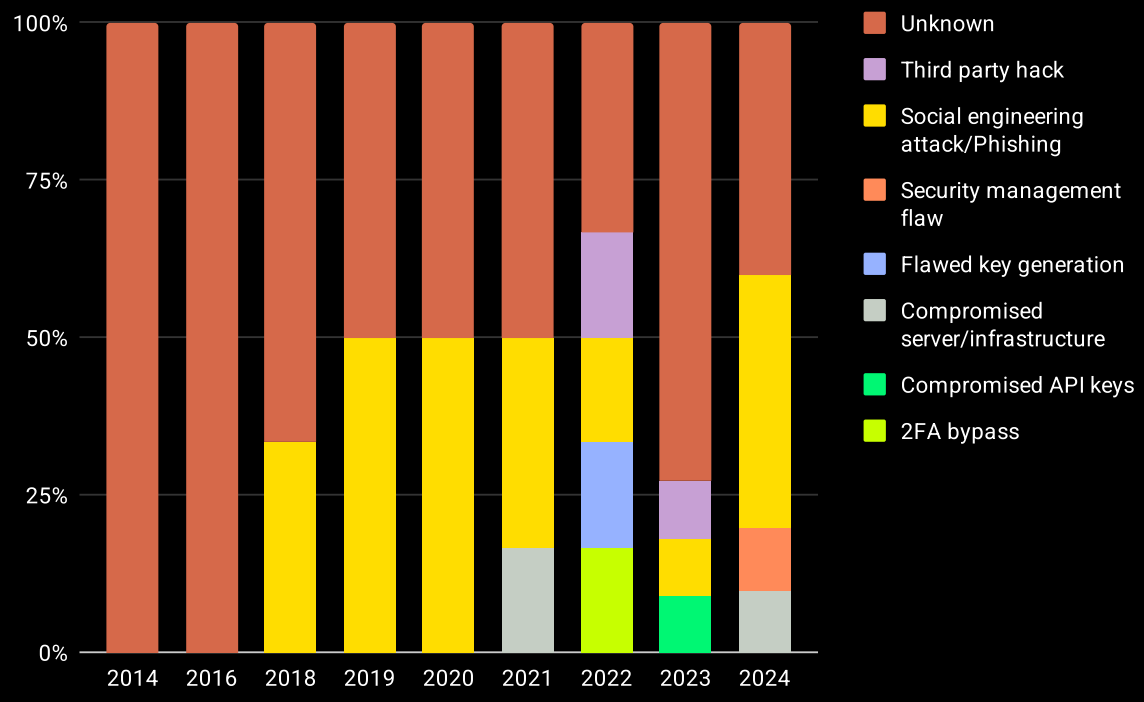

Figure 107: Number of reasons causing a compromised private key per year [percentage]

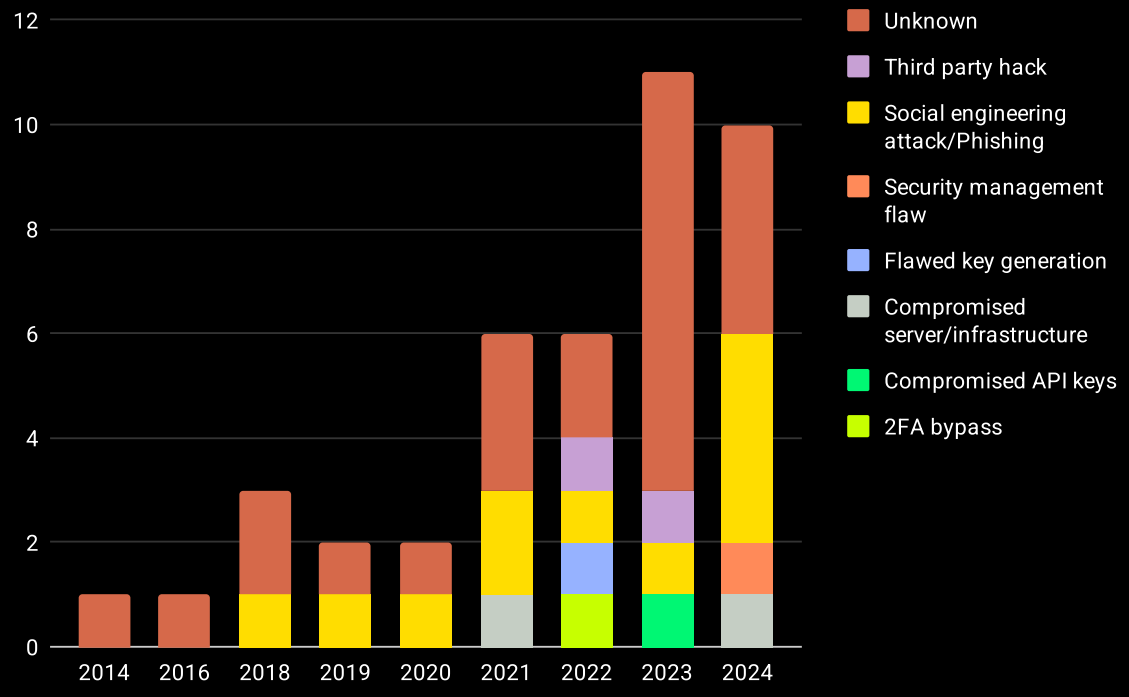

Figure 108: Number of reasons causing a compromised private key per year [count]

Figures 109 and 110 show the financial losses over the years from attacks leading to compromised accounts.

The data indicates that losses from these types of attacks peaked in recent years, particularly in 2024, when the total loss reached $1,032,664,888 USD. This was the highest recorded, with 2022 and 2023 following closely behind with losses of $985,000,000 USD and $848,279,951 USD, respectively.

There is a notable discrepancy in losses compared to occurrence rates for social engineering and phishing attacks. In 2018, these attacks were responsible for 86.1% of the losses, totaling $534,000,000 USD, despite occurring in only 33.3% of cases. Similarly, in 2022, such attacks accounted for 63.4% of the financial losses, equating to $624,000,000 USD, against an occurrence rate of 16.7%. In 2024, there was a drastic increase in losses from these attacks to 62.7% ($647,470,000 USD) compared to a 40% occurrence rate.

In contrast, 2019 and 2020 saw fewer losses from social engineering and phishing, with a higher proportion of losses from unknown or undisclosed causes. In 2019, unknown causes accounted for 52.9% of the losses ($45,000,000 USD), and in 2020, these causes represented 92.6% of the financial impact ($275,000,000 USD) against their rate of occurrence of 50%. Unknown or undisclosed causes also resulted in more losses in 2021, with 63.9% ($413,700,000 USD) of amount lost against a rate of occurrence of 50%. In 2024, however, the contrary occurs, with unknown causes leading to 32.7% of the value hacked ($338,094,888 USD) compared to a rate of occurrence of 40%.

Third-party hacks in 2023 also reported more losses than their rate of occurrence, accounting for 23.6% of the financial losses ($200,000,000 USD) compared to a 9.1% occurrence rate.

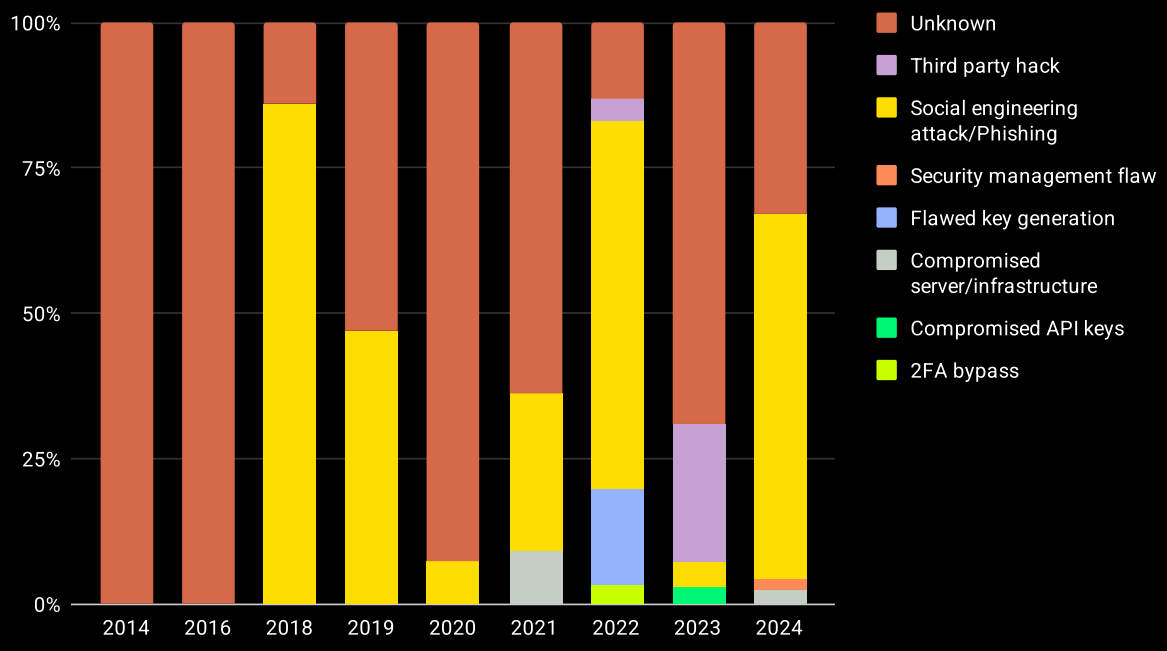

Figure 109: Loss caused by reasons leading to a compromised private key per year [percentage]

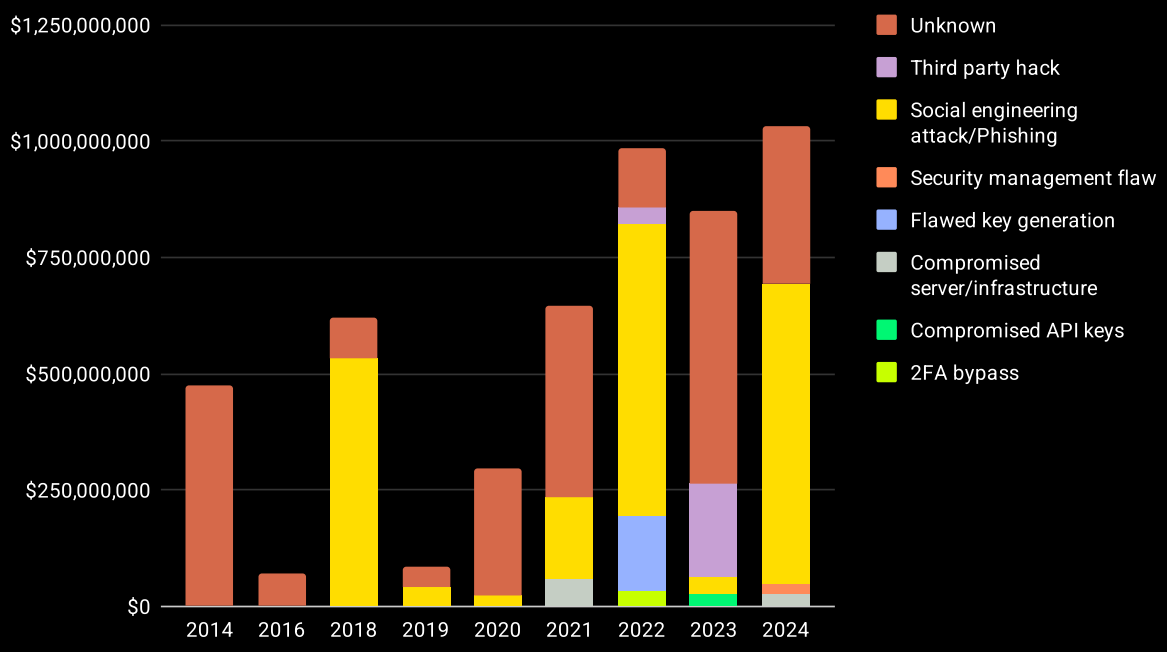

Figure 110: Loss caused by reasons leading to a compromised private key per year [USD]

ATTACKS PER CHAINS

This report investigates the relationship between the types of attacks previously defined and the blockchain networks previously analyzed.

The findings from Figures 111 and 112 highlight the primary causes of attacks across various chains.

For most of the chains, including Bitcoin, Bitcoin Cash, Linea, Ethereum, multi chains attacks (“Multi”), Mona Coin, NEM, Polygon, and Tron, the predominant cause of attacks is a compromised account. This type of attack also represents half of the incidents on the Blast and Mixin chains and is equally prevalent alongside market manipulation attacks on Avalanche, Base, and Optimism.

Direct contract exploitation emerges as the main cause of security breaches on Aptos, Solana, and Terra, which could indicate a particular vulnerability in the contract designs or implementations on these platforms.

Interestingly, market manipulation attacks are not the majority cause for any chain, which could suggest either a lower occurrence or perhaps more effective countermeasures against this type of attack on most networks.

Rug pulls and scams dominate the attack landscape on Moonriver and Dogechain, where they constitute all recorded incidents. They also account for half of the incidents on Blast and Fantom, with the latter also seeing an equal prevalence of direct contract exploitation.

Base presents a unique case with an equal division of incidents among compromised accounts, market manipulation attacks, and rug pulls, illustrating a diverse threat landscape. Arbitrum similarly shows a balanced spread among direct contract exploitation, market manipulation, and compromised accounts.

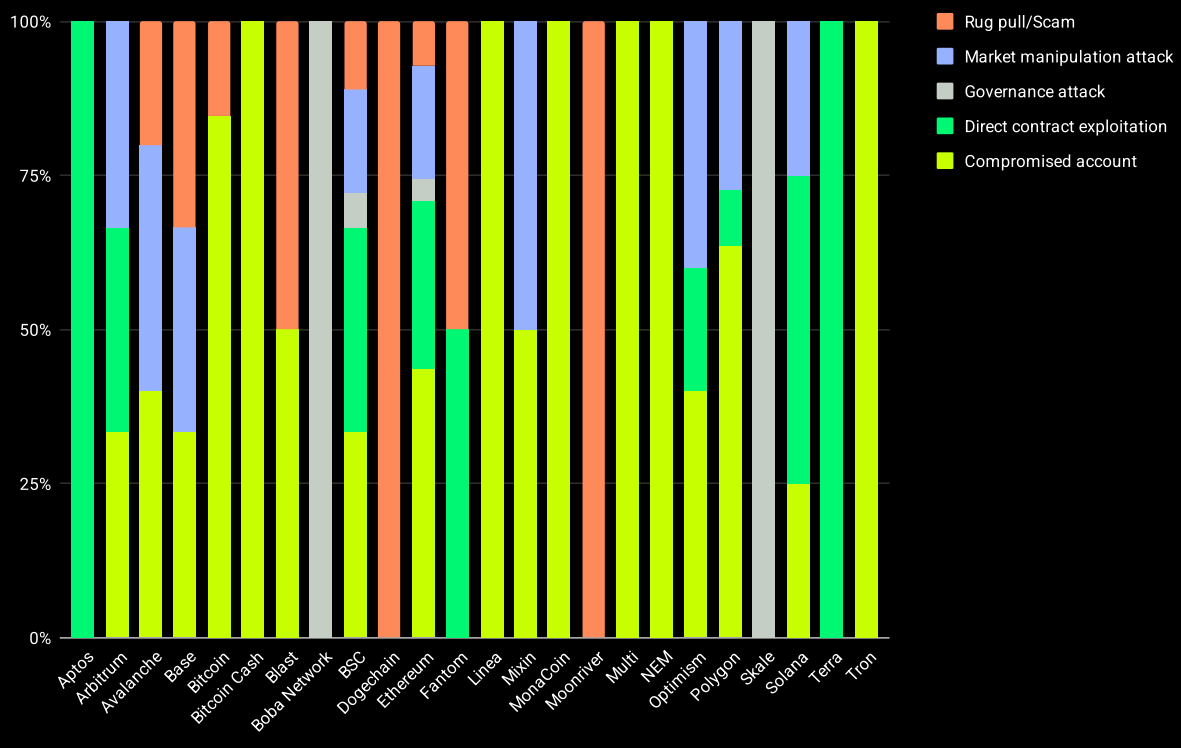

Figure 111: Number of types of attack per chain [percentage]

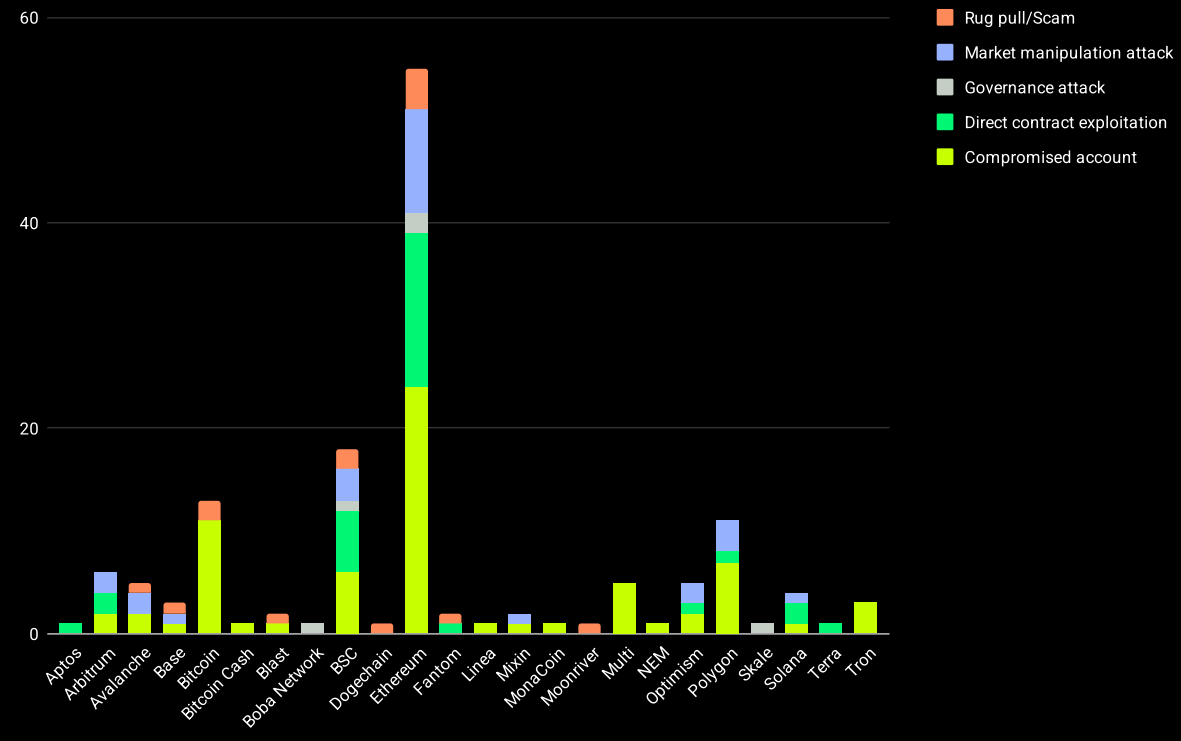

Figure 112: Number of types of attack per chain [count]

Figures 113 and 114 illustrate the distribution of financial losses per blockchain network, segmented by type of attack.

This data reveals distinct patterns and key discrepancies between the occurrence rates of attacks and the financial impacts they cause.

Arbitrum experienced significant losses due to direct contract exploitation, accounting for 66.9% or $122,600,000 USD of the losses, despite this type of attack only occurring 33.3% of the time.

Avalanche saw higher losses from compromised accounts than might be expected from their occurrence rate, with these attacks causing 51% of the losses ($54,291,966 USD) compared to a 40% occurrence rate.

Base and Bitcoin both show a notable discrepancy with rug pulls and scams, where on Base, this attack type caused 90.3% of the losses ($23,000,000 USD) against a 33.3% occurrence rate, and on Bitcoin, it accounted for 44.6% of the financial impact ($822,000,000 USD) versus a 15.4% occurrence rate.

Blast also experienced nearly 100% of its losses ($62,500,000 USD) due to rug pulls and scams, despite these only happening 50% of the time.

BSC sees a substantial impact from direct contract exploitation, which caused 75.1% of the losses ($1,010,000,000 USD) against a 33.3% occurrence rate.

In Ethereum, market manipulation attacks caused disproportionately less loss (6.9%, $313,379,000 USD) compared to their occurrence (18.2%), whereas rug pulls and scams led to significantly higher losses (12.5% or $570,000,000 USD) than their occurrence rate (7.3%).

Fantom's major losses from rug pulls and scams were 80% ($120,000,000 USD), much higher than their 50% occurrence rate.

Mixin witnessed most of its losses from compromised accounts, with these accounting for 74.1% ($200,000,000 USD) compared to a 50% occurrence rate.

Optimism had significant discrepancies, especially in losses caused by direct contract exploitation, 41.7% ($30,500,000 USD) against a 20% occurrence rate, and market manipulation, which led to 47.8% of the losses ($35,000,000 USD) versus a 40% occurrence rate.

Polygon shows a high contrast in the impact of direct contract exploitation, which, though only 9.1% of occurrences, led to 24% of the losses ($85,000,000 USD). Market manipulation was also a leading cause of financial loss, representing 40.2% ($142,400,000 USD) against a 27.3% occurrence rate.

Solana also reported a higher impact from direct contract exploitation than might be expected from its occurrence rate, with 73.3% of losses ($374,000,000 USD) compared to a 50% occurrence rate.

Interestingly, while market manipulation attacks are not the leading cause of loss by occurrence on any chain, they are the primary cause of financial loss on both Optimism and Polygon when considering the actual financial impact.

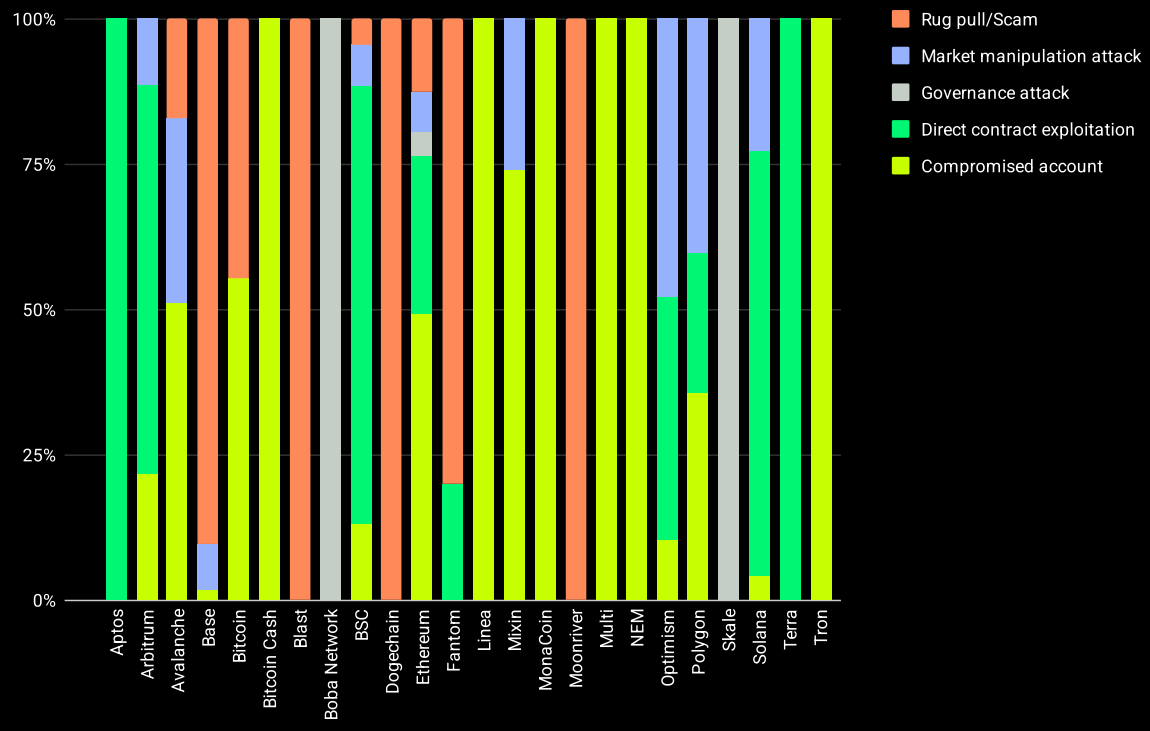

Figure 113: Loss caused by type of attack per chain [percentage]

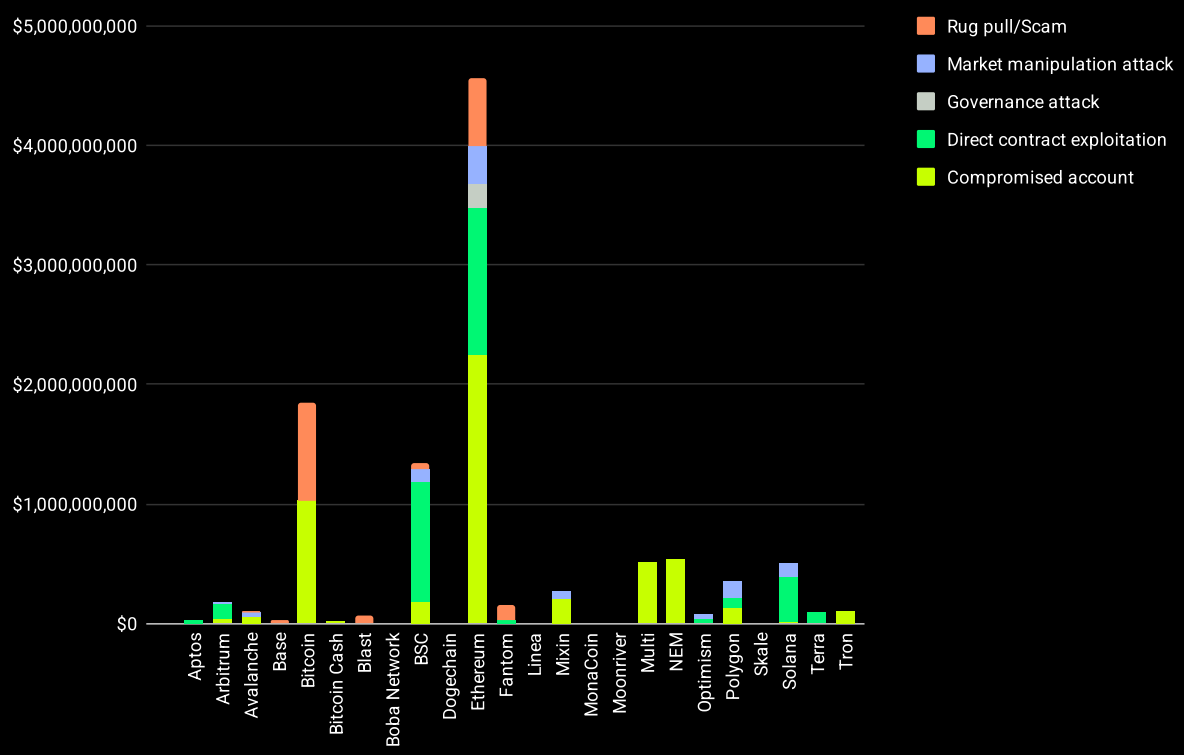

Figure 114: Loss caused by type of attack per chain [USD]

Figures 115 and 116 illustrate the evolution of attack types across various blockchain networks over the years, showing how certain types of attacks have become more prominent on some chains while others have shifted in nature.

Arbitrum initially saw attacks predominantly due to direct contract exploitation. Over time, this shifted towards market manipulation and ultimately to compromised accounts being the primary issue by 2024.

Avalanche and Base started with attacks primarily categorized as market manipulation and rug pulls but evolved to predominantly involve compromised accounts by 2024.

Bitcoin has consistently been targeted by compromised account attacks, except for 2019, where rug pulls and scams constituted 66.7% of the incidents.

BSC began with a mix of compromised accounts, direct contract exploitation, and market manipulation in 2021. The focus shifted to direct contract exploitation in 2022 and then back to compromised accounts in subsequent years.

Ethereum has shown a varied pattern: starting with direct contract exploitation in 2016 and 2017, shifting to compromised accounts in the following two years, then back to direct contract exploitation in 2020, followed by market manipulation in 2021, and finally returning to a predominance of compromised account attacks in the most recent years.

On the other hand, Fantom saw a shift from direct contract exploitation to predominantly rug pulls and scams.

For those attacks that affected multiple chains (“Multi”), compromised accounts have consistently been the most common issue across all years.

Optimism displayed a progression from direct contract exploitation in 2022 to market manipulation in 2023 and then to compromised accounts in 2024.

Polygon has mostly been affected by compromised accounts, except in 2023, when market manipulation became the leading cause of attacks.

Solana experienced a transition from direct contract exploitations in 2022 to compromised accounts in 2024, while Tron has seen compromised accounts as the primary attack vector across all years.

Overall, the trend indicates that while direct contract exploitation was the initial predominant issue for many chains, there has been a notable shift towards compromised accounts being the leading cause of attacks in recent years. Additionally, there was a noticeable spike in chains experiencing market manipulation attacks in 2022 and 2023.

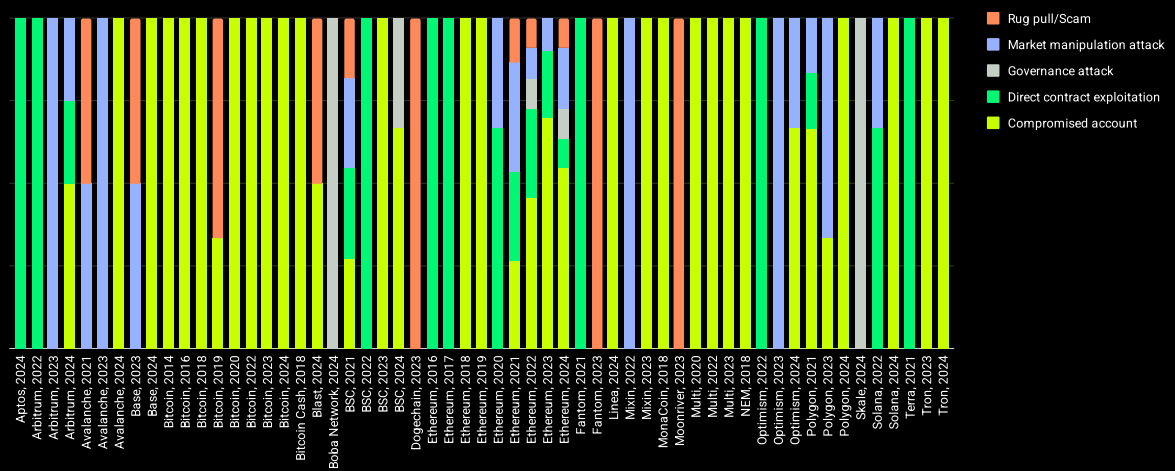

Figure 115: Number of types of attack per chain and year [percentage]

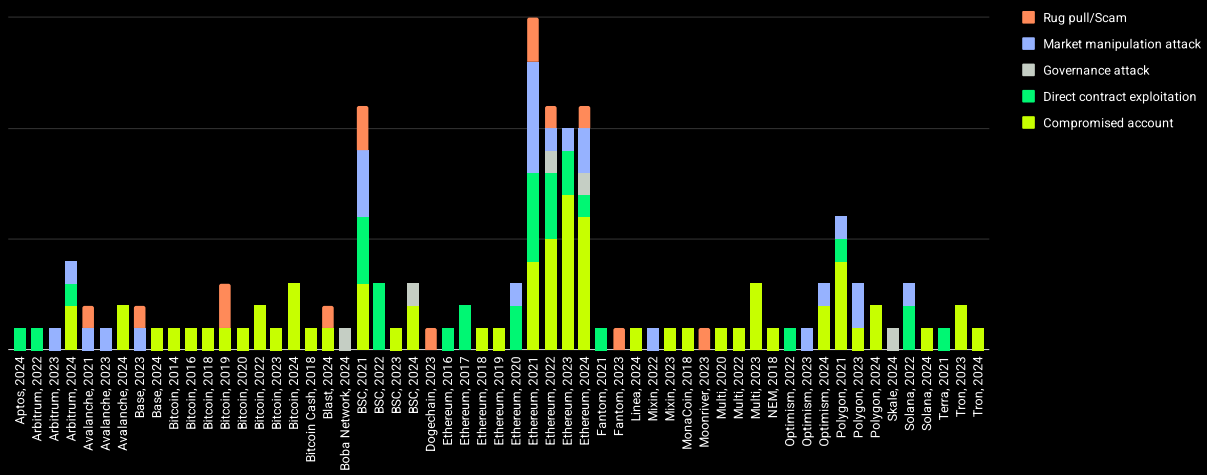

Figure 116: Number of types of attack per chain and year [count]

Figures 117 and 118 reveal the evolution of financial losses by attack type over various years, highlighting discrepancies between the occurrence rates of attacks and the resultant financial impacts on different blockchain networks.

In 2024, while compromised accounts were the predominant attack vector in Arbitrum, the main source of financial loss was direct contract exploitation, accounting for 51.1% of the losses ($42,600,000 USD) despite only a 25% occurrence rate.

For Avalanche in 2021, although rug pulls and market manipulation occurred at the same rate, market manipulation was responsible for a greater share of financial losses, making up 65.3% of the total ($34,000,000 USD).

Equally, in Base during 2023, even though the attacks were evenly distributed across types, rug pulls and scams resulted in 92% of the financial losses ($23,000,000 USD).

Bitcoin saw a significant impact from rug pulls and scams in 2019, where these attacks accounted for 95.4% of the losses ($822,000,000 USD) compared to their 66.7% occurrence rate.

In BSC during 2021, a substantial portion of the financial damage was due to direct contract exploitation, which represented 53.1% of the losses ($328,000,000 USD) against an occurrence rate of 27.3%.

Ethereum in 2021 experienced higher losses from compromised accounts and direct contract exploitation than their occurrence rates might suggest, with losses of 34.6% ($404,460,046 USD) and 39.2% ($458,800,000 USD), respectively, against a 26.7% rate for both. By 2024, compromised accounts led to a disproportionately high number of losses, accounting for 84.7% ($542,882,985 USD) compared to a 54.5% occurrence rate.

In Optimism during 2024, despite most attacks being due to compromised accounts, the main cause of financial loss was market manipulation, which accounted for 72.3% of the losses ($20,000,000 USD) despite only a 33.3% occurrence rate.

Finally, Polygon in 2023 also suffered significant losses from market manipulation attacks, which, while being the primary attack type for that year, led to a staggering 94.1% of the financial losses ($123,000,000 USD), aligning with a 66.7% occurrence rate.

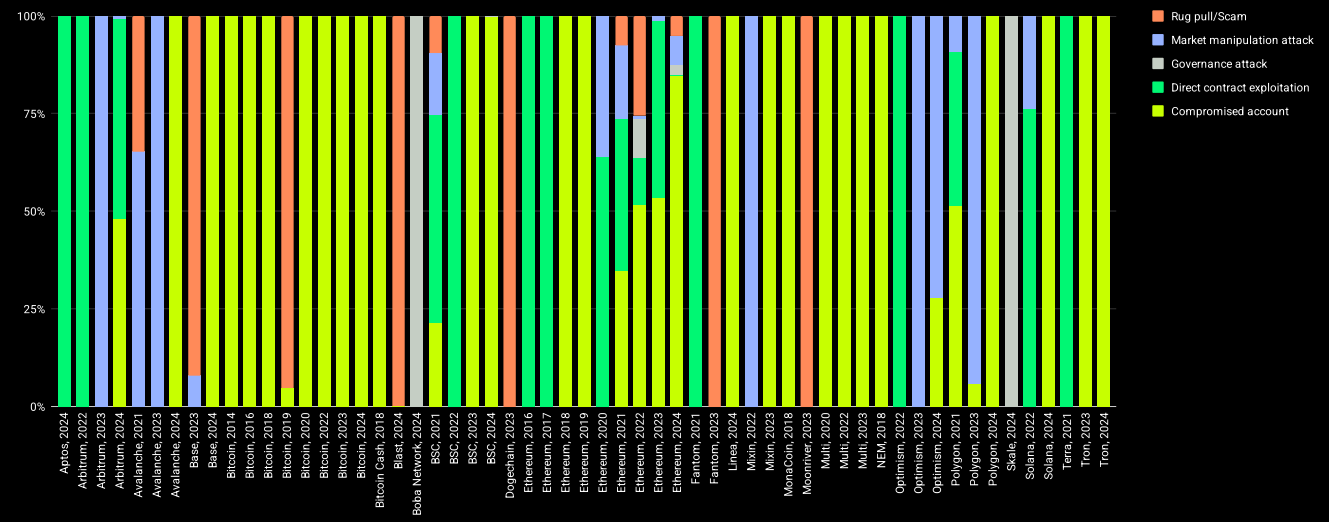

Figure 117: Loss caused by type of attack per chain and year [percentage]

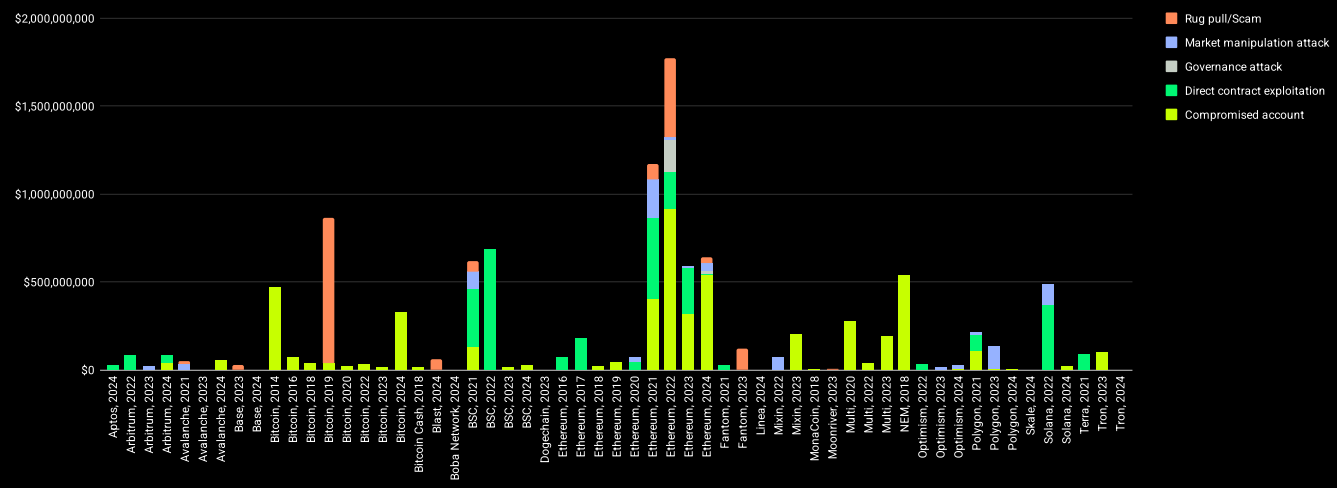

Figure 118: Loss caused by type of attack per chain and year [USD]

TYPE OF PROTOCOLS

In the DeFi space, numerous protocols offer a range of services, making it crucial to assess their vulnerability to various types of attacks.

To facilitate a coherent and comprehensive analysis, we adopt the protocol categories and nomenclature provided by DefiLlama. This standardized classification helps in comparing the security profiles of different protocols effectively.

DefiLlama categorizes protocols based on their primary function and utility within the DeFi ecosystem. This includes categories including, but not limited to:

- **Algo-Stables:** Algorithmic stablecoins that use algorithms to maintain their peg to a reserve asset, such as the US dollar, without relying on physical reserves.
- **Bridge:** Protocols that connect two different blockchain networks, allowing for the transfer of assets or data between them.
- **CDP (Collateralized Debt Position):** A type of DeFi protocol that allows users to lock up assets as collateral to mint or borrow other assets.
- **CEX (Centralized Exchange):** A traditional cryptocurrency exchange where transactions are managed by a central authority.
- **Chain:** Refers to a specific blockchain network or the underlying technology that supports the creation and management of decentralized applications.
- **Derivatives:** Financial securities that derive their value from an underlying asset, used for hedging or speculative purposes within decentralized finance.
- **DEX Aggregator:** Platforms that pool liquidity from various decentralized exchanges to offer users better trading rates.
- **Dexes (Decentralized Exchanges):** Peer-to-peer marketplaces where transactions occur directly between traders without the need for an intermediary. We will address them as DEXes throughout this report instead of ‘Dexes’ since this term is more commonly used.
- **Farm:** Protocols in DeFi that allow users to stake or lock up cryptocurrencies in return for rewards, often in the form of additional tokens.

- **Gaming:** Blockchain-based games or gaming platforms that utilize cryptocurrency or NFTs as in-game assets or for governance.
- **Indexes:** Financial instruments that track the performance of a basket of assets, allowing investors to gain exposure to multiple assets through a single investment.
- **Launchpad:** Platforms that support the launch of new projects or tokens, often providing early access to tokens for participants.
- **Lending:** Protocols where users can lend out their crypto assets in return for interest payments or take loans against their crypto holdings.
- **Liquid Staking:** A form of staking where users receive a liquid token in return for the staked asset, which can then be used within other DeFi protocols.
- **Liquidity manager:** Tools or protocols that help users optimize the liquidity they provide to decentralized exchanges or other DeFi platforms.
- **Payments:** Solutions that facilitate the use of cryptocurrencies for everyday transactions and payments.
- **Ponzi:** Schemes promising high returns that are paid from the incoming funds contributed by new participants, unsustainable and often fraudulent.
- **Prediction Market:** Platforms where users can speculate on the outcome of future events, with payouts based on the accuracy of their predictions.
- **Reserve Currency:** A cryptocurrency that holds value and is used to stabilize the price of other tokens or to act as a store of value.
- **Services:** Various service-oriented protocols that offer functionalities like custody, asset management, or advisory within the blockchain ecosystem.
- **Wallets:** Digital tools that allow users to store, send, and receive cryptocurrencies.
- **Yield:** The returns earned on various cryptocurrency investments, often through staking, lending, or trading.
- **Yield Aggregator:** Platforms that automate the process of maximizing yield by moving assets between different DeFi protocols.

We have introduced an additional category titled "Other Currency" to encompass memecoins and shitcoins. These types of currencies frequently appear in our analyzed sample but do not align with any specific category in DefiLlama's classification system.

Additionally, there are other categories available on DefiLlama's website that are not listed here, as they do not pertain to any protocols discussed in this report. For a complete understanding of all potential categories, one can refer to the detailed listings on DefiLlama's page.

It should be noted that our analysis includes an attack on a whale's Externally Owned Account (EOA), which targets an individual user rather than a protocol. As a result, this instance does not correspond to any specific protocol in our study. Therefore, we have 99 samples in our dataset for this section of the report instead of 100.

Figures 119 and 120 illustrate the distribution of attacks across different types of DeFi protocols, providing insight into which categories are most frequently targeted by attackers.

Centralized Exchange (CEX) protocols emerge as the most attacked, comprising 20.2% of the total incidents. This is indicative of their prominent role and substantial asset holdings, which make them attractive targets for cybercriminals.

Lending protocols follow closely, accounting for 15.2% of the attacks. Their complex interactions and significant liquidity positions likely contribute to their high vulnerability.

Decentralized Exchanges (DEXes) also see a considerable number of attacks, making up 11.1% of the total. This reflects the inherent risks associated with trading platforms, where asset exchanges are managed without central oversight.

Bridges, which facilitate the transfer of assets between different blockchains, have followed closely, being targeted in 10.1% of the incidents. The technical complexities and sometimes lower security measures in bridges can make them susceptible to security breaches.

The remainder of the protocols each account for 6.1% or less of the total attacks, with no more than six cases each. This suggests that while all protocol types are at risk, those handling significant volumes of user transactions and funds are particularly vulnerable to cyber threats.

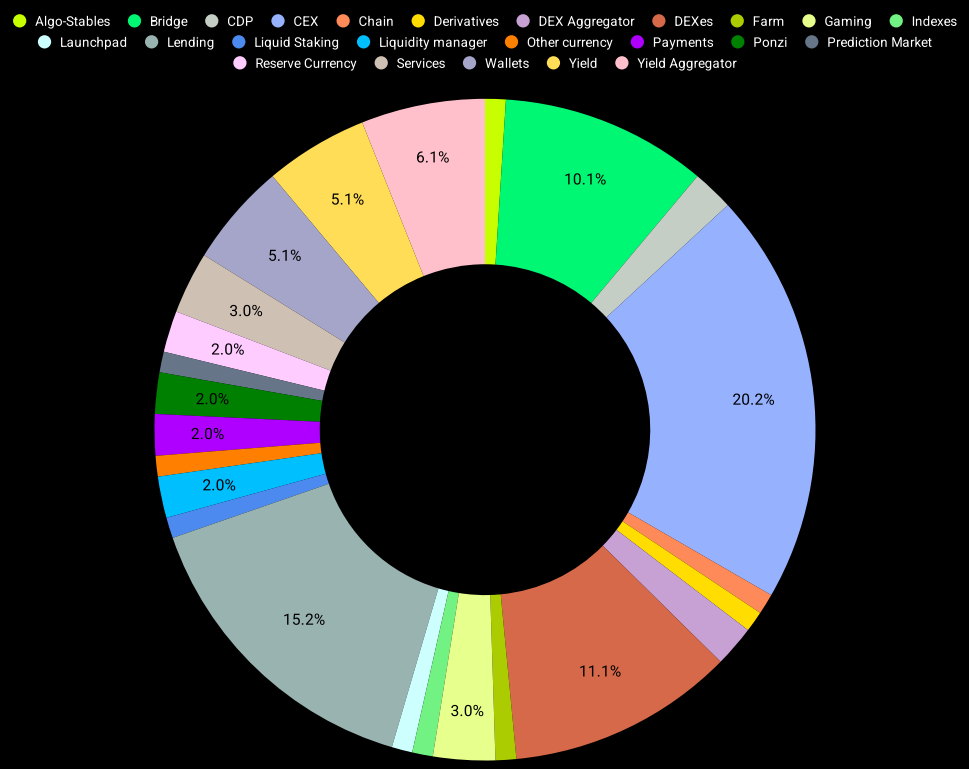

Figure 119: Number of types of protocol [percentage]

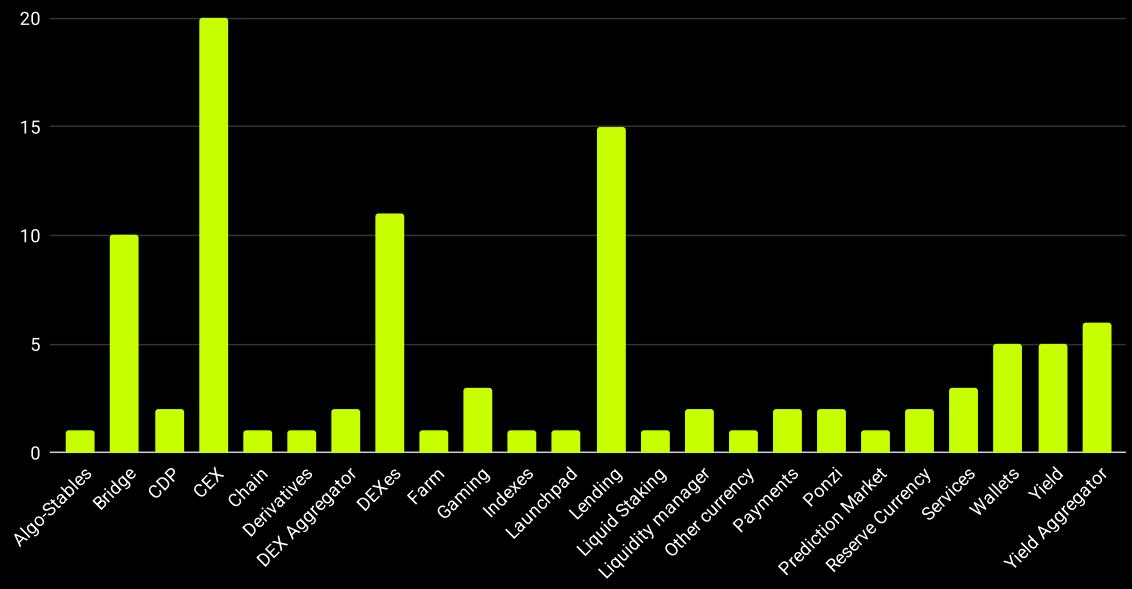

Figure 120: Number of types of protocol [count]

Figures 121 and 122 display the distribution of financial losses by type of protocol, revealing how the economic impact of attacks correlates with their frequency across different DeFi categories.

Centralized Exchange (CEX) protocols, while being the most frequently attacked category with 20.2% of occurrences, also lead in terms of financial losses. They account for a substantial 29.4% of the total losses, amounting to $3,152,494,888 USD. This indicates that attacks on CEXs not only occur more frequently but also tend to result in more significant financial damage.

Bridges stand out notably in terms of financial impact relative to their occurrence. While they rank fourth in terms of attack frequency at 10.1%, they suffer from disproportionately high losses, representing 26.4% of the total, which translates to $2,825,066,000 USD. This suggests that while bridges are less frequently targeted compared to other protocols, the individual attacks often result in substantial financial losses.

In contrast, lending protocols, which are the second most frequent targets with significant occurrences (15.2%), rank third in financial losses, accounting for 10.3% of the total stolen funds or $953,000,000 USD. Despite their high attack frequency, the relative financial impact is slightly lower, indicating that attacks on lending protocols, while common, might involve lower individual sums compared to CEXs or bridges.

