FAIRYPROOF

Review of Blockchain Security in 2022

Presented by Fairyproof
January 2023

Executive Summary

The overall crypto market entered a bear market in and through 2022. However attacks against the crypto ecosystem were still active.

- Crypto assets worth around US $2.52 billion were exploited in 378 prominent security incidents.

- 11 attacks against cross-chain bridges totaled a loss of US $1.01 billion accounting for 39.94% of the overall total loss in 378 incidents. The security of cross-chain bridges has become a prominent issue.

- Attacks that exploited logic vulnerabilities, flash-loans, price manipulation, governance vulnerabilities and re-entrancy vulnerabilities resulted in a loss of US $571.34 million and this loss accounted for 69.64% of the total loss in the attacks against smart contracts alone. These vulnerabilities could have been uncovered and the loss could have been prevented if these attacked contracts had been professionally audited.

- The loss (US $999.79 million) caused by private keys leaked accounted for 42.18% of the total loss in the attacks from hackers. Safely and securely managing private keys should always be the Number 1 thing any crypto users should keep in mind.

- The loss (US $35 million) caused by attacks against layer 2 solutions far surpassed the loss(US $5.95 million) caused by attacks against blockchain mainnets. The security of layer 2 solutions is a much serious concern than the security of blockchain mainnets.

- In 2022, Fairyproof had extensively researched the ZK(zero-knowledge proof [1]) related technologies and has been familiar with the existing mainstream solutions in the industry. Fairyproof has established its own development process and model, and can promptly deliver solutions based on application requirements. With regards to ZK-related audits, Fairyproof has rich experience and is proficient in converting a problem to ZK circuits, auditing circuits, proof generation, proof verification, and more. In addition, Fairyproof has been actively working on optimizing ZK-related implementation and improving its security such as using MPC technology to decentralize the initial setup in ZK-Snark implementations.

- In 2022, Fairyproof had established strong technical strength in MPC [2] related technologies and has established its own development process and model, and can promptly deliver solutions for popular applications such as using MPC to do omnichain transactions

BACKGROUND

Before proceeding, the following terms and technologies are introduced in this report:

CCBS

CCBS stands for “Centralized Crypto or Blockchain Service”. A CCBS refers to a platform or service that provides crypto or blockchain related products or services, and is run by a conventional / centralized organization, entity or company such as conventional crypto exchanges (eg. Binance or Tether).

FLASHLOAN

Flash loans are a popular feature that hackers utilize when attacking EVM-Compatible smart contracts. Flash loans were developed by the team behind the famous DeFi application AAVE [3]. This feature “allows users to borrow any available amount of assets without putting up any collateral, as long as the liquidity is returned to the protocol within one block transaction” [4]. Flash loans are quite often used to borrow ERC-20 tokens [5] and attack DeFi applications. To initiate a flash loan, users will need to write a contract that borrows an available amount of assets and pay back the loan + interest + necessary fees all within the same transaction.

CROSS-CHAIN BRIDGE

A cross-chain bridge is an infrastructure that connects multiple independent blockchains and enables an exchange of cryptos, data or information from one blockchain to another.

As more blockchains have their own ecosystems, cryptos and dApps, the need for exchanging cryptos or data across different blockchains becomes increasingly high while the volume of cross-chain transactions dramatically increase. This causes cross-chain bridges to suffer more attacks.

FOCUS OF THIS REPORT

In this report we list our statistics collected from typical security incidents that happened in the blockchain industry in 2022, give an in-depth analysis of their root causes, and present our recommended best practices.

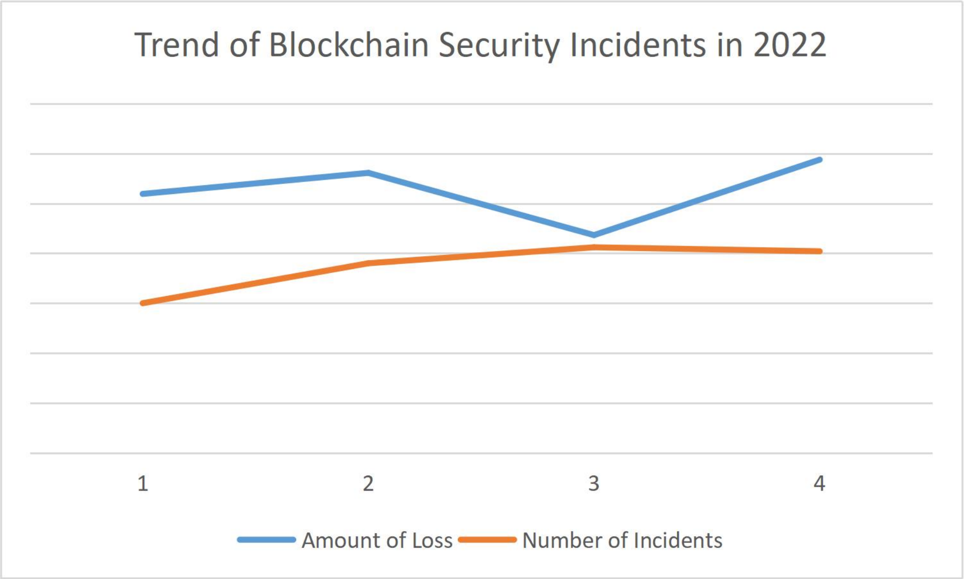
STATISTICS AND ANALYSIS OF SECURITY INCIDENTS OF 2022