Ponzi schemes, despite their low occurrence rate at only 2% of attacks, cause a significant portion of financial losses, accumulating 7.7% of the total or $822,000,000 USD. This highlights the severe financial impact Ponzi schemes can have when they do occur.

Decentralized Exchanges (DEXes), the third most attacked category at 11.1%, contribute to only 5% of the total financial losses, totaling $530,823,000 USD. This lower relative financial impact suggests that while DEXes are frequently targeted, the individual attacks may involve smaller amounts of lost funds compared to other more heavily impacted protocols.

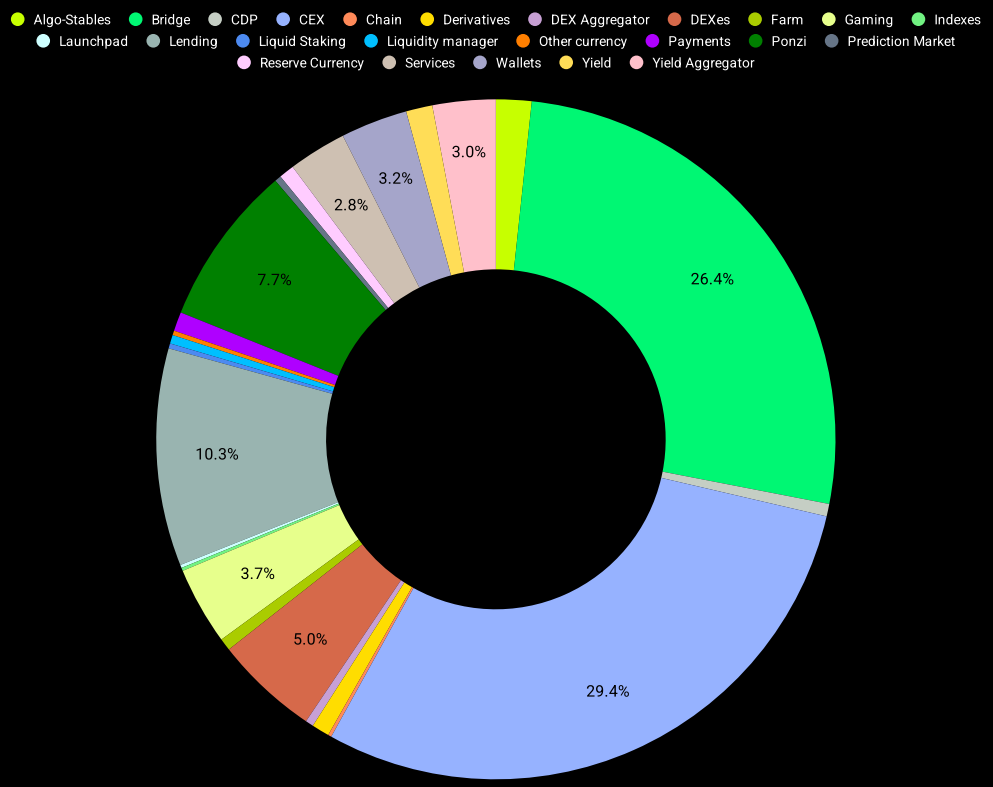

Figure 121: Loss caused by type of protocol [percentage]

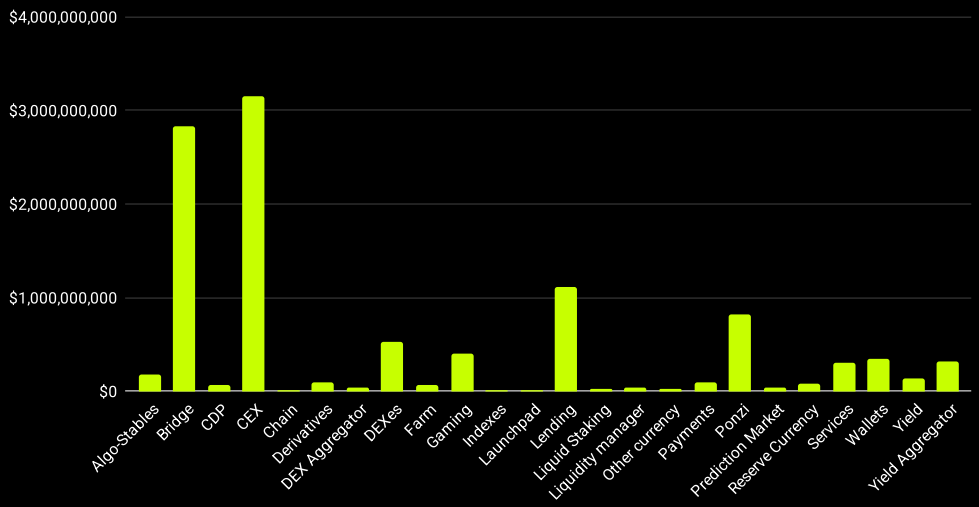

Figure 122: Loss caused by type of protocol [USD]

Figure 123 provides a revealing comparison between the prevalence of various types of DeFi protocols in the overall market and their susceptibility to attacks based on data sourced from DefiLlama.

DEXes, despite being the most numerous type of protocol, accounting for 32.86% of the total, surprisingly constitute only 11.11% of the attacks. This indicates a lower relative rate of attack compared to their prevalence, suggesting that DEXes might be better protected or less targeted than other protocol types.

Similarly, Yield protocols, which make up 11.59% of the total protocols, are also underrepresented in attack statistics, facing only 5.05% of the attacks. This could indicate effective security measures or inherent features that deter exploitation.

On the other hand, Bridges, CEXs, and Wallets, which are less common in the DeFi ecosystem, representing only 2.21%, 1.24%, and 0.11% of the total protocols respectively, show a disproportionate number of attacks: 10.10%, 20.20%, and 5.05% respectively. This disproportionate representation suggests that these protocols are either more vulnerable to attacks or offer more lucrative targets for hackers due to potentially higher value transactions or lower security protocols.

Lending protocols, Gaming, and Yield Aggregators also demonstrate a certain level of vulnerability. Lending protocols, for instance, comprise 10.20% of the total but account for 15.15% of attacks. Similarly, Gaming and Yield Aggregators, which make up 1.40% and 3.52% of the total, are involved in 3.03% and 6.06% of attacks, respectively. This again suggests a higher-than-average risk of attack relative to their presence in the market.

This analysis underscores the need for heightened security measures that are tailored to the specific characteristics and vulnerabilities of each protocol type, especially those that, despite their lower numbers, face a higher risk of attack.

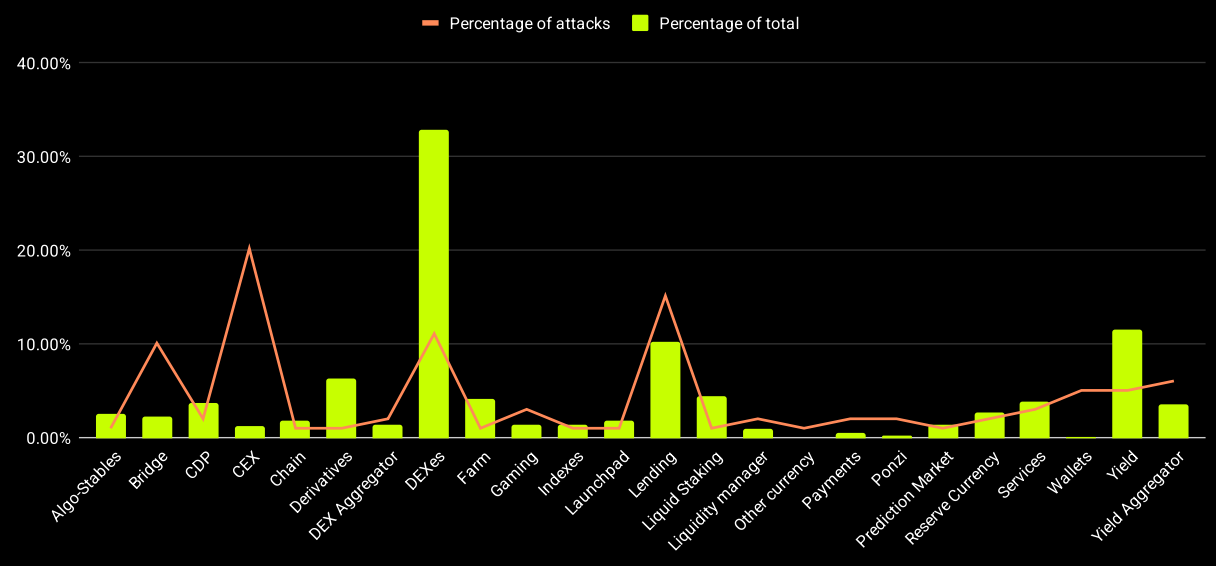

Figure 123: Percentage of type of protocol attacked versus percentage of type of protocol in sample

Over the years, the types of DeFi protocols targeted by hackers have varied, as detailed in Figures 124 and 125.

In 2014, the focus was primarily on a Centralized Exchange (CEX), a trend that continued into 2016, although that year also saw attacks on Service protocols in an equal percentage. By 2017, the targeted protocols shifted entirely to Wallets, indicating a change in hacker focus on individual asset storage.

In 2018, most breaches (66.7%) targeted CEXs again, suggesting a return to attacking major liquidity hubs. The following year, 2019, saw an equal distribution of attacks between CEXs and Ponzi schemes.

The year 2020 marked a significant diversification in the types of protocols attacked, with Yield Aggregators being the most targeted at 40%. This shift could reflect the growing popularity and vulnerability of these protocols during the DeFi boom.

From 2021 onwards, the diversity of attacked protocols increased further. In 2021, Lending protocols were the most attacked, making up 21.4% of the total, followed by DEXes and Yield protocols, each with 14.3%. This suggests that as the DeFi space matured, the array of lucrative targets for hackers expanded.

In 2022, Bridges became the primary target, accounting for 30% of the total attacks, likely due to their critical role in enabling cross-chain transactions and their complex security challenges. CEXs followed with 15% of the attacks.

By 2023, the attacks were evenly spread among DEXes, CEXs, and Bridges, each with 17.6% of total incidents, followed by payment and Lending protocols at 11.8%. This even distribution underscores the ongoing broad appeal of various protocol types to attackers.

In the most recent year, 2024, CEXs were once again the most frequently attacked protocols, making up 29.4% of the total, closely followed by Lending protocols at 23.5%. This reflects the continuous high value and vulnerability associated with these platforms.

Overall, CEXs have consistently been a target every year except for 2017, highlighting their continuous appeal to attackers due to their significant transaction volumes and central role in the crypto ecosystem.

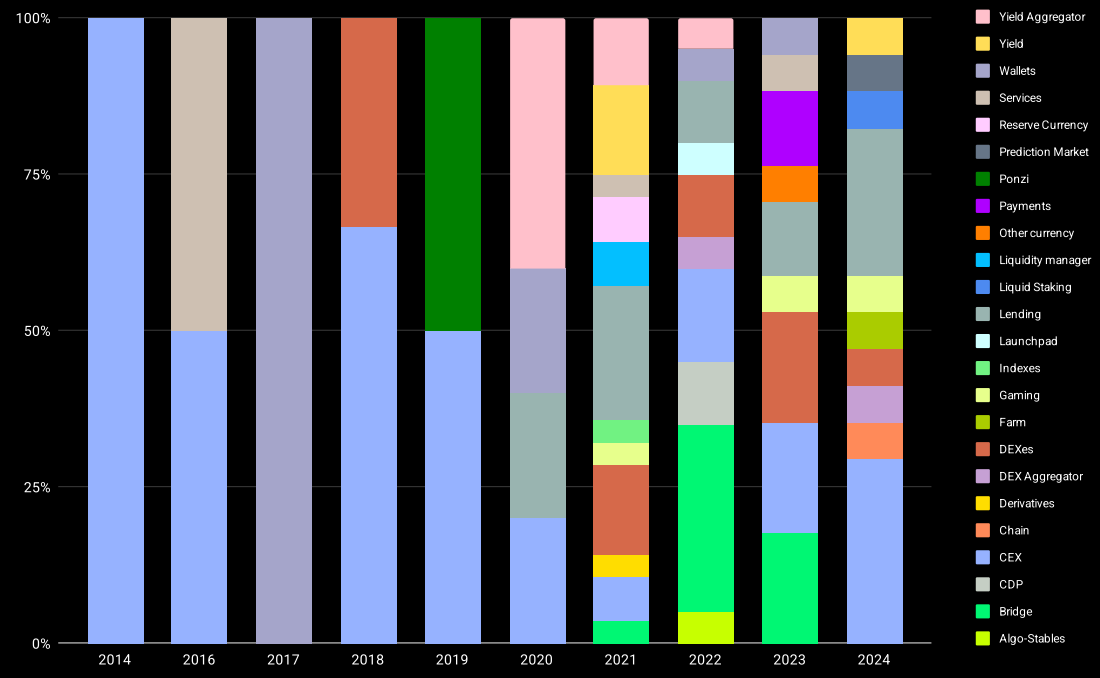

Figure 124: Number of types of protocol per year [percentage]

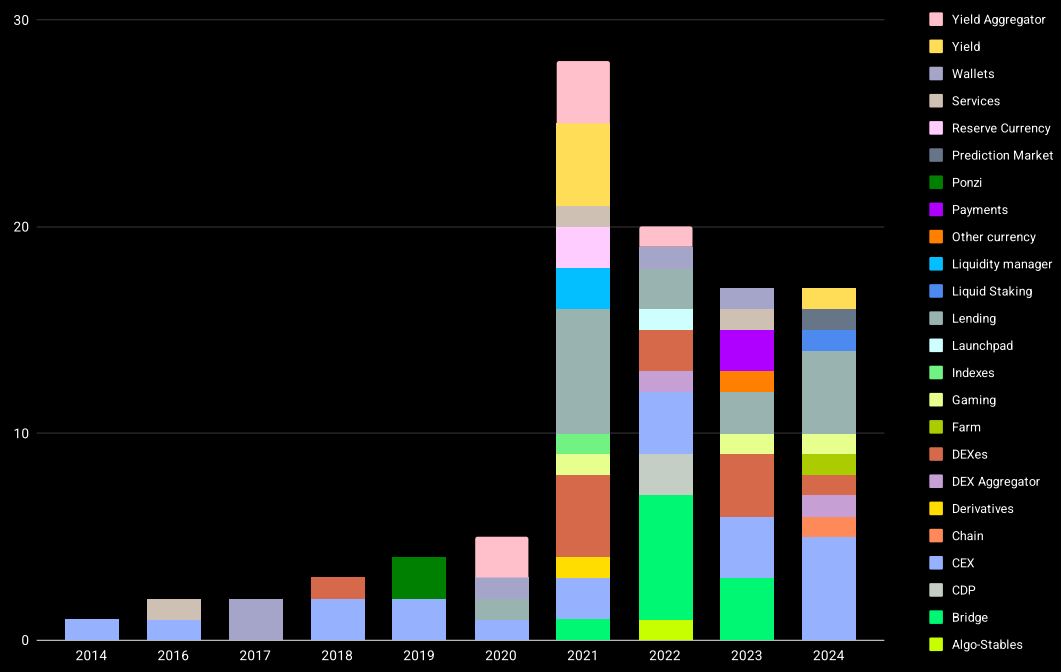

Figure 125: Number of types of protocol per year [count]

Figures 126 and 127 provide a detailed breakdown of financial losses by type of protocol and year, showing how certain protocols have led to disproportionately high losses compared to their rate of occurrence.

In 2016, CEXs recorded losses slightly above their occurrence rate, accounting for 50.7% of the total financial losses ($72,000,000 USD) against an occurrence rate of 50%.

By 2018, CEXs caused a disproportionately high percentage of losses—96.2% ($597,000,000 USD) of the total—compared to their occurrence rate of 66.7%. This indicates a significant vulnerability or targeted attacks that resulted in substantial financial impact.

2019 saw a similar trend with Ponzi schemes, which accumulated 90.6% of the losses ($822,000,000 USD) against a 50% occurrence rate. This highlights the severe financial damage that such schemes can inflict when they occur.

In 2020, CEXs were again responsible for major losses, totaling 75% ($275,000,000 USD) of the financial damages, despite only a 20% occurrence rate. This underscores the ongoing risk associated with CEX platforms.

2021 and 2022 featured Bridges as a major source of financial losses. In 2021, Bridges were responsible for 28.1% of the losses ($611,000,000 USD) against an occurrence rate of just 3.6%. In 2022, this figure soared to 59.7% of the losses ($1,906,000,000 USD) against a 30% occurrence rate. These years highlight the significant financial risks associated with vulnerabilities in bridge protocols.

In 2023, despite attacks being evenly spread among DEXes, CEXs, and Bridges, Lending protocols led to the largest share of financial losses, accounting for 22.1% ($317,000,000 USD) while only representing 11.8% of the attack occurrences. This suggests an increasing financial vulnerability within Lending protocols.

2024 marked a resurgence in losses caused by CEXs, which led to 53.9% of the total financial losses ($661,094,888 USD) against a 29.4% occurrence rate. Additionally, Gaming protocols also caused significant losses, representing 17.6% of the total ($216,000,000 USD) against a mere 5.9% occurrence rate. This points to emerging vulnerabilities or lucrative targets within the gaming sector.

Overall, the data clearly indicates that CEXs, Bridges, and Ponzi schemes are particularly destructive in terms of financial losses, often causing far greater financial damage than their relative frequency of occurrence might suggest.

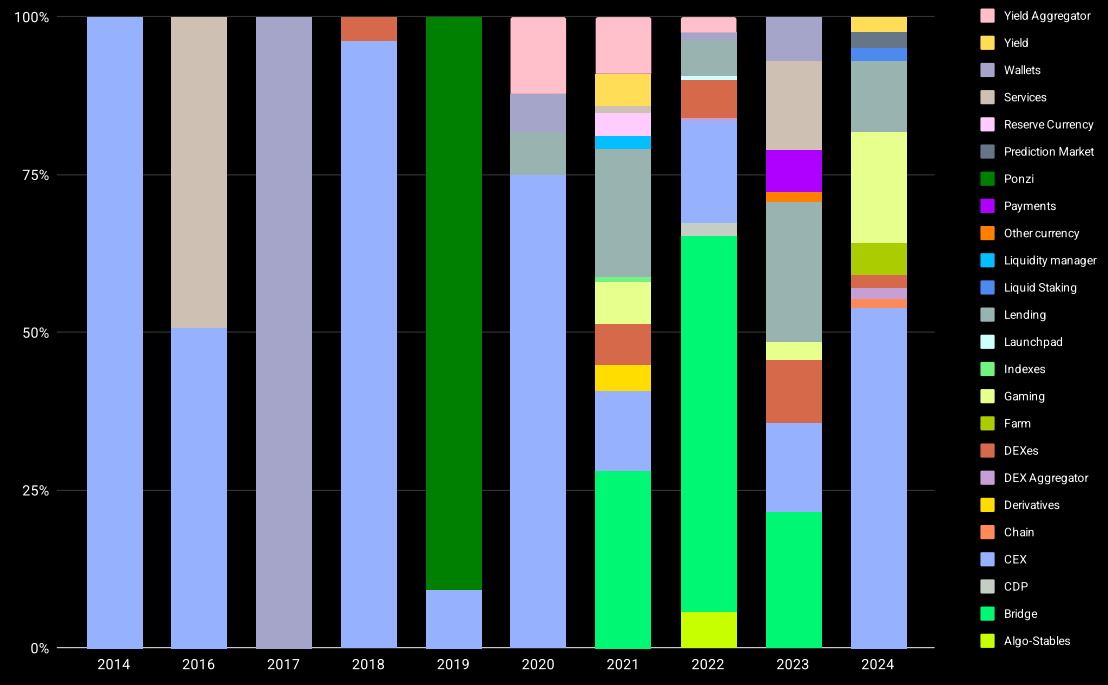

Figure 126: Loss caused by type of protocol per year [percentage]

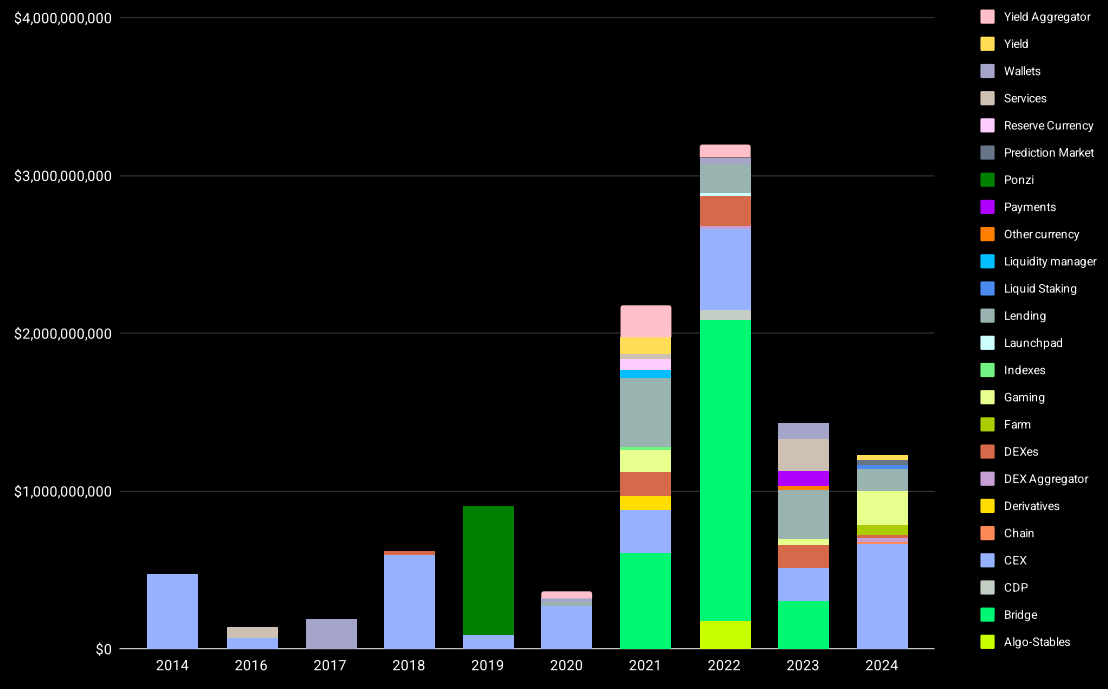

Figure 127: Loss caused by type of protocol per year [USD]

Governance

Figures 128 and 129 provide an insightful comparison of the frequency of attacks on centralized versus decentralized organizations within the DeFi ecosystem based on the governance model of each protocol.

The data reveals that centralized organizations have experienced a significantly higher number of attacks, accounting for 61.6% of the total incidents. This is nearly double the rate of attacks on decentralized ones, which stand at 38.4%.

This trend might suggest that centralized organizations, despite potentially having more robust financial and technical resources, are more attractive targets for attackers due to factors such as:

- **Central points of failure:** Centralized systems often have single points of failure, making them more susceptible to targeted attacks that can compromise the entire system.
- **Higher value targets:** Centralized entities typically handle larger volumes of transactions and store more significant amounts of assets, making them more lucrative targets.

On the other hand, decentralized organizations, while generally thought to be more resilient to certain types of attacks due to their distributed nature, still represent a substantial portion of the total attacks. This indicates that decentralization alone does not inherently confer immunity to security threats. Vulnerabilities in smart contracts, governance mechanisms, or user interfaces can still be exploited.

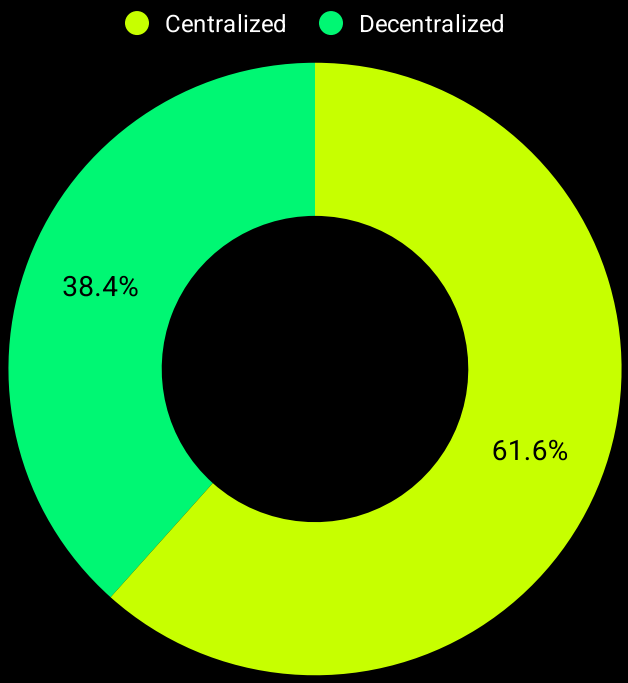

Figure 128: Usage of type of governance [percentage]

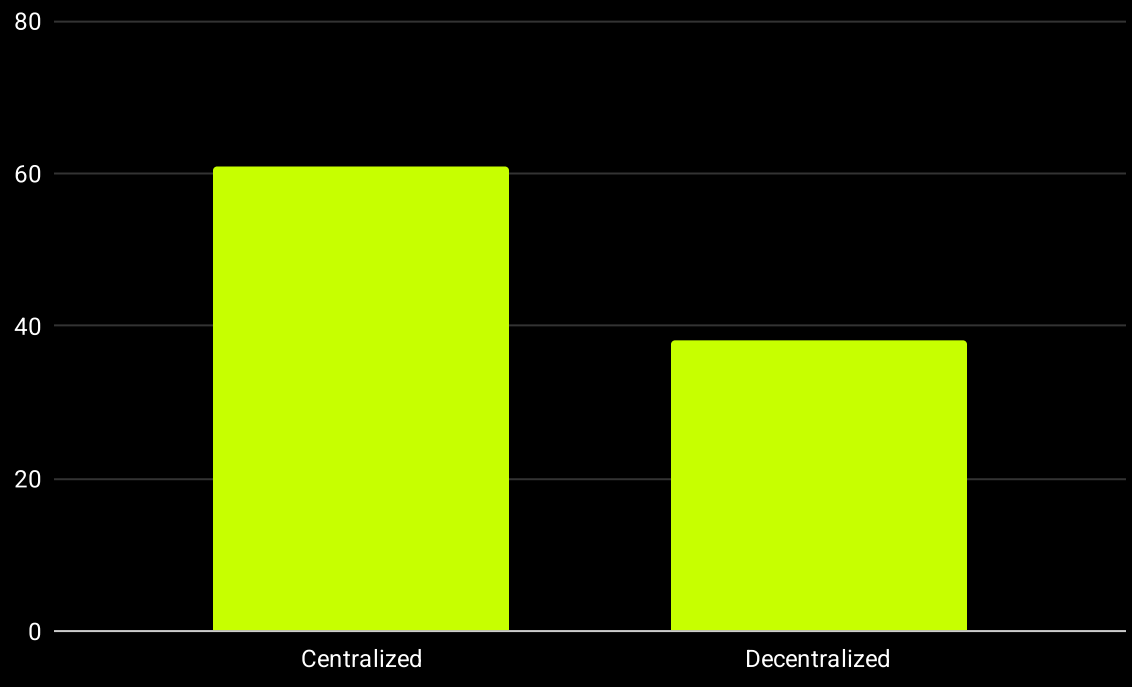

Figure 129: Usage of type of governance [count]

Figures 130 and 131 delve deeper into the financial impact of attacks on centralized versus decentralized organizations by examining the distribution of losses associated with each governance type.

The analysis indicates that while decentralized protocols account for 38.4% of the attack occurrences, they represent only 22.2% of the total financial losses, amounting to $2,384,486,071 USD. This discrepancy suggests that although decentralized protocols are frequently targeted, the financial damage from each incident tends to be lower compared to centralized ones.

On the other hand, centralized organizations, despite their higher frequency of attacks at 61.6%, account for a disproportionately large share of the financial losses—77.8% or $8,333,174,839 USD. This substantial figure highlights that attacks on centralized protocols not only occur more frequently but also tend to result in significantly larger financial losses. This seems to make them high-value targets for financially motivated attackers.

The data suggests that while decentralization may not completely deter attacks, it potentially mitigates the severity of financial losses when incidents occur.

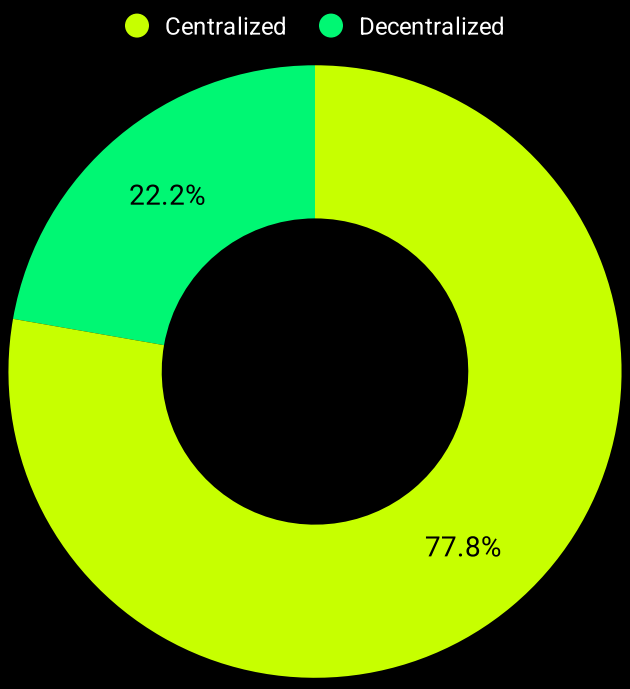

Figure 130: Loss per type of governance [percentage]

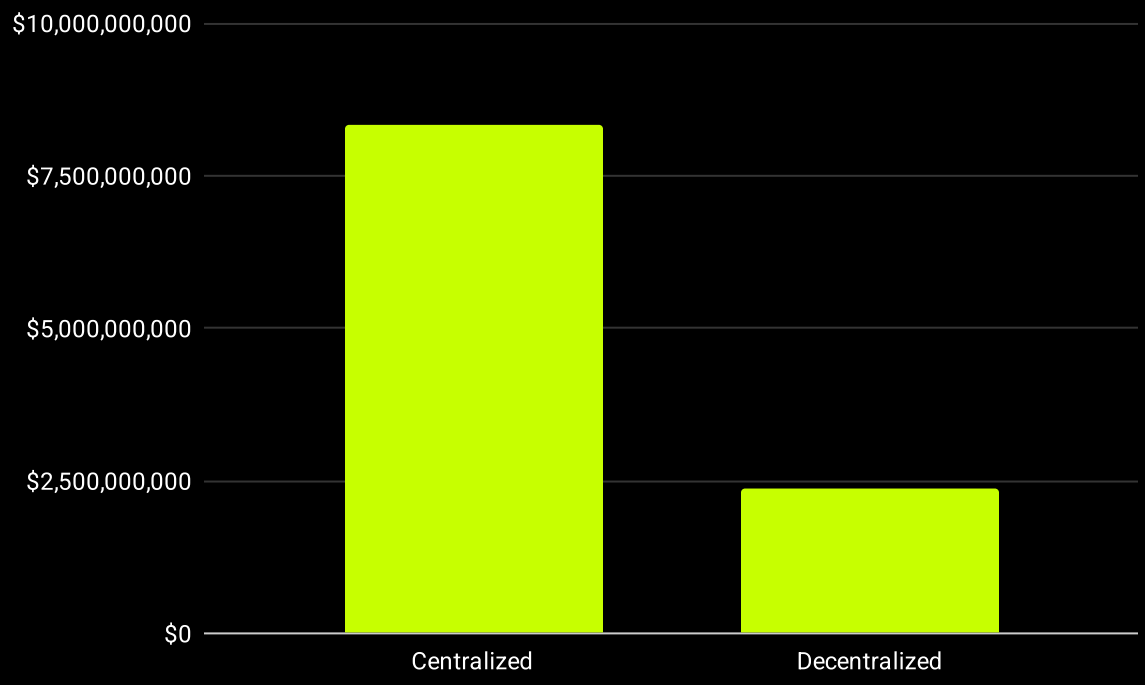

Figure 131: Loss per type of governance [USD]

Figures 132 and 133 provide a year-by-year breakdown of attacks on centralized and decentralized protocols.

The data illustrates that centralized protocols have generally been more frequently attacked across most years. The exceptions are 2016, when attacks on centralized and decentralized protocols occurred at equal rates, and notably in 2021, when decentralized protocols experienced a higher rate of attacks, accounting for 53.6% of incidents. This spike could be indicative of evolving attack vectors or an increase in the adoption and visibility of decentralized platforms during this period.

Post-2021, the trend shows a temporary decline in the proportion of attacks on decentralized protocols in 2022, which dropped to 30%. However, this trend reversed in the following years, with attacks on decentralized protocols increasing to 35.3% in 2023 and further to 41.2% in 2024. This resurgence might reflect changes in attacker focus, perhaps due to shifts in security practices, the growing value locked in decentralized protocols, or their increasing complexity and integration within the broader digital ecosystem.

This fluctuating pattern suggests that both types of protocols face significant threats, albeit with variations over time that may be influenced by technological developments, market dynamics, and the changing tactics of attackers.

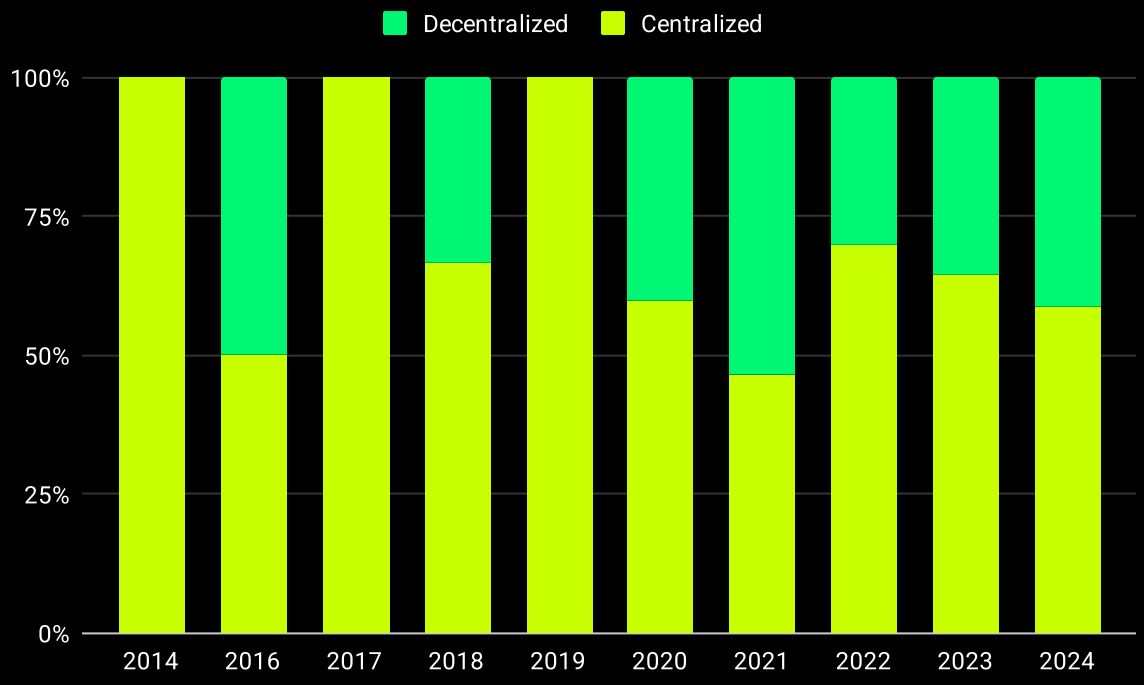

Figure 132: Usage of type of governance per year [percentage]

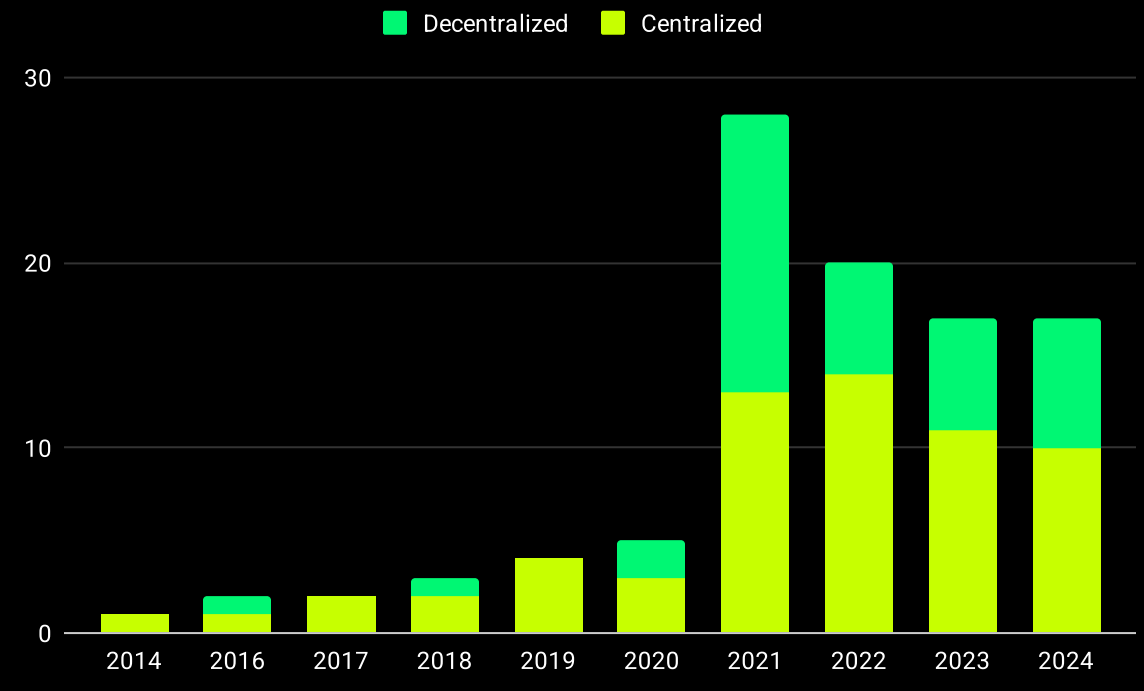

Figure 133: Usage of type of governance per year [count]

Figures 134 and 135 illustrate the distribution of financial losses by year and type of governance within DeFi protocols.

The data consistently shows that losses attributed to centralized protocols are typically greater than those from decentralized ones. Even in 2016, when the attack rates on centralized and decentralized protocols were equal at 50%, the losses from centralized protocols slightly surpassed their occurrence rate, accounting for 50.7% of total losses.

The trend of centralized protocols incurring more losses than their attack rates would suggest continues across multiple years. In 2018, while centralized protocols were involved in 66.75% of the attacks, they were responsible for a staggering 96.2% of the financial losses ($597,000,000 USD). Furthermore, in 2020, centralized protocols constituted 60% of the attacks but accounted for 86.4% ($316,700,000 USD) of the losses. In 2021, they represented 46.4% of the attacks but accounted for 66.4% ($1,442,700,000 USD) of the total financial damage. Additionally, in 2022, although they were 70% of the attacks, they were responsible for 84.9% ($2,711,300,000 USD) of the losses. Finally, in 2024, centralized protocols were involved in 58.8% of the attacks, yet they resulted in 68.6% ($841,694,888 USD) of the losses.

The exception to this trend is observed in 2023, where decentralized protocols not only had a substantial share of attacks at 35.3% but also surpassed this figure in terms of financial impact, accounting for 44.9% ($642,789,000 USD) of the losses. This anomaly could suggest a shift in attack targets or an increase in the severity of attacks on decentralized platforms during that year.

Overall, these figures underscore the significant financial risks associated with centralized protocols within the DeFi space. They consistently consist in a disproportionate share of the financial damage relative to their occurrence rates, indicating that while centralized platforms may offer operational efficiencies and control, they also concentrate risk, making them prime targets for financially motivated attacks.

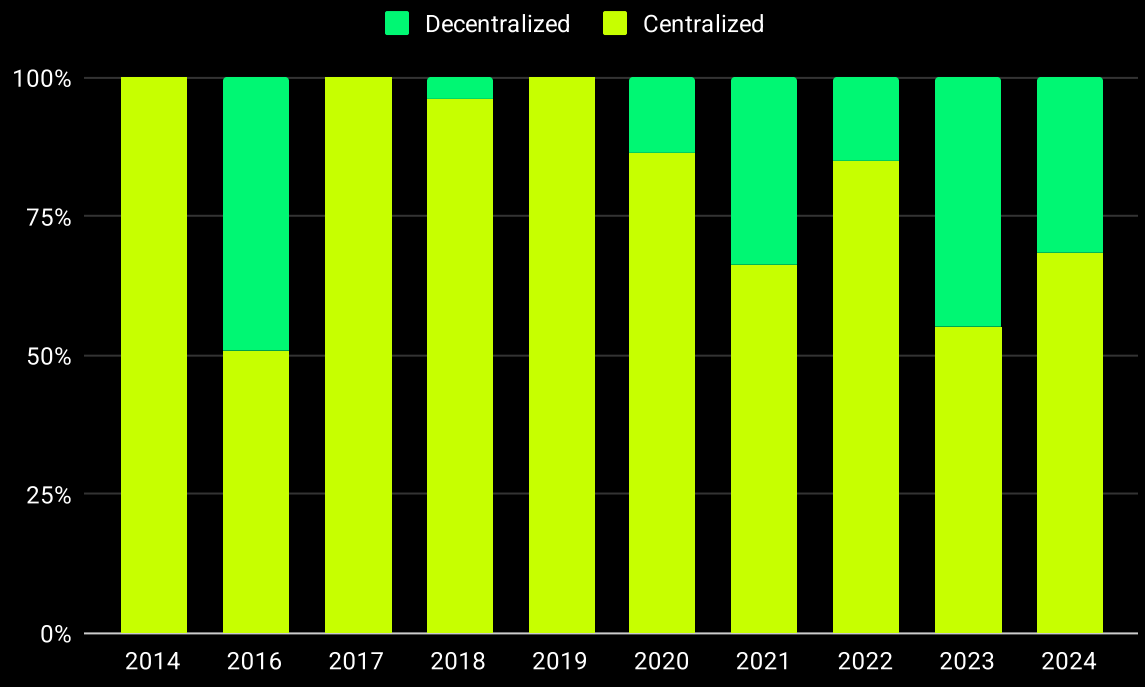

Figure 134: Loss per type of governance per year [percentage]

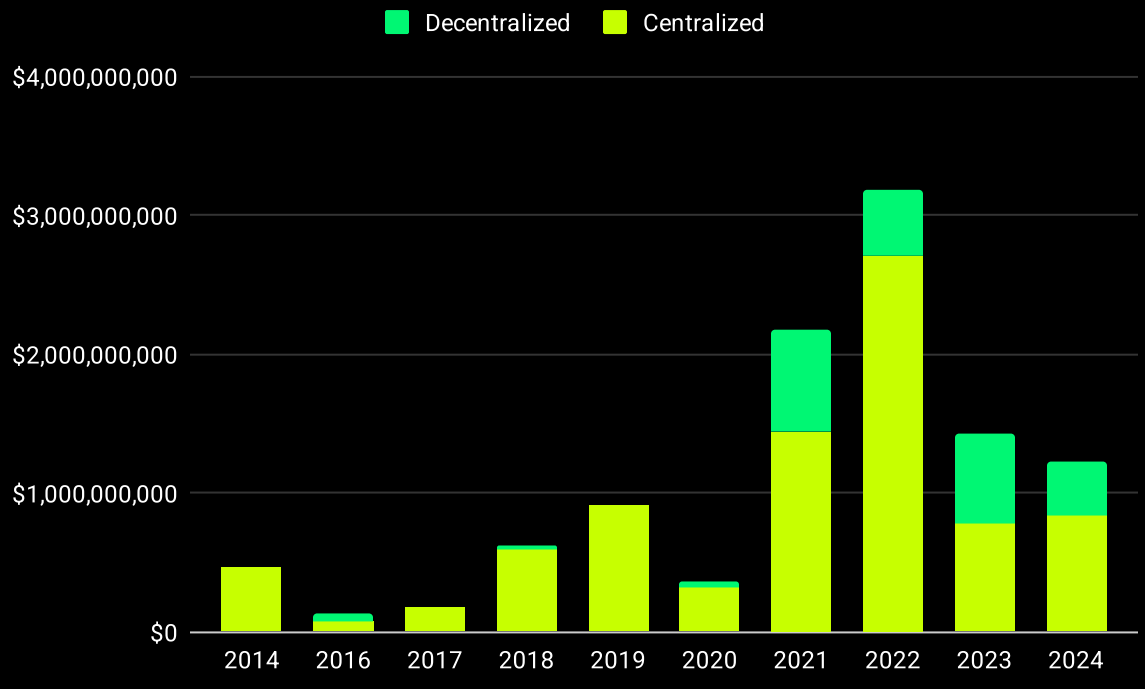

Figure 135: Loss per type of governance per year [USD]

Type of Protocols per Chains

Figures 136 and 137 provide a detailed overview of the types of DeFi protocols that have been most frequently attacked across various blockchain networks.

In Aptos, the primary target has been Liquid Staking protocols. Arbitrum has seen a significant focus on Lending protocols, constituting 33.3% of the attacks. Avalanche and Bitcoin have primarily experienced attacks on Centralized Exchanges (CEXs), with these types of protocols accounting for 40% and 66.7% of attacks, respectively.

Base shows a diverse attack landscape, with attacks evenly distributed between CEXs, DEXes (Decentralized Exchanges), and Other Currency categories. Similarly, Bitcoin Cash has been targeted at its CEX protocol. Blast features a split focus with equal attacks on CEXs and Farms.

In the Boba Network, it was a chain protocol that was compromised. BSC (Binance Smart Chain) sees an even spread of attacks among its three most attacked protocols: Bridges, DEXes, and CEXs, each with 16.7% of attacks. For Dogechain, Bridges have been the main vulnerability point, whereas Ethereum has shown a slightly more varied distribution with CEXs leading at 20.4%, followed by lending protocols and DEXes at 13% each.

Fantom's attacks are evenly split between Yield protocols and Bridges. In chains like Linea, MonaCoin, and NEM, CEXs have been the targets. Mixin presents a balanced attack rate between Lending protocols and Services, and Moonriver has seen Bridges as the focal point of attacks.

For attacks involving multiple chains, labeled as "Multi," CEXs and Wallets have been equally targeted, each representing 40% of the attacks. Optimism and Polygon share a similar distribution pattern, with CEXs and DEXes and CEXs and Lending protocols sharing the top, making up 40% and 27.3% of attacks, respectively. Skale had a chain protocol attacked.

Solana shows a diverse distribution with equal attacks across Bridges, CDP (Collateralized Debt Positions), DEX Aggregators, and Lending protocols. In Terra, the focus has been on a Derivatives protocol, and finally, in Tron, a significant 66.7% of the attacks have targeted CEXs.

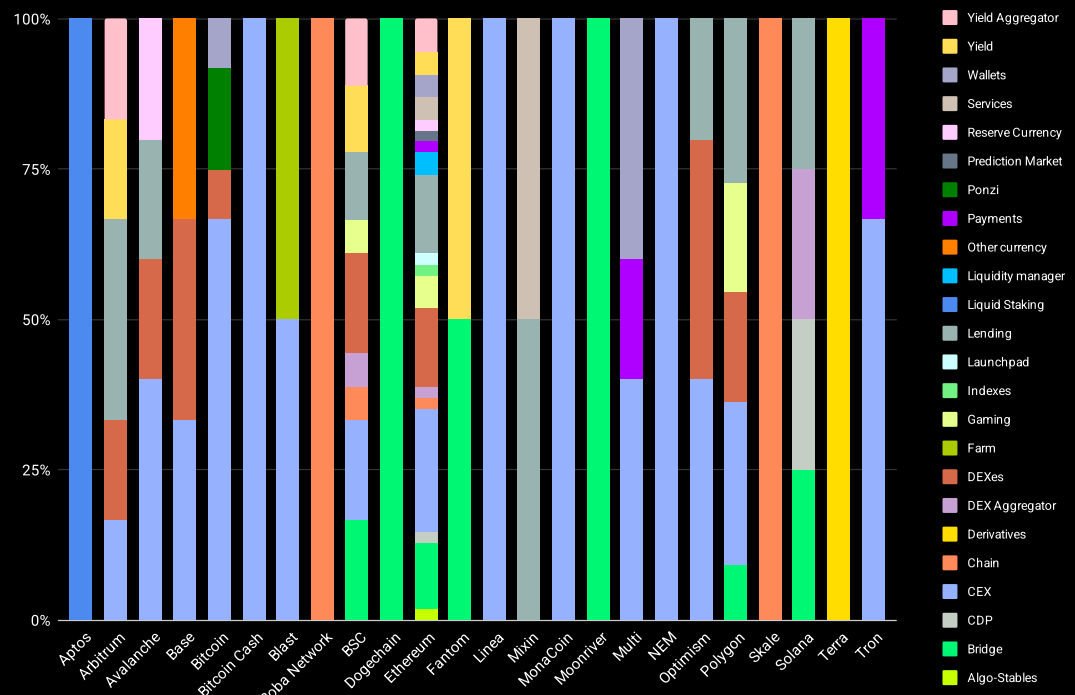

Figure 136: Number of type of protocols per chain [percentage]

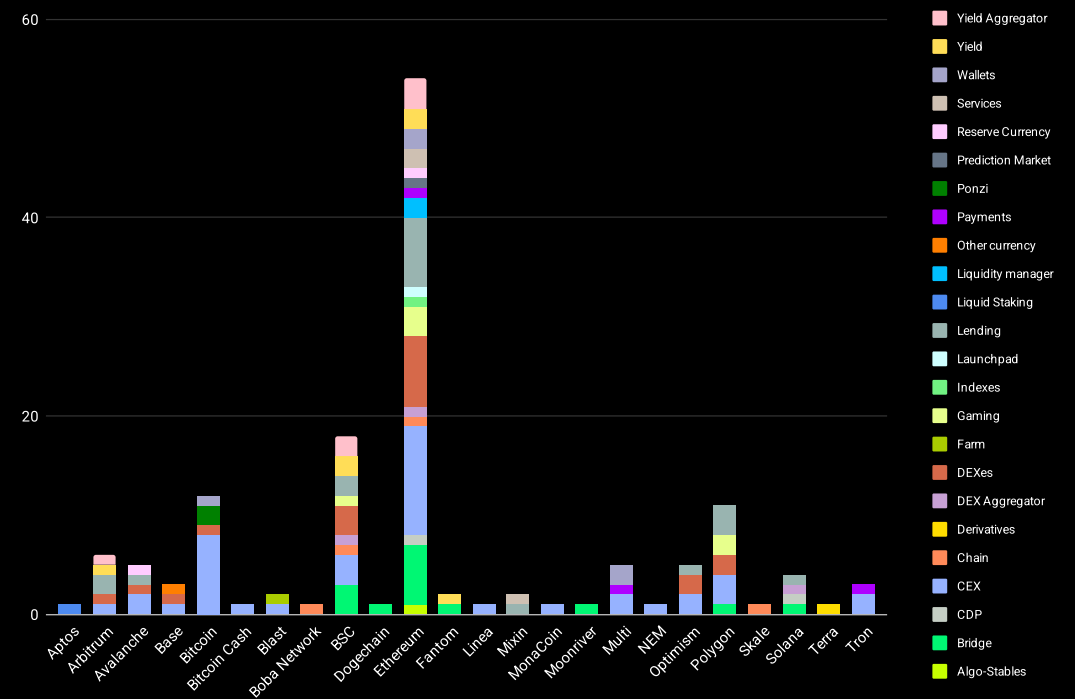

Figure 137: Number of type of protocols per chain [count]

Figures 138 and 139 examine the distribution of financial losses by type of protocol.

Arbitrum shows that while Lending protocols are frequently attacked, accounting for 33.3% of incidents, they are not the top by loss, despite their significant share of 41.6% ($76,200,000 USD). Yield Aggregators in Arbitrum lead in terms of financial impact, with 43.6% ($80,000,000 USD) of the losses.

Avalanche and Bitcoin both see CEXs as not only the most attacked but also the most financially impacted protocols, with losses amounting to 51% ($54,291,966 USD) and 53.1% ($978,400,000 USD), respectively. In Avalanche, Lending protocols, and in Bitcoin, Ponzi schemes also report higher losses relative to their frequency, accumulating 32% ($34,000,000 USD) and 44.6% ($822,000,000 USD) against an occurrence rate of 20% and 16.7%, respectively.

Base has a diverse attack profile, but Other Currency categories lead the losses significantly, accounting for 90.3% ($23,000,000 USD) of the financial damages.

Blast sees an equal number of attacks on CEXs and Farms, but Farms dominate the financial impact, accounting for nearly all the losses at $62,500,000 USD.

In the Binance Smart Chain (BSC), despite Bridges, DEXes and CEXes having an equal number of attacks, Bridges lead in financial losses, accounting for a substantial 68.3% ($919,000,000 USD) of the financial impact.

Ethereum presents a similar trend where Bridges are responsible for a disproportionate share of losses at 30.3% ($1,367,600,000 USD), far exceeding their occurrence rate of 11.1%. This is followed by CEXs, which also incur substantial losses slightly above their attack rate, 22.9% (($ 1,032,962,985 USD) against an attack rate of 20.4%.

Fantom shows an equal attack rate between Yield protocols and Bridges, but Bridges dominate the losses, reflecting 80% ($120,000,000 USD).

Mixin has a balanced attack rate between Lending and Services, but Services account for a major portion of losses, 74.1% ($200,000,000 USD).

For multi-chain attacks labeled as "Multi," while CEXs and Wallets are equally targeted, CEXs bear a greater brunt of the losses, 65.4% ($329,300,000 USD), while only representing 40% of the attacks.

DEXes in Optimism and Lending protocols in Polygon lead to most financial losses, with 62.2% ($45,500,000 USD) and 58.3% ($206,500,000 USD), respectively, against an occurrence rate of 40% and 27.3%.

Solana displays a diversity of attacks across Bridges, CDP, DEX Aggregators, and Lending protocols, yet Bridges are responsible for most of the financial losses, 63.9% ($326,000,000 USD).

In Tron, while CEXs are heavily targeted, Payments protocols cause the highest losses, 49.1% ($49,428,000 USD) against a lower occurrence rate of 33.3%.

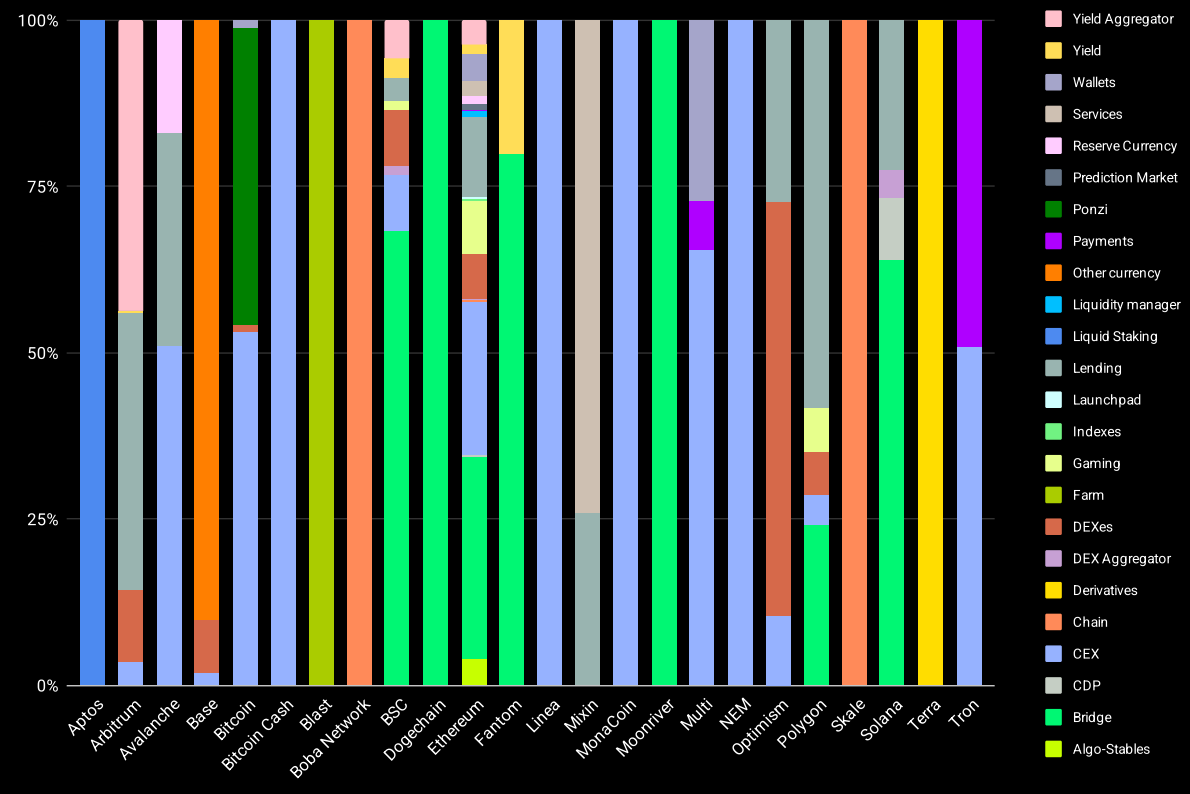

Figure 138: Loss per type of protocols per chain [percentage]

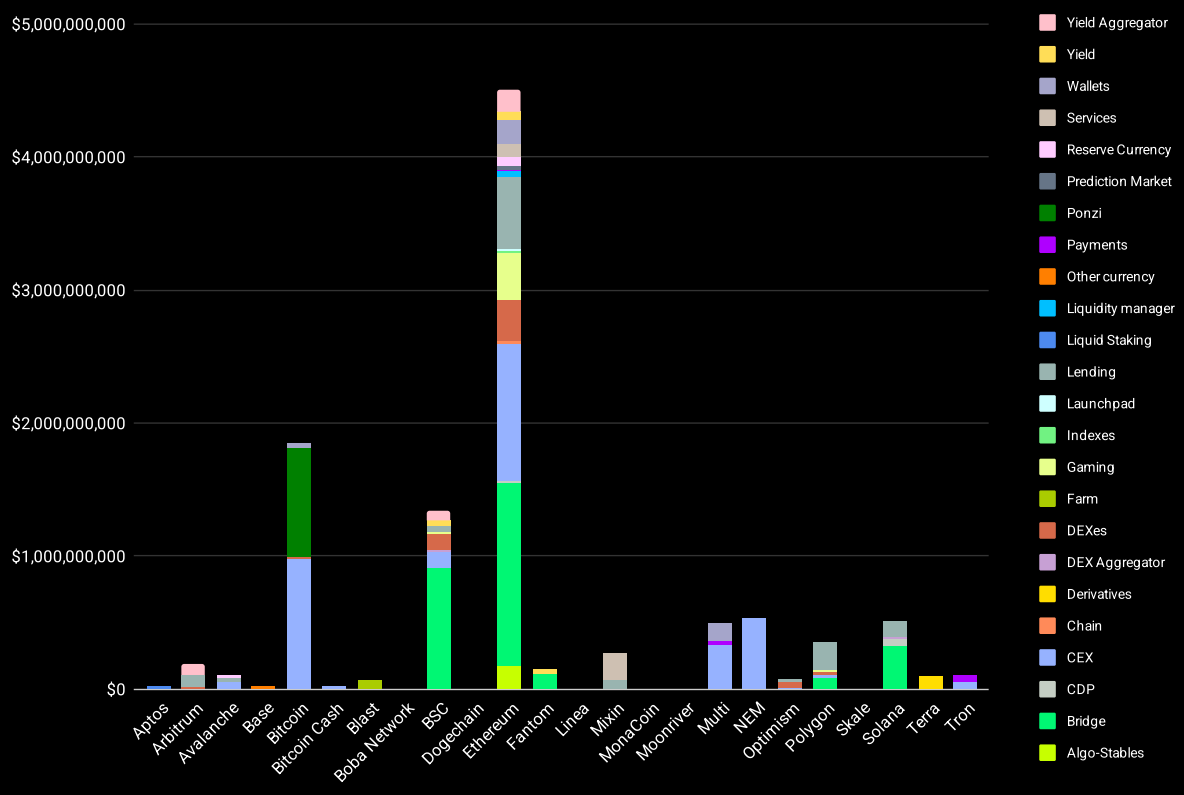

Figure 139: Loss per type of protocols per chain [USD]

Figures 140 and 141 detail the distribution of attacks by type of protocol across different chains and years.

Arbitrum showcases varying targeted protocols each year, with lending protocols dominating in 2024, representing 50% of the attacks. Similarly, Avalanche and Base display fluctuating preferences among attackers, with a notable focus on CEXs in 2024 for Avalanche.

Bitcoin has consistently seen CEXs as a primary target over the years, except in 2019 when Ponzi schemes prevailed, constituting 66.7% of the attacks. In 2020, the focus shifted to a wallet, and by 2024, attacks were evenly split between CEXs and DEXes.

BSC has experienced a variety of attacked protocols through the years. Notably, CEXs were targeted in 2021 and 2024 (18.2% and 33.3%, respectively), Lending protocols appeared in 2021 and 2024 (9.1% and 33.3%, respectively), and Bridges were highlighted in 2021 and 2022 (9.1% and 66.7%, respectively). In the latest year, attacks on BSC were evenly distributed across CEXs, Chain, and Lending.

Ethereum's attack landscape has diversified over time. In the early years, Ethereum attacks focused on a single protocol type each time; for instance, 2018 saw all recorded attacks (100%) directed at DEXes, while in 2019, every attack (100%) targeted CEXs. By 2020, Ethereum's landscape had begun to expand, with Yield Aggregators representing 66.7% of the attacks and Lending protocols making up the remaining 33.3%. In 2021, the ecosystem grew even more varied, as CEXs accounted for 13.3% of attacks, DEXes for 6.7%, Lending for 20%, and other protocols filling out the rest. The following year saw CEXs rise to 27.3% of attacks. By 2023, the distribution included 20% of attacks on CEXs, 30% on DEXes, and 10% on Lending. Most recently, in 2024, CEXs claimed 30% of the attacks, with Lending protocols at 20% and DEXes at 10%. We can observe, therefore, the persistent presence of CEXs, DEXes and Lending protocols for this chain.

Fantom and Mixin each displayed yearly shifts in the types of protocols attacked, with Fantom alternating between Yield and Bridge and Mixin between Lending and Services.

For multi-chain attacks labeled as "Multi," there's been a consistent focus on CEXs and Wallets, with CEXs being the sole target in 2020, and both sharing prominence with payments in subsequent years.

Optimism saw an initial preference for DEX attacks in earlier years, shifting to predominantly CEX attacks in 2024, where they constituted 66.7% of the incidents.

Polygon has varied its focus, with Lending protocols consistently prominent in 2021 and 2023 (33.33% each year) and a significant shift towards CEXs by 2024, which were targeted in 100% of the attacks.

Solana transitioned from a balanced attack distribution across Bridges, CDP, and Lending in 2022 to a focus on DEX Aggregators in 2024.

In Tron, CEXs have been a continual focus, culminating in equal prominence with payments in 2023 (50% each) and being the sole focus in 2024.

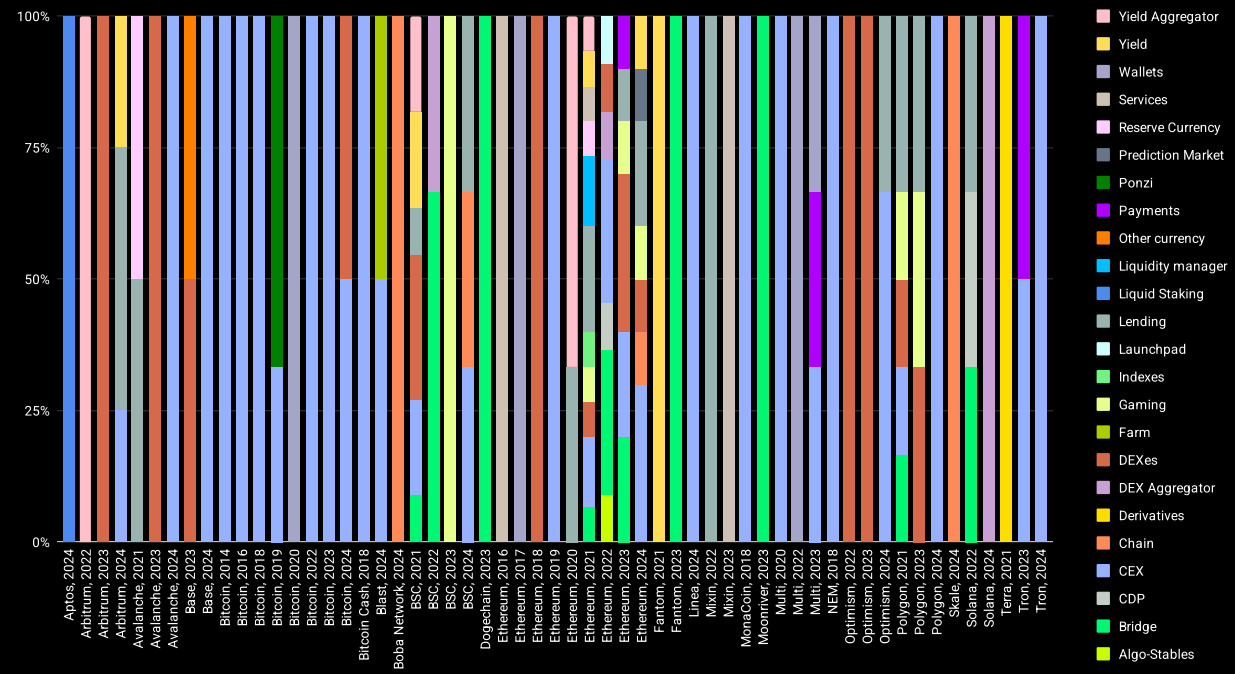

Figure 140: Number of type of protocols per chain and year [percentage]

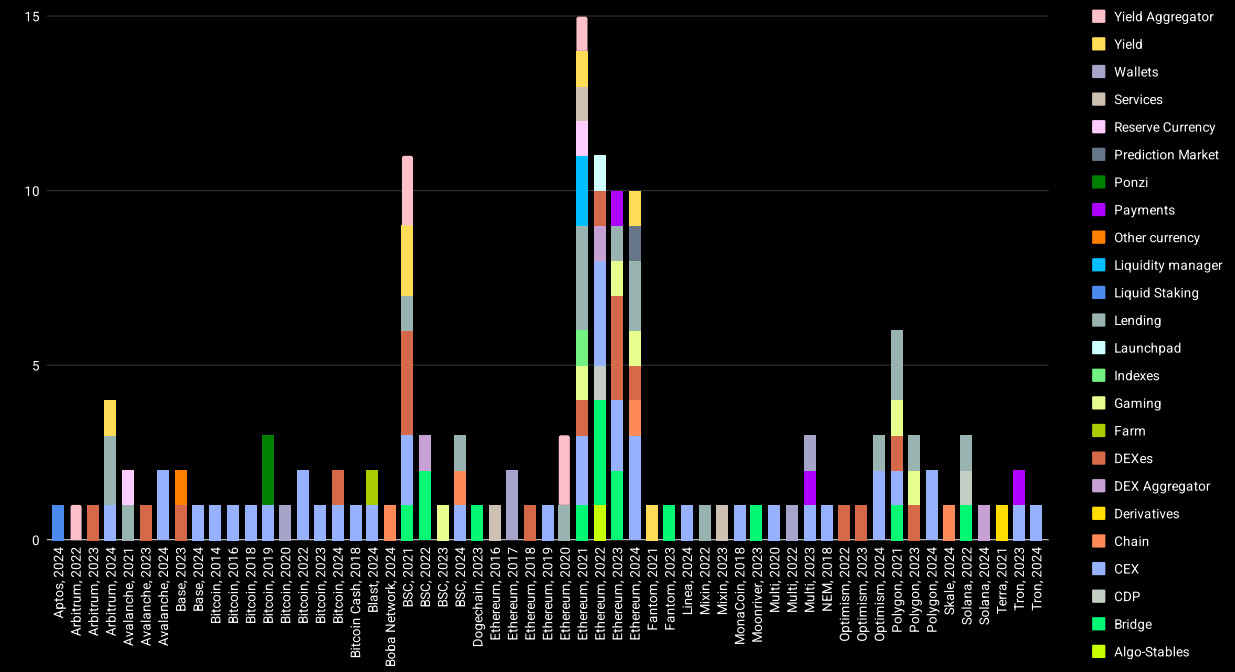

Figure 141: Number of type of protocols per chain and year [count]

Figures 142 and 143 illustrate the distribution of financial losses by year and chain,

In Arbitrum during 2024, lending protocols were attacked in 50% of the incidents but accounted for 91.5% of the financial losses, totaling $76,200,000 USD. A similar pattern is observed in Avalanche for 2021, where lending protocols also had a 50% occurrence rate but led to 65.3% of the losses, amounting to $34,000,000 USD.

In Base for 2023, the Other currency category showed a higher loss percentage of 92% ($23,000,000 USD) compared to its 50% occurrence rate. Bitcoin in 2019 saw Ponzi schemes causing 95.4% of the losses ($822,000,000 USD) against a 66.7% occurrence rate, and in 2024, CEXs were responsible for 93.5% of the losses ($304,000,000 USD) with only a 50% occurrence rate.

In BSC, bridges consistently led to substantial losses: in 2021, they accounted for 41% ($253,000,000 USD) of losses against a 9.1% attack rate, and in 2022, they were responsible for 97.7% of the losses ($666,000,000 USD) against a 66.7% occurrence rate.

Ethereum also displayed a trend where bridge attacks led to disproportionate losses: 23.3% ($273,000,000 USD) in 2021 against a 6.7% occurrence rate, 51.6% ($914,000,000 USD) in 2022 against a 27.3% rate, and 30.7% ($180,600,000 USD) in 2023 against a 20% rate. Recent years have seen substantial losses in other protocols as well: lending led to 33.4% ($197,000,000 USD) of the losses in 2023 against a 10% occurrence rate, while in 2024, CEXs and gaming caused 45.5% ($266,562,985 USD) and 36.9% ($216,000,000 USD) of the losses, respectively, against occurrence rates of 30% and 10%.

For multi-chain attacks labeled as "Multi," wallets in 2023 led to a significant portion of the losses, 52.2% ($100,000,000 USD), against a 33.3% occurrence rate.

In Optimism for 2024, lending protocols accounted for more losses than their occurrence rate, 72.3% ($20,000,000 USD) against 33.3%. Polygon saw a similar trend in lending, with this protocol causing 40.2% ($86,500,000 USD) of the losses in 2021 and 91.8% ($120,000,000 USD) in 2023, despite having a consistent attack rate of 33.3% in both years.

Solana in 2022 experienced significant losses from bridges, which caused 66.7% ($326,000,000 USD) of the financial damage against a 33.3% occurrence rate. Tron, on the other hand, has similar rates of occurrence and amount lost.

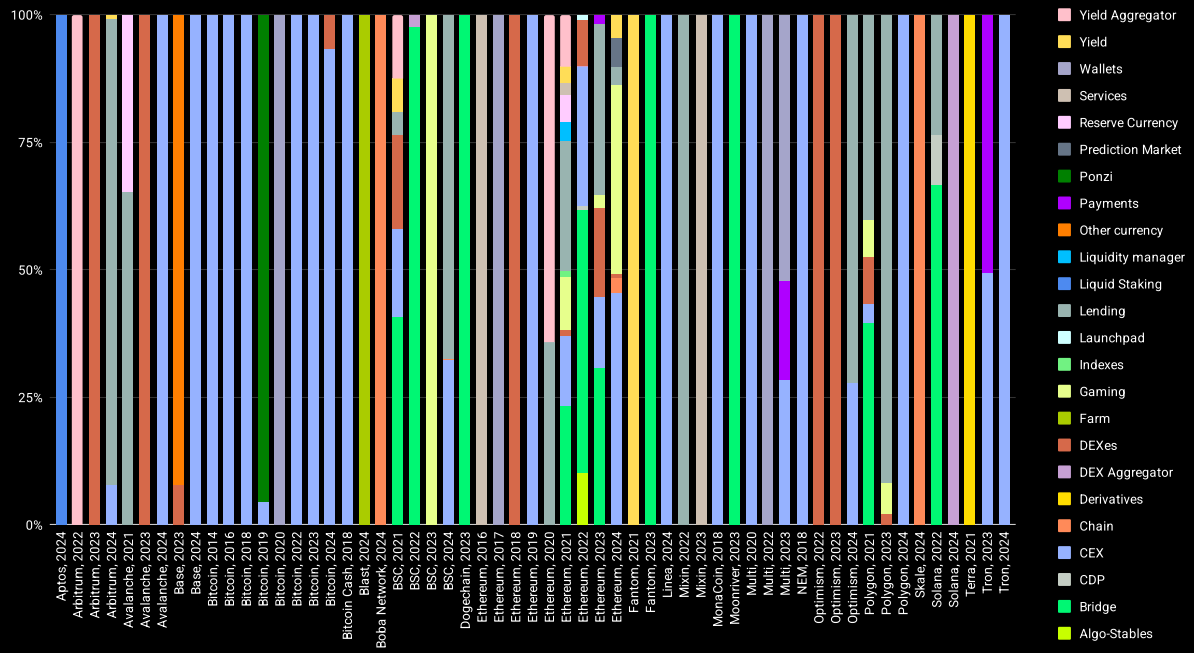

Figure 142: Loss per type of protocols per chain and year [percentage]

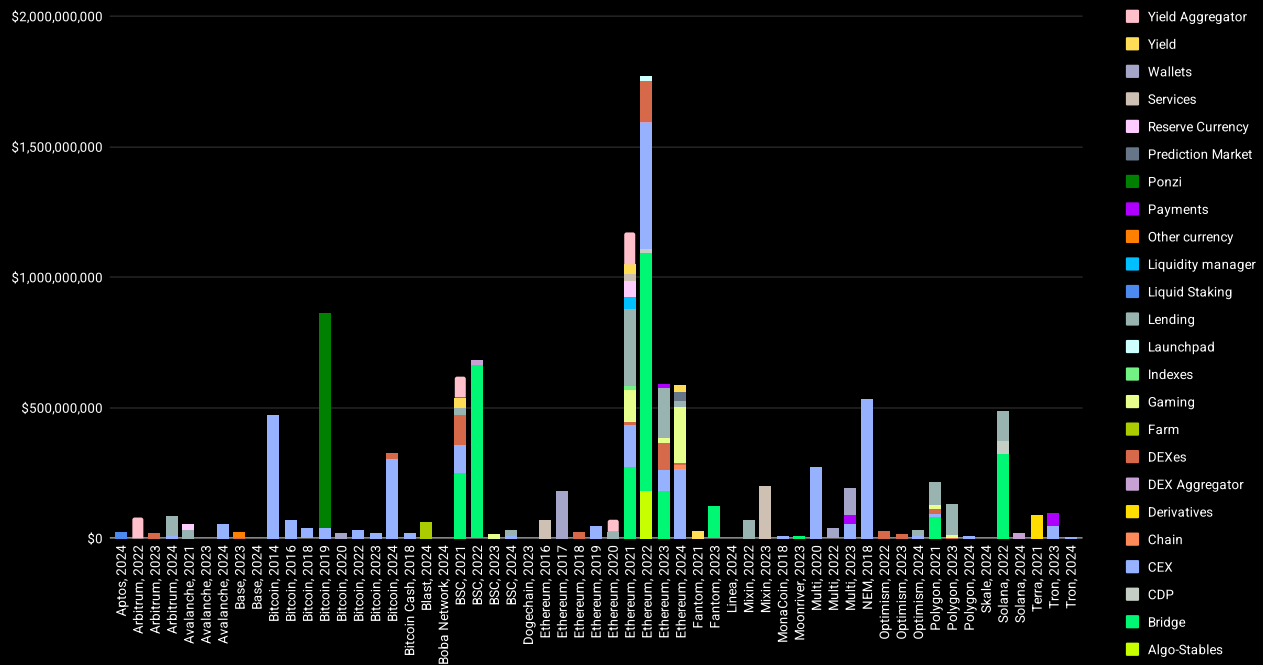

Figure 143: Loss per type of protocols per chain and year [USD]

Type of Protocols per Type of Attacks

Figures 144 and 145 detail the correlation between the types of attacks and the specific protocols targeted.

Direct contract exploitation emerges as the primary attack vector for Bridges at 50%, Derivatives at 100%, Launchpads at 100%, and Liquid Staking at 100%. It also ties for first place with market manipulation attacks in CDP at 50% each, Liquidity Manager at 50% each, and Yield Aggregators at 33.3%; with compromised accounts in DEX Aggregators at 50%; and with both compromised accounts and rug pulls or scams in Services.

Governance attacks uniquely impact Algo-Stables and Chain protocols, being the exclusive type of attack leading to losses in these areas.

Market manipulation attacks dominate in Indexes, accounting for all incidents (100%), and are a major cause of loss in lending protocols, responsible for 46.7% of the attacks.

Rug pulls and scams are particularly detrimental in several areas, being the sole cause of hacks in Farms, Other currency categories, Ponzi schemes, Prediction Markets, and Reserve Currency protocols.

Compromised accounts are a prevalent issue in more transaction-oriented protocols. They are the primary cause of loss in Centralized Exchanges (CEXs) at 95%, Decentralized Exchanges (DEXes) at 36.4%, and are entirely responsible for incidents in Payment protocols (100%) and 60% of attacks on Wallets.

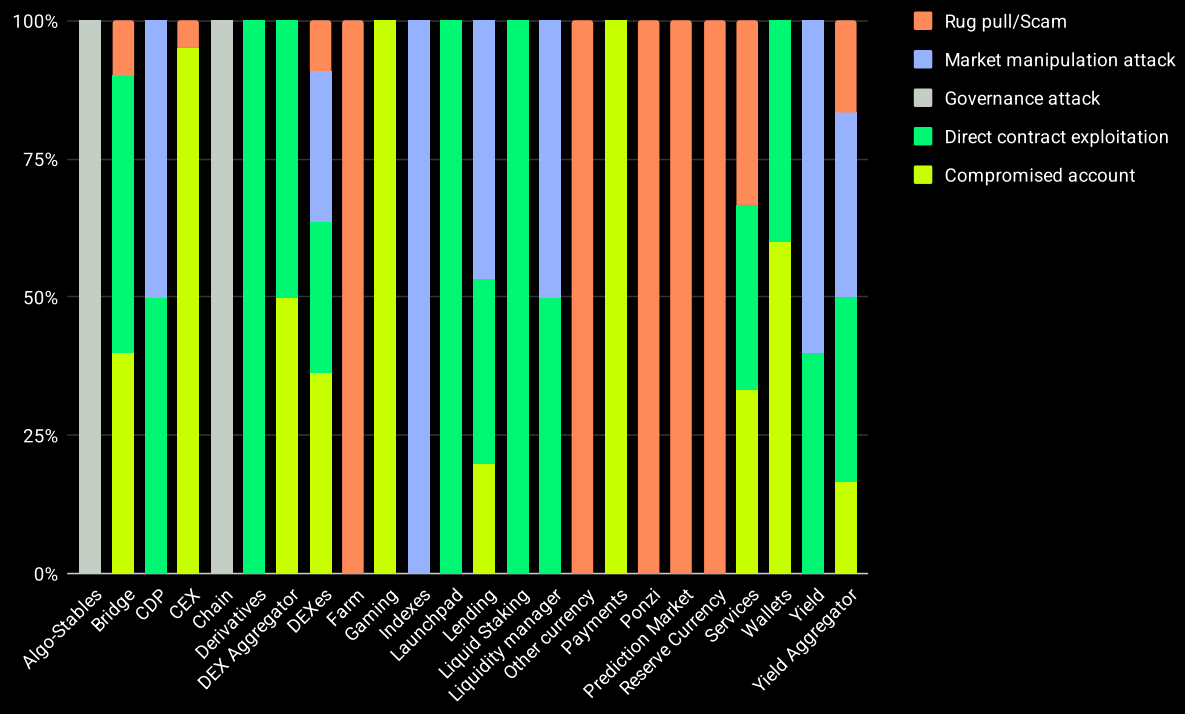

Figure 144: Number of type of attacks per type of protocol [percentage]

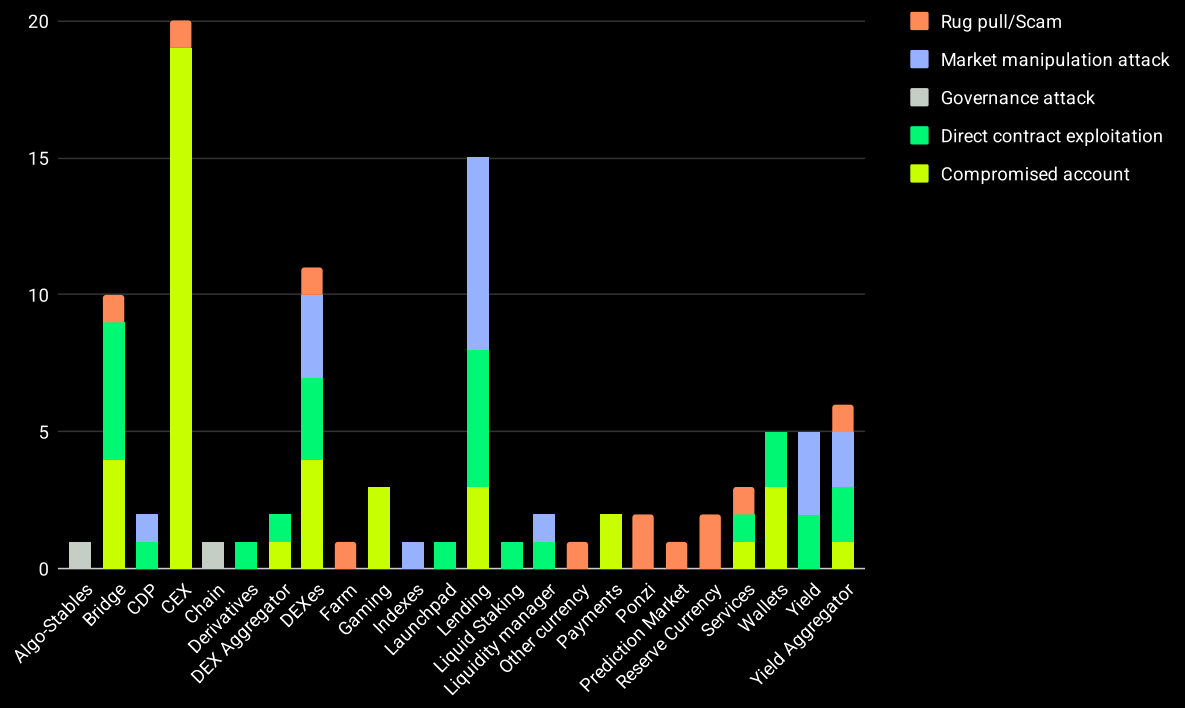

Figure 145: Number of type of attacks per type of protocol [count]

Figures 146 and 147 reveal the financial losses across various protocols by type of attack and protocol.

For instance, in Bridges, direct contract exploitation leads to significant financial distress, causing losses of 63.5% ($1,793,000,000 USD) despite only a 50% occurrence rate. Similarly, CDPs see 75.5% ($48,000,000 USD) in losses against a 50% attack rate, while lending protocols experience 39% ($432,500,000 USD) of losses with a 33.3% occurrence rate. Wallets also report higher losses than attack rates, recording 53.4% ($182,000,000 USD) in losses against occurrence rates of 40%.

Compromised accounts present another critical threat, leading to more losses than occurrences in several protocol types. DEX Aggregators face losses of 51% ($21,000,000 USD) compared to a 50% attack rate, while DEXes show a loss rate of 44.8% ($237,600,000 USD) against an attack occurrence of 36.4%. Services are particularly vulnerable, with losses of 67.3% ($200,000,000 USD) greatly exceeding a 33.3% attack rate, and Yield Aggregators incur 37.3% ($120,000,000 USD) in losses versus an occurrence rate of 16.7%.

Rug pulls, too, cause substantial damage in CEXs, accounting for 14.3% ($450,000,000 USD) of the financial losses while only occurring in 5% of the cases.

Market manipulation attacks increase the financial toll on Liquidity Managers and Yield protocols, leading to 54.5% ($24,000,000 USD) and 64.4% ($86,700,000 USD) in losses, respectively, both of which are higher than their corresponding rates of occurrence of 50% and 60% respectively.

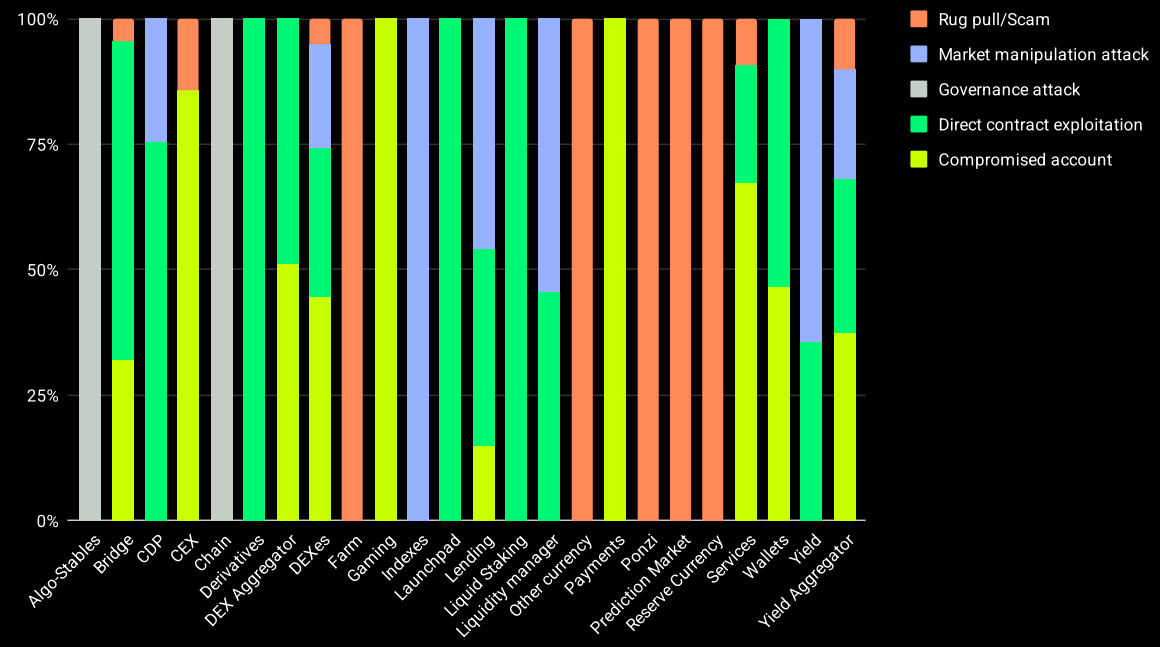

Figure 146: Loss per type of attacks per type of protocol [percentage]

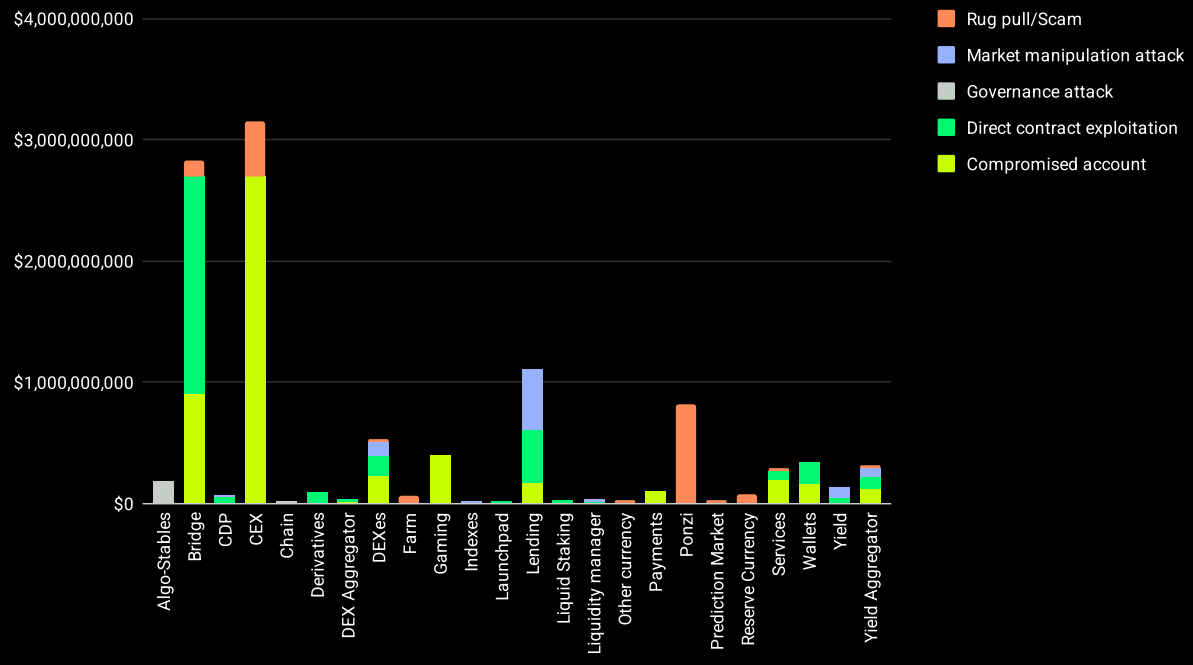

Figure 147: Loss per type of attacks per type of protocol [USD]

Figures 148 and 149 illustrate the evolving landscape of types of attacks on various DeFi protocols over the years.

Initially, Bridges predominantly experienced hacks due to direct contract exploitation. However, by 2023, the nature of attacks shifted significantly, with compromised accounts becoming the predominant method, accounting for 66.7% of attacks, supplemented by the emergence of rug pulls or scams.

In CEXs (Centralized Exchanges), compromised accounts have consistently been the primary cause of hacks across all years, with a notable exception in 2022 where, although still leading at 66.7%, the remainder of the attacks involved rug pulls or scams.

DEX Aggregators saw a transition from being compromised due to direct contract exploitation in 2022 to compromised accounts by 2024, indicating a shift in attack focus.

DEXes have seen varied attack vectors, starting in 2018 with compromised accounts as the sole cause, transitioning in 2021 to primarily market manipulation attacks (50%). By 2022, the attacks were evenly split between compromised accounts and direct contract exploitation. In 2023, the attacks diversified further among compromised accounts, direct contract exploitation, and market manipulation. However, by 2024, compromised accounts once again emerged as the sole attack vector.

Lending protocols initially faced attacks solely via direct contract exploitation in 2020. In 2021, the attacks were evenly distributed among direct contract exploitation, compromised accounts, and market manipulation. By 2022, market manipulation became the sole attack method, but in 2023, attacks were again evenly split between direct contract exploitation and market manipulation. By 2024, most attacks (50%) were due to market manipulation.

In Services, each year brought different attack types: direct contract exploitation in 2016, rug pulls or scams in 2021, and compromised accounts in 2023.

Yield protocols in 2021 had market manipulation and direct contract exploitation, each accounting for half of the attacks. By 2024, market manipulation became the sole cause of hacks, signaling an evolving threat landscape.

Yield Aggregators in 2020 saw equal causes from market manipulation attacks and direct contract exploitation. In 2021, these factors, along with rug pulls or scams, contributed equally to attacks. However, by 2022, direct contract exploitation was the singular cause of attacks.

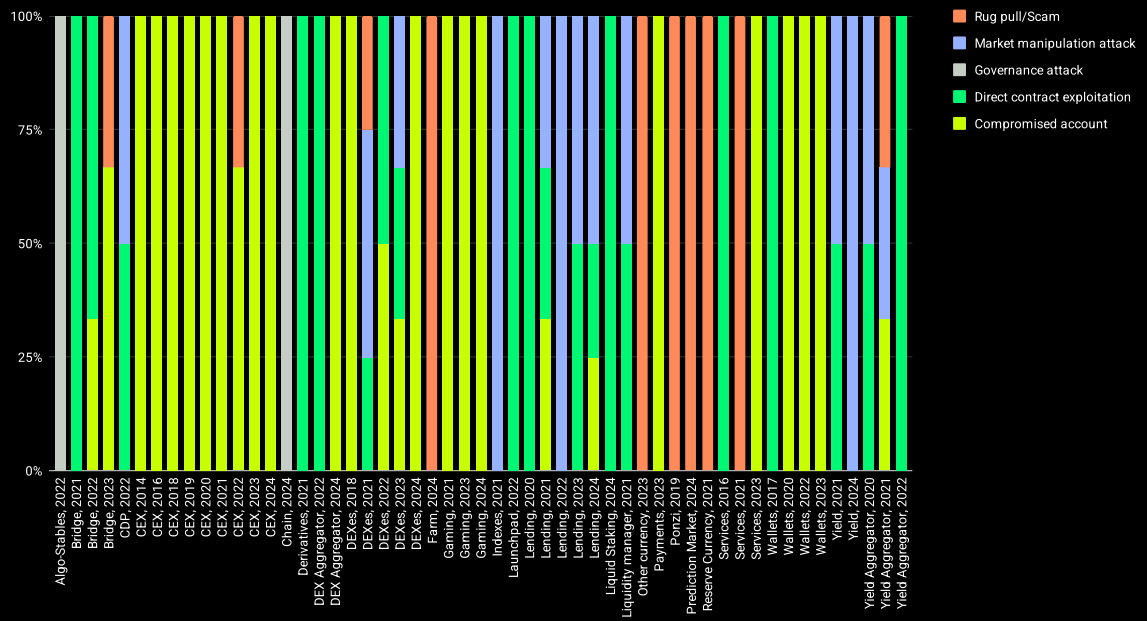

Figure 148: Number of type of attacks per type of protocols [percentage]

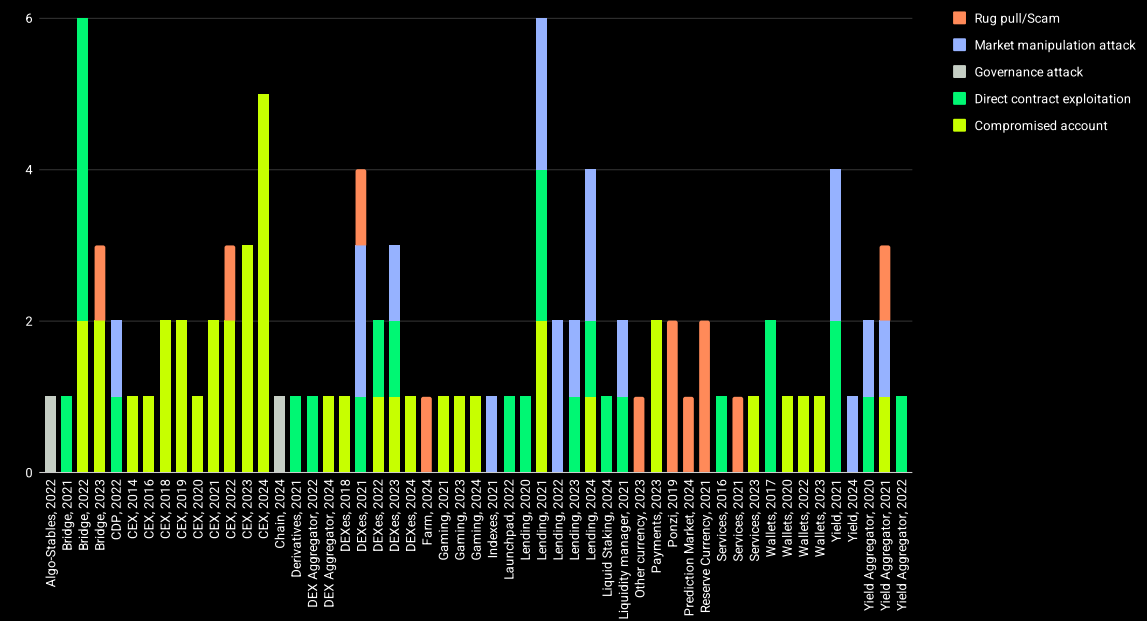

Figure 149: Number of type of attacks per type of protocols [count]

Figures 150 and 151 detail the financial losses attributed to different types of attacks across various protocols and years.

In Bridges, 2022 witnessed compromised accounts causing a disproportionate share of financial damage—38% ($724,000,000 USD) compared to their occurrence rate of 33.3%. By 2023, the trend shifted, allowing rug pulls and scams to account for a higher percentage of losses, 41.4% ($127,466,000 USD), again against an occurrence rate of 33.3%.

CEXs in 2022 experienced substantial financial damage from rug pulls and scams, which were responsible for 87.9% ($450,000,000 USD) of the losses despite only occurring in 33.3% of the cases.

For DEXes, 2021 saw a significant impact from direct contract exploitation, which, while only representing 25% of the attacks, accounted for 39.1% ($57,000,000 USD) of the financial losses. In 2023, this type of attack occurred 33.3% of the time but was responsible for 48.5% ($69,300,000 USD) of the losses. The next year, however, saw compromised accounts as the primary cause of financial loss, accumulating 84.2% ($162,000,000 USD) against a 50% occurrence rate.

Lending protocols in 2021 faced equal attack rates from direct contract exploitation and market manipulation (33.3%), but the losses deviated, with direct contract exploitation causing 37.4% ($165,800,000 USD) and market manipulation close behind at 37% ($164,000,000 USD) of the financial losses. In 2023, direct contract exploitation continued to lead, causing 62.1% ($197,000,000 USD) of the losses against a 50% occurrence rate. In 2024, although direct contract exploitation still caused more loss than its occurrence (32.6% or $44,700,000 USD versus an occurrence rate of 25%), compromised accounts were the leading cause of financial damage, representing 38.7% ($53,000,000 USD) of the losses against a 25% rate.

Liquidity Managers saw market manipulation attacks causing slightly more damage than expected, with 54.5% ($24,000,000 USD) of the losses against a 50% attack rate. Yield protocols in 2021 and Yield Aggregators in 2020 experienced similar trends, with losses amounting to 55.4% ($59,700,000 USD) and 55.9% ($25,000,000 USD), respectively, against a 50% occurrence rate. Moreover, in 2021, Yield Aggregators saw compromised accounts causing 60.9% ($120,000,000 USD) of the losses, significantly higher than their 33.3% occurrence rate.