We studied 378 prominent security incidents that occurred in 2022 and present our statistics and analysis based on the targets and root causes.

In 2022 the total value of the exploited assets was US $2.52 billion and the overall market cap of the cryptocurrency according to Tradingview was US $756.15 billion. The value of the exploited assets accounted for 0.33% of the total market cap of the cryptocurrency.

OVERALL TREND OF BLOCKCHAIN SECURITY INCIDENTS OF 2022

We studied each quarter's blockchain security incidents and came up with the following trend graph:



From this graph we can see that the number of incidents throughout the year had been increasing except Q4 and the amount of loss had been increasing as well except Q3.

INCIDENTS CATEGORIZED BY TARGETS

Our researched incidents can be categorized into four types of targets:

1. CCBS
2. Blockchains
3. DApps
4. Cross-chain Bridges

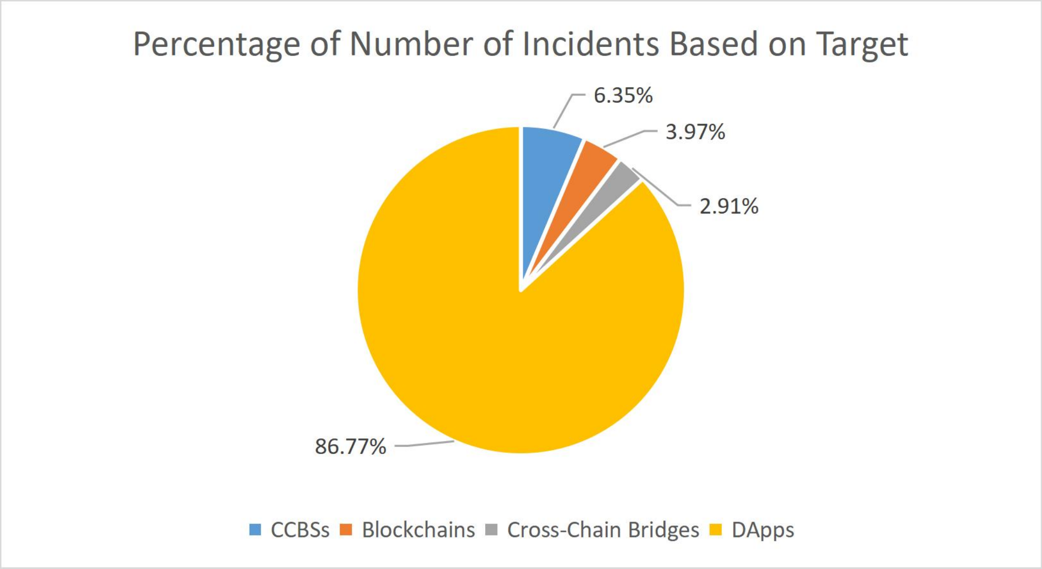
A CCBS-related incident is one in which a centralized crypto or blockchain service platform is attacked by hackers resulting in the failure of its services or a loss of crypto assets under its custody.

A blockchain-related incident is one where a blockchain mainnet, side chain or layer 2 is attacked by malicious actors from inside, outside, or both, resulting in its operation going out of order, or that a blockchain fails to work properly due to issues related to software, hardware, or both. Attackers will then be able to exploit the consensus for profits.

A dApp-related incident is one where a dApp's daily operation goes out-of-order or is attacked, leaving it open for attackers to exploit users and crypto assets under the custody of the dApp.

A cross-chain bridge-related incident occurs when a cross-chain bridge is attacked resulting in a loss of crypto assets under its custody or a failure of the exchange function between multiple blockchains.

There were 378 incidents in total. Here is a figure that shows the percentage for each of these targets respectively.



The number of dApp-related incidents account for more than 86.77% of the total incidents. Out of 378 incidents, 24 were CCBS-related, 15 were blockchain-related, 11 were cross-chain bridge-related, and 328 were dApp-related.