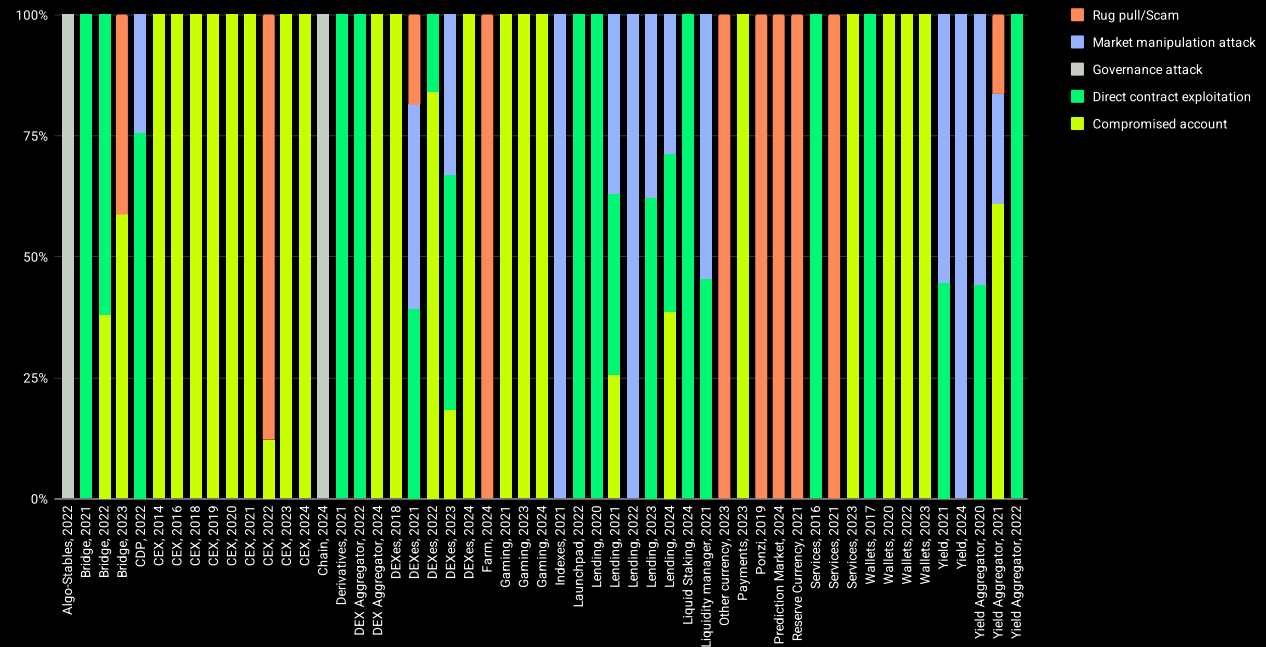

Figure 150: Loss per type of attacks per type of protocols [percentage]

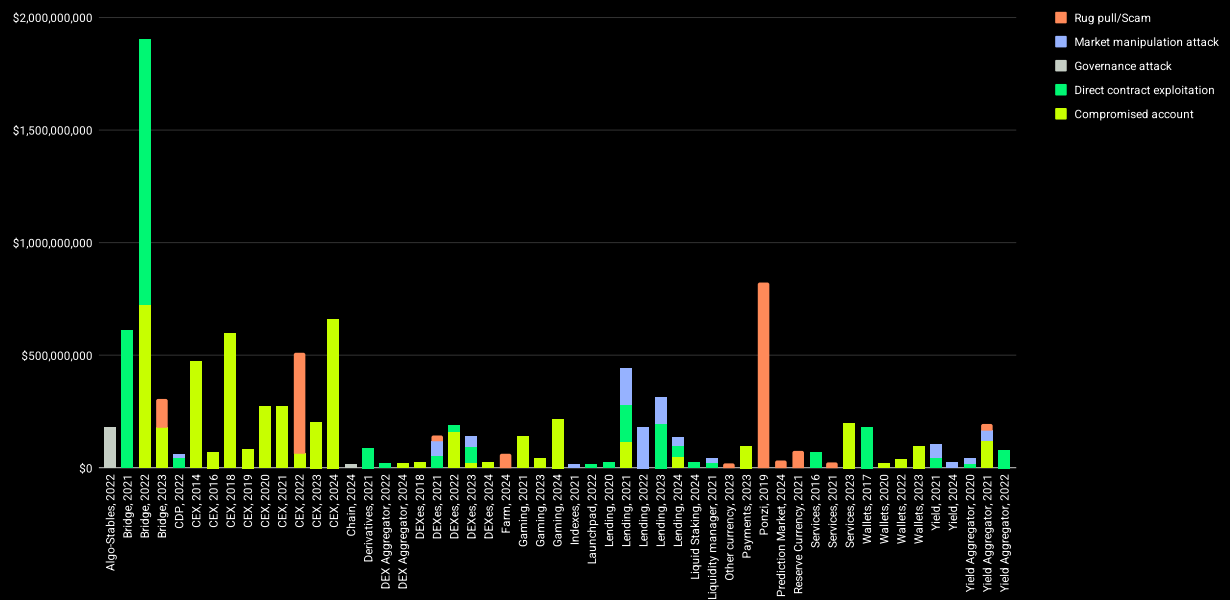

Figure 151: Loss per type of attacks per type of protocols [USD]

TYPE OF FUNCTIONS

When examining potential vulnerabilities in the protocol's smart contracts, especially those related to functions callable by users (either public or external), it's crucial to understand the various types of functions based on their functionality. This categorization helps identify which functions are commonly targeted by attackers and the nature of their use in exploits.

- `deposit:` Functions in this category are designed to deposit assets into the protocol.
- `withdraw:` This function category includes withdrawing assets from the protocol, and it also includes borrowing actions.
- `swap:` Functions under this category facilitate the swapping of one type of asset for another within the protocol. They typically involve calling internal functions to determine exchange amounts.
- `mint:` These functions are used to mint new assets, often requiring calls to internal functions to establish how many assets to mint based on specific criteria.
- `execute:` This category includes functions that execute specific functionalities within the protocol, such as processing proposals.
- `transferOwnership:` Functions in this category handle the transfer of ownership or special privileges of a contract or the entire protocol.
- `initialize:` These functions are used primarily at the start to initialize the protocol's settings and parameters.
- `calculateAmount:` Functions here are designed to compute quantities relevant to the protocol, like calculating pool liquidity or ratio.
- `verifyProof:` Especially important in cross-chain functionalities and bridges, these functions verify certain actions or roles on the blockchain.
- `migrate:` This involves functions used for upgrading or migrating from one protocol version to another.
- `create:` Functions that are used to create additional contracts within the ecosystem.
- `vote:` This involves functions that allow stakeholders to vote on key aspects or changes within the protocol, integral to decentralized governance mechanisms.
- **Protocol specific:** These are unique functions tailored to meet specific needs or features unique to a particular protocol.

Figures 152 and 153 showcase the distribution of attacks based on the type of function targeted within smart contracts.

`Withdraw`-like functions are the most frequently attacked, constituting 25.7% of the total attacks. This high rate indicates that functions enabling the removal of assets from a protocol are particularly attractive targets, likely due to the direct access they offer to liquid assets.

The second most targeted are `deposit`-like functions, accounting for 17.1% of the attacks. These functions are critical for adding assets to a protocol, and their exploitation can disrupt the inflow of funds or manipulate asset balances, posing significant risks to the protocol's integrity and user funds.

Sharing the third spot, `mint`, `initialize`, and `swap` functions each represent 8.6% of the attack distribution. `Mint` functions, which involve creating new assets, can be exploited to artificially inflate supply or misappropriate value. Initialize functions are crucial during the setup phase of contracts and can be targeted to alter the foundational parameters of a protocol. `Swap` functions, involved in exchanging one asset type for another, are key components in trading platforms and can be manipulated to manipulate trading outcomes or siphon funds through slippage attacks or unfavorable rate executions.

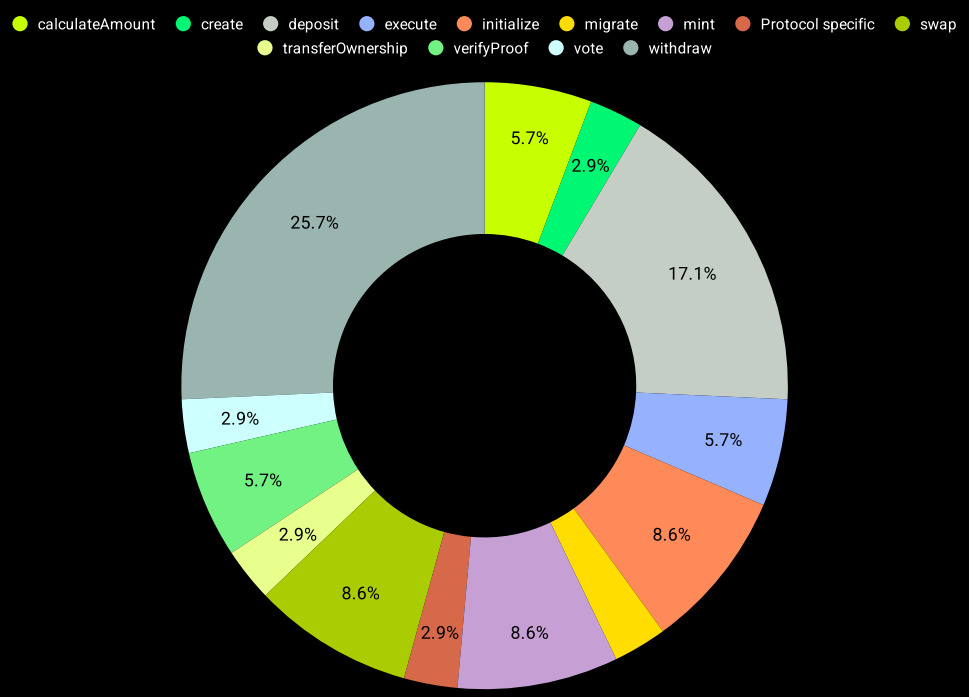

Figure 152: Number of types of function [percentage]

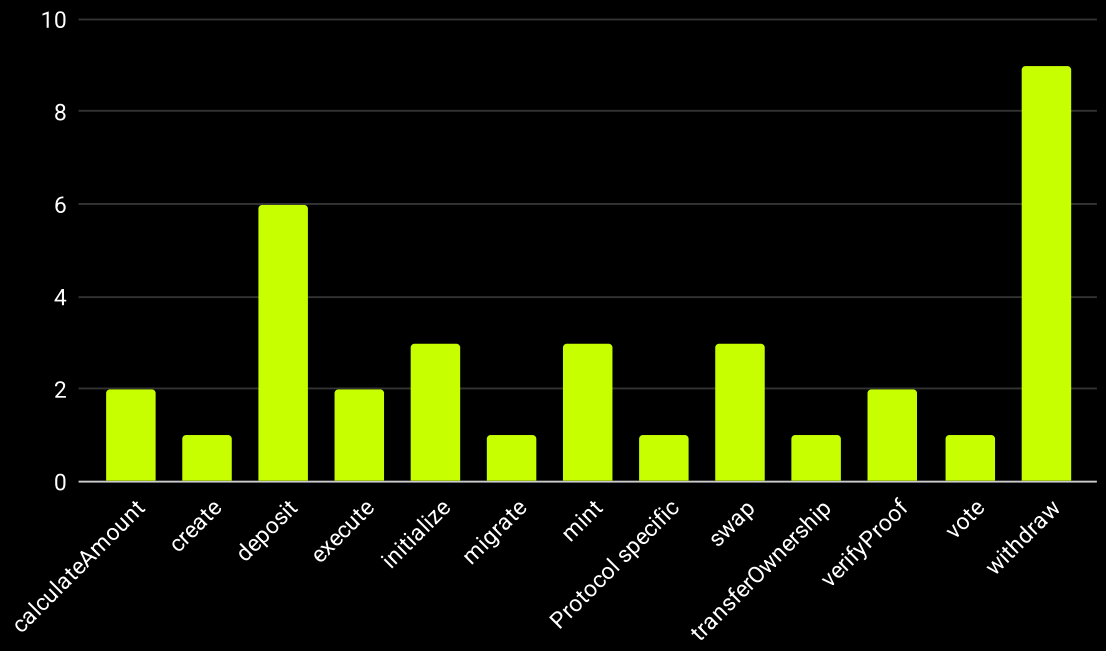

Figure 153: Number of types of function [count]

Figures 154 and 155 explore the financial impact of attacks based on the types of functions targeted within smart contracts.

The function `verifyProof` stands out with a disproportionately high financial impact, accumulating 27% of the total losses ($912,000,000 USD) despite being involved in only 5.7% of the attacks. This function typically verifies certain conditions or credentials on blockchain networks, particularly in bridge operations where validations are crucial for security. The high losses associated with these functions suggest that attacks here can undermine critical security mechanisms, leading to substantial breaches.

`TransferOwnership` functions, which are essential for administrative control over contracts, follow as the second most financially damaging, representing 18.1% ($611,000,000 USD) of the total losses while accounting for only 2.9% of the attacks. The exploitation of these functions can result in attackers gaining full control of the protocols, enabling them to redirect funds or alter the protocol operations drastically.

In third place, `deposit` functions account for 11.4% of the total value lost ($386,000,000 USD) but are more frequently targeted, involved in 17.1% of the attacks. While they do not match the financial impact of `verifyProof` or `transferOwnership` functions, the higher rate of occurrence still marks them as significant vulnerabilities.

The analysis indicates that `verifyProof` and `transferOwnership` functions, though less frequently attacked, result in higher losses when compromised. This points to the strategic targeting by attackers, who may opt for less frequently used but more critical functions that can yield higher returns when successfully exploited.

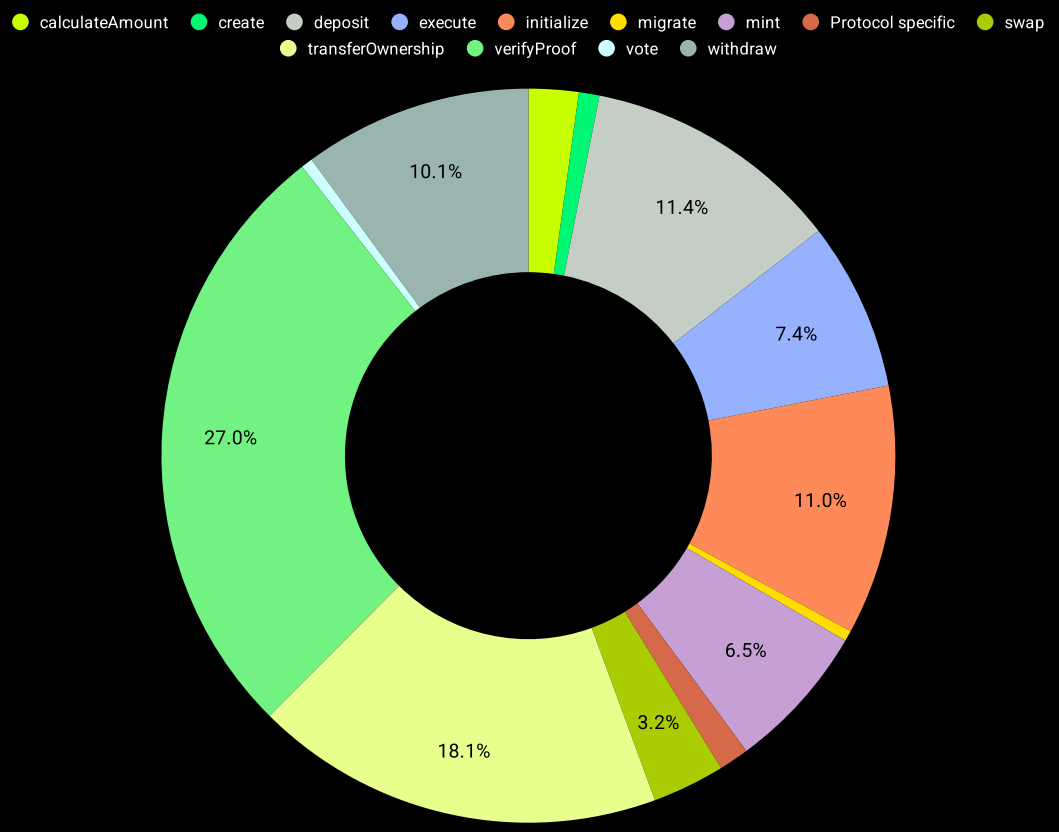

Figure 154: Loss caused by type of function [percentage]

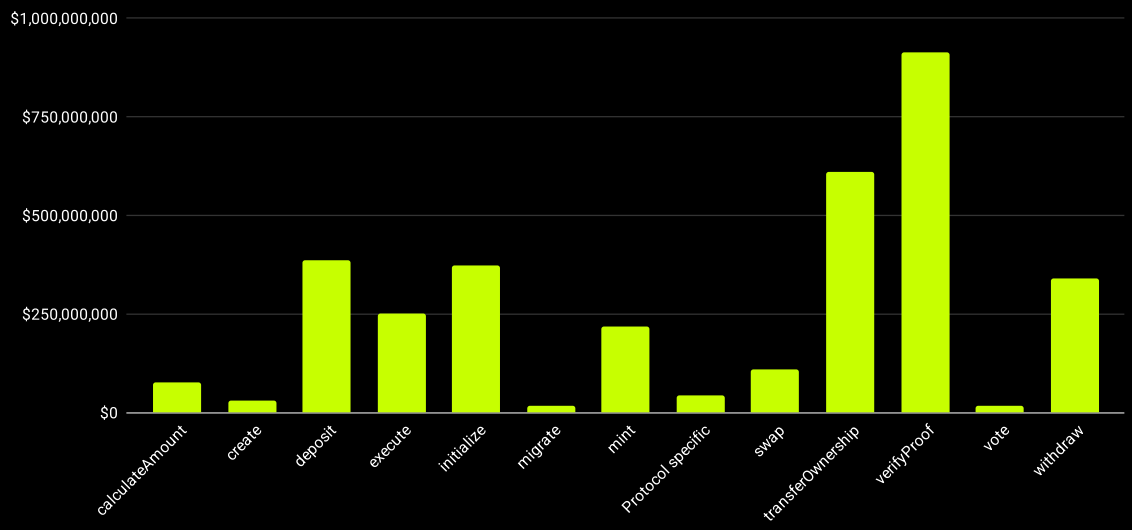

Figure 155: Loss caused by type of function [USD]

Figures 156 and 157 illustrate a detailed timeline of blockchain attacks, organized by the type of function exploited each year.

In 2016, the exploited protocols were compromised through an `execute` function, indicating that attackers targeted functions that triggered specific protocol actions. The following year, 2017, saw attacks due to vulnerabilities in `initialize` functions, which are often used to set initial parameters or states in contracts, highlighting early-stage vulnerabilities in protocol deployments.

By 2020, the landscape of attacks had diversified, with losses being equally distributed between `swap` and `deposit` functions. This reflects a broader interest in exploiting financial mechanisms within DeFi protocols, particularly those involving asset exchanges and deposits.

2021 marked a significant shift towards `withdraw`-like functions, which accounted for 46.2% of the losses. This suggests a targeted approach to functions allowing direct asset withdrawals, posing higher financial risks. The same year also saw considerable impacts from attacks on `mint`, `swap`, and `deposit` functions, each contributing 15.4% to the total losses.

In 2022, the focus of attacks was evenly split between `withdraw` and `verifyProof` functions, each at 20%. The prominence of `verifyProof` functions could be linked to their critical role in validating transactions or user actions, especially in the context of increasing bridge usage, which often involves complex cross-chain interactions.

2023 saw a balanced distribution of attacks between `deposit` and `calculateAmount` functions, suggesting a nuanced approach by attackers towards exploiting financial calculation functions and deposit mechanisms.

2024 demonstrated an even distribution among several function types, including `withdraw`, `vote`, protocol-specific, `deposit`, and `calculateAmount`. This equal distribution across diverse functions underscores a broadening of attack surfaces and suggests that attackers are leveraging a wide array of vulnerabilities across different functional aspects of protocols.

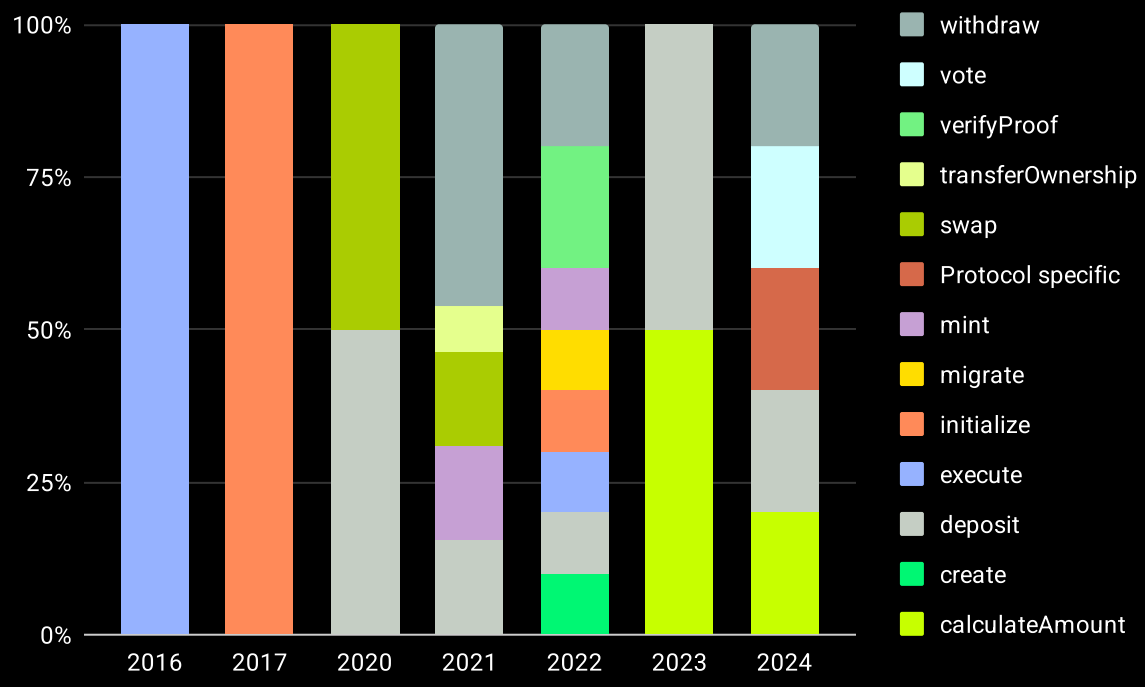

Figure 156: Number of type of function per year [percentage]

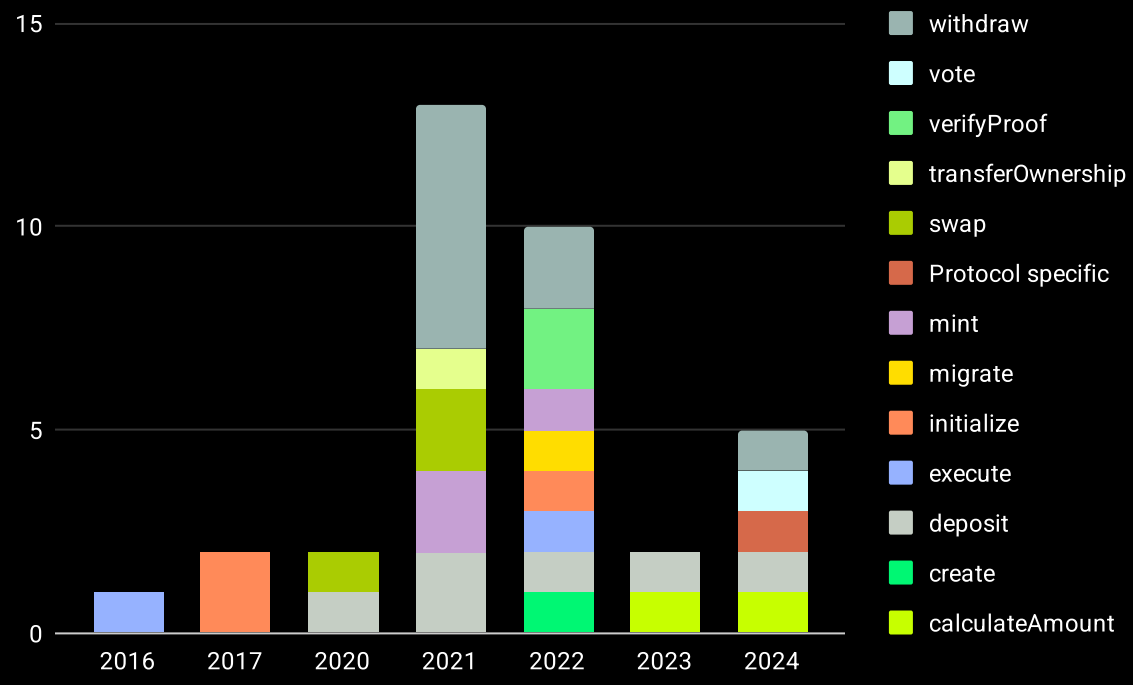

Figure 157: Number of type of function per year [count]

Figures 158 and 159 provide a chronological assessment of blockchain attacks categorized by the type of function exploited and the associated financial losses each year.

In 2020, `deposit` functions were notably vulnerable, causing the majority of the financial damage, accounting for 55.9% of the total losses ($25,000,000 USD) even though they constituted only 50% of the attacks. This underscores the high financial stakes involved when deposit functions are exploited.

2021 saw a significant shift with `transferOwnership` functions leading to the most substantial losses. They accumulated 53.2% of the total losses ($611,000,000 USD), which is exceptionally high considering their relatively low occurrence rate of only 7.7%. This suggests that attacks targeting ownership controls within protocols can lead to disproportionately high financial damages.

In 2022, `verifyProof` functions were a major target, resulting in substantial losses amounting to 58.6% of the year's total ($912,000,000 USD), while only being involved in 20% of the attacks. The critical role of `verifyProof` functions in validating transactions or user actions makes them lucrative targets for attackers, as evidenced by the high proportion of losses they caused.

2023 highlighted vulnerabilities in `deposit` functions once again, where they were responsible for a staggering 80.6% of the total financial losses ($197,000,000 USD), despite accounting for only 50% of the incidents. This reiterates the ongoing risk associated with deposit functions in blockchain protocols.

By 2024, the focus of attackers had shifted towards protocol specific functions, which led to significant financial damage, representing 33.2% of the year's losses ($44,700,000 USD) against only 20% of the attacks. The exploitation of these functions suggests a trend towards more sophisticated attacks that target unique aspects of specific protocols.

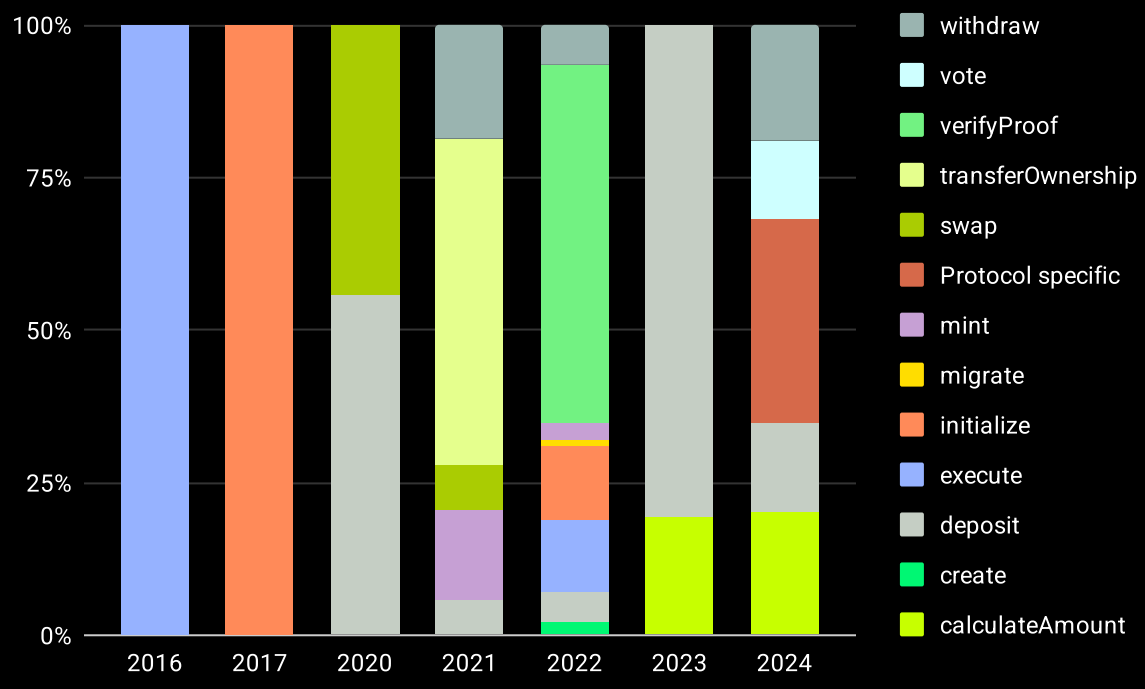

Figure 158: Loss caused per type of function per year [percentag

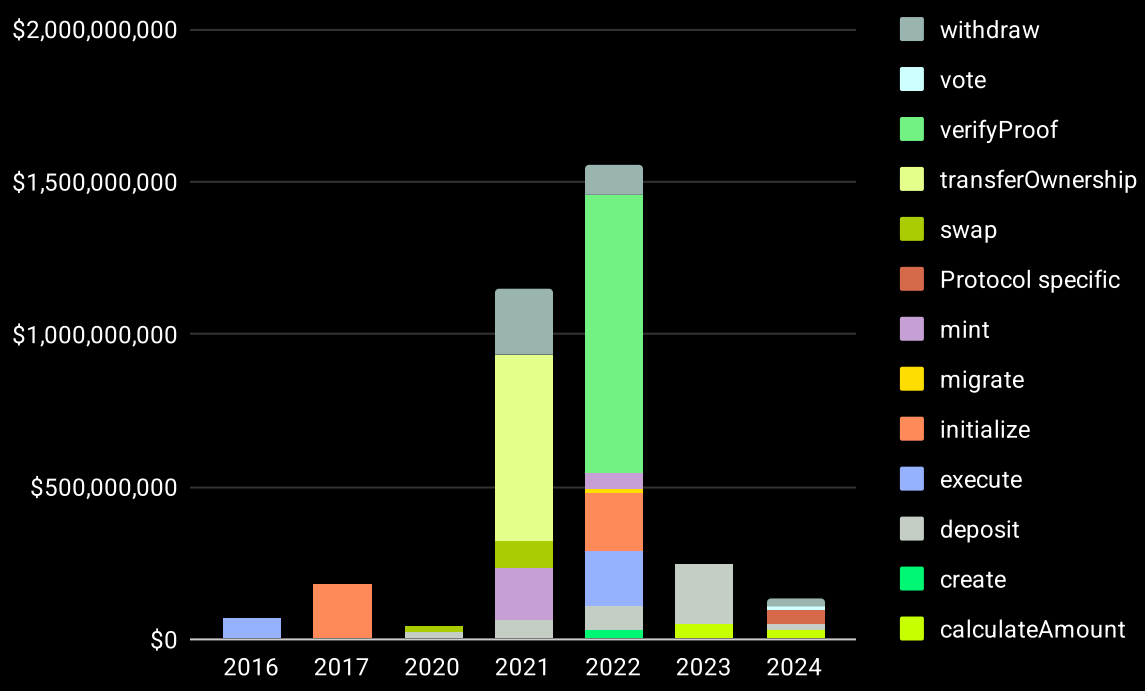

Figure 159: Loss caused per type of function per year [USD]

Type of Functions vs Chains

Figures 160 and 161 present the distribution of attacked smart-contract functions across various chains, noting that any chain not shown experienced no specific smart-contract function exploits.

In Aptos, the primary function targeted by attacks was `withdraw`, suggesting a focus on functions that enable the direct extraction of assets. Arbitrum presents a different vulnerability, with `calculateAmount` being the most compromised function, accounting for 50% of the attacks, indicating an exploitation of financial calculation mechanisms within the chain.

Avalanche shows a balance in vulnerabilities with `calculateAmount` and `deposit` functions each facing significant targeting. Base similarly sees `calculateAmount` as the sole function attacked.

In the Boba Network, the function `vote` was targeted. Both BSC and Ethereum show a prevalence of attacks on `withdraw` functions, at 37.5% and 19%, respectively, again emphasizing the attractiveness of functions that facilitate asset outflows.

Fantom experienced attacks primarily on `deposit` functions, contrasting with the trend in other networks, suggesting that the entry points for assets into the network are also critical vulnerabilities. Optimism displayed a more distributed attack pattern, with `deposit`, `create`, and `calculateAmount` each equally targeted.

Polygon sees an equal distribution of attacks among `transferOwnership`, swap, and `calculateAmount`, pointing to varied attack vectors from ownership control to asset exchange and financial calculations. Skale was attacked via a `vote` function, like Boba Network, emphasizing the vulnerabilities in functions associated with governance.

Solana exhibited equal targeting between mint and `verifyProof` functions. Lastly, in Terra, the `withdraw` function was primarily attacked, consistent with the trends seen in other networks like Aptos, BSC, and Ethereum.

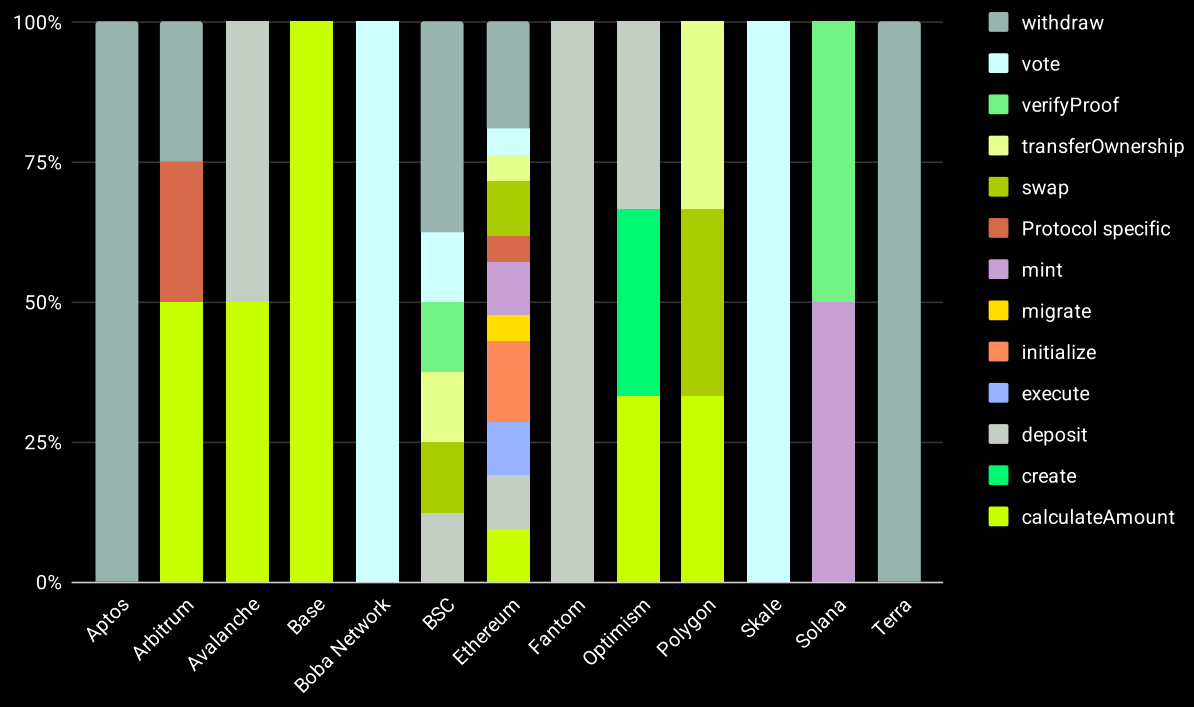

Figure 160: Number of type of function per chain [percentage]

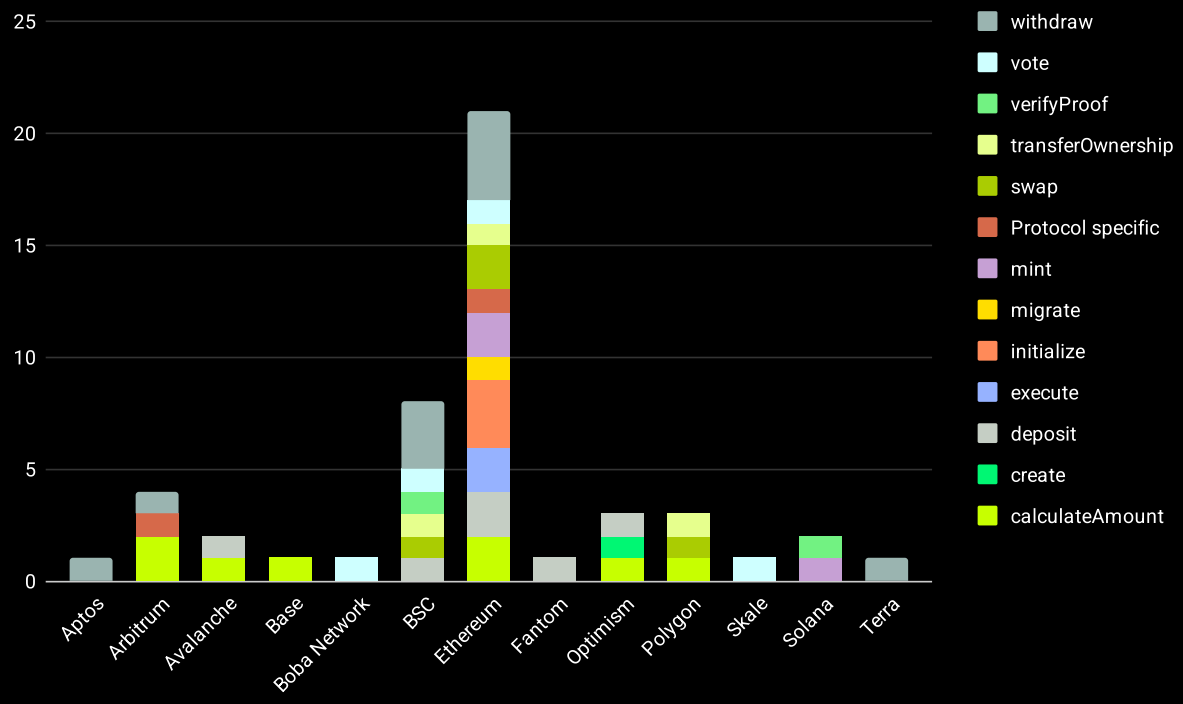

Figure 161: Number of type of function per chain [count]

Figures 162 and 163 show the financial losses attributed to different types of functions across various blockchain networks.

For chains like Arbitrum, `withdraw` functions are a significant source of loss, accounting for 55.9% ($80,000,000 USD) of the total financial damage, despite only representing 25% of the attack occurrences. Protocol-specific functions also result in slightly more losses than their occurrence rate, causing 29.7% ($42,600,000 USD) of the financial impact against a 25% attack rate.

In BSC, the `verifyProof` function stands out as particularly detrimental, responsible for 56.3% of the total losses ($586,000,000 USD) while occurring in just 12.5% of the cases. `TransferOwnership` functions also cause significant financial damage, accounting for 24.3% ($253,000,000 USD) of the losses with the same 12.5% occurrence rate.

Ethereum shows several functions leading to considerable financial losses compared to their rates of occurrence. `TransferOwnership` functions result in 18.6% of the financial damage ($273,000,000 USD), `initialize` accounts for 25.3% ($372,000,000 USD), and `execute` functions lead to 17.1% ($251,000,000 USD) of the losses, all notably higher than their respective rates of occurrence of 4.8%, 14.3%, and 9.5%.

Optimism highlights `create` functions as a major cause of loss, making up 46.6% ($30,500,000 USD) of the financial impact against a 33.3% attack rate.

In Polygon, `transferOwnership` functions are responsible for a substantial portion of the financial damage, comprising 79.1% ($85,000,000 USD) of the losses while only being involved in 33.3% of the attacks.

Lastly, in Solana, `verifyProof` functions again prove to be the costliest, accumulating 87.2% ($326,000,000 USD) of the losses, illustrating their critical vulnerability and substantial impact when compromised.

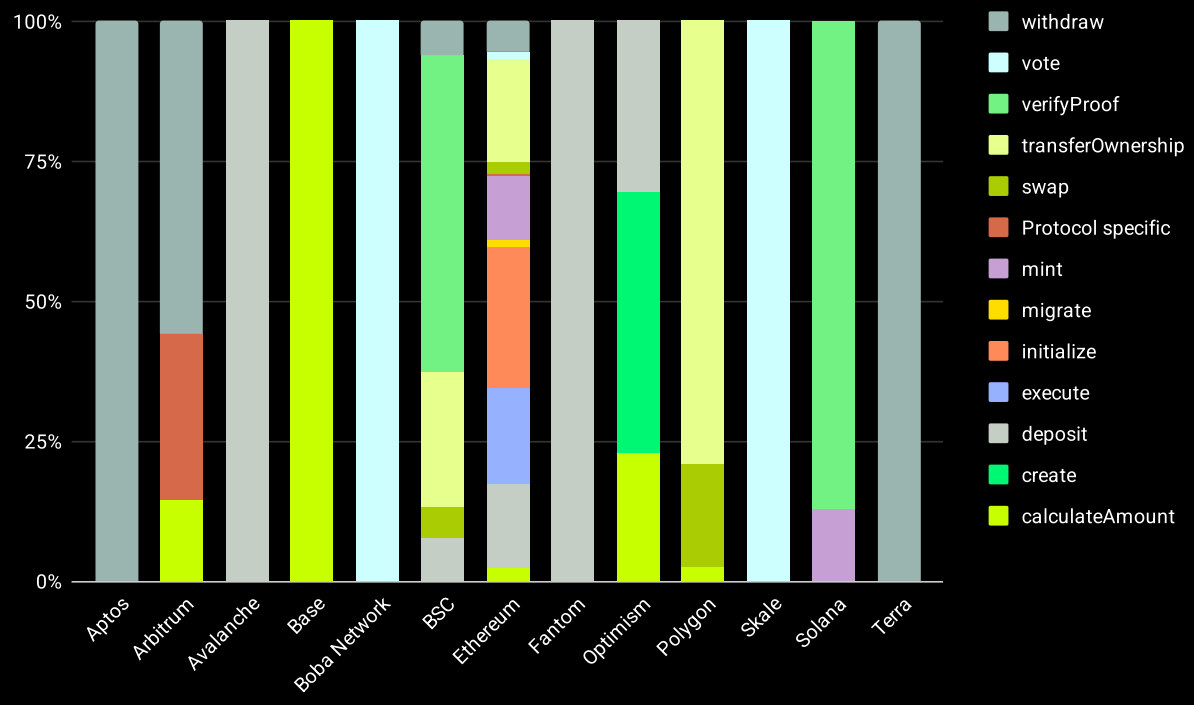

Figure 162: Loss caused per type of function per chain [percentage]

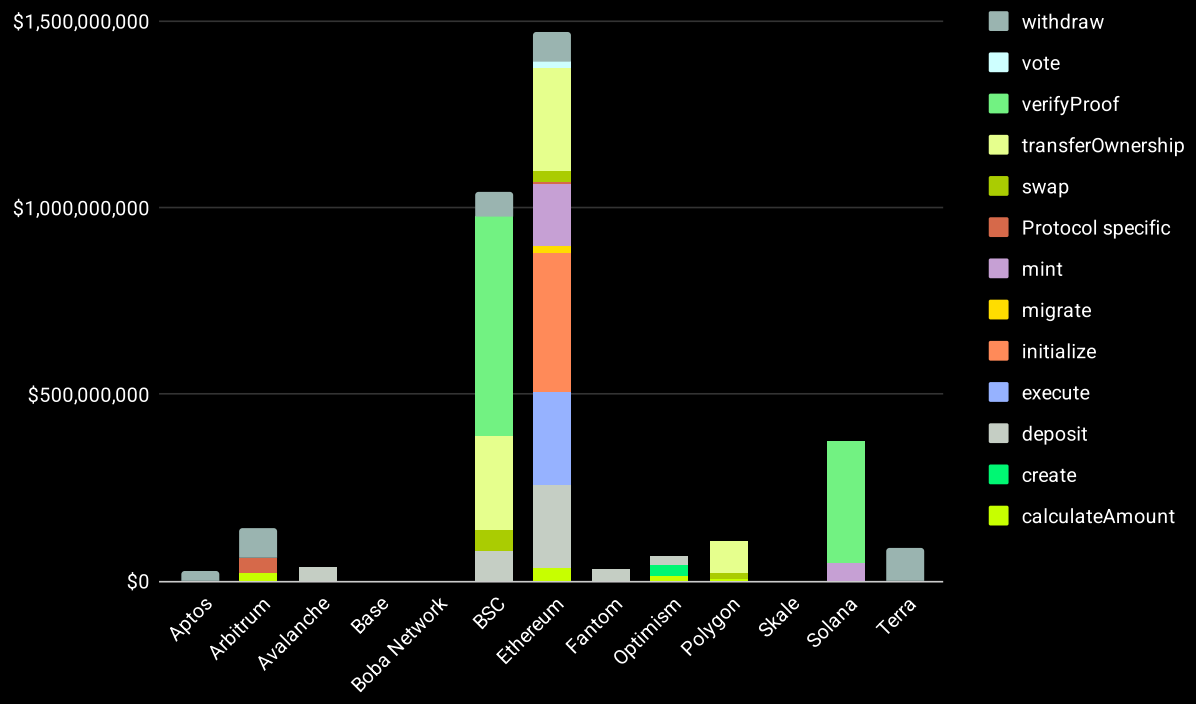

Figure 163: Loss caused per type of function per chain [USD]

Figures 164 and 165 showcase the distribution of attacked functions across various chains and years.

In Arbitrum, the function attacked in 2022 was a `withdraw`, while the year 2023 saw an attack via a `calculateAmount` function. In 2024, attacks involved both this type of function and a protocol-specific function.

BSC experienced attacks primarily through `withdraw` functions in 2021, accounting for 50% of the incidents that year. By 2022, these attacks comprised a third of the total, alongside `verifyProof` and `deposit` functions. In 2024, the focus shifted to a `vote` function.

In Ethereum, the landscape of attacks has shifted notably over the years. An `execute` function was exploited in 2016, followed by attacks via a faulty `initialize` function in 2017. The year 2020 saw equal involvement of `swap` and `deposit` functions in the attacks. By 2021, most attacks were executed via `withdraw` functions, constituting 42.9% of the incidents, with `mint` functions also playing a significant role at 28.6%. The year 2022 was characterized by an equal distribution among `withdraw`, `migrate`, `initialize`, and `execute` functions. In 2023, attacks were equally driven by `calculateAmount` and `deposit` functions. The year 2024 saw a diverse mix, with attacks equally distributed among vote, protocol-specific, and `calculateAmount` functions.

Optimism displayed a variation in the attack vectors used each year, with `create` being the primary function attacked in 2022, followed by `calculateAmount` in 2023, and deposit in 2024, each year seeing a shift in the focus of attacks.

In Polygon, 2021 witnessed attacks equally carried out via `transferOwnership` and swap functions. By 2023, the attacks had shifted focus to `calculateAmount`, reflecting changes in the attack strategies over time.

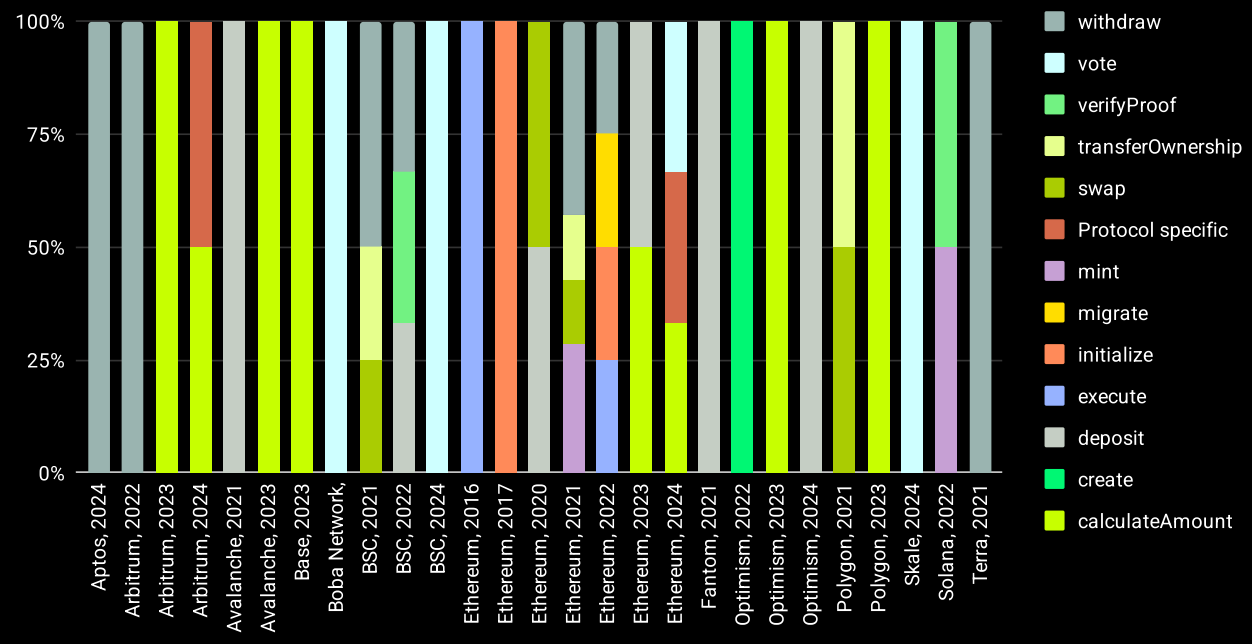

Figure 164: Number of type of function per chain and year [percentage]

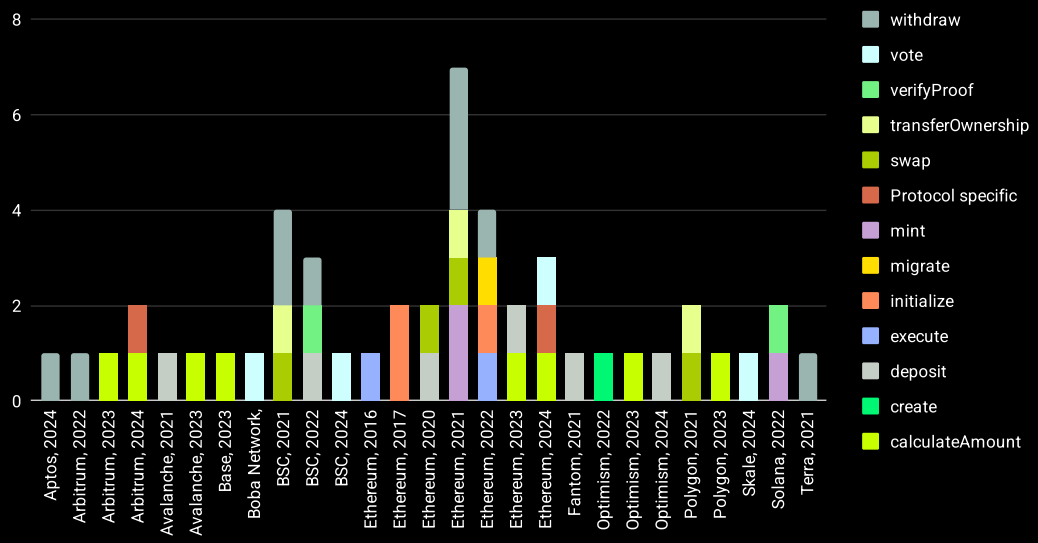

Figure 165: Number of type of function per chain and year [count]

Reviewing the distribution of the loss caused by attacked functions across different blockchain networks over time, as shown in Figures 166 and 167, it seems that there is no consistent trend in the types of functions targeted year over year within any specific chain.

However, significant disparities are evident between the frequency of attacks on functions and the financial losses they cause.

In Arbitrum during 2024, despite protocol-specific functions being involved in 50% of the incidents, they were responsible for 98.6% of the financial losses, amounting to $42,600,000 USD. This highlights a significant vulnerability and impact that could be associated with these functions.

BSC in 2021 observed that `transferOwnership` functions, while only comprising 25% of the attacks, led to 70.6% of the financial losses ($253,000,000 USD). The following year, `verifyProof` functions, accounting for a third of the attacks, disproportionately accumulated 85.9% of the losses ($586,000,000 USD), pointing to their critical security implications.

In Ethereum, the year 2020 saw `deposit` functions involved in half of the attacks, yet they resulted in a slightly higher proportion of losses at 55.9% ($25,000,000). By 2021, `transferOwnership` functions, although occurring in just 14.3% of cases, caused 51.3% of the losses ($273,000,000 USD). Similarly, `mint` functions that year were responsible for 32.1% of the losses ($171,000,000 USD) against a 28.6% occurrence rate. In 2022, `initialize` and `execute` functions led to losses of 48.6% ($190,000,000 USD) and 46.3% ($181,000,000 USD), respectively, each occurring in 25% of cases. The following year, 2023, saw `deposit` functions, representing half the attacks but accumulating 96.3% of the losses ($197,000,000 USD). In 2024, `calculateAmount` and `vote` functions, each involved in a third of the incidents, were responsible for 57.7% ($26,379,000 USD) and 37.7% ($17,230,071 USD) of the losses, respectively.

Polygon in 2021 also showed a marked disparity, with `transferOwnership` functions involved in half of the attacks yet accounting for 81.4% of the losses ($85,000,000 USD).

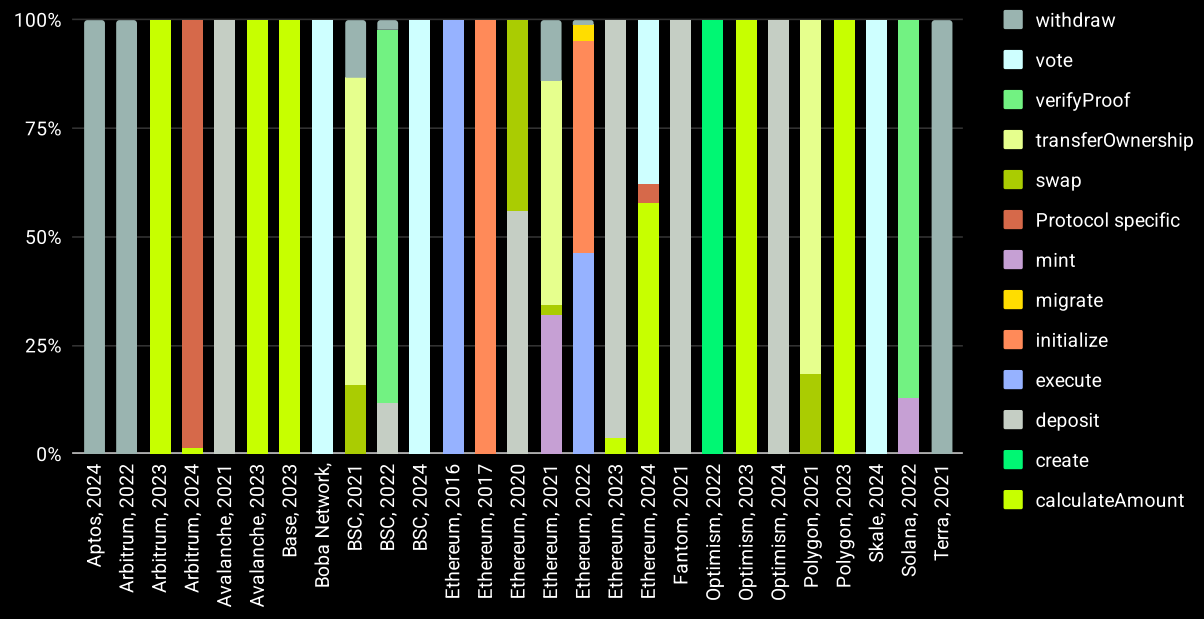

Figure 166: Loss caused by type of function_per chain and year [percentage]

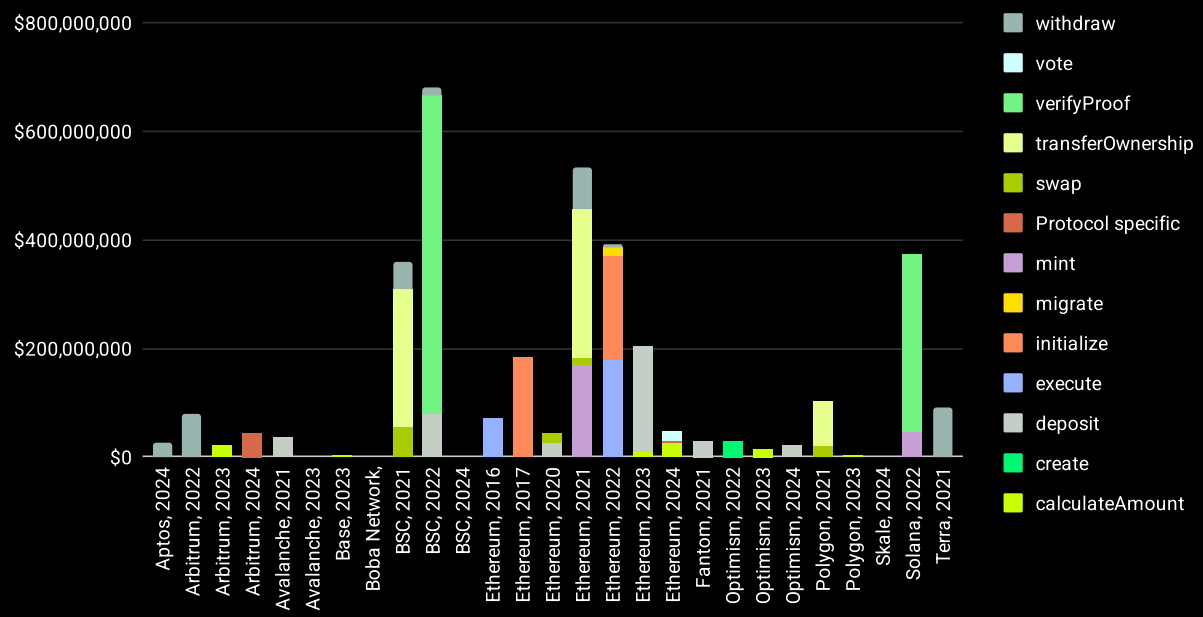

Figure 167: Loss caused by type of function per chain and year [USD]

Type of Functions vs Types of Attacks

Figures 168 and 169 provide an insightful breakdown of the types of functions targeted in different kinds of attacks on blockchain protocols.

From the data presented in Figures 158 and 159, it's clear that only the types of attacks that directly interact with smart contract functions are included.

From the data presented, it's evident that for direct contract exploitation, the `withdraw` function is the most utilized, being involved in 28% of such attacks. This is followed by `deposit` functions at 16% and `initialize` functions at 12%. These functions are crucial in managing assets within the protocols, making them prime targets for attackers looking to exploit vulnerabilities for unauthorized asset transfers or alterations to protocol settings.

In the realm of governance attacks, the functions predominantly targeted are `execute` and `vote`. These functions are integral to the administration and decision-making processes within blockchain protocols, where malicious entities might manipulate outcomes or execute unauthorized changes.

For market manipulation attacks, there is an equal prominence of `withdraw`, `deposit`, and `calculateAmount` functions, each constituting 25% of such attacks. These functions are essential for adjusting holdings within the protocol and manipulating market dynamics, such as liquidity and pricing, to the attackers' advantage. The `swap` and `mint` functions, each at 12.5%, also play roles in these scenarios, often involved in recalculating values or generating assets as part of complex strategies to manipulate market conditions. The usage of these functions aligns logically with the nature of the attacks. Market manipulation typically requires the ability to move and recalibrate assets quickly, making functions that allow depositing, withdrawing, swapping, and recalculating amounts critical for executing such schemes effectively.

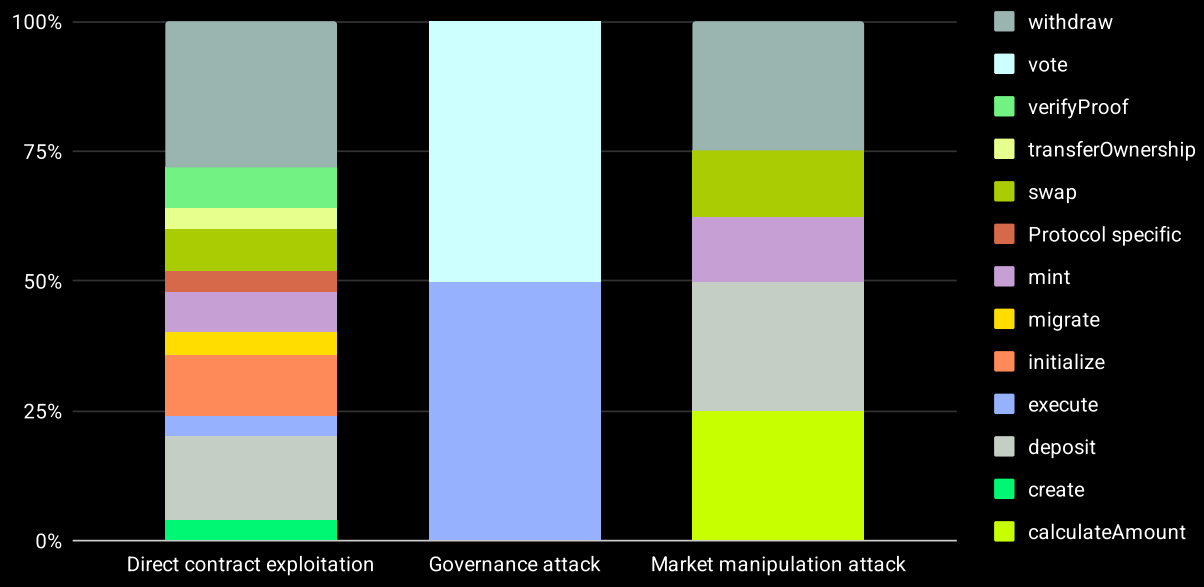

Figure 168: Number of type of function per chain [percentage]

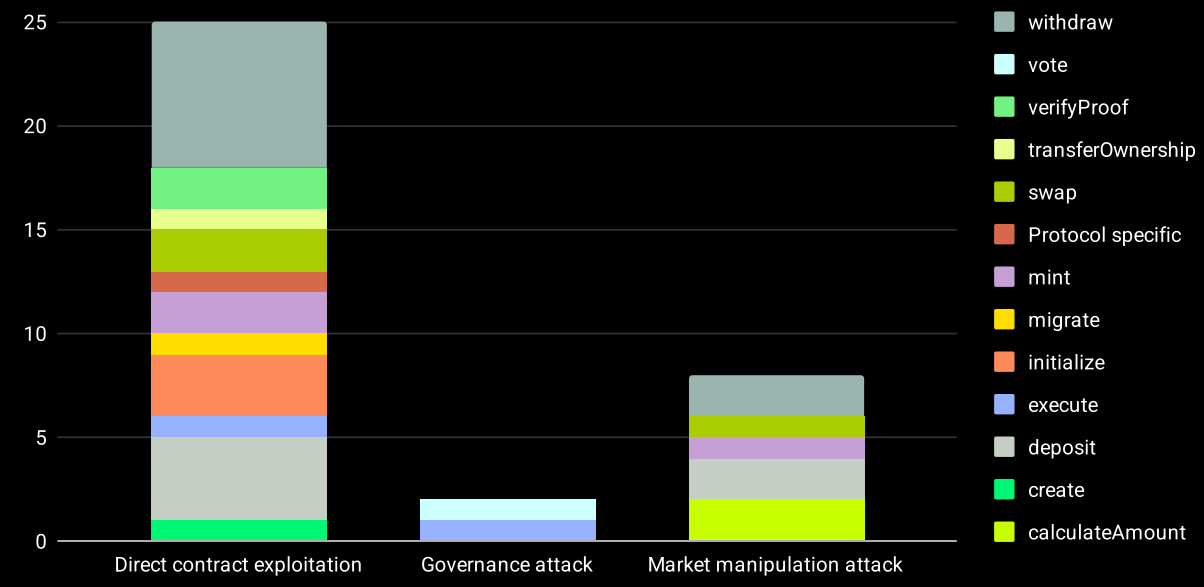

Figure 169: Number of type of function per chain [count]

Figures 170 and 171 delineate the distribution of financial losses by function type across various attack methods,

In the realm of direct contract exploitation, the `verifyProof` function stands out as the most significant contributor to financial losses, accounting for 31.1% ($912,000,000 USD) of the total. This occurs despite `verifyProof` being involved in only 8% of the attacks, indicating its critical vulnerability and high impact when compromised. `TransferOwnership` functions also exhibit a higher impact relative to their frequency, causing 20.8% ($611,000,000 USD) of the losses. Conversely, withdraw functions, despite being the most attacked, result in a relatively lower proportion of financial damage at 9.3% ($272,500,000 USD).

In governance attacks, `execute` functions prove particularly damaging, responsible for a significant 91.3% ($181,000,000 USD) of the financial losses. This highlights their critical role within governance mechanisms and the substantial impact when such functions are exploited.

For market manipulation attacks, `calculateAmount` functions lead to most financial losses, totaling 29.6% ($74,523,000 USD), which is slightly higher than their occurrence rate of 25%. This suggests that attacks leveraging these functions can manipulate financial calculations to the attackers' advantage. Similarly, `withdraw` functions also result in a greater loss than their occurrence rate, with 27% ($68,000,000 USD) of the losses against a 25% frequency, indicating their pivotal role in the execution of market manipulation strategies.

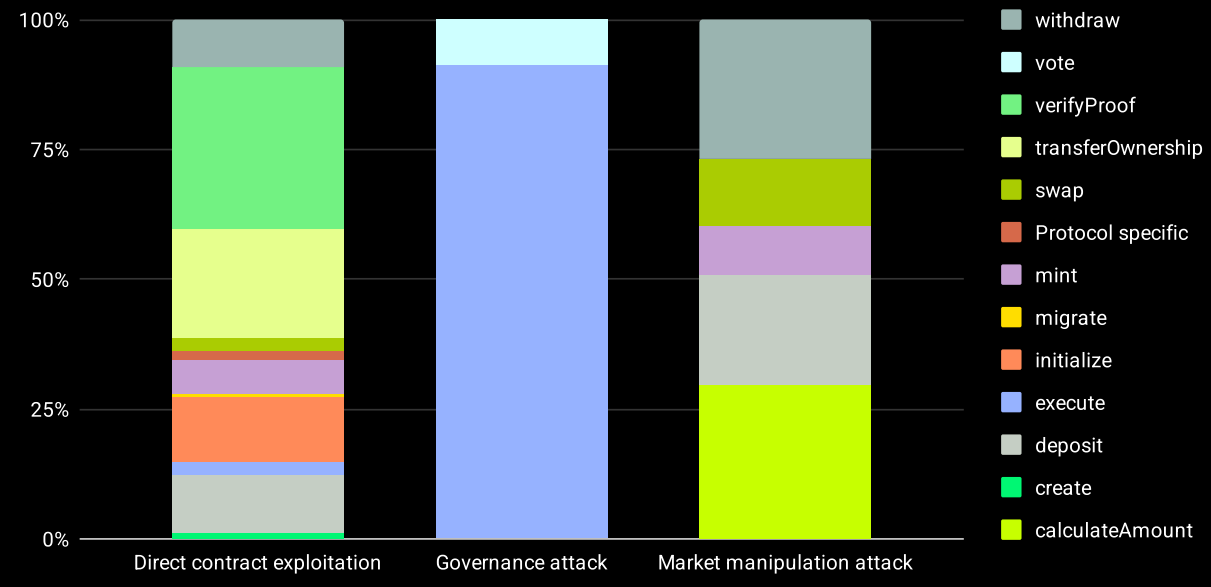

Figure 170: Loss caused by type of function per chain [percentage]

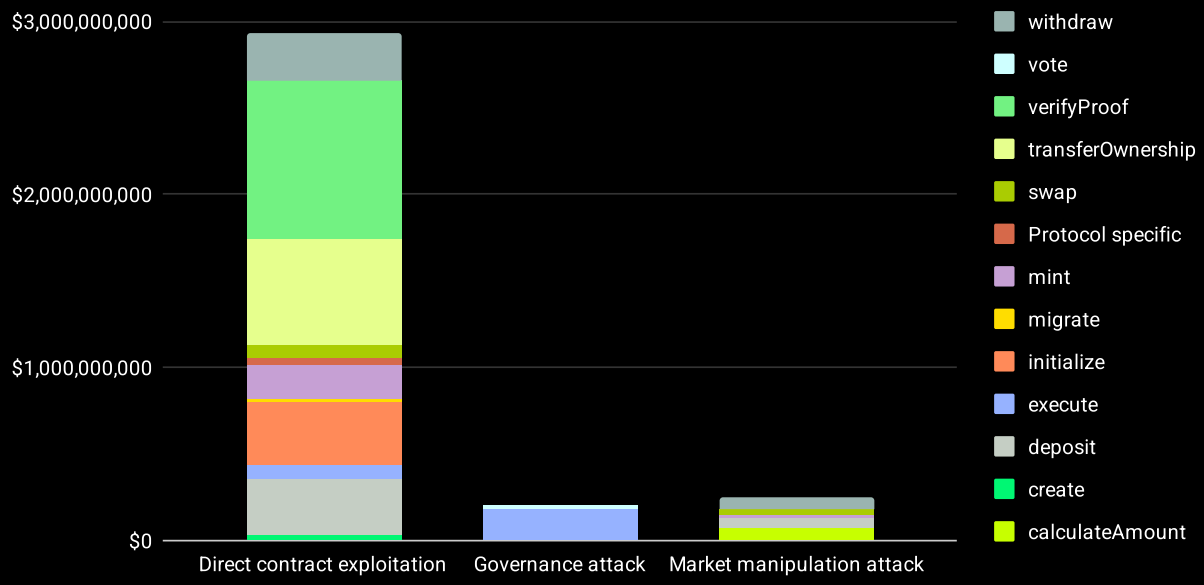

Figure 171: Loss caused by type of function per chain [USD]

Figures 172 and 173 provide a detailed breakdown of the types of functions targeted in various attacks, categorized by year and the nature of the exploitation.

In the realm of direct contract exploitation, the distribution of attacks varied annually, reflecting a shift in attacker focus over time. In 2020, the attacks were evenly split between `swap` and `deposit` functions. By 2021, `withdraw` functions became predominant, accounting for 50% of the attacks. In 2022, the focus was shared equally between `withdraw` and `verifyProof` functions, each with a 22.2% rate of occurrence. The following year, 2023, saw `deposit` functions primarily used to execute attacks. Moving into 2024, the attacks were evenly split between `withdraw` functions and those specific to the protocol.

Governance attacks also showed evolution over time. The initial attack in 2022 involved an `execute` function, while by 2024, the attacks shifted to predominantly involve a `vote` function.

Market manipulation attacks demonstrated a variety of targeted functions. In 2021, `withdraw` functions were most exploited, constituting 40% of these attacks, with `swap`, `mint`, and `deposit` functions each contributing to 20% of the incidents. By 2023, `calculateAmount` functions took center stage in these types of attacks. In 2024, `calculateAmount` functions continued to be a focal point, responsible for half of the market manipulation attacks, with the remaining half due to `deposit` functions.

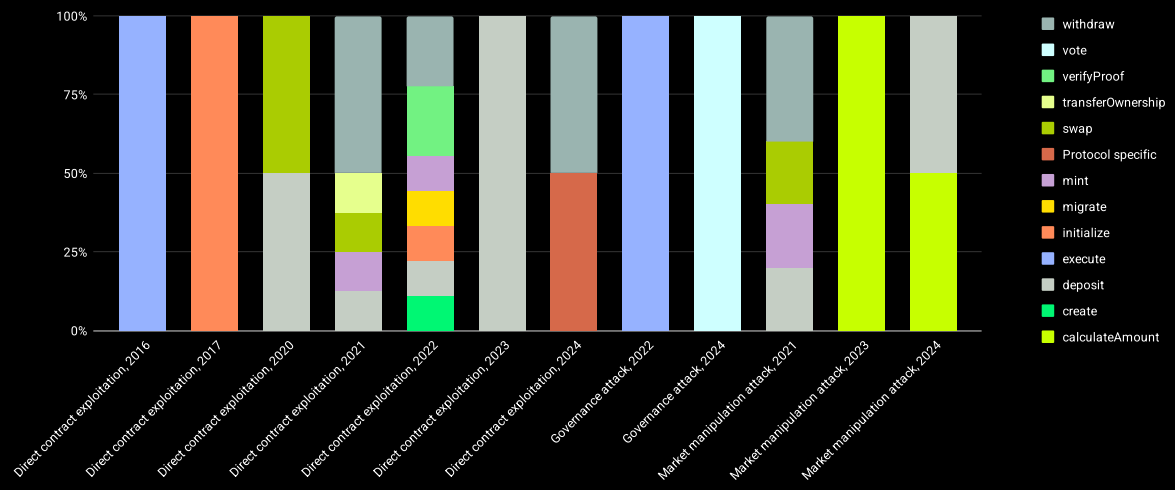

Figure 172: Number of type of function_per chain and year [percentage]

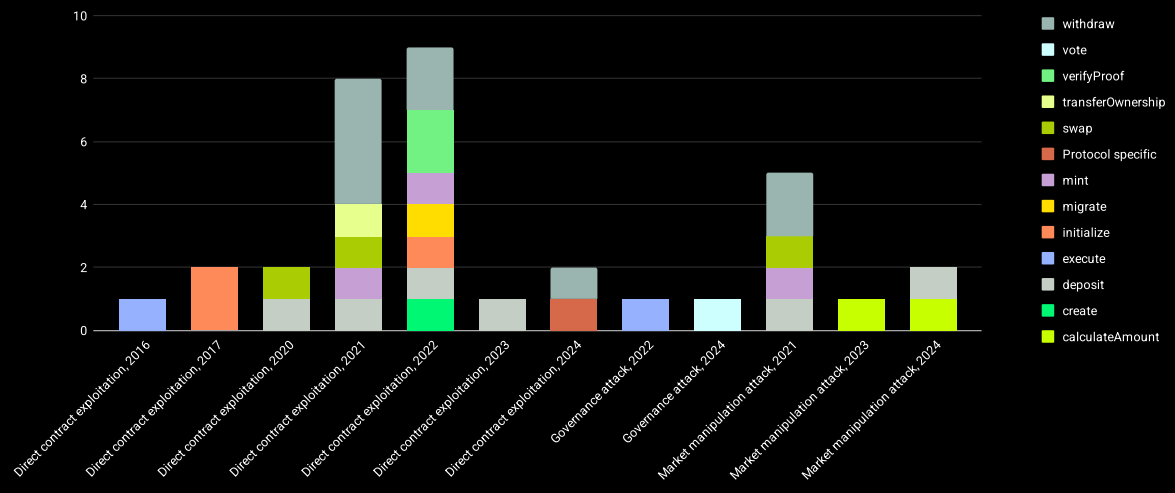

Figure 173: Number of type of function per chain and year [count]

Figures 174 and 175 illustrate the distribution of financial losses by year, type of attack, and type of function.

In 2020, in direct contract exploitation, the `deposit` function was responsible for 55.9% of the financial losses, totaling $25,000,000 USD, even though it accounted for 50% of the attacks. This shows a slightly higher impact relative to its frequency.

The following year, 2021, saw the `transferOwnership` function causing a disproportionately high amount of damage, 61.6% ($611,000,000 USD) of the total losses, despite representing only 12.5% of the attacks. `Mint` functions also inflicted slightly more financial damage than their occurrence would suggest, 14.8% ($147,000,000 USD) versus an occurrence rate of 12.5%.

In 2022, the `verifyProof` function emerged as a significant contributor to financial losses in direct contract exploitation, responsible for 66.3% ($912,000,000 USD) of the total, despite being involved in only 22.2% of the attacks. `Initialize` functions also led to more losses than expected, with 13.8% ($190,000,000 USD) of the financial damage against an 11.1% occurrence rate. By 2024, protocol-specific functions, while constituting 50% of the attacks for that year, led to 63.7% ($44,700,000 USD) of the losses.

In the context of market manipulation attacks in 2021, `withdraw` functions caused 43.2% ($68,000,000 USD) of the losses, higher than their 40% occurrence rate. `Deposit` functions also resulted in more loss than their occurrence, 21.6% ($34,000,000 USD) against a rate of 20%. Fast forward to 2024, `calculateAmount` functions also led to greater losses than their involvement rate, accounting for 57.4% ($27,000,000 USD) of the losses compared to a 50% rate of attack occurrence.

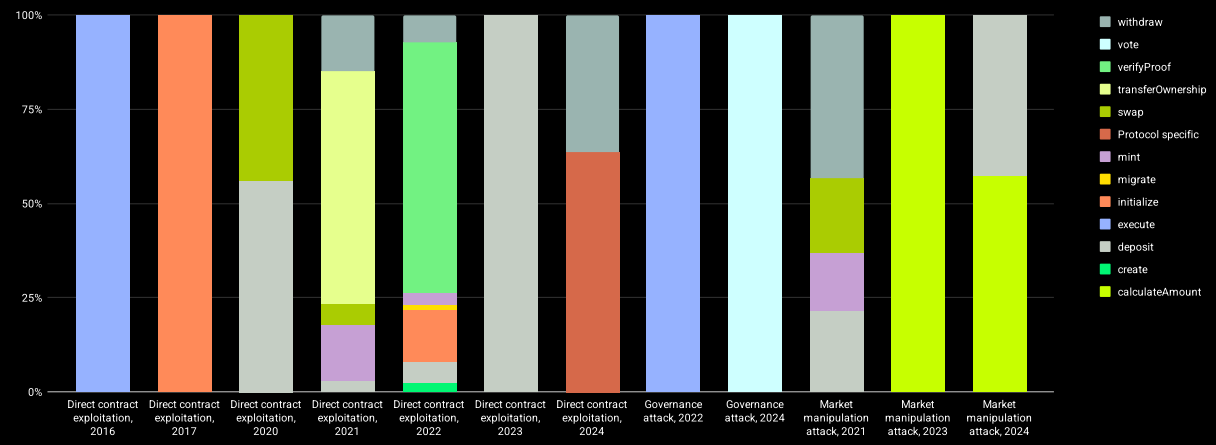

Figure 174: Loss caused by type of function per chain and year [percentage]

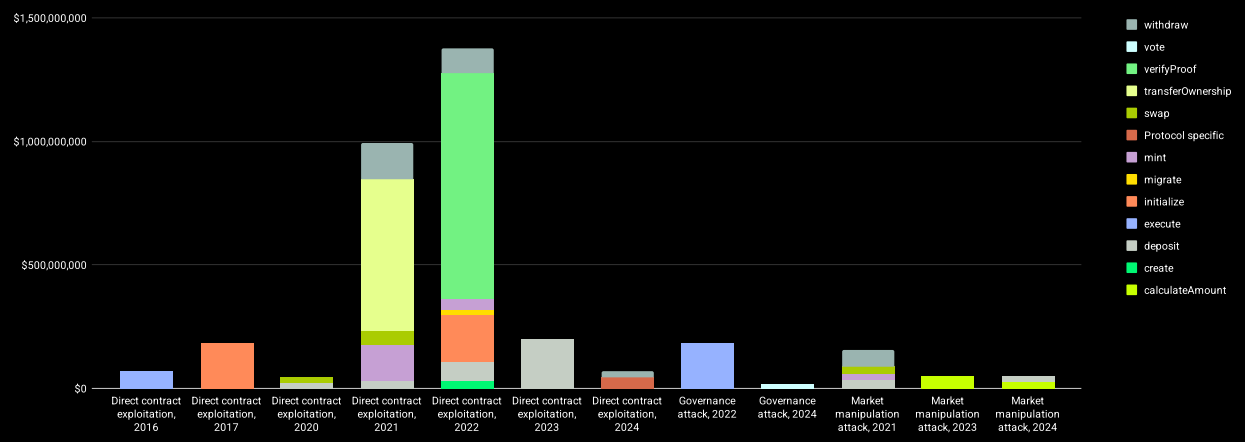

Figure 175: Loss caused by type of function per chain and year [USD]

Type of Functions vs Protocols

Figures 176 and 177 provide a detailed look at the distribution of attacks by type of function across various protocols.

`Withdraw` functions have emerged as the primary attack vector in protocols like Derivatives, DEX Aggregators, and Liquid Staking, where these functions facilitate unauthorized asset transfers. `Execute` functions, crucial for executing specific commands or contract clauses, have been targeted in Algo-Stables and Services, affecting the core operations of these protocols.

`Migrate` functions, which are vital during protocol upgrades or transitions, have been exploited in Launchpads, posing risks during critical update phases. `Mint` functions, used for creating new tokens or assets, have been the attack focus in CDPs (Collateralized Debt Positions), while `vote` functions, which are essential for governance decisions, have been compromised in Chains. `Initialize` functions, which set initial parameters for contracts, have been the primary attack route in Wallets.

In the case of Bridges, `verifyProof` functions, crucial for validating cross-chain transactions, have constituted 40% of the attacks. DEXes have seen `swap` functions, integral to trading operations, as the main exploit target, also making up 40% of the attacks. For Lending protocols, `deposit` functions have been heavily targeted, making up 57.1% of the attacks, due to their role in managing user deposits and interactions with the protocol's liquidity.

Liquidity managers face attacks divided equally between `mint` and `withdraw` functions, affecting both the creation of new tokens and the withdrawal of funds. In Yield protocols, `withdraw` functions account for 50% of the attacks, emphasizing the vulnerabilities associated with asset withdrawals. Yield Aggregators see an even split between attacks on `withdraw` and `swap` functions, impacting both asset management and exchange functionalities.

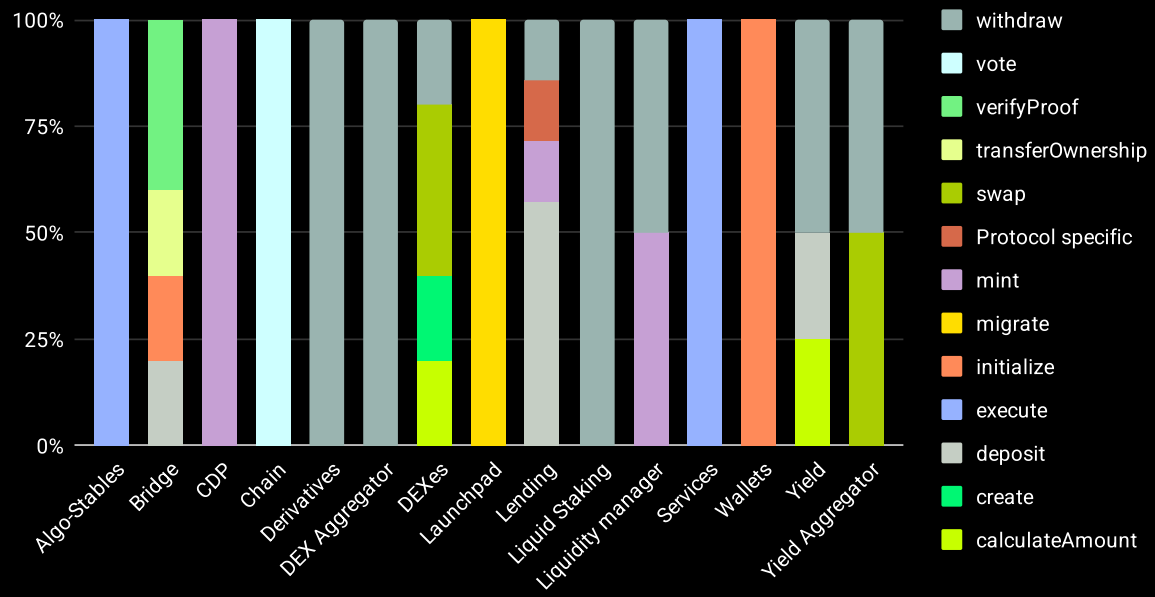

Figure 176: Number of type of function per type of protocol [percentage]

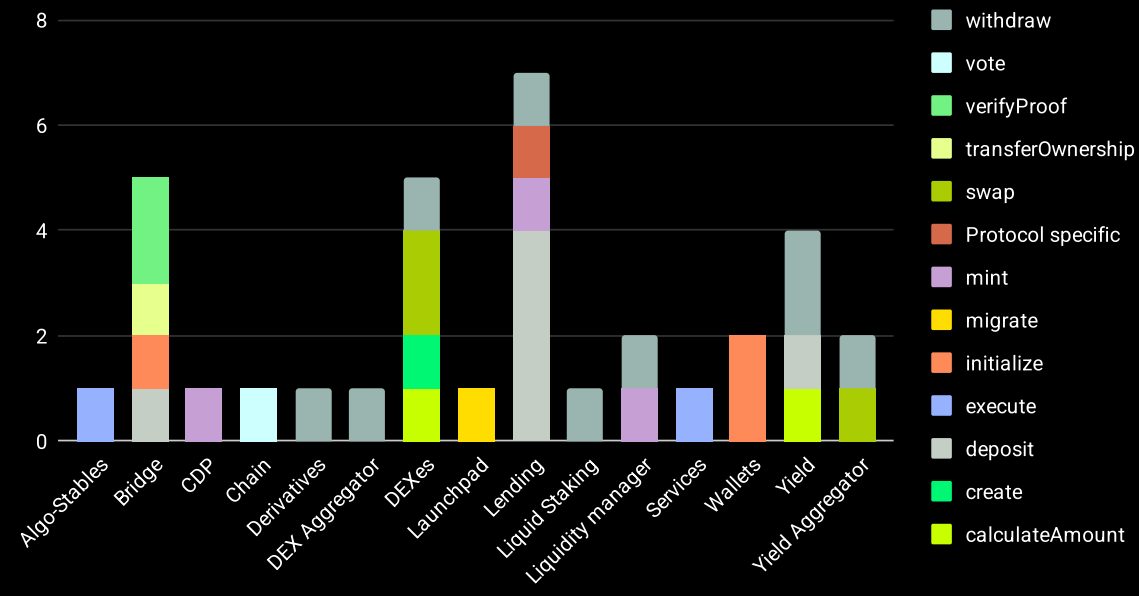

Figure 177: Number of type of function per type of protocol [count]

Figures 178 and 179 provide a detailed breakdown of financial losses by type of function and protocol.

In Bridges, the function primarily responsible for the losses aligns with the most frequently attacked function. `VerifyProof`, crucial for cross-chain operations, not only is the most attacked but also results in higher losses than its occurrence, with 50.9% ($912,000,000 USD) of the total financial impact against a 40% occurrence rate. `TransferOwnership` functions also play a significant disruptive role, accounting for 34.1% of the financial losses ($611,000,000 USD) despite only a 20% rate of occurrence, indicating their critical security implications when compromised.

In DEXes, the `swap` function, integral to trading operations, is both the most common by occurrence and the main cause of financial loss, responsible for 44.9% of the losses ($88,400,000 USD), which is slightly above its occurrence rate of 40%. `CalculateAmount` functions also lead to greater losses than their occurrence rate would suggest, with 24.1% ($47,523,000 USD) against a 20% occurrence rate, reflecting their importance in financial calculations within these platforms.

For Lending protocols, while `deposit` functions are the primary cause of financial loss, the percentage of loss is slightly less than their occurrence, at 56.7% ($276,000,000 USD) against 57.1%. On the other hand, `mint` functions, which are less frequently attacked, cause disproportionately higher losses at 30.2% ($147,000,000 USD) compared to their 14.3% occurrence rate, highlighting a significant vulnerability.

In Yield protocols, the distribution of financial loss closely mirrors the rate of occurrence, with `deposit` functions causing a bit more loss than their occurrence rate (26.7% or $30,000,000 USD versus 25%). However, `withdraw` functions remain the leading cause of both loss and occurrence, comprising 49.3% ($55,500,000 USD) of the financial impact.

Finally, in Yield Aggregators, despite an equal distribution of attacks across functions, `withdraw` functions dominate the financial losses, accounting for an overwhelming 80.2% ($80,000,000 USD) of the total, underscoring their critical financial impact when exploited.

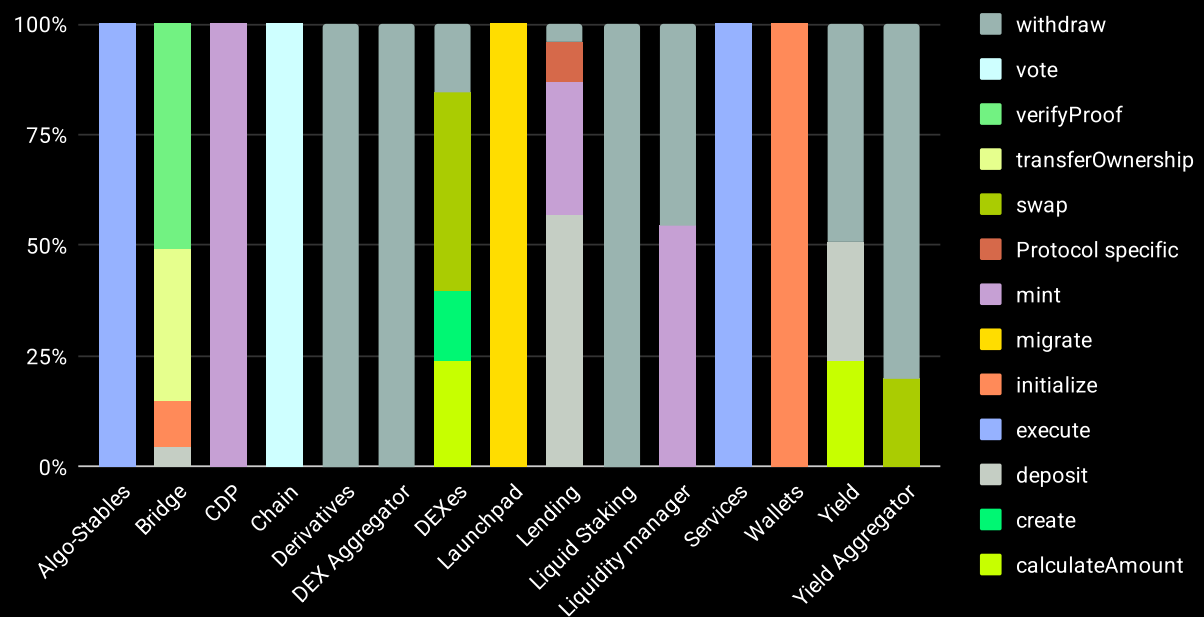

Figure 178: Loss caused by type of function per type of protocol [percentage]

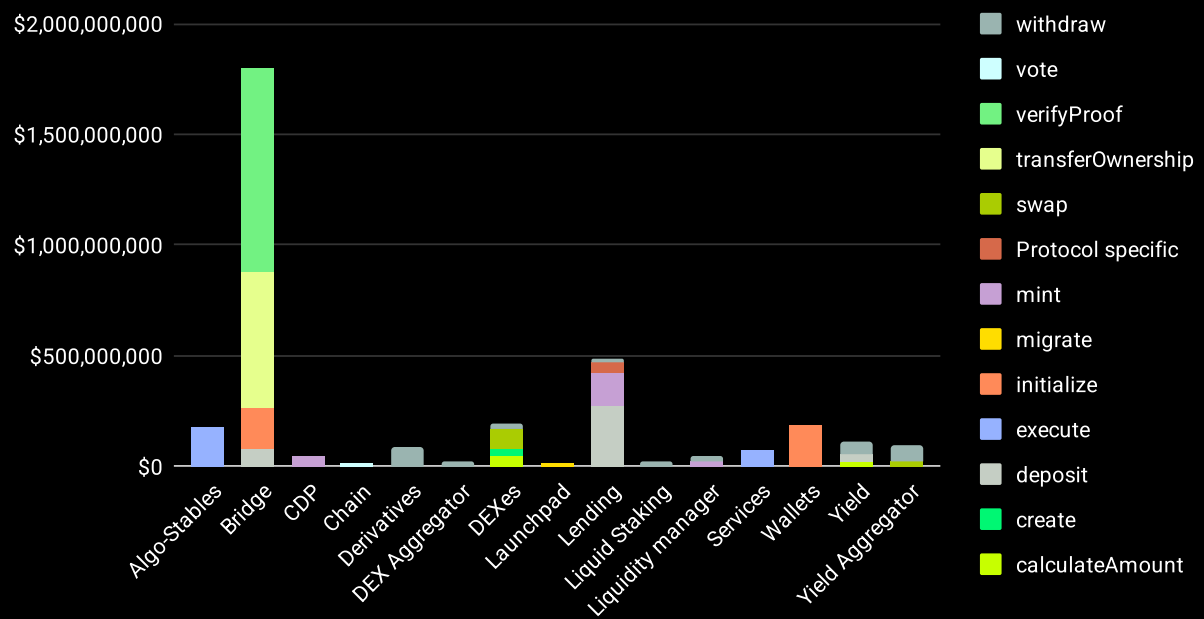

Figure 179: Loss caused by type of function per type of protocol [USD]

Figures 180 and 181 illustrate the distribution of attacks by type of function across various protocols and over different years.

In the case of Bridges, the attack dynamics shifted over the years. In 2021, the primary function exploited was `transferOwnership`, indicating a focus on gaining control over protocol governance. By 2022, the focus shifted to `verifyProof` functions, which made up 50% of the attacks, reflecting an emphasis on exploiting validation mechanisms essential for cross-chain interactions.

DEXes also showed a progression in the types of functions targeted. In the earliest recorded year, 2021, `swap` functions were predominantly attacked, making up 66.7% of the incidents, reflecting their critical role in asset exchanges within these platforms. In 2022, the attacks were due to a `create` function, shifting in 2023 to attacks primarily exploiting `calculateAmount` functions, which are crucial for determining the protocol's values.

Lending protocols experienced a variation in the targeted functions over the years. Initially, in 2020, attacks focused on `deposit` functions. By 2021, the attacks were evenly distributed among `withdraw`, `mint`, and `deposit` functions, indicating a broader range of vulnerabilities being exploited. The focus returned to deposit functions solely in 2023, but by 2024, it was split between `deposit` and a protocol-specific function, suggesting an evolution in attack strategies to include more sophisticated or tailored approaches.

Yield protocols transitioned from primarily being attacked via `withdraw` functions, which accounted for 66.7% of the attacks in 2021, to solely `calculateAmount` functions by 2024. This change underscores a shift towards exploiting functions critical for financial calculations and manipulations within these protocols.

Yield Aggregators saw a shift from being hacked by a `swap` function in 2020 to a `withdraw` function in 2022, highlighting the ongoing vulnerability of functions associated with asset management and reallocation.

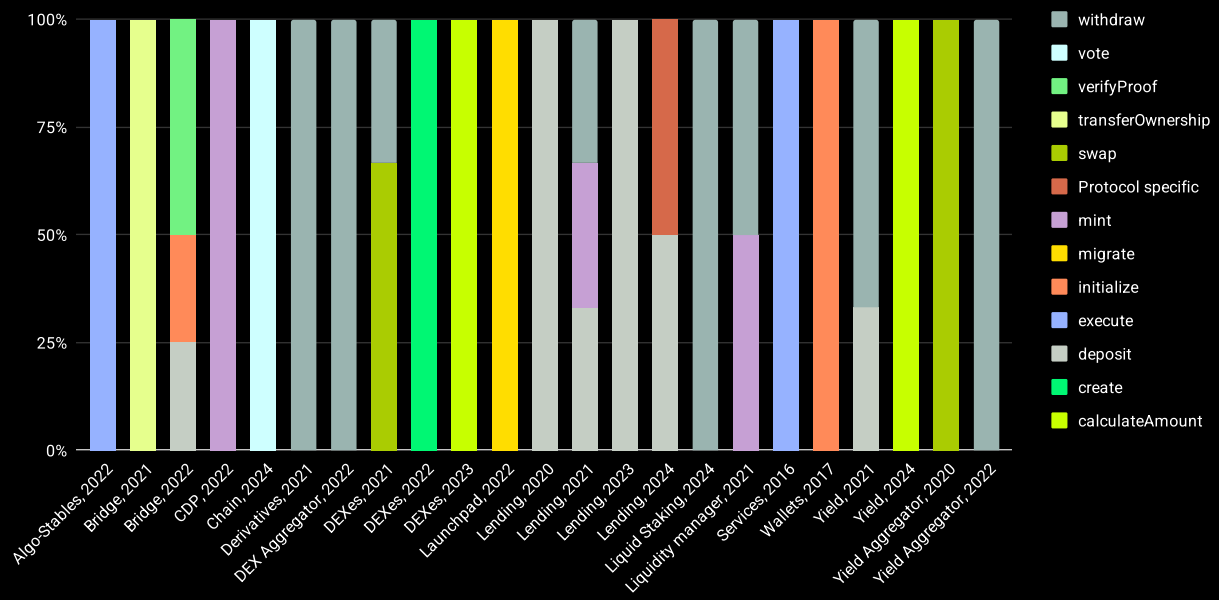

Figure 180: Number of type of function per type of protocol and year [percentage]

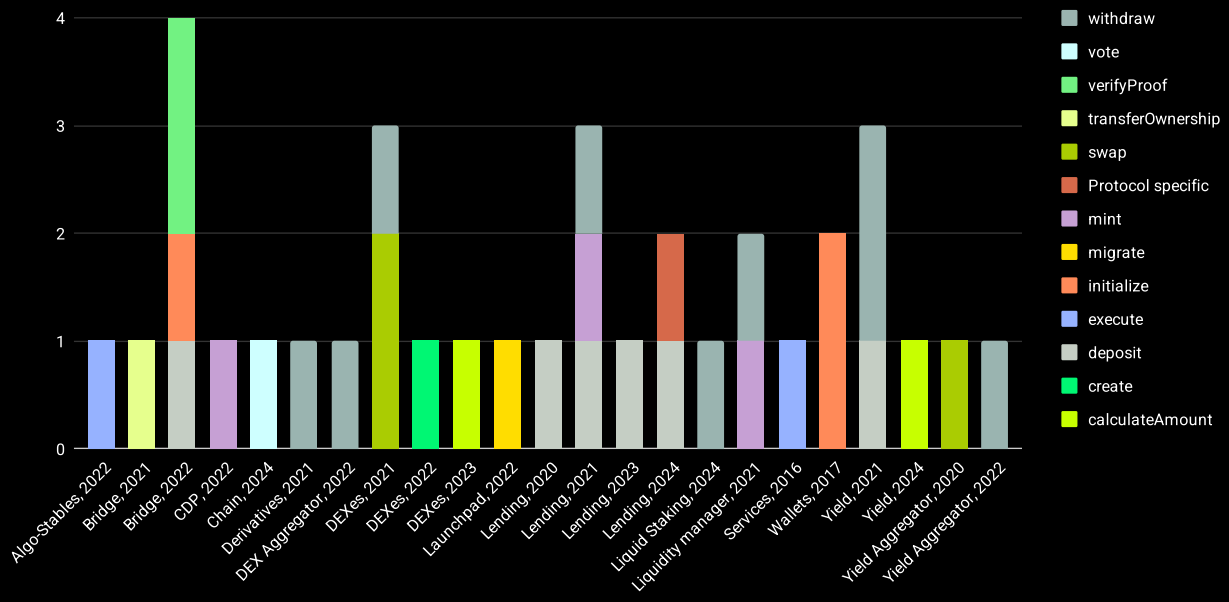

Figure 181: Number of type of function per type of protocol and year [count]

Figures 182 and 183 present an in-depth analysis of the financial impact associated with specific types of functions within various protocols through the years.

In Bridges during 2023, the `verifyProof` function was particularly damaging, accounting for 77.2% of the stolen amount, significantly higher than its occurrence rate of 50%. This indicates a high financial impact from attacks exploiting this function.

In DEXes for 2021, the `swap` function, while constituting 66.7% of the attacks, was responsible for an even larger share of financial losses at 74.3% ($88,400,000 USD). This overrepresentation in losses highlights the `swap` function's critical role in asset exchanges within DEXes and its vulnerability to exploitation.

For Lending protocols in the same year, `mint` functions, involved in 33.3% of the attacks, led to a disproportionate 73.6% ($147,000,000 USD) of the total losses. This underscores the significant financial risks associated with vulnerabilities in functions that handle the creation of new assets. By 2024, protocol-specific functions also demonstrated higher financial damage than their occurrence rate, accounting for 69.1% ($44,700,000 USD) of the losses while being involved in 50% of the attacks.

Liquidity managers saw `mint` functions responsible for 54.5% ($24,000,000 USD) of the losses against a 50% rate of occurrence, indicating that these functions, too, are particularly susceptible to high-value exploits.

In Yield protocols, during 2021, while `withdraw` functions were the primary cause of loss at 64.9% ($55,500,000 USD), this was slightly below their occurrence rate of 66.7%. On the other hand, `deposit` functions caused more financial damage than anticipated, 35.1% ($30,000,000 USD) compared to a 33.3% occurrence rate.

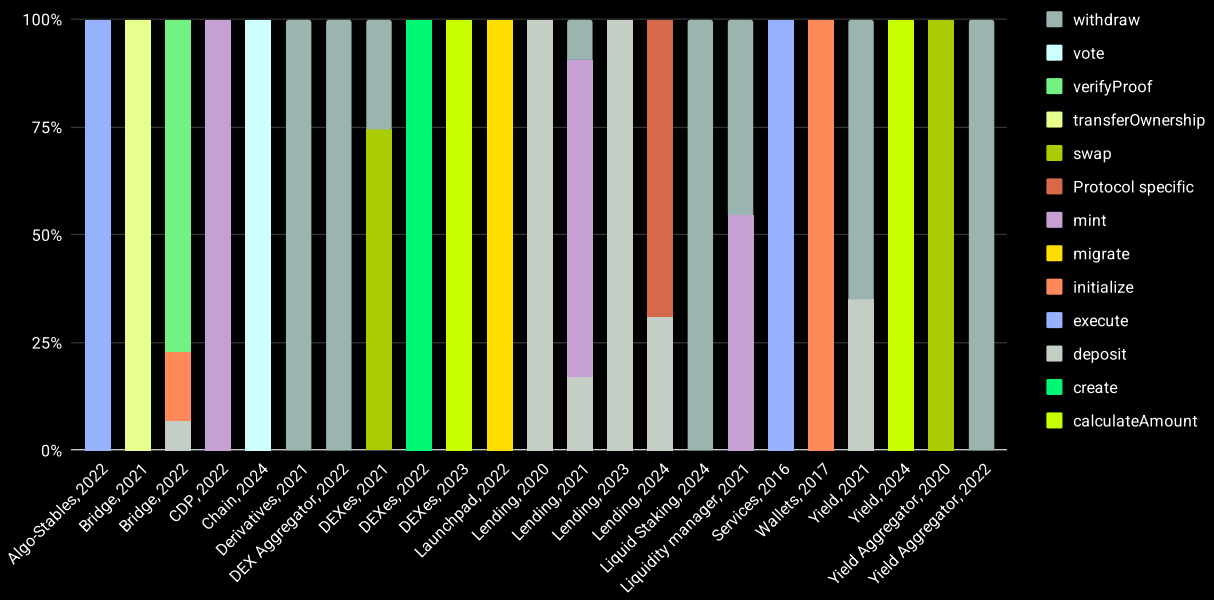

Figure 182: Loss caused by type of function per type of protocol and year [percentage]

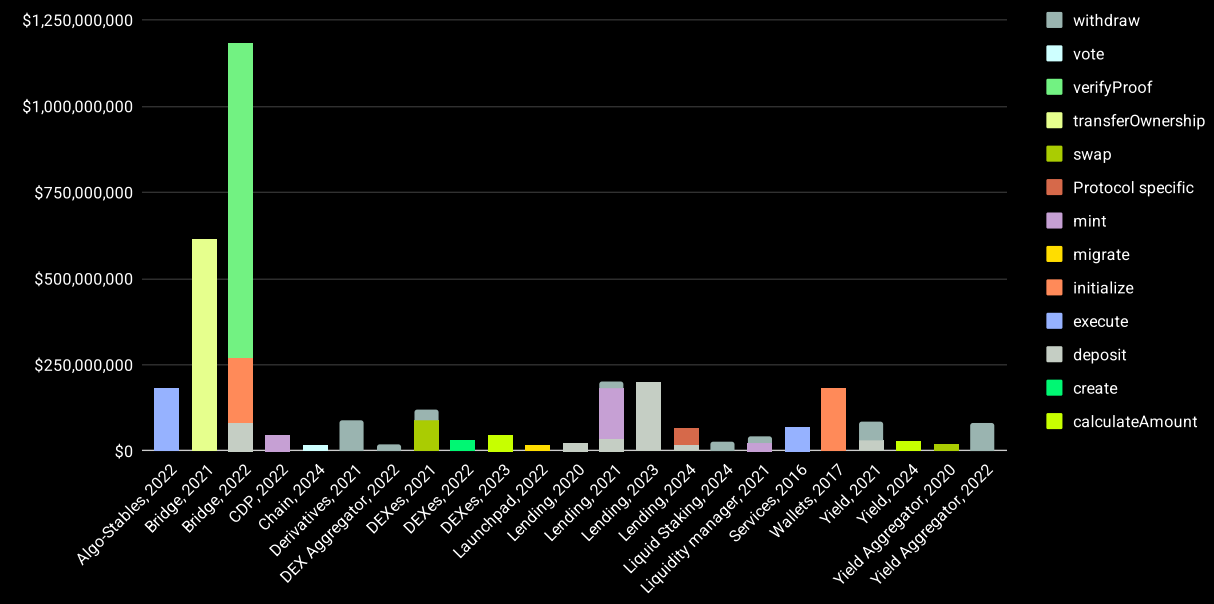

Figure 183: Loss caused by type of function per type of protocol and year [USD]

WERE THEY AUDITED?

Figures 184 and 185 shed light on the role of security audits in preventing attacks on blockchain protocols by examining the audit status of the protocols that were hacked.

Only 20% of the protocols that suffered attacks had undergone security audits. This relatively low percentage suggests that while audits were conducted, they may not have been sufficiently thorough or that the scope of the audits did not cover the eventual vectors of attack. Conversely, 24% of the hacked protocols had not been audited at all, highlighting a clear vulnerability and the increased risk of attacks associated with the absence of preemptive security measures.

A notable 56% of the incidents fall into the 'not applicable' (N/A) category, which includes rug pulls and off-chain attacks. These types of attacks often involve elements that are not directly related to the smart contract code itself. Rug pulls, for instance, involve malfeasance by insiders who misuse their access to the protocol's assets, a risk that traditional smart contract audits may not address.

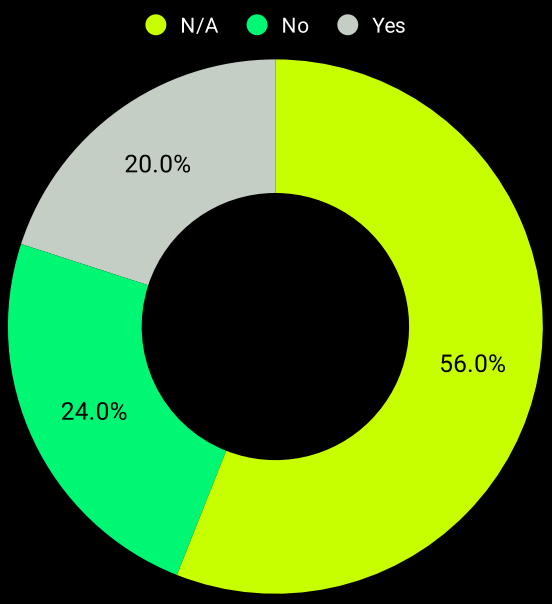

Figure 184: State of audition [percentage]

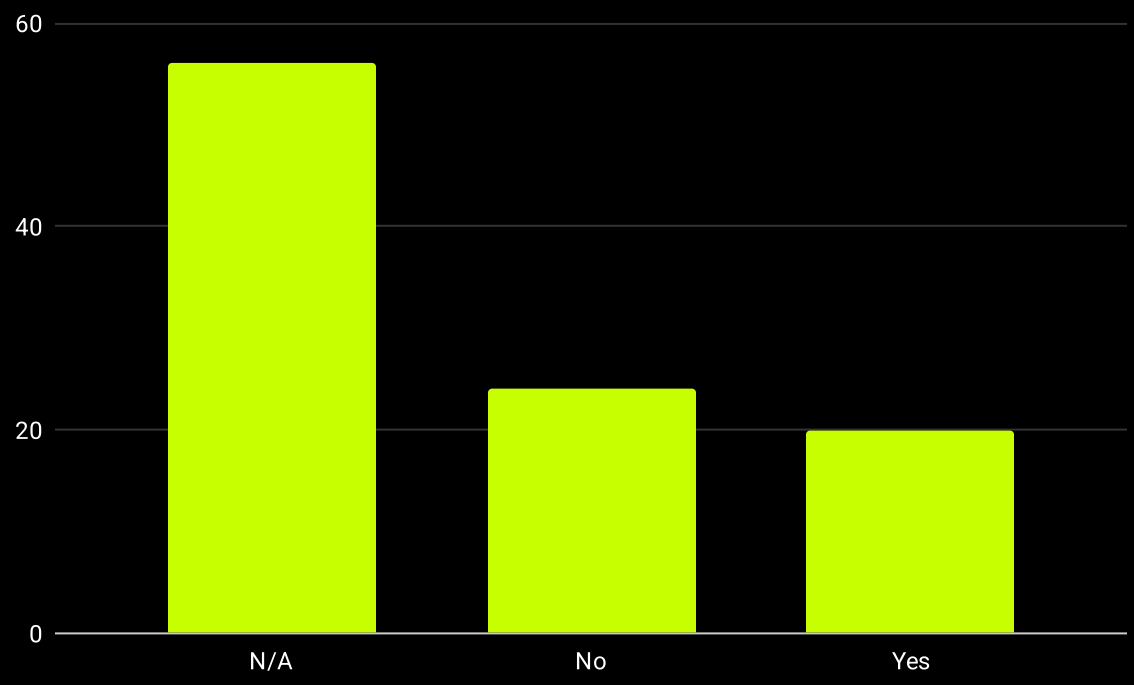

Figure 185: State of audition [count]

Figures 185 and 186 analyze the financial impact of attacks on blockchain protocols relative to their audit status.

The data reveals that audited protocols experience slightly lower financial losses in proportion to their occurrence rates. Despite representing 20% of the total attacked, these audited protocols accounted for only 10.8% of the total financial losses, totaling $1,159,523,000 USD. This suggests that while audits do not completely insulate protocols from attacks, they appear to mitigate the severity of losses when breaches do occur.

On the other hand, protocols without audits showed a higher propensity for loss relative to their occurrence. These protocols constituted 24% of the attacks but were responsible for a higher proportion of the losses, 25.7% or $2,770,597,071 USD. This underscores the increased risk and potential financial impact associated with lacking preemptive security reviews.

For the category labeled not applicable, which includes scenarios such as rug pulls and off-chain attacks where traditional smart contract audits might not apply, the losses were significantly higher. This group accounted for 56% of the occurrences yet was responsible for 63.5% of the total financial losses, amounting to $6,843,010,839 USD. This substantial figure highlights the broader scope of security considerations beyond smart contract vulnerabilities, pointing to the necessity of comprehensive risk management strategies that address both on-chain and off-chain risks.

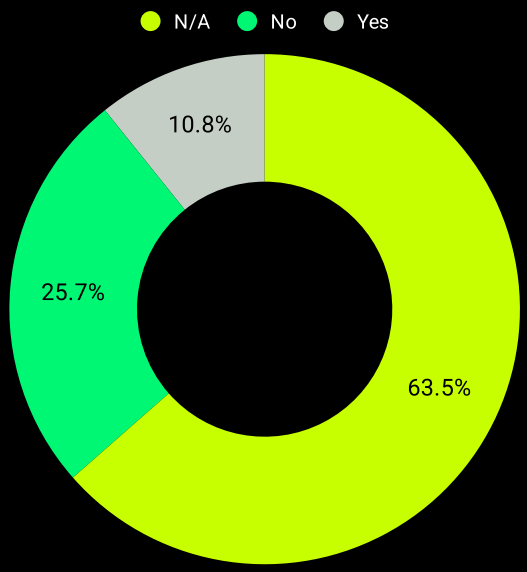

Figure 185: Loss caused per state of audition [percentage]

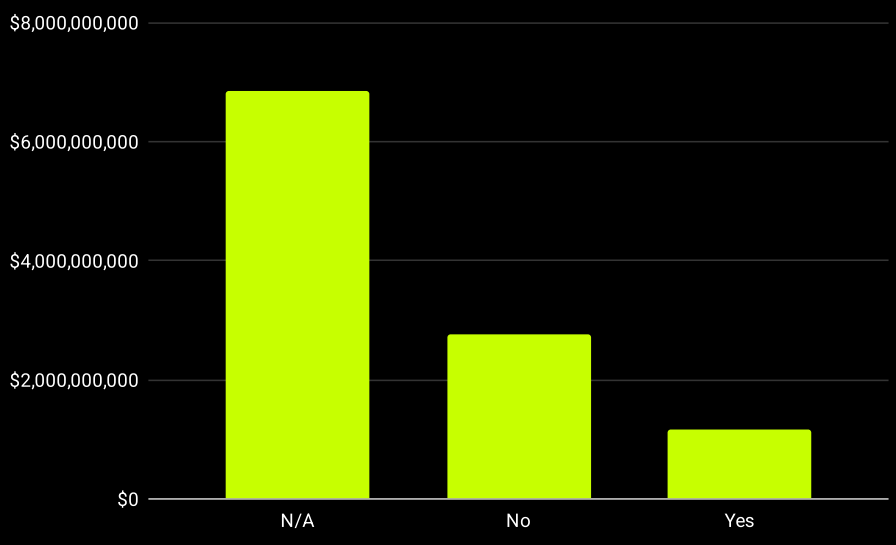

Figure 186: Loss caused per state of audition [count]

Figures 187 and 188 provide an analysis of the audit status of blockchain protocols over time and how it correlates with the incidence of hacks.

In the early years, the status of audits in relation to hacks is largely not applicable (N/A), such as in 2014, where all hacks fall into this category, a focus on types of attacks where audits are irrelevant (such as rug pulls or off-chain issues). In 2016, the scenario is mixed; one hack occurred in an audited protocol, and another was categorized as N/A.

The year 2017 marks a shift with all hacks occurring in audited protocols. However, in 2018 and 2019, the trend reverses back to all hacks being N/A.

By 2020, there's a diverse distribution, with 20% of hacks in audited protocols, 40% in non-audited, and another 40% being N/A. The year 2021 sees an increase in hacks against audited protocols to 28.6%, although this is still lower than the rates for non-audited (32.1%) and N/A (39.3%).

The trend in 2022 shows a decrease in hacks against audited protocols to 10%, while the incidence in non-audited protocols jumps to 50%, and N/A accounts for 40%. In 2023, however, there's a slight uptick in hacks against audited protocols to 11.8%, a drastic reduction in non-audited to 5.9%, and a significant increase in N/A to 82.4%.

By 2024, the analysis notes a further increase in attacks on audited protocols to 27.8%, a slight decrease in non-audited to 5.6%, while N/A accounts for 66.7% of the cases.

This data illustrates an increasing trend in hacks against audited protocols in the most recent year, alongside a sustained high level of attacks categorized as N/A since 2023. This suggests a growing challenge in ensuring the effectiveness of audits against evolving security threats and emphasizes the complexity of cybersecurity in blockchain technologies, where not all threats are mitigated by traditional smart contract audits.

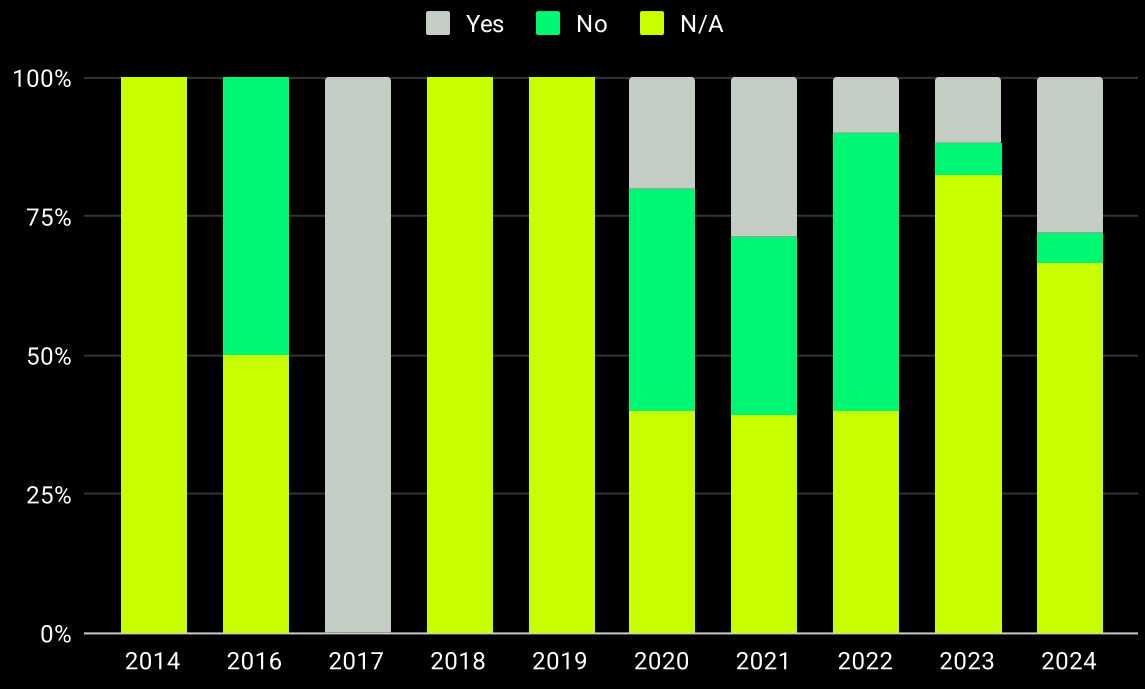

Figure 187: State of audition per year [percentage]

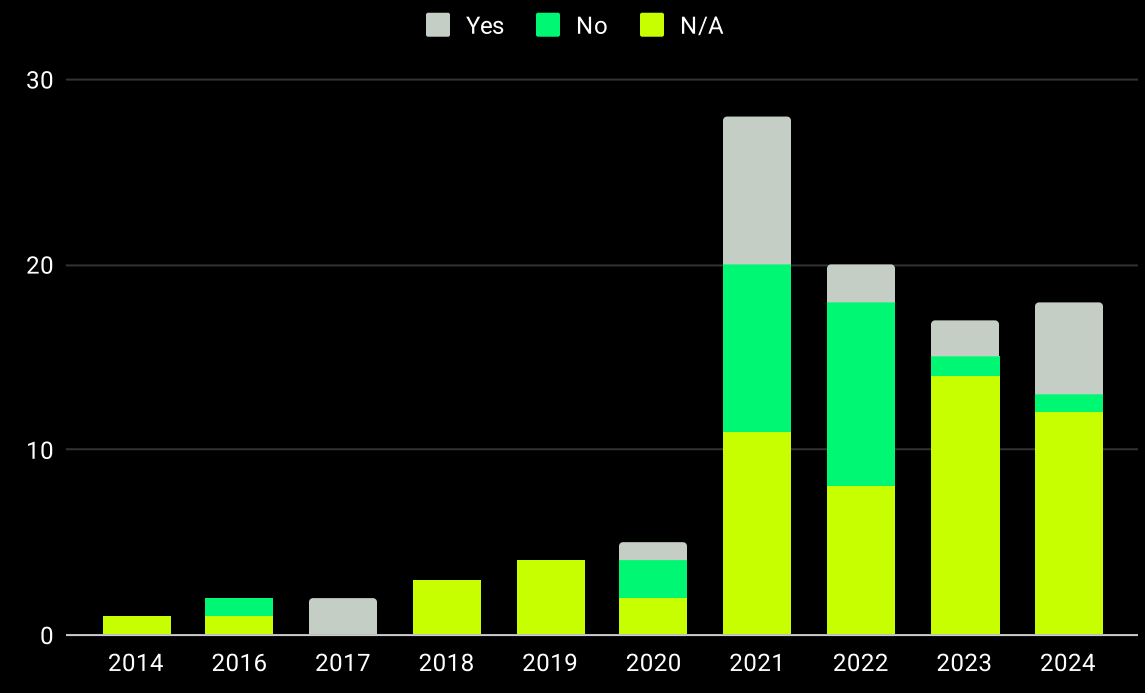

Figure 188: State of audition per year [count]

Figures 189 and 190 offer a comprehensive view of the financial impact of hacks on blockchain protocols over several years.

In 2016, the financial losses align closely with the occurrence rates across the categories. N/A type attacks, however, show a slightly higher financial impact, accounting for 50.7% ($72,000,000 USD) of the losses, compared to an occurrence rate of 50%.

By 2020, the disparity in financial impacts becomes more pronounced. Audited protocols, which made up 20% of the occurrences, were responsible for only 6.8% ($25,000,000 USD) of the losses. However, N/A attacks accounted for a disproportionately high 81% ($297,000,000 USD) of the losses, far exceeding their 40% occurrence rate. Not audited protocols caused 12.2% ($44,700,000 USD) of the losses against an occurrence rate of 40%.

In 2021, the trend shifts significantly with not audited protocols driving most of the financial damage, accumulating 52.1% ($1,132,800,000 USD) of the year's losses. Audited protocols, meanwhile, accounted for less financial loss than their occurrence would suggest, only 10.6% ($229,600,000 USD) against a 20% occurrence rate.

In 2022, losses from audited protocols slightly exceeded their occurrence rate at 10.7% ($341,800,000 USD) compared to 10%. Losses from not audited protocols decreased to 43.4% ($1,385,800,000 USD) against a 50% occurrence rate. Meanwhile, N/A attacks accounted for 45.9% ($1,465,500,000 USD) of losses, which is higher than their 40% occurrence rate.

In 2023, the financial impact of N/A increased to 74.6% ($1,068,045,951 USD) even though their occurrence was high at 82.4%. Audited protocols generated 17.1% ($244,523,000 USD) of the losses, higher than their 11.8% occurrence rate. Not audited protocols represented a smaller fraction of the losses at 8.4% ($120,000,000 USD) against a 5.9% occurrence rate.

By 2024, N/A attacks once again caused a significant portion of the financial damage, accounting for 88% ($1,128,164,888 USD) of the losses, which is much higher than their occurrence rate of 66.7%. Audited protocols resulted in 10.7% ($136,600,000 USD) of the losses, significantly less than their 27.8% occurrence rate. Not audited protocols contributed minimally to the financial losses at 1.3% ($17,297,071 USD) against a 5.6% occurrence rate.

The trend over the years suggests that N/A-type attacks are becoming increasingly damaging, highlighting an evolving landscape where the nature of threats may be outpacing traditional audit and security measures.

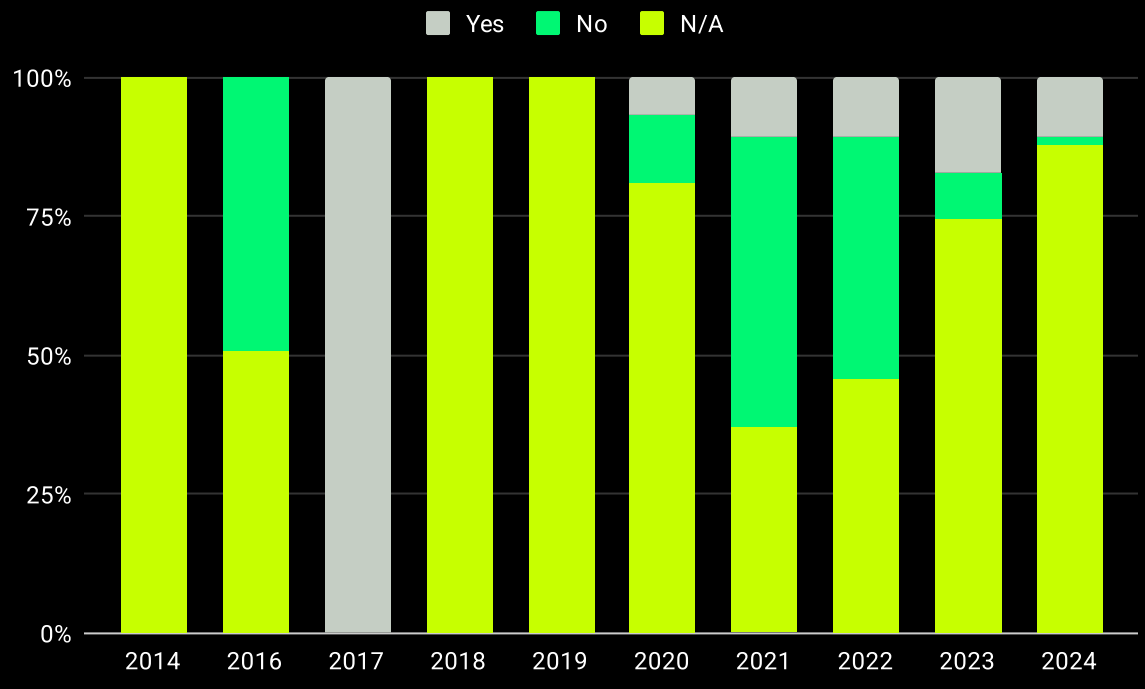

Figure 189: Loss caused per state of audition per year [percentage]

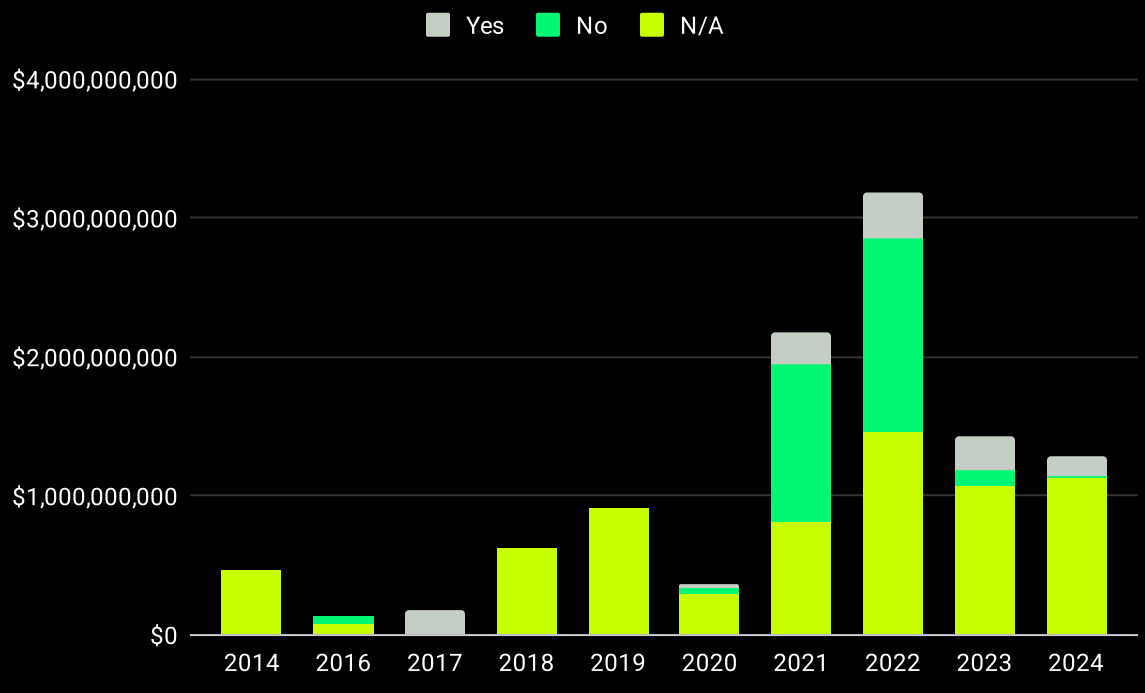

Figure 190: Loss caused per state of audition per year [USD]

Audited Protocols by Chain

Figures 191 and 192 delve into the audit status of protocols by chain, revealing a varied landscape in terms of security checks prior to breaches.

Notably, for several chains like Bitcoin, Bitcoin Cash, Blast, Dogechain, Linea, MonaCoin, Moonriver, Multi-chain attacks, NEM, and Tron, all protocols that were hacked fall into the N/A category.

On the other hand, certain chains show a lack of audits across all affected protocols. Boba Network, Skale, and Terra experienced hacks in protocols that had not been audited. Aptos stands out as the only chain where all hacked protocols had been audited.

The situation is mixed for other chains. Arbitrum shows a balanced approach, with half of the protocols being audited, one-third falling into the N/A category, and the remainder not audited. In Avalanche, the majority (60%) are N/A, with the rest having been audited. Base follows a similar pattern, with two-thirds in the N/A category and the remaining one-third audited.

BSC presents an even distribution among protocols that were not audited and those categorized as N/A, each constituting 44.4%, with the rest being audited. Ethereum has a majority (54.5%) in the N/A category, 23.6% audited, and the rest not audited. Fantom shows an equal split between audited and N/A categories, each at 50%.

Mixin reflects a division between not audited and N/A. On Optimism, 60% of the attacks are in the N/A category, and the rest involve audited protocols. Polygon shows 63.6% of the hacks categorized as N/A, while the remaining 36.4% are equally divided at 18.2% each for audited and not audited. Solana's distribution shows half of the protocols not audited and the other half evenly divided between audited and N/A.

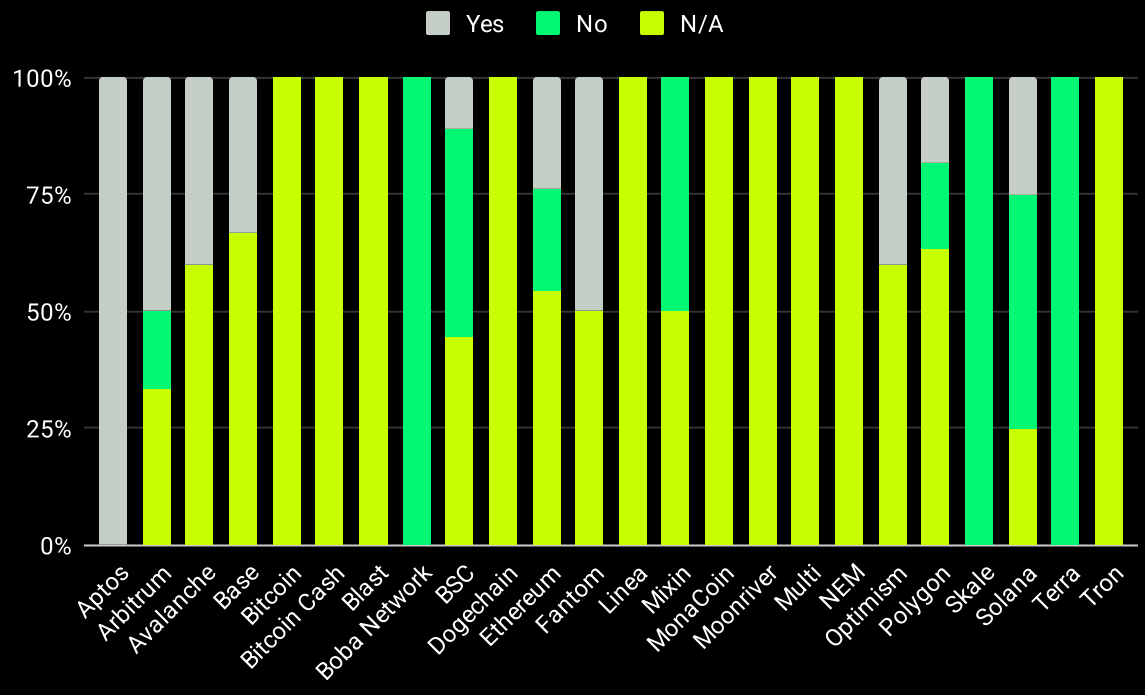

Figure 191: State of audition per chain [percentage]

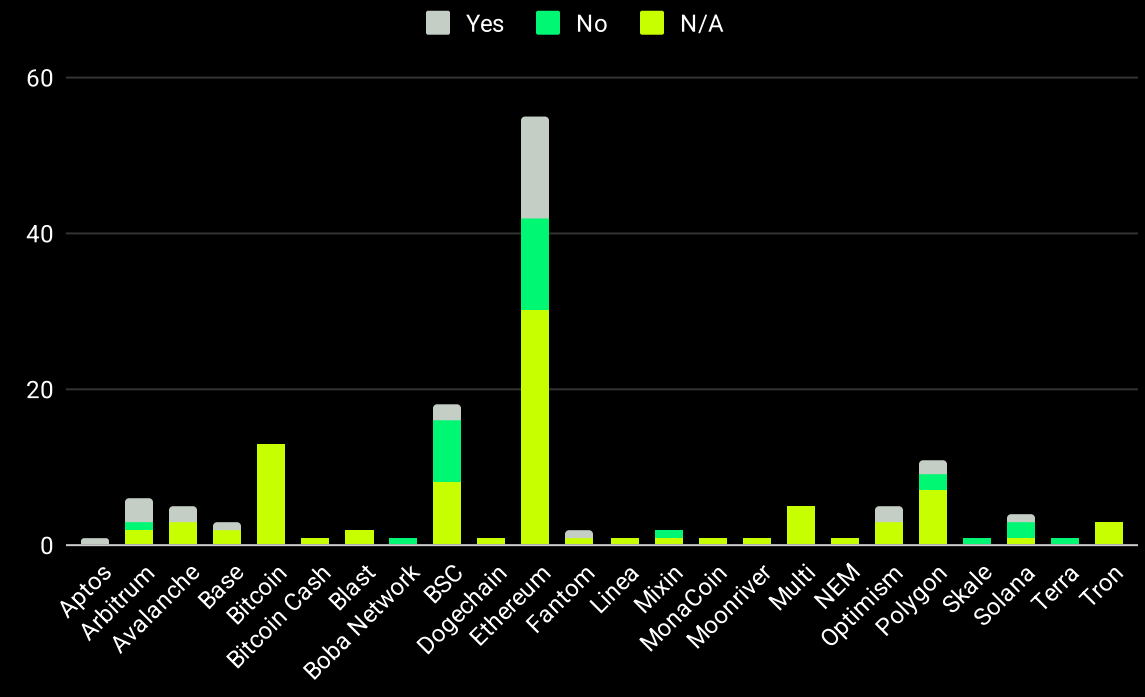

Figure 192: State of audition per chain [count]

Figures 193 and 194 provide a comprehensive view of the distribution of financial losses by chain and audit status.

In Arbitrum, the financial impact of hacks on protocols not audited is significantly higher than their occurrence rate, with such protocols accounting for 43.6% ($80,000,000 USD) of the total losses while only representing 16.7% of the attacks.

Avalanche shows a higher financial burden for protocols categorized as N/A, with these making up 68% ($72,391,966 USD) of the losses, which is higher than their occurrence rate of 60%. A similar trend is observed in Base, where N/A protocols account for 92.1% ($23,474,092 USD) of financial damages, well above their occurrence rate of 66.7%.

In BSC, protocols that have not been audited are the primary contributors to financial losses, making up 78.4% ($1,055,038,000 USD) of the total, which is substantially higher than their attack rate of 44.4%. This indicates a clear correlation between the lack of audits and the extent of financial losses.

Ethereum experiences slightly higher losses than the occurrence rates for both audited and N/A protocols, with audited protocols causing 23.7% ($1,082,530,071 USD) of the losses against an occurrence rate of 21.8%, and N/A protocols causing 63.8% ($2,910,494,982 USD) against a 54.5% rate of occurrence.

Fantom also shows higher losses for N/A protocols, accumulating 80% ($120,000,000 USD) of the losses against an occurrence rate of 50%.

In Optimism, audited protocols account for a slightly higher percentage of the total financial damage at 47.8% ($35,000,000 USD), suggesting that even audited protocols can still be vulnerable to significant losses.

Polygon sees a particularly stark discrepancy in not audited protocols, which cause 57.9% ($205,000,000 USD) of the financial losses against only an 18.2% occurrence rate.

Solana presents a case where the financial losses attributed to audited protocols are disproportionately high, with these protocols accounting for 63.9% ($326,000,000 USD) of the losses against a rate of occurrence of only 25%.

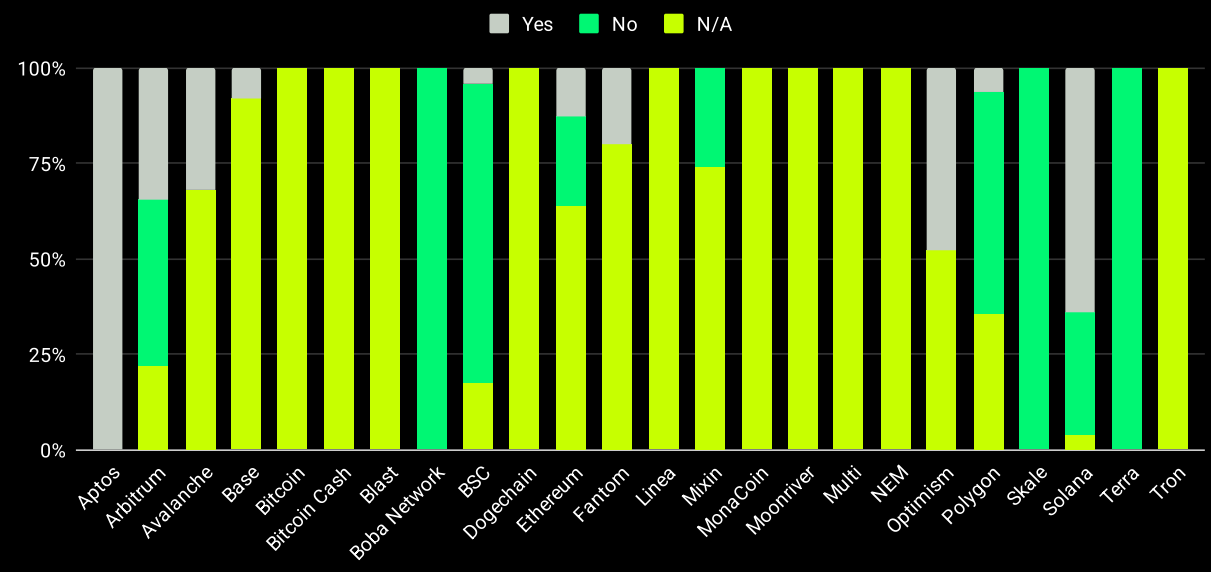

Figure 193: Loss caused per state of audition per chain [percentage]

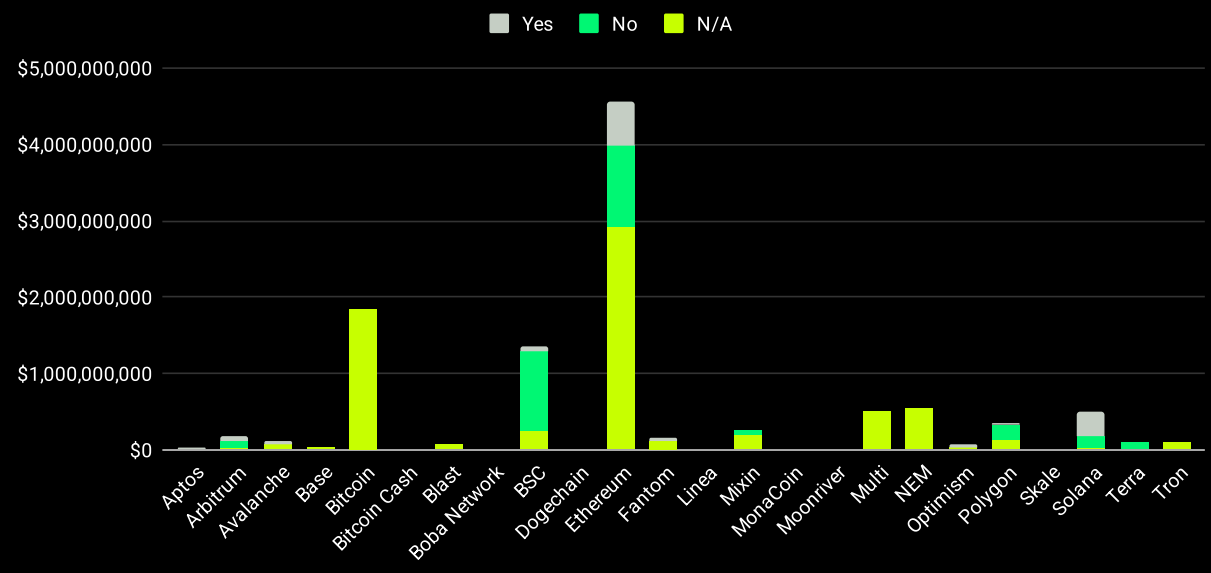

Figure 194: Loss caused per state of audition per chain [USD]

Figures 195 and 196 illustrate the dynamic evolution of attack occurrences in relation to the audit status of protocols across various blockchain networks over the years.

Arbitrum's attack landscape shifted dramatically from all attacks targeting non-audited protocols in 2022 to exclusively audited protocols in 2023 and then a mix of half N/A and half audited by 2024. Avalanche's trend moved from an even split between N/A and audited in 2021 to fully audited in 2023, transitioning to entirely N/A by 2024. Base followed a similar path from a 50-50 split in 2023 to fully N/A by the next year. Bitcoin consistently saw attacks in the N/A category across all observed years.

BSC's attack pattern evolved from a majority N/A in 2021 (45.5%), with 36.4% not audited and the remainder audited, to fully non-audited in the following year, shifting to entirely N/A in 2023, and a mix of 66.7% N/A and the rest non-audited in 2024.

Ethereum showed a significant evolution from non-audited in 2016 to all audited in 2017, followed by all N/A in 2018 and 2019. By 2020, attacks were equally distributed across all categories. In 2021, 40% were N/A, 33.3% not audited, and 26.7% audited. In 2022, 54.5% were N/A, 36.4% not audited, and 9.1% audited. By 2023, 80% of attacks were N/A, with the rest on audited protocols, and in 2024, 63.6% were N/A, with 9.1% not audited and 27.3% audited.

Fantom saw all attacks on audited protocols in 2021, switching to entirely N/A by 2023. Mixin moved from non-audited in 2022 to all N/A in 2023. Attacks involving multiple chains were consistently categorized as N/A for all years.

Optimism varied from all N/A in 2022 to all audited in 2023 and then a mix in 2024 with 66.7% N/A and the remainder audited.

Polygon in 2021 had 66.7% of attacks categorized as N/A and 16.7% each for non-audited and audited. By 2023, the attacks were evenly split across all categories, shifting to all N/A in 2024.

Solana had 66.7% of its 2022 attacks from non-audited protocols, with the rest from audited protocols. In 2024, all attacks were N/A.

Tron consistently showed all attacks as N/A throughout the observed years.

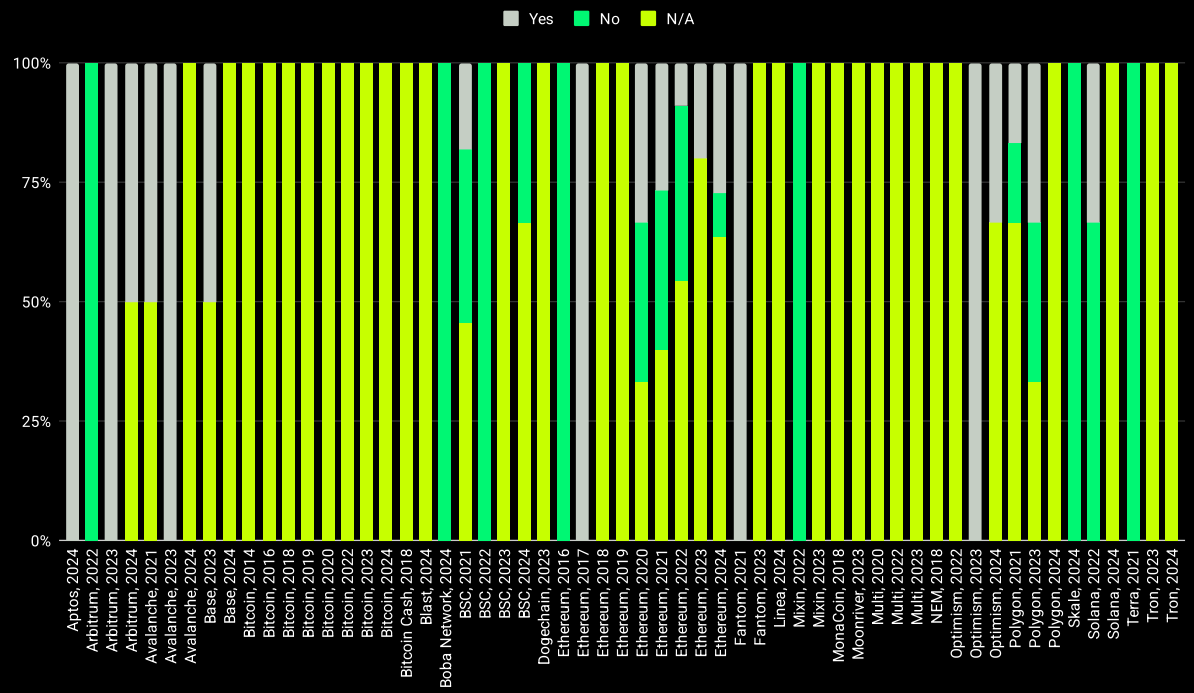

Figure 195: State of audition per chain and year [percentage]

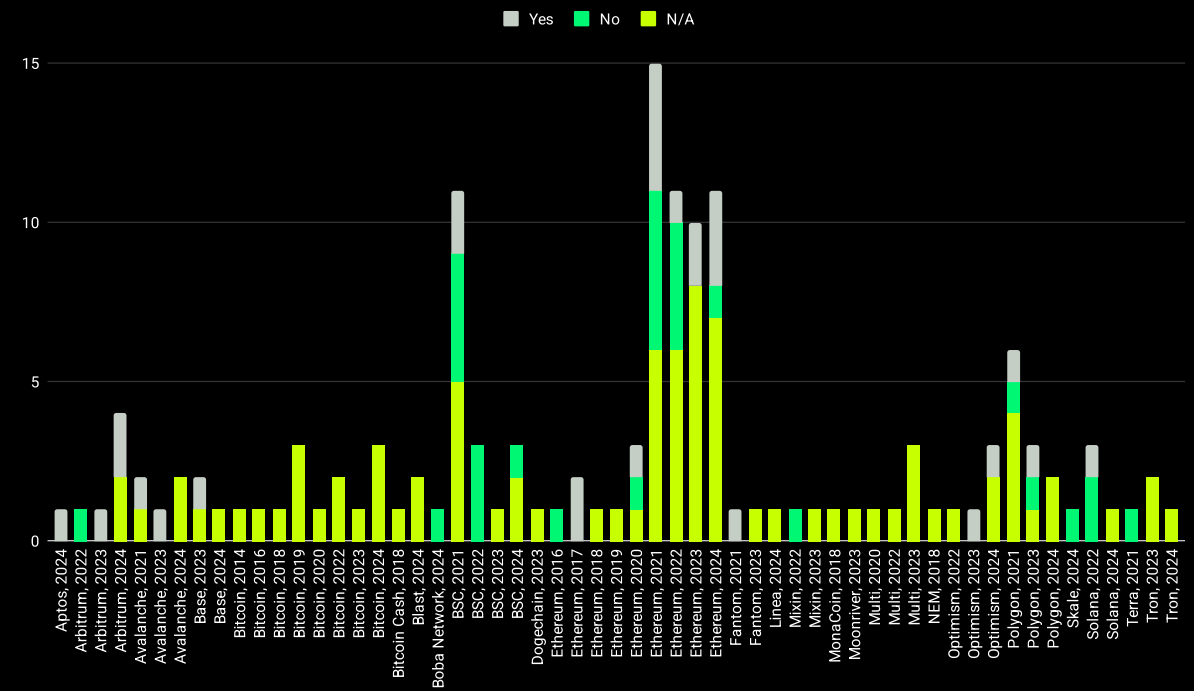

Figure 196: State of audition per chain and year [count]

Figures 197 and 198 detail the financial impact of attacks on blockchain protocols categorized by their audit status over various years.

In Arbitrum during 2024, audited protocols were associated with slightly higher financial losses than their occurrence would suggest, incurring 51.9% of the losses ($43,221,000 USD) against an occurrence rate of 50%.

Avalanche in 2021 also saw audited protocols bearing a larger share of the financial damage at 65.3% ($34,000,000 USD), suggesting vulnerabilities in protocols despite the presence of audits.

For Base in 2023, most financial losses were attributed to N/A attacks, accounting for 92% ($23,000,000 USD) of the losses against an occurrence rate of 50%, highlighting significant gaps in areas not covered by traditional smart contract audits.

BSC in 2021 experienced substantial losses from non-audited protocols, which surpassed their rate of occurrence with 60.4% of the losses ($373,000,000 USD) compared to a 36.4% occurrence rate. By 2024, almost the entirety of financial damage on this chain ($28,737,403 USD) resulted from N/A category attacks, constituting a significantly higher proportion of the total compared to their occurrence rate of 66.7%.

In Ethereum, the year 2020 showed that both audited and N/A attacks incurred more loss than their respective rates of occurrence, each causing 35.9% of the financial losses ($25,000,000 USD) against a 33.3% rate. By 2022, N/A attacks led to the most significant financial impact, with 77.1% of the losses ($1,365,200,000 USD) against a rate of occurrence of 54.5%. In 2024, N/A attacks continued to cause disproportionate losses, accumulating 89.8% ($575,882,985 USD) of the financial damage against an occurrence rate of 63.6%.

Optimism in 2024 observed audited protocols resulting in 72.3% of the financial losses ($20,000,000 USD) while representing only 33.3% of the attacks.

In Polygon, 2021 saw non-audited protocols causing more financial damage than their occurrence rate would suggest, with 51.4% of the losses ($110,539,954 USD) against a 16.7% occurrence rate. This trend continued into 2023, with non-audited protocols causing 91.8% of the financial losses ($120,000,000 USD) while constituting only a third of the attacks.

In Solana during 2022, audited protocols accounted for two-thirds of the financial losses ($326,000,000 USD) despite only being involved in a third of the attacks.

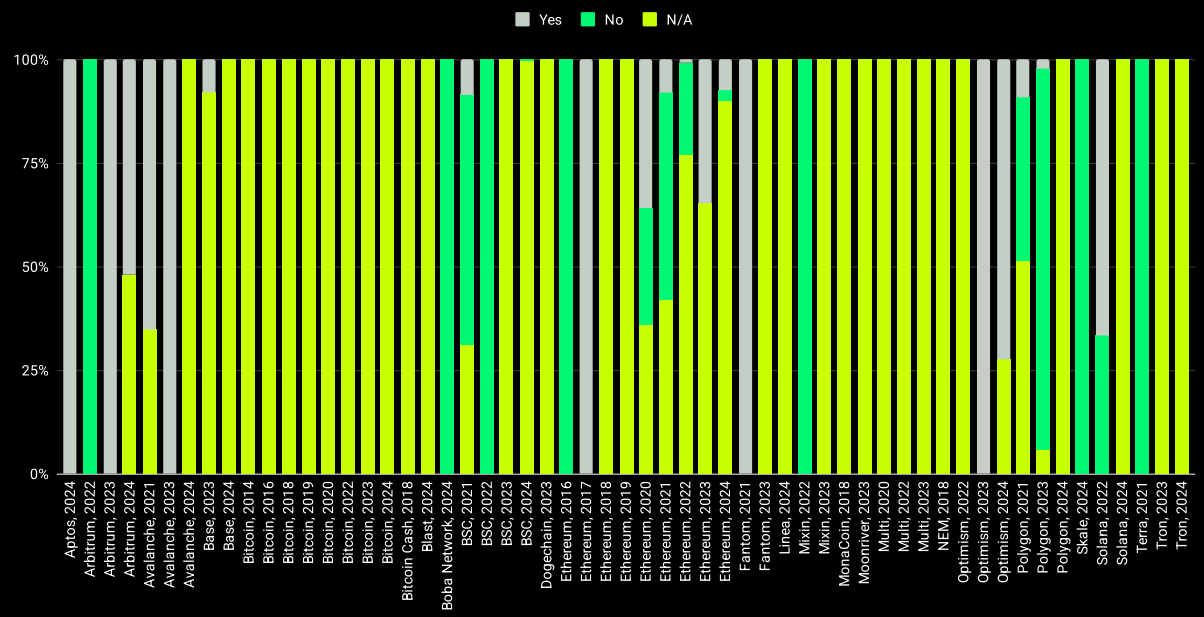

Figure 197: Loss caused per state of audition per chain and year [percentage]

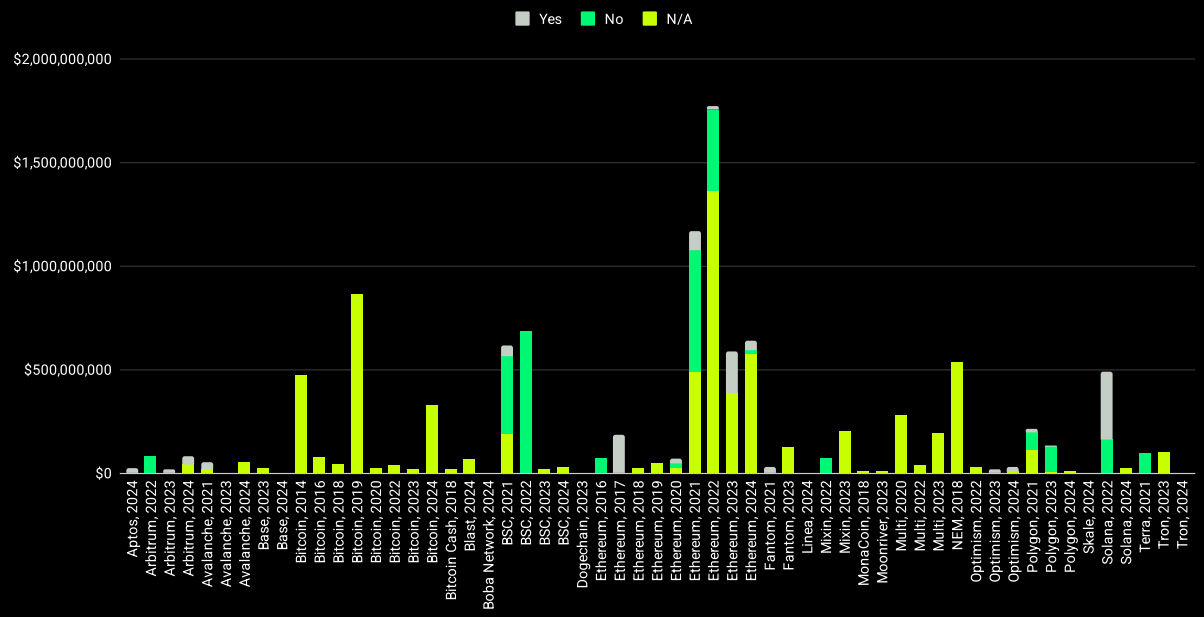

Figure 198: Loss caused per state of audition per chain and year [USD]

Audited Protocols by Type of Attack

Figures 199 and 200 provide a detailed analysis of whether attacked protocols were audited, categorized by the type of attack they suffered.

The analysis reveals that only incidents directly related to smart contract vulnerabilities were categorized as either audited or not audited. Cases considered N/A—meaning they fall outside the usual parameters of smart contract audits—include two notable instances of direct contract exploitation. The first, the Wintermute multi-sig deployment hack, involved a manipulation of how Gnosis Safe proxies are deployed, a situation complicated by human error rather than a direct smart contract flaw, thus rendering it beyond a standard audit's scope. Similarly, the Curve Vyper vulnerability originated from a compiler bug, also typically outside the scope of conventional smart contract auditing processes. Rug pulls, which often involve deceptive practices by insiders rather than code vulnerabilities, are also categorized as N/A.

In scenarios of direct contract exploitation, a significant 57.7% of the hacks occurred in unaudited protocols, underscoring the risk associated with the absence of auditing. However, 34.6% of such attacks did target audited protocols, indicating that even rigorous audits can sometimes fail to catch exploitable vulnerabilities.

For market manipulation attacks, a majority (61.1%) occurred in audited protocols. This suggests that market manipulation, which typically requires deep knowledge of a protocol and its interactions within the broader DeFi ecosystem, may be harder to detect in a standard code audit.

Governance attacks noted in the data were also linked to unaudited protocols, aligning with the notion that such attacks, like market manipulations, involve sophisticated strategies that can be difficult to detect through traditional or simpler smart contract audit processes.

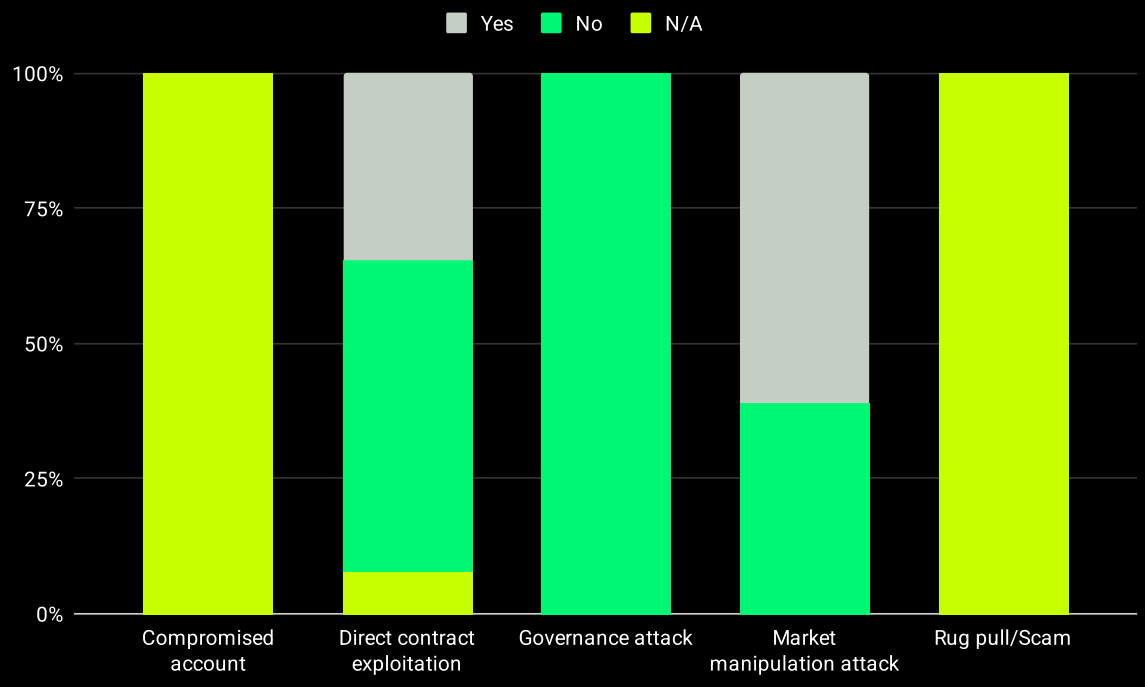

Figure 199: State of audition per type of attack [percentage]

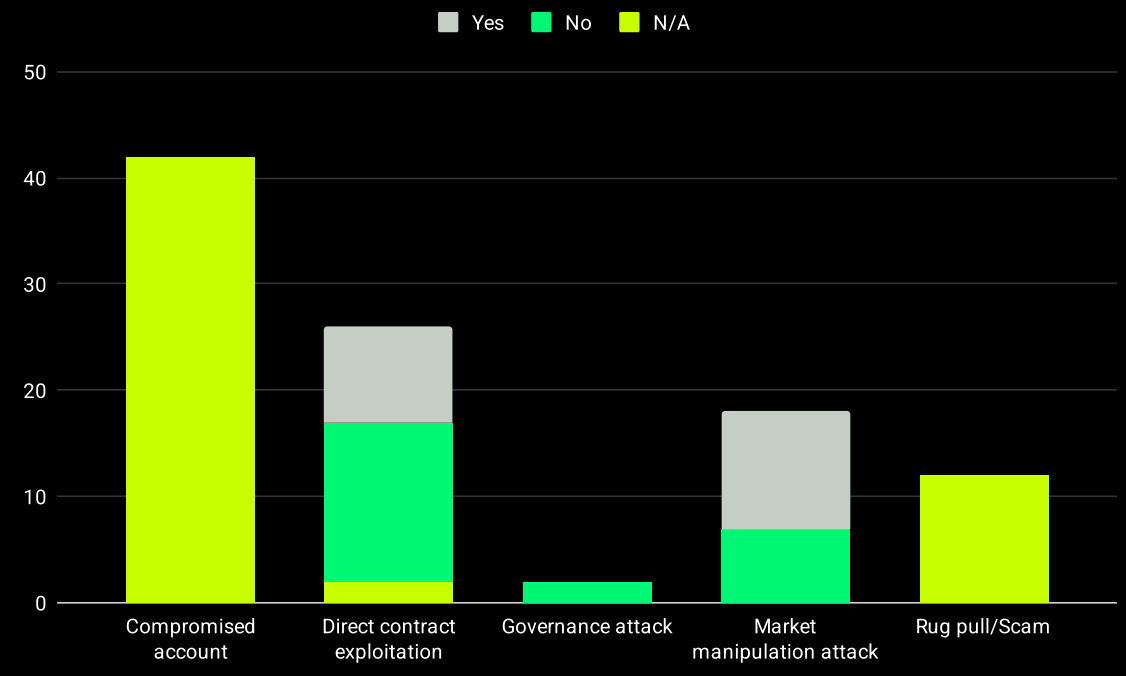

Figure 200: State of audition per type of attack [count]

Figures 201 and 202 analyze the financial impact of different types of attacks, particularly focusing on the relationship between the audit status of protocols and the resultant losses from hacks.

The analysis reveals that non-audited protocols consistently suffer higher financial losses relative to their incidence of attacks. Specifically, in the realm of direct contract exploitation, non-audited protocols accounted for 57.7% of the hacks but were responsible for a disproportionately higher percentage of the financial damage, contributing to 68.7% ($2,060,700,000 USD) of the total losses. This significant discrepancy underscores the vulnerability and potential financial risks associated with protocols that have not undergone rigorous auditing processes.

Similarly, in market manipulation attacks, even though non-audited protocols constituted only 38.9% of the occurrences, they were responsible for a much larger share of the financial losses, amounting to 61.6% ($511,600,000 USD. This suggests that even though fewer non-audited protocols were targeted by market manipulations, the sophistication and the severe impact of these attacks make them particularly costly when they occur.

These data highlight the substantial risks associated with non-audited protocols, particularly in scenarios that involve sophisticated attack vectors such as market manipulation. It also underscores the importance of comprehensive security audits.

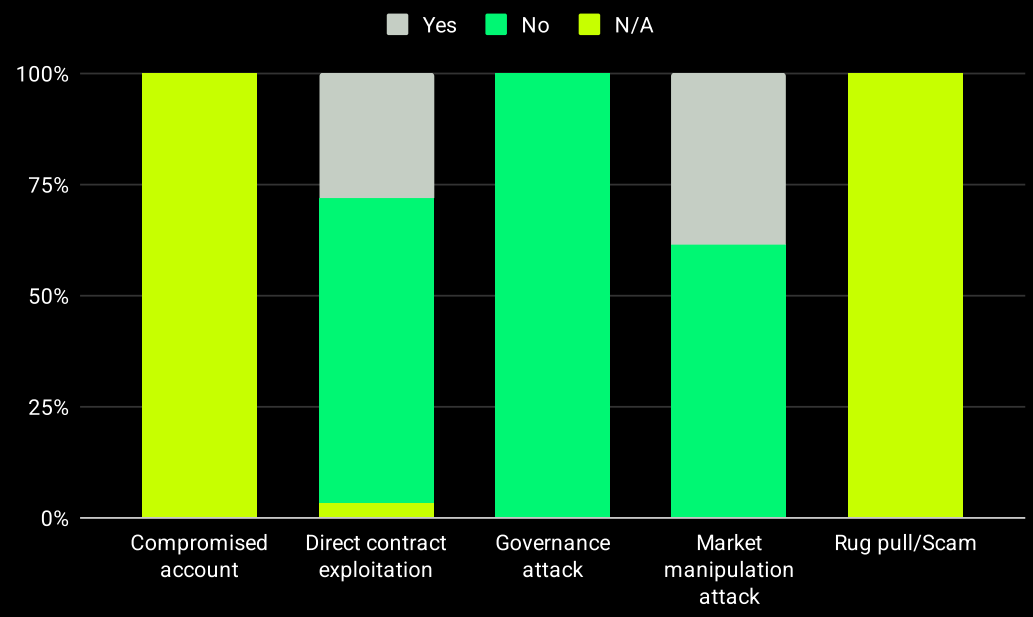

Figure 201: Loss caused per state of audition per type of attack [percentage]

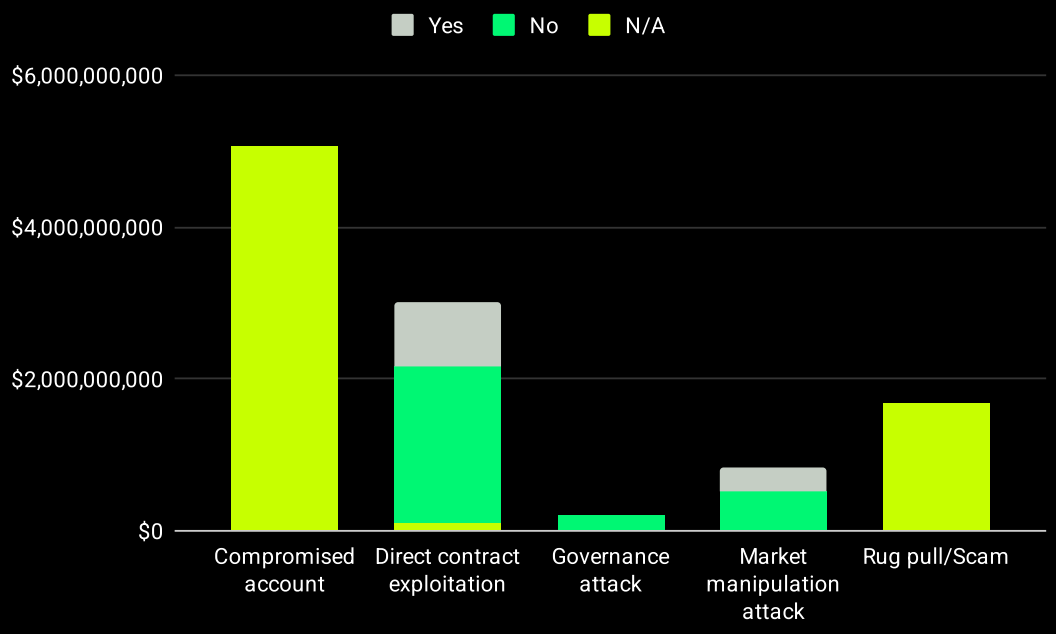

Figure 202: Loss caused per state of audition per type of attack [USD]

Figures 203 and 204 provide a detailed look at the distribution of attacks per type and the audit status of the protocols over the years.

For direct contract exploitation, the data shows a fluctuation in the audit status of the protocols targeted. In 2016, the protocol that was attacked was not audited. By 2017, this shifted to audited protocols being attacked. In 2020, the trend reverted back to attacks on non-audited protocols. By 2021, a majority (75%) of the attacks targeted non-audited protocols, with the remainder affecting audited ones. In 2022, non-audited protocols continued to be the most targeted at 66.7%, with 22.2% of attacks on audited protocols and 11.1% categorized as N/A. The year 2023 saw an equal split between N/A and audited protocols, with one attack each, and by 2024, both incidents of direct contract exploitation involved audited protocols.

In the case of market manipulation attacks, the initial attack in 2020 targeted an audited protocol. By 2021, 66.7% of the attacks were on audited protocols, with the rest on non-audited ones. In 2022, a shift occurred with all market manipulation attacks targeting non-audited protocols. However, in 2023, the attacks were evenly split between audited and non-audited protocols. By 2024, a concerning trend emerged as all market manipulation attacks targeted audited protocols.

This data highlights a worrying trend in the last year where all protocols attacked, across both types of attacks, were audited. This suggests that while audits are essential, they are not foolproof in preventing attacks. The evolution indicates that attackers are becoming more sophisticated and capable of exploiting vulnerabilities in protocols despite them being audited. This underscores the need for continuous improvement in auditing processes towards comprehensive audits.

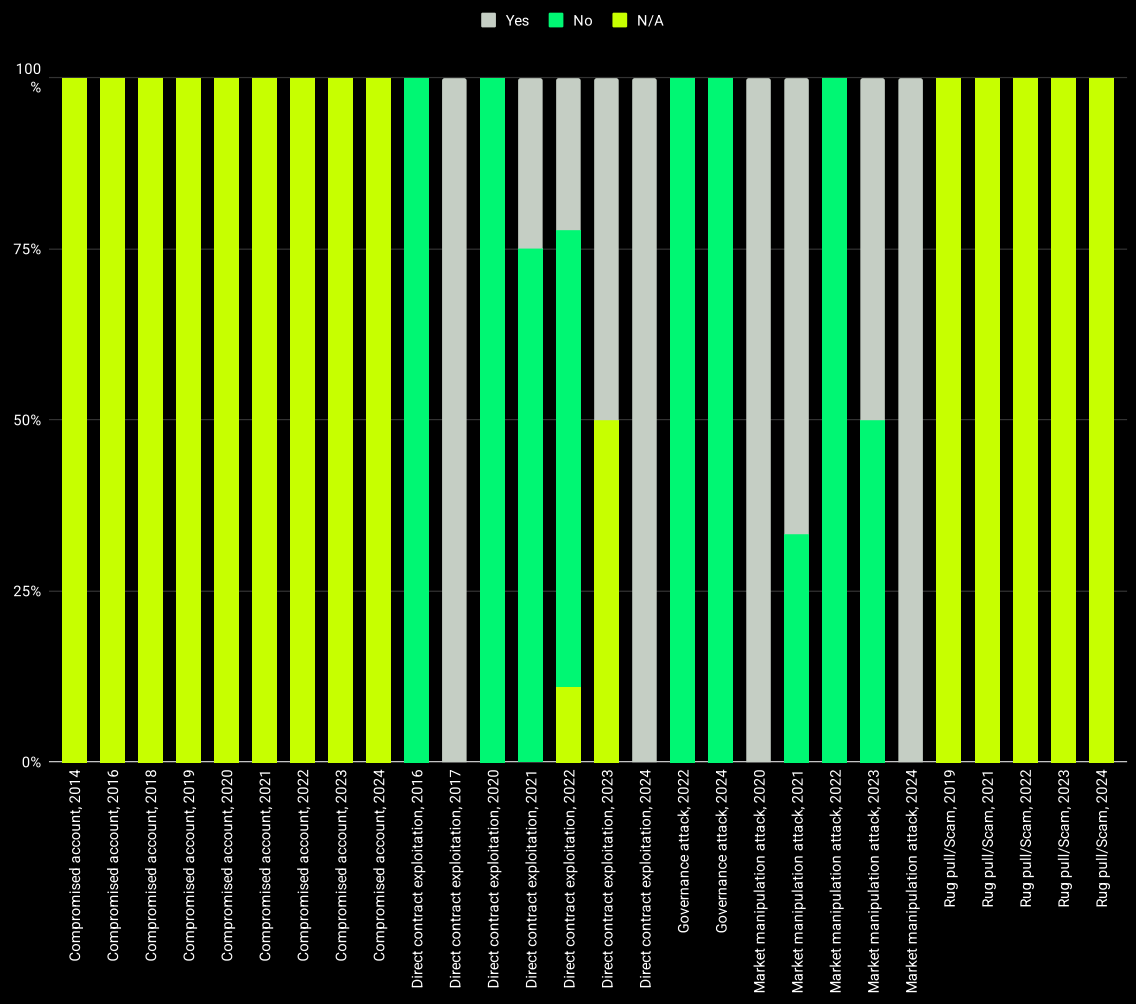

Figure 203: State of audition per type of attack and year [percentage]

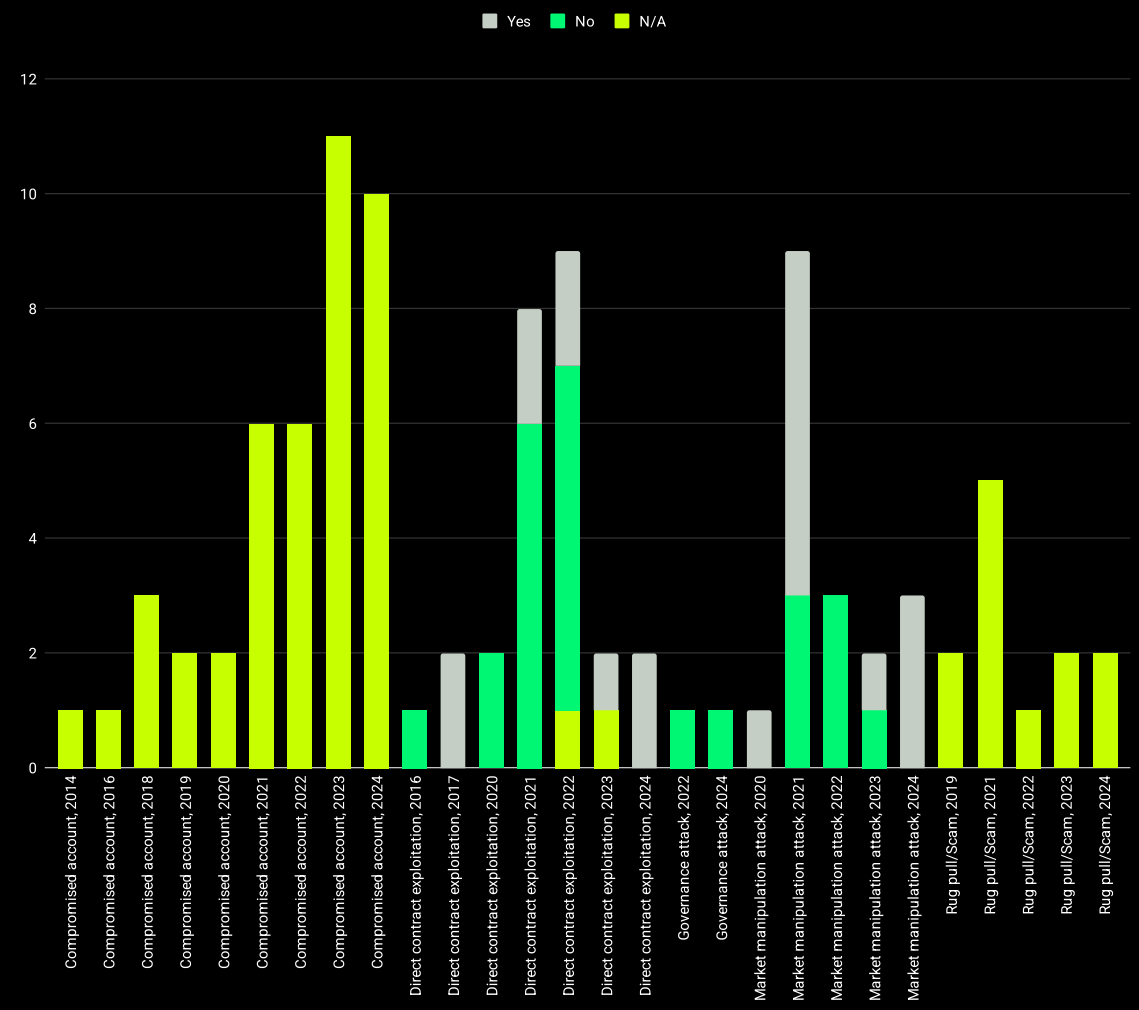

Figure 204: State of audition per type of attack and year [count]

Figures 205 and 206 delve into the financial impact of different types of attacks on blockchain protocols over the years.

For direct contract exploitation attacks in 2021, a significant discrepancy is evident as these attacks accounted for 95% ($941,800,000 USD) of the financial losses while only making up 75% of the occurrences. This trend persisted into 2022, with these attacks resulting in 73% ($1,004,200,000 USD) of the losses despite constituting 66.7% of the attacks. In contrast, 2023 saw a shift with audited protocols contributing disproportionately to losses—74% ($197,000,000 USD) of the losses originated from audited protocols, although they only represented 50% of the attacks. This marks a significant shift in the impact of attacks on audited versus non-audited protocols.

In the context of market manipulation attacks, the trend shows that non-audited protocols consistently cause more financial damage than might be expected based on their occurrence rates. In 2021, non-audited protocols were responsible for 51.5% ($191,000,000 USD) of the losses, significantly higher than their occurrence rate of 33.3%. By 2023, this pattern intensified, with non-audited protocols causing 71.6% ($120,000,000 USD) of the losses despite only accounting for half of the attacks.

This historical data suggest that non-audited protocols typically incur higher losses when hacked, highlighting the critical importance of audits in mitigating financial risks. However, the trend observed in 2023 in direct contract exploitation attacks and the fact that all protocols hacked in 2024 by direct contract exploitation and market manipulation attacks were audited suggest a potential paradigm shift where even audited protocols are becoming increasingly targeted by sophisticated attackers, leading to significant financial losses. This suggests a potential need for evolving audit practices to better detect and mitigate sophisticated attacks that current auditing measures might be failing to prevent.

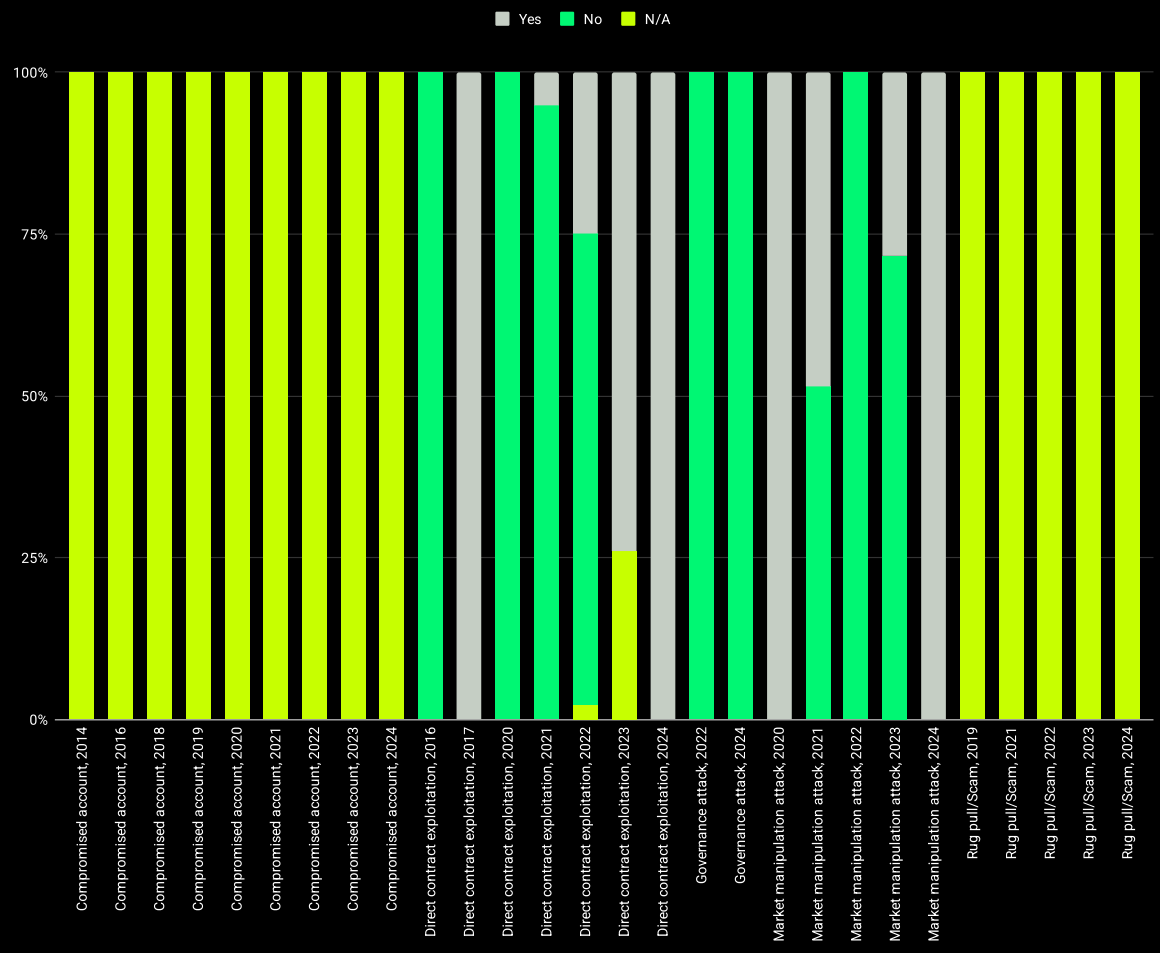

Figure 205: Loss caused per state of audition per type of attack and year [percentage]

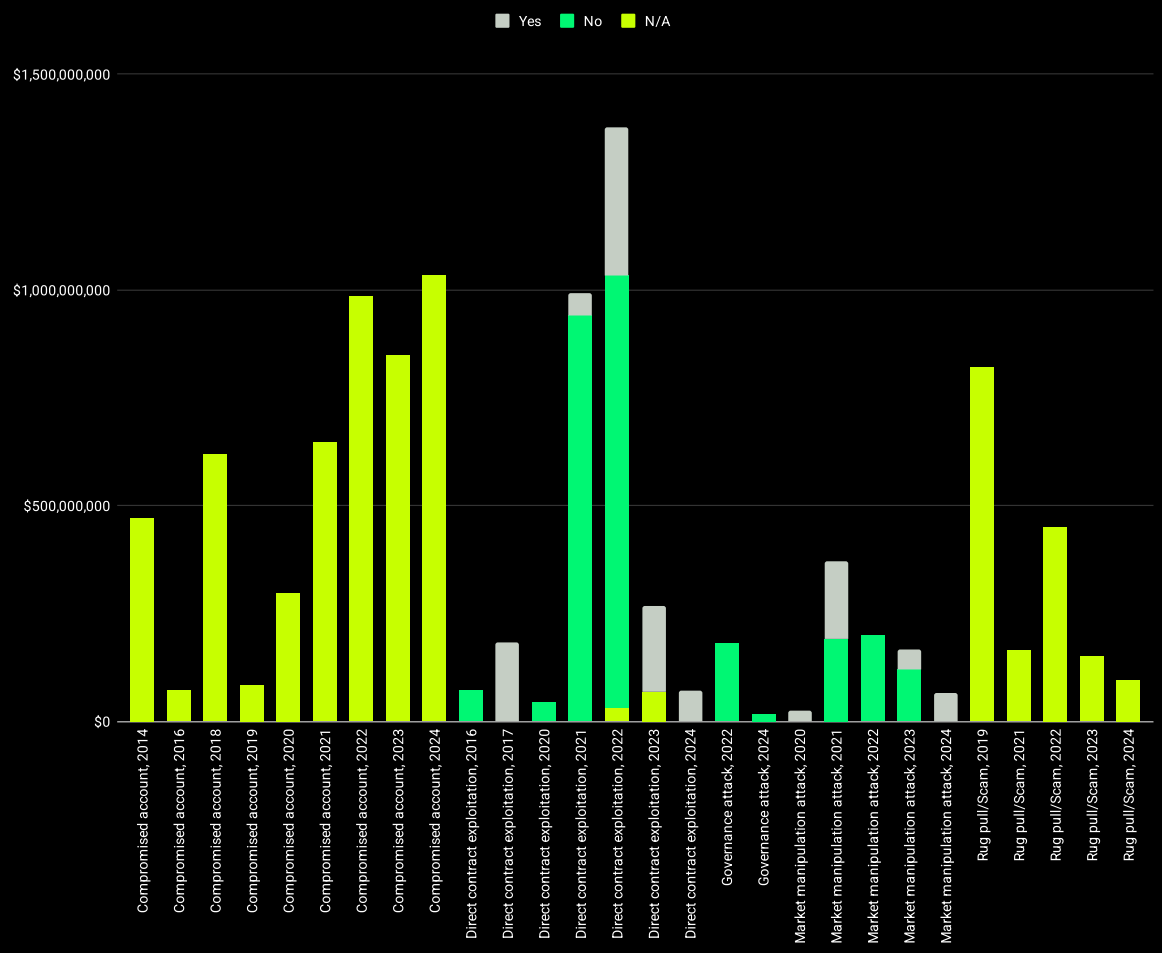

Figure 206: Loss caused per state of audition per type of attack and year [USD]

Audited Protocols by Type of Protocol

Figures 207 and 208 illustrate the audit status of various types of blockchain protocols that have been attacked.

Some types of protocols, such as Launchpads, Liquid Staking, and Liquidity Managers, experienced attacks despite all being audited. This indicates that even protocols that have undergone audits are not immune to breaches, which may call for more rigorous or specialized auditing practices to identify and mitigate vulnerabilities that go beyond typical security checks.

On the other hand, certain protocol types hacked, like Algo-Stables, CDPs (Collateralized Debt Positions), Chains, Derivatives, and Indexes, were not audited at all, which may have left them particularly vulnerable to exploits due to the absence of any formalized security review.

Other protocol categories such as CEXs (Centralized Exchanges), Farms, Gaming, Other Currencies, Payments, Ponzi Schemes, Prediction Markets, and Reserve Currencies' attacks were categorized under N/A, indicating that these attacks involved elements outside the typical scope of smart contract audits or involved other types of operational or systemic vulnerabilities.

Furthermore, the distribution in Bridges shows that the majority (50%) of the attacks were categorized as N/A, followed by 40% that were not audited and 10% that were audited. DEX Aggregators saw an even split with 50% not audited and 50% falling under N/A. For DEXes, the largest segment at 63.6% fell under N/A, with 27.3% involving audited protocols and the remainder not audited.

In the case of Lending protocols, most attacks occurred on non-audited protocols, representing 46.7% of the incidents, followed by 33.3% that targeted audited protocols, and the rest categorized as N/A. Services showed a predominance of N/A categories at 66.7%, with the rest involving non-audited protocols. Wallets also had a majority marked as N/A at 60%, while the remaining attacks targeted audited protocols.

In the case of Yield protocols, 80% of the hacked ones were audited, and the remaining 20% were not audited, reflecting a high level of scrutiny in this category, yet still not entirely preventing breaches. This is particularly noteworthy, as Yield is one of seven protocol categories with five or more recorded attacks.

Yield Aggregators presented a more mixed picture with 50% non-audited, 33.3% N/A, and the remaining portion audited.

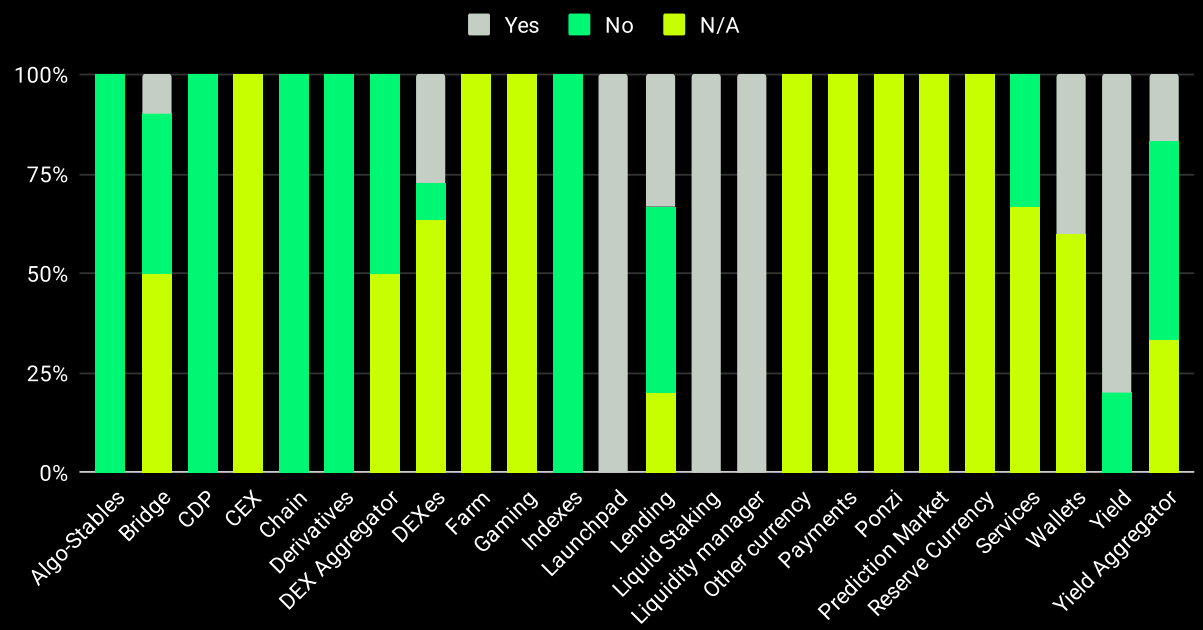

Figure 207: State of audition per type of attack [percentage]

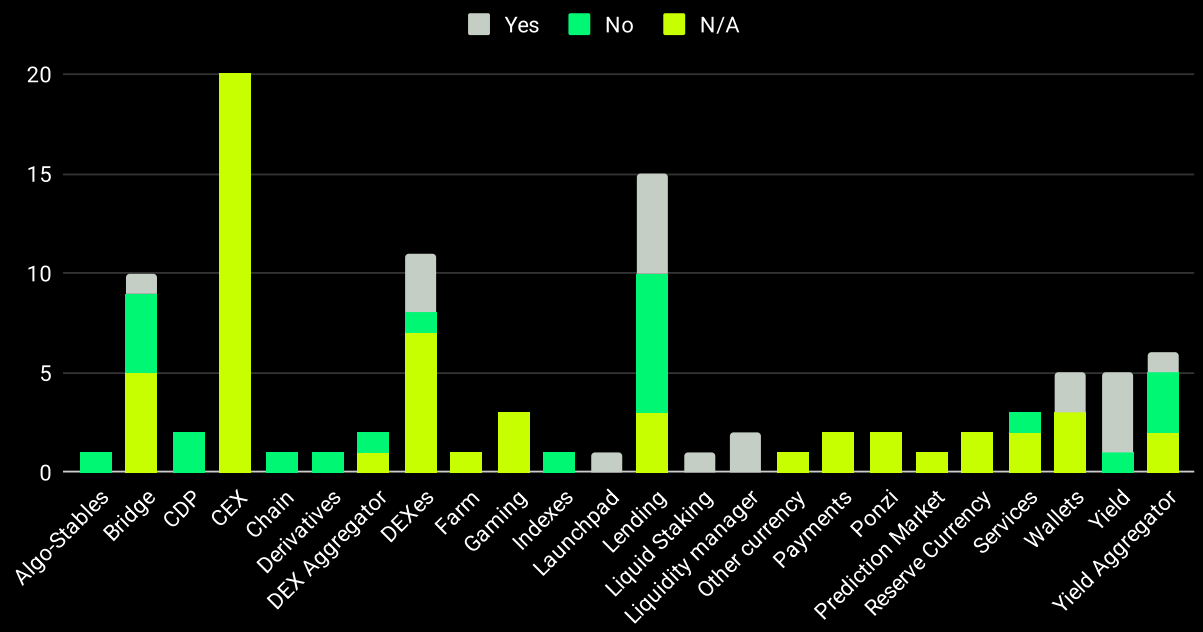

Figure 208: State of audition per type of attack [count]

Figures 209 and 210 provide a detailed look at the financial losses associated with different types of blockchain protocols, segmented by their audit status.

In the case of Bridges, non-audited protocols are responsible for a significant majority of financial losses, accounting for 51.9% ($1,467,000,000 USD) of the total, which is higher than their occurrence rate of 40%. This suggests that a lack of audits for bridges significantly enhances financial risk.

For DEX Aggregators, attacks categorized as N/A lead to slightly more losses than their occurrence rate would predict, with 51% ($21,000,000 USD) of the losses against a 50% occurrence rate, indicating vulnerabilities that audits may not address.

DEXes see a similar pattern where N/A attacks result in 68.6% ($364,400,000 USD) of losses, higher than their occurrence rate of 63.6%. Additionally, non-audited protocols contribute 10.7% ($57,000,000 USD) to the losses, slightly above their occurrence rate of 9.1%, highlighting the importance of comprehensive audits in these environments.

In Lending, the primary source of loss comes from non-audited protocols, which accumulate 56.5% ($625,800,000 USD) of the total financial damage, exceeding their occurrence rate of 46.7%. This indicates a critical need for rigorous audits to mitigate risks in lending protocols.

Services exhibit a notable discrepancy where N/A attacks account for most of the losses at 76.4% ($227,000,000 USD), significantly above their occurrence rate of 66.7%, suggesting that the vulnerabilities leading to these losses might be beyond the typical scope of smart contract audits.

Wallets demonstrate that audited protocols are the main contributors to financial losses, representing 53.4% ($182,000,000 USD) of the total, compared to their occurrence rate of 40%. This might indicate a level of complexity and challenges in auditing wallet protocols effectively.

For Yield protocols, the losses are closely aligned with their audit status, with audited protocols causing slightly more than their proportionate share of losses at 86.6% ($116,700,000 USD) against an 80% occurrence rate, indicating that even rigorous audits cannot always prevent sophisticated attacks.

Yield Aggregators show that N/A protocols lead to the highest losses at 47.2% ($152,000,000 USD), which is higher than their occurrence rate of 33.3%, followed closely by non-audited protocols at 45% ($144,700,000 USD), which is slightly less than their occurrence rate of 50%.

These figures illustrate the significant financial impact associated with the lack of smart contracts audits and attacks that are not covered by them, particularly in certain types of protocols where the absence of an audit correlates with higher financial losses.

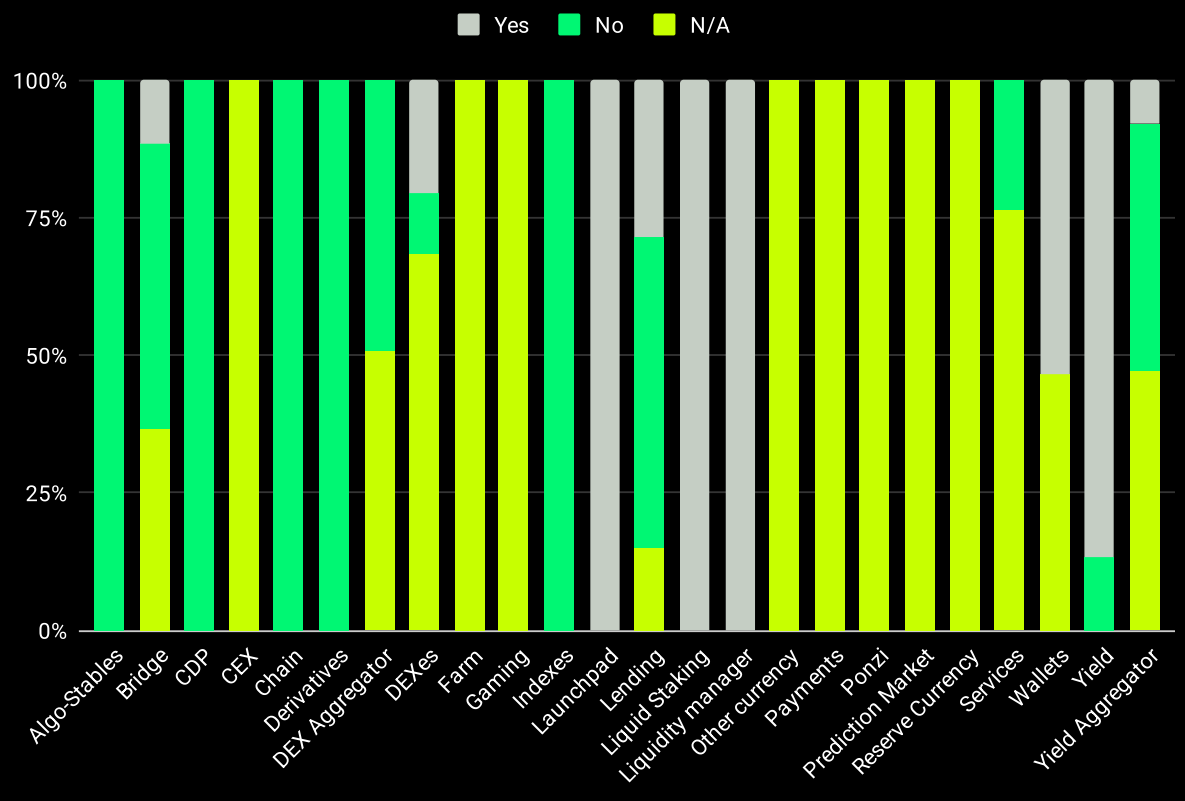

Figure 209: Loss caused per state of audition per type of attack [percentage]

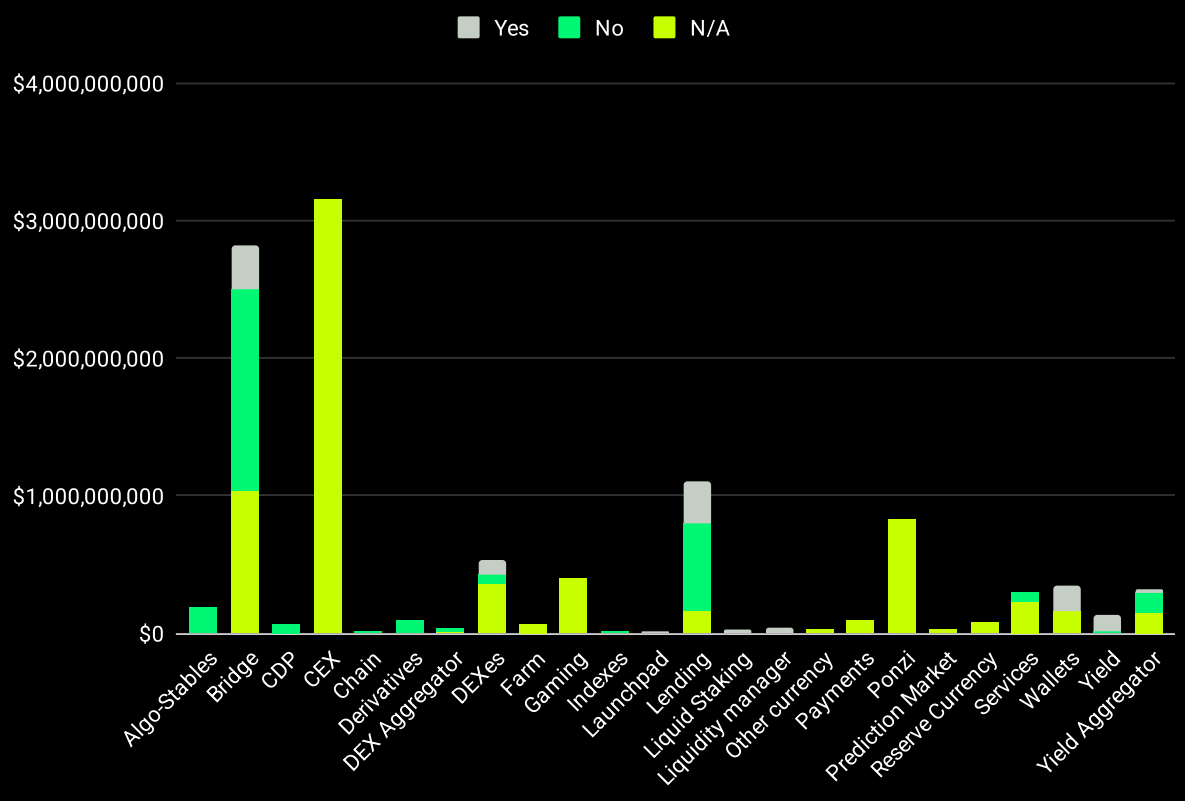

Figure 210: Loss caused per state of audition per type of attack [USD]

Figures 211 and 212 provide a detailed breakdown of the audit status of protocols by type across several years.

In the category of Bridges, 2021 saw all hacked protocols being not audited. The following year, the majority (50%) remained not audited, with 33.3% falling under the N/A category and the remainder being audited. By 2023, all attacks on Bridges were categorized as N/A, indicating a shift away from direct smart contract vulnerabilities to other forms of exploits that audits typically do not cover.

For CEXs, all instances across the years were categorized under N/A, indicating that the attacks were of a nature not preventable through traditional smart contract auditing.

In the case of DEX Aggregators, the protocol attacked in 2022 was not audited, whereas by 2024, the attack fell under the N/A category. DEXes started in 2018 with all attacks being categorized as N/A. By 2021, the landscape diversified, with half of the attacks on audited protocols and the rest split evenly between N/A and not audited. The subsequent year returned to all attacks being N/A. In 2023, the majority (66.7%) of attacks were N/A with the remainder audited, and in 2024, the attacked protocol was again categorized as N/A.

Gaming protocols consistently fell under the N/A category across all years, reflecting the nature of the attacks, which involved elements outside of conventional smart contract vulnerabilities.

For Lending protocols, an evolution in audit status is apparent. In 2020, the hacked protocol was not audited. By the following year, 50% remained not audited, 33.3% were categorized as N/A, and the rest were audited. In 2022, all were not audited again, but in 2023, the attacks were evenly split between audited and not audited. By 2024, a significant 75% of the hacked protocols were audited, with the remaining classified as N/A.

Services saw a shift from an unaudited protocol in 2016 to all subsequent years being categorized as N/A.

For Wallets, all instances across the years fell under the N/A category, indicating that the attacks exploited factors beyond the scope of audits.

In Yield protocols, 2021 saw the majority (75%) being audited, with the rest not audited. By 2024, the attacked protocol was audited. Yield Aggregators in 2020 were evenly split between audited and not audited, but by 2021, 66.7% of attacks were caused by N/A and the rest by not audited protocols. In 2022, the protocol attacked was not audited.

In general, we can observe that a noticeable trend across many protocol types, especially in more recent years, is the shift towards the N/A category. This indicates that attacks are increasingly exploiting areas not covered by traditional audits. Furthermore, there is an evident increase in attacks on audited protocols, particularly in sectors like Yield and Lending, where sophisticated financial mechanisms might be involved. This suggests that while audits are crucial, they are not foolproof. Attackers may be adapting and finding ways to exploit even audited contracts, possibly due to the increasing complexity of DeFi protocols, which may leave room for oversight during audits.

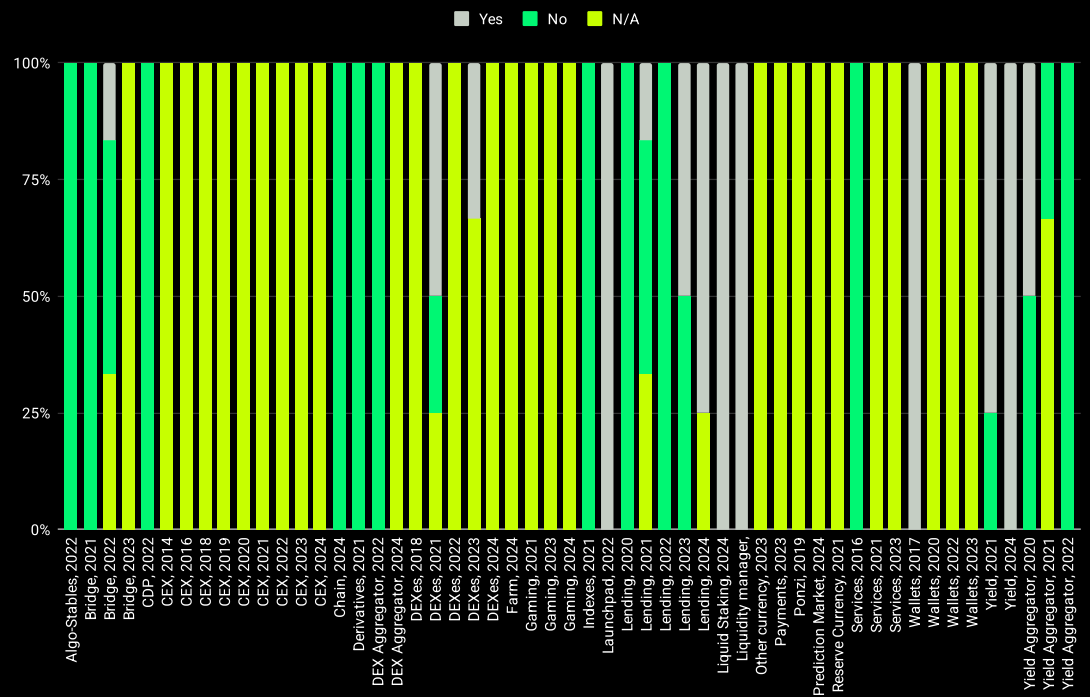

Figure 211: State of audition per type of attack and year [percentage]

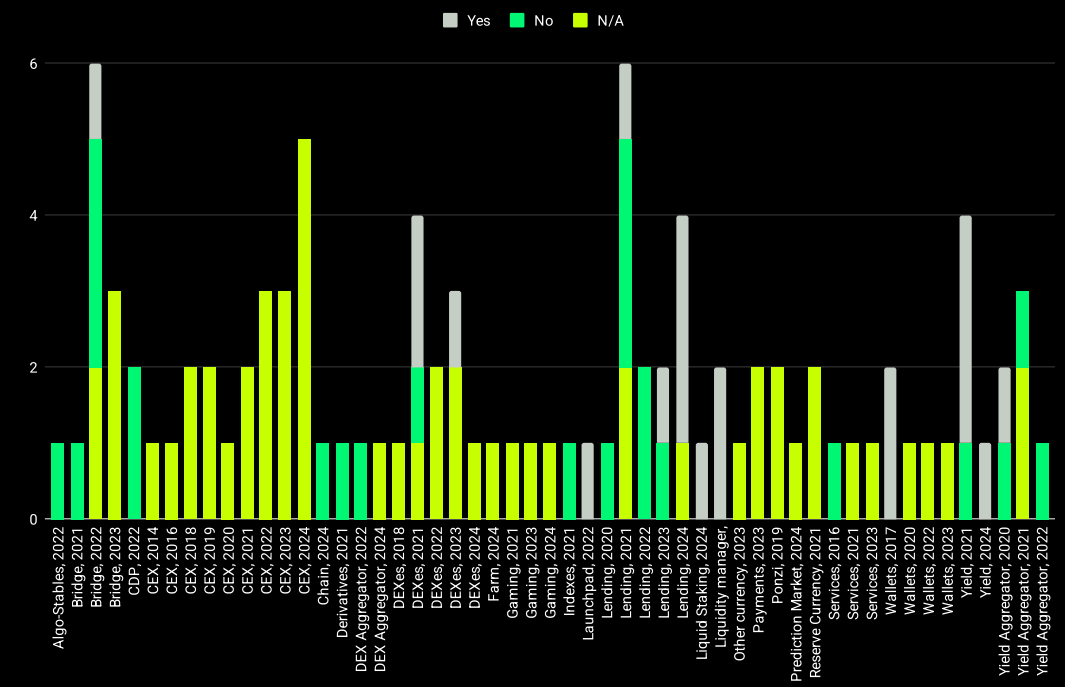

Figure 212: State of audition per type of attack and year [count]

Figures 213 and 214 detail the financial impact of blockchain protocol hacks, comparing the monetary losses based on whether the protocols were audited or not.

For Bridges in 2022, while most of the financial losses were due to not audited protocols, accounting for 44.9% ($856,000,000 USD), this percentage was slightly lower than their occurrence rate of 50%. In contrast, the financial damage from N/A attacks and audited protocols was proportionally higher, at 38% ($724,000,000 USD) and 17.1% ($326,000,000 USD), respectively, compared to their occurrence rates of 33.3% and 16.7%. This indicates a mismatch between the perceived security provided by audits and the actual vulnerability exposed during attacks.

For DEXes in 2021, while audited protocols constituted most attacks at 50%, they resulted in a slightly smaller proportion of the financial losses at 42.4% ($61,900,000 USD). Not audited protocols, representing 25% of the attacks, accounted for a disproportionately high 39.1% of the losses ($57,000,000 USD), with the remainder attributed to N/A categories. By 2023, the financial losses mirrored the rate of occurrence, indicating an alignment between the expected and actual financial impact based on audit status.

In Lending protocols in 2021, not audited protocols were responsible for most losses at 66.7% ($295,800,000 USD), which was higher than their occurrence rate of 50%. However, by 2023, although attacks were evenly split between audited and not audited protocols, audited ones led to a larger share of financial damage at 62.1% ($197,000,000 USD). By the following year, audited protocols accounted for a lower percentage of losses at 61.3% ($84,100,000 USD) compared to their occurrence rate of 75%, indicating a shift in the loss distribution towards N/A attacks.

In Yield protocols in 2021, audited protocols resulted in more losses than their rate of occurrence, with 83.3% ($89,700,000 USD) of the financial damage versus an occurrence rate of 75%.

Finally, in Yield Aggregators in 2020, audited protocols led to more losses at 55.9% ($25,000,000 USD) compared to their occurrence rate of 50%. The following year, however, the N/A category dominated the financial damage, accumulating 77.2% ($152,000,000 USD) against an occurrence rate of 66.7%.

This data suggests a significant discrepancy between audited and non-audited protocols in terms of the financial impact of hacks. Non-audited protocols consistently contribute to higher-than-expected financial losses compared to their rate of occurrence. This underscores the critical importance of audits in potentially reducing the severity of hacks but also highlights that audits are not infallible.

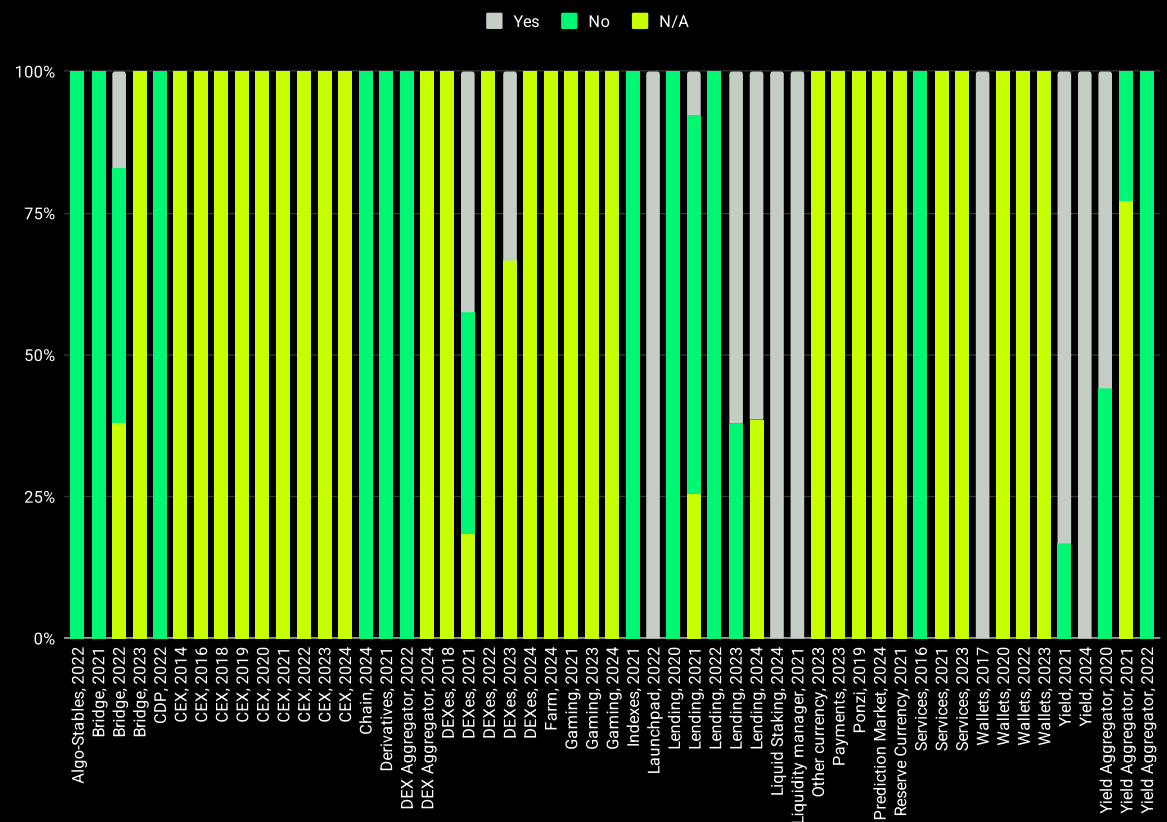

Figure 213: Loss caused per state of audition per type of attack and year [percentage]

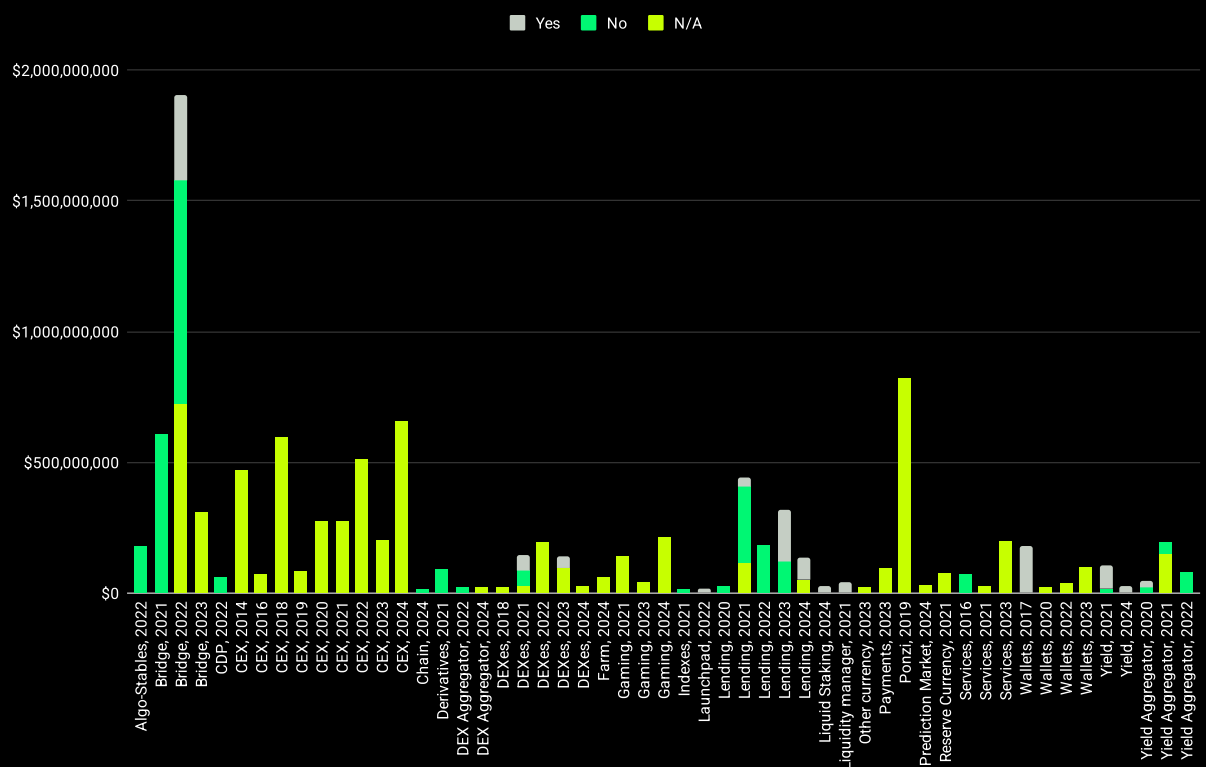

Figure 214: Loss caused per state of audition per type of attack and year [USD]

Audited Protocols by Type of Function

Figures 215 and 216 detail the audit status of various blockchain protocol functions that were exploited in attacks

`CalculateAmount` functions that were exploited all occurred within audited protocols, suggesting that despite being audited, vulnerabilities were present that audits did not catch. The `create` function was linked to the Wintermute hack, categorized as N/A due to the nature of the exploit, as explained before in this report.

For `deposit` functions, a majority (66.7%) were within audited protocols, indicating that audits might not always effectively mitigate vulnerabilities in these types of functions. `Execute` functions exploited were all from non-audited protocols, highlighting a clear gap in security measures for these operations.

`Initialize` functions showed a similar trend to `deposit`, with 66.7% of exploited functions residing in audited protocols, again suggesting potential oversights in audit processes. `Migrate` functions that were attacked were also within audited environments.

`Mint` functions predominantly occurred in non-audited protocols (66.7%), which underscores the risks associated with not having rigorous audits for such critical functions. On the other hand, all protocol-specific functions exploited were within audited protocols, indicating the need for a deeper knowledge of the protocol by the auditor.

`Swap` functions showed a distribution identical to `mint`'s, with 66.7% occurring in audited protocols. For `transferOwnership`, all instances were not audited, representing a significant security oversight given the high stakes of ownership transfer capabilities.

The `verifyProof` function saw a split between audited and non-audited, with one exploited function from each category. The vote function was not audited, which might reflect lower perceived risk or oversight in security prioritization.

`Withdraw`-like functions mostly occurred in non-audited protocols (55.6%), highlighting a critical area where audit coverage is lacking, potentially leading to substantial financial losses.

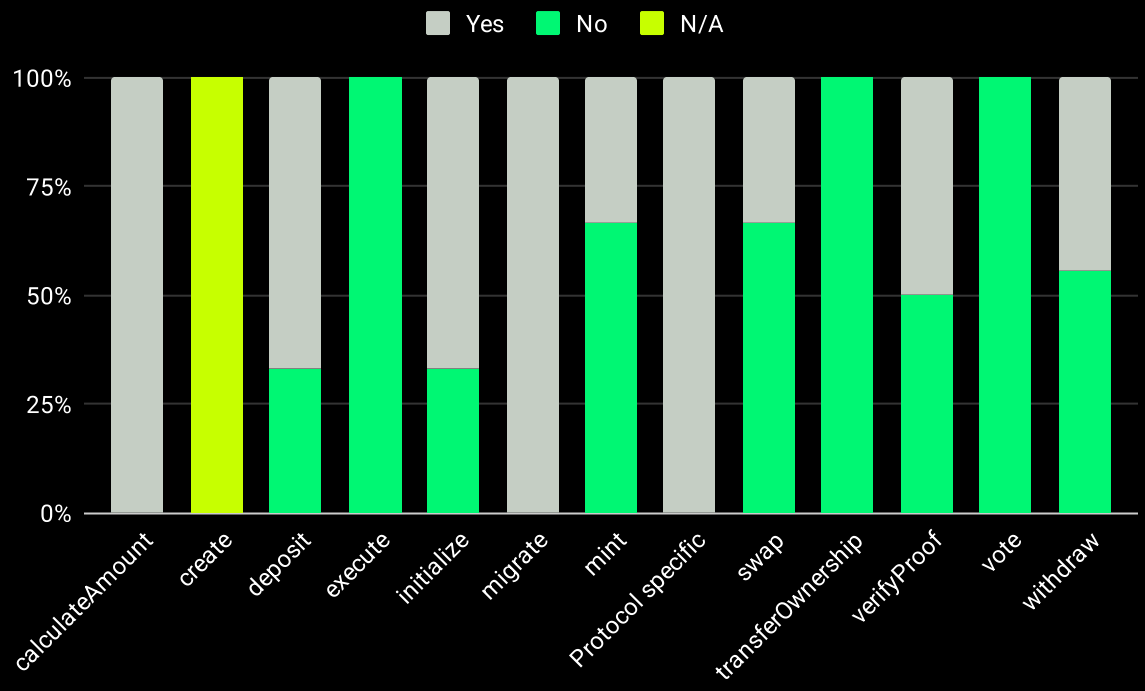

Figure 215: State of audition per type of function [percentage]

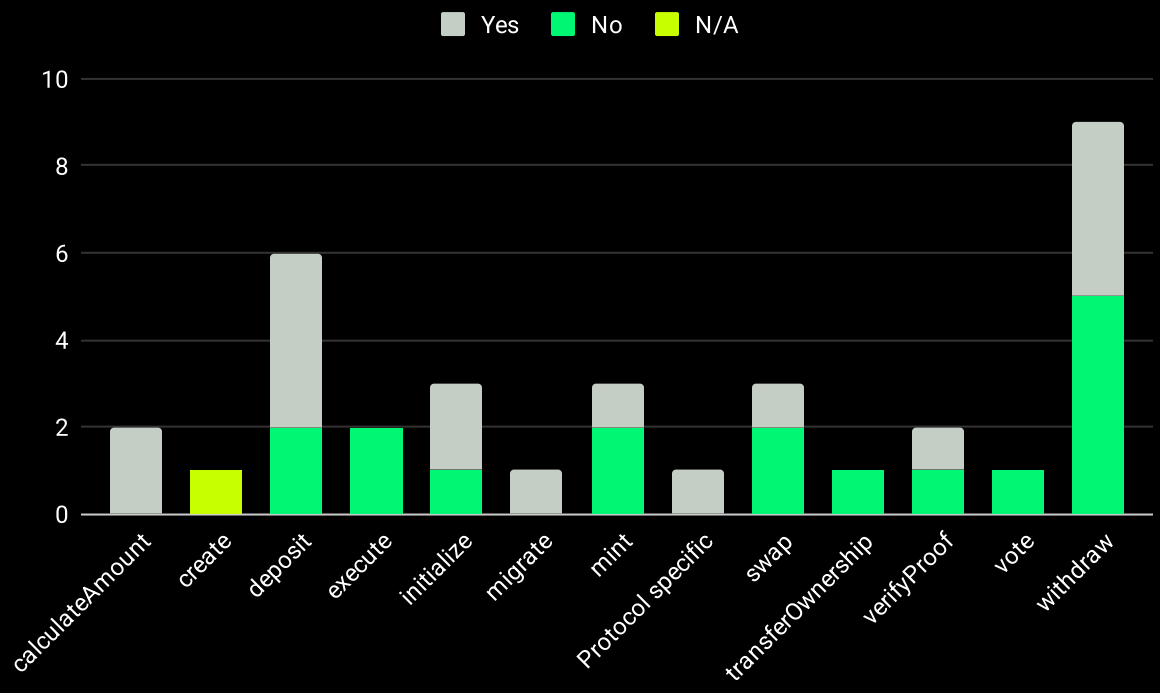

Figure 216: State of audition per type of function [count]

Figures 217 and 218 explore the financial impact of blockchain attacks based on the audit status of the exploited functions

For `deposit` functions, those that were audited accounted for a significant portion of the losses, accumulating 72.8% ($281,000,000 USD) of the total financial damage, which is higher than their occurrence rate of 66.7%. This suggests that while these functions were audited, the audits may not have adequately addressed all potential vulnerabilities.

`Initialize` functions show a contrasting trend where non-audited functions were responsible for a larger share of losses, amounting to 51.1% ($190,000,000 USD), significantly above their occurrence rate of 33.3%.

`Mint` functions predominantly experienced losses from non-audited functions, with these accounting for 89% ($195,000,000 USD) of the losses, much higher than the occurrence rate of 66.7%. This indicates a potential higher loss in non-audited mint functions that attackers can exploit.

For `swap` functions, a similar pattern emerges, with non-audited functions leading to 71% of the financial losses ($76,700,000 USD), again exceeding their occurrence rate of 66.7%. This suggests that the risks associated with swap functions, when not audited, can lead to substantial damages.

In the case of `verifyProof` functions, non-audited ones led to a substantial 64.3% ($586,000,000 USD) of the losses, which is significantly higher than their occurrence rate of 50%. This indicates that critical vulnerabilities in `verifyProof` functions are more prevalent or more severe in non-audited setups.

Finally, `withdraw`-like functions saw most losses originating from non-audited functions, accounting for 66.7% ($227,000,000 USD) of the losses, despite these functions making up 55.6% of the occurrences. This highlights potentially a significant vulnerability in non-audited withdraw functions that can lead to considerable financial losses.

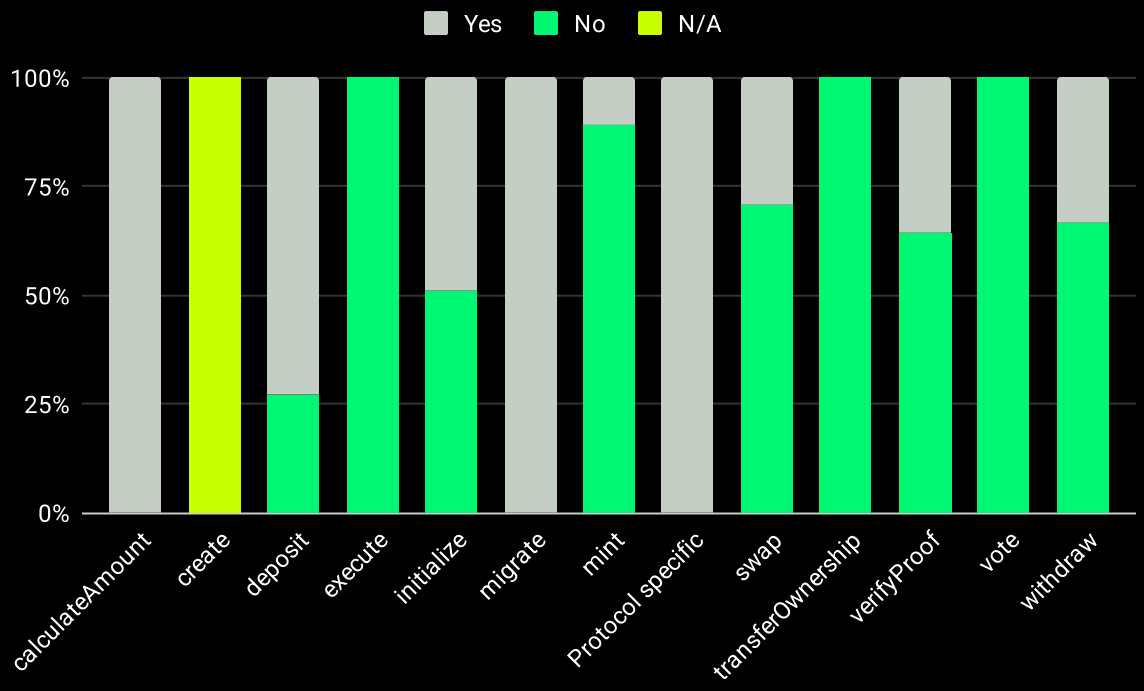

Figure 217: Loss caused per state of audition per type of function [percentage]

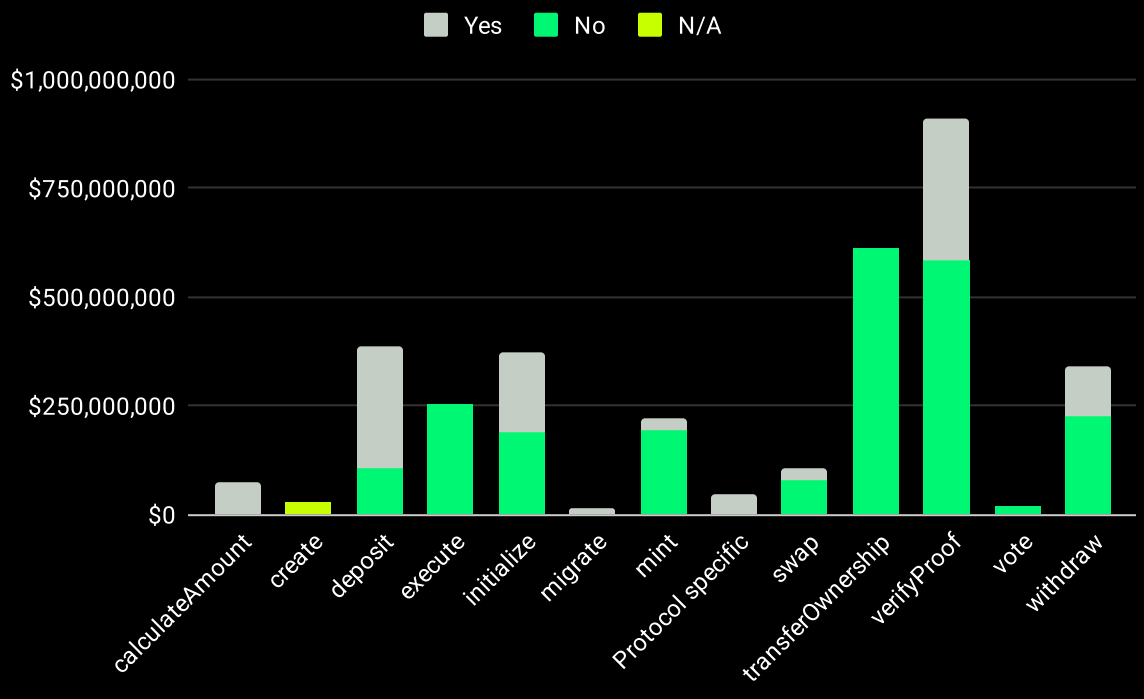

Figure 218: Loss caused per state of audition per type of function [USD]

Figures 219 and 220 provide a detailed chronological analysis of the audit status of blockchain functions that have been exploited over the years.

For the `calculateAmount` function, it consistently remained audited across both years documented.

The audit status for `deposit` functions showed significant variability over the years. In 2020, the deposit function was not audited, which shifted to all being audited in 2021, reverting back to non-audited in 2022, and then returning to audited status in 2023 and 2024. This fluctuation in audit status suggests changes in security practices or varying levels of perceived risk associated with deposit functions across different years.

`Initialize` functions experienced a shift from being audited in 2017 to not audited in 2022, indicating a potential decrease in security focus or changes in the usage or complexity of these functions that might have impacted auditing decisions.

For `mint` functions, the year 2021 saw an even split between audited and non-audited status, while in 2022, the mint function exploited was not audited, suggesting a lapse in security coverage during this period or a perception of less potential danger caused by these types of functions.

`Swap` functions in 2020 were not audited, but by the following year, there was a mix of audited and non-audited, indicating an increased recognition of the risks associated with swap functions or, possibly, an adjustment in audit practices to cover more instances.

`Withdraw` functions showed a mix of audit statuses in 2021, with half being audited and half not, but in 2022, both instances of withdraw functions exploited were non-audited. By 2024, the withdraw function that was exploited was audited.

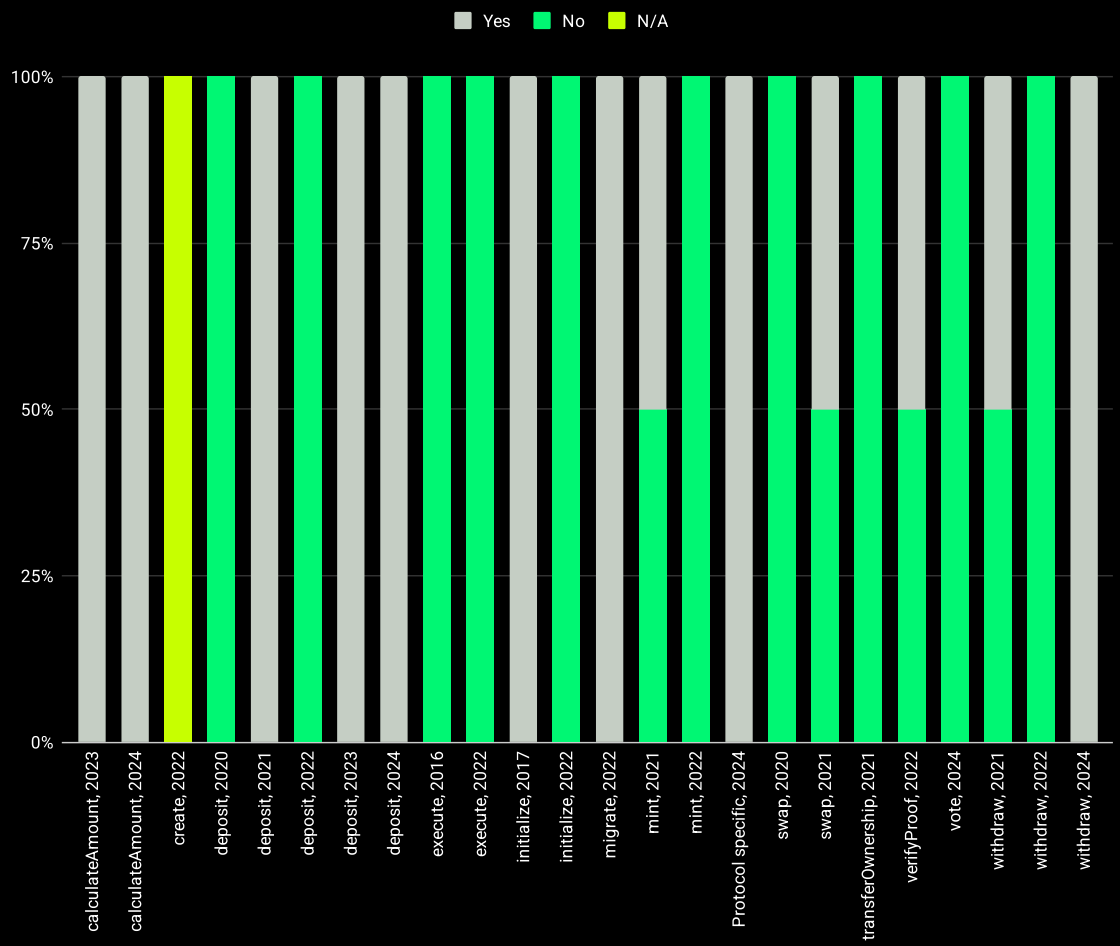

Figure 219: State of audition per type of function and year [percentage]

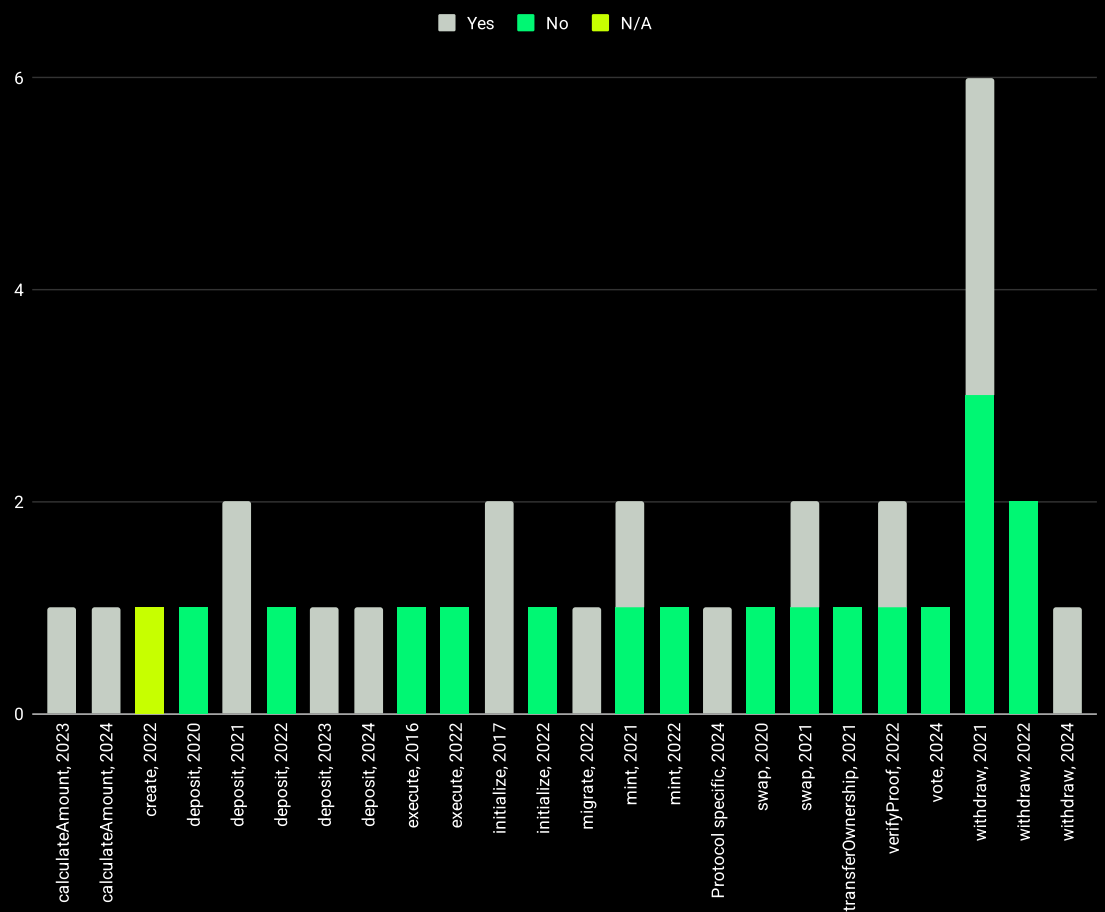

Figure 220: State of audition per type of function and year [count]

Figures 221 and 222 delve into the financial impacts of blockchain function exploits, segmented by the audit status of the functions across different years.

In 2021, `mint` functions, which were responsible for half of the hacks involving this type of function, accounted for a disproportionately large segment of the financial losses, amounting to 86% or $147,000,000 USD

Similarly, `swap` functions in 2021 also demonstrated a significant discrepancy between the number of incidents and the extent of loss; while only involved in half of the `swap`-related attacks, they were responsible for 64.5% of the financial losses, totaling $57,000,000 USD.

In 2022, `verifyProof` functions followed a similar pattern, with half of the breaches in these functions accounting for 64.3% of the year's total financial losses from such exploits, which amounted to $586,000,000 USD.

For `withdraw` functions in 2021, although they constituted half of the incidents, they resulted in 59% of the financial losses, amounting to $126,800,000 USD.

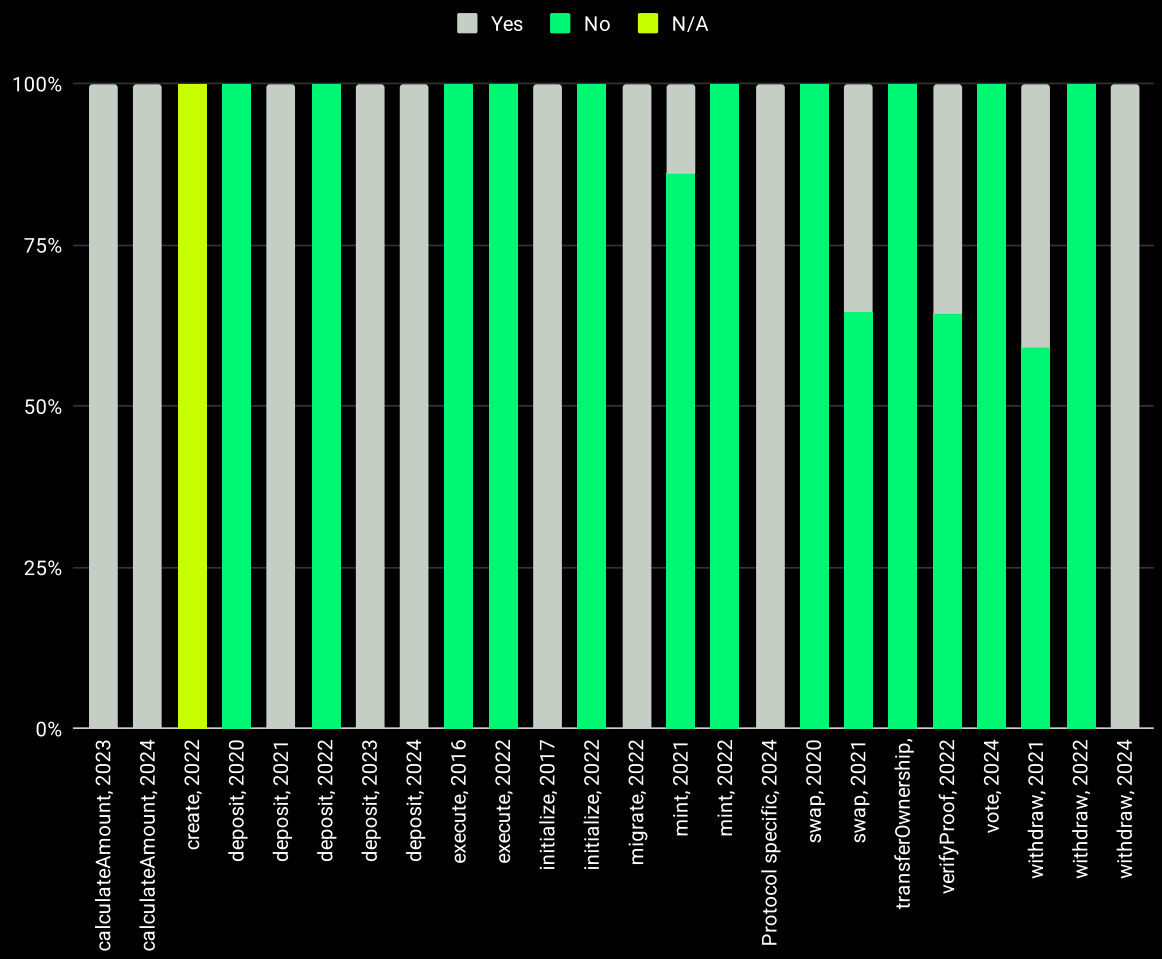

Figure 221: Loss caused per state of audition per type of function and year [percentage]

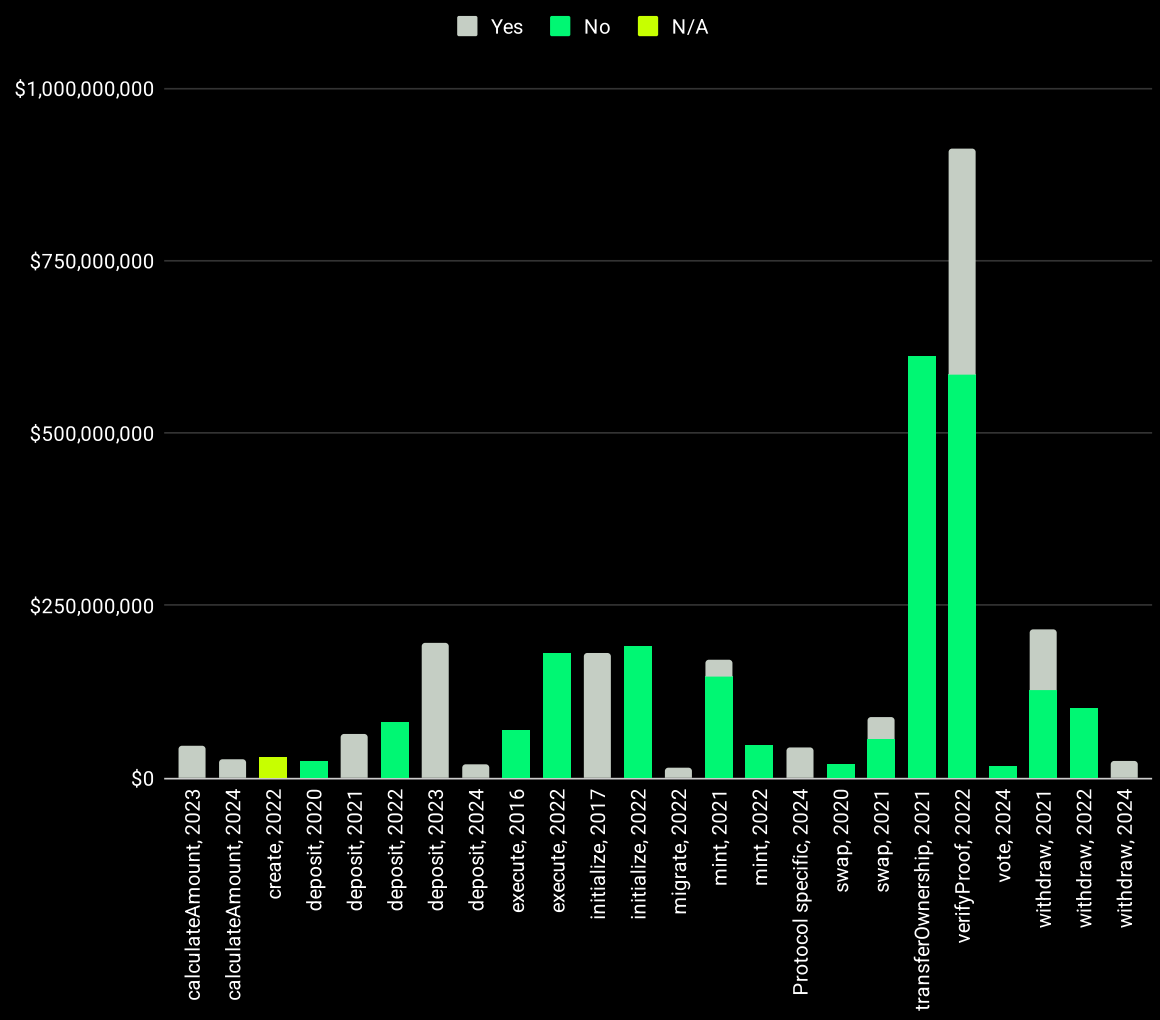

Figure 222: Loss caused per state of audition per type of function and year [USD]

ACTIONABLE TAKEAWAYS

Based on the data analyzed and the key findings discussed earlier, several actions are recommended to enhance the security of blockchain protocols:

- **Comprehensive Auditing**: Developers should not only audit smart contracts but also consider the entire ecosystem, including traditional security audits. This comprehensive approach should include the protection of private keys and the systems where they are stored. Users should seek out protocols that undergo full audits beyond just smart contracts to ensure robust security.
- **Enhanced Key Management**: Implementing multi-signature or Multi-Party Computation (MPC) and using cold wallets can significantly reduce the risk of theft. These measures ensure that even if one component is compromised, the overall system remains secure.
- **Mitigate Flash Loan Risks**: Developers should design protocols to consider the implications of flash loans, such as using snapshots for calculating exchange prices and voting power to prevent exploitation through these mechanisms.
- **Oracle Integrity**: To avoid the pitfalls of flawed oracles, utilize reputable, multi-source, decentralized, and incentive-driven oracles like Chainlink. Additionally, maintaining a backup oracle can provide a fail-safe against the primary oracle's failure.
- **Targeted Protocol Protection:** Given the high risk associated with Lending protocols, Bridges, Wallets, and CEXs, developers should focus on preventing direct contract exploitation and market manipulations as well as enhancing key management. Careful code reviews and securing administrative keys are crucial. Users should exercise caution and prioritize protocols that have undergone thorough audits, potentially favoring DEXes or other safer alternatives.
- **Focus on High-Risk Functions**: Special attention should be paid to programming critical functions such as withdrawals, deposits, ownership transfers, and proof verifications, which have been identified as high-risk areas. Developers should be meticulous in avoiding coding errors that could lead to vulnerabilities.

- **Decentralization as a Defense:** Decentralized protocols tend to be less targeted by attacks and incur lower losses. This should be a consideration for both developers in the design of new protocols and users when choosing which platforms to engage with.
- **Regular Updates and Patches**: As seen with the shifts in vulnerabilities and attacks over time, regularly updating and patching smart contracts in line with the latest security developments and threat intelligence can help preempt potential exploits.