BLOCKCHAIN-RELATED INCIDENTS

Incidents that had occurred in blockchains can be further categorized into three sub-categories:

i. Blockchain mainnets
ii. Side chains
iii. Layer 2 solutions

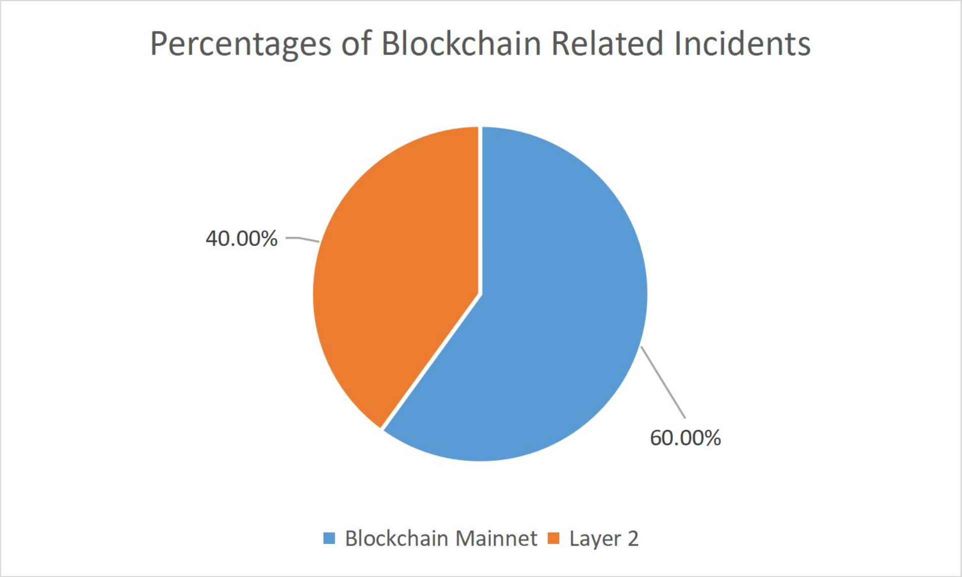
A blockchain mainnet, also known as layer 1, is an independent blockchain that has its own network with its own protocol, consensus, and validators. A blockchain mainnet can validate transactions, data, and blocks generated in its network by its own validators and reach a finality. Bitccoin and Ethereum are typical blockchain mainnets.

A side chain is a separate, independent blockchain which runs in parallel to a blockchain mainnet. It has its own network consensus and validators. It is connected to a blockchain mainnet (eg. by a two-way peg [6]).

A layer 2 solution refers to a protocol or network that relies on a blockchain as its base layer (layer 1) for security and finality [7]. Its main purpose is to solve scalability issues of its base layer. It processes transactions faster and costs less resources compared to its base layer. Since 2021, there has been a huge surge in the growth and development of layer 2 solutions for the Ethereum ecosystem.

Both side chains and layer 2 solutions exist to solve the scalability issues of a blockchain mainnet. The significant difference between a side chain and a layer 2 solution is that a side chain does not necessarily rely on its blockchain mainnet for security or finality whereas a layer 2 solution does.

There were 15 blockchain-related incidents in total in 2022. The figure below shows the percentages of blockchain mainnet related incidents, side-chain related incidents, and layer 2 related incidents respectively.



The number of blockchain mainnet related incidents and layer 2 related incidents account for 60% (9) and 40% (6) of the total incidents respectively. No prominent side-chain related incidents were covered in our statistics. The layer 2 solutions that were attacked included 4 Ethereum layer 2 solutions and they were Loopring [8], zkSync [9], Optimism[10] and Arbitrum[11], while the majority of the attacked blockchain mainnet were non-EVM blockchains.

DAPP RELATED INCIDENTS

Among the 328 incidents that occurred toward dApps, 35 were rug-pulls, 148 were involved in exploitations and 145 were directly attacked. An attack against a dApp can specifically target its front-end, server side, or smart contract(s). We can therefore further classify these 145 incidents into three sub-categories:

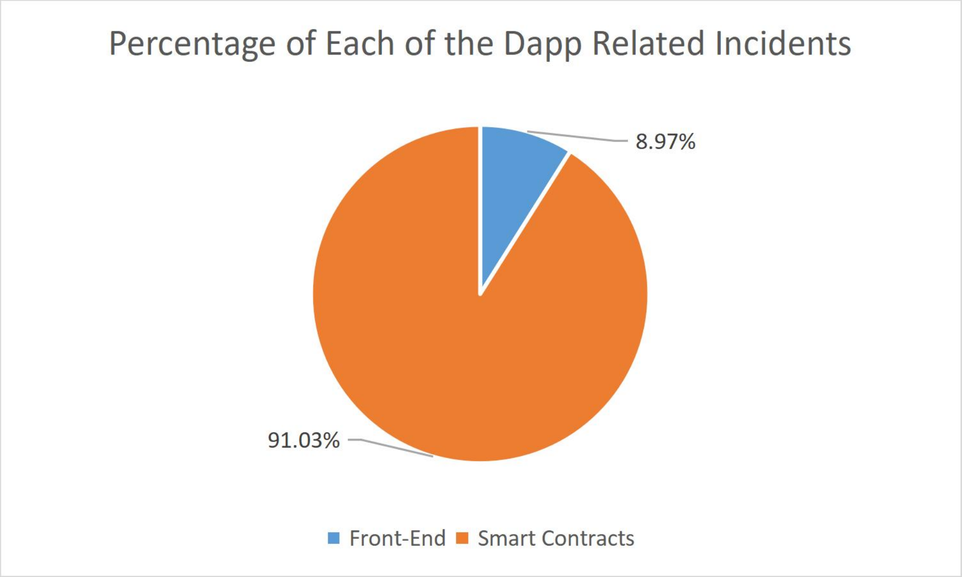
i. dApp's front-end
ii. dApp's server side
iii. dApp's smart contract(s)

dApp's front-end related incidents refers to events where vulnerabilities from the conventional client side are exploited, compromising on the account information and personal details of users which can be used to steal their crypto assets.

dApp's server side related incidents are those where vulnerabilities present in the conventional server side are exploited, leaving on-chain and off-chain communication open for hijacking and crypto assets of users open for exploitation.

Smart contract related incidents refer to vulnerabilities in a smart contract's design or implementation, which are leveraged to exploit crypto assets from users.

Here is a figure that shows the percentages of front-end, server-side and smart contract related incidents respectively.

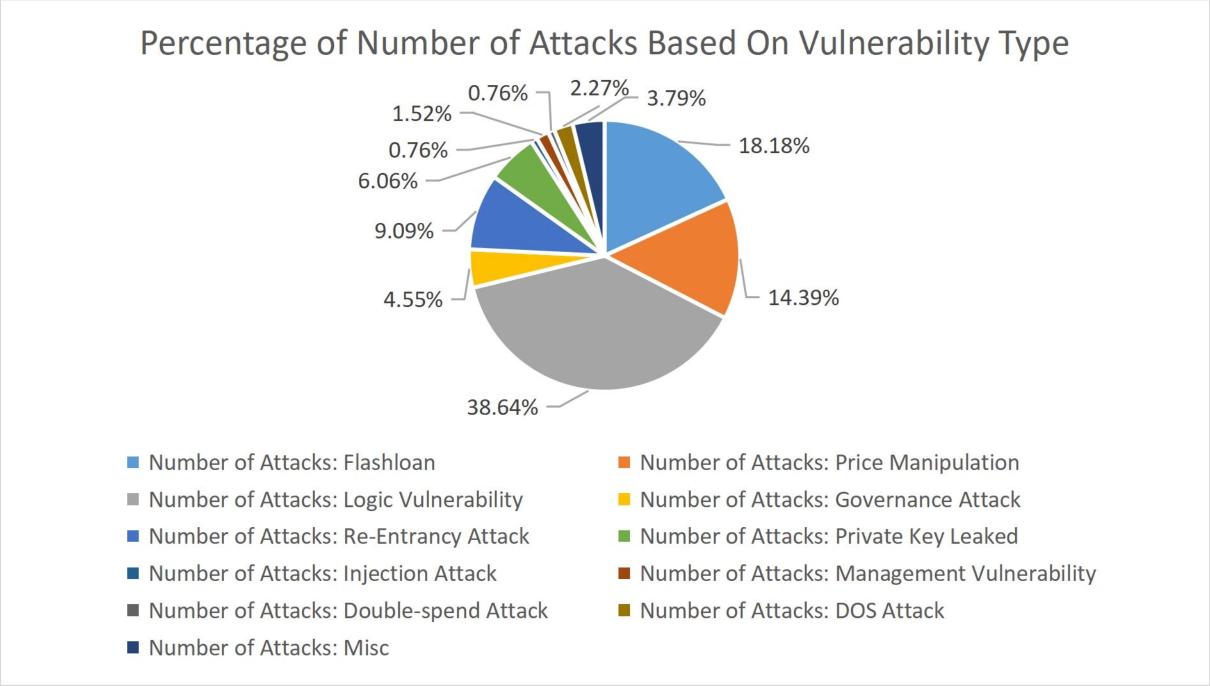


The above figure shows the number of smart contract related incidents, server side related incidents, and front-end related incidents, accounting for 91.03%, 0%, and 8.97% of the total incidents respectively. Among 145 incidents, 13 were front-end related and 132 were smart contract related.

We further studied the amount of loss incurred from these sub-categories. Our study showed that the amount of losses in both front-end related incidents was US $6.06 million, and the amount of loss in smart contract related incidents was US $820.26 million.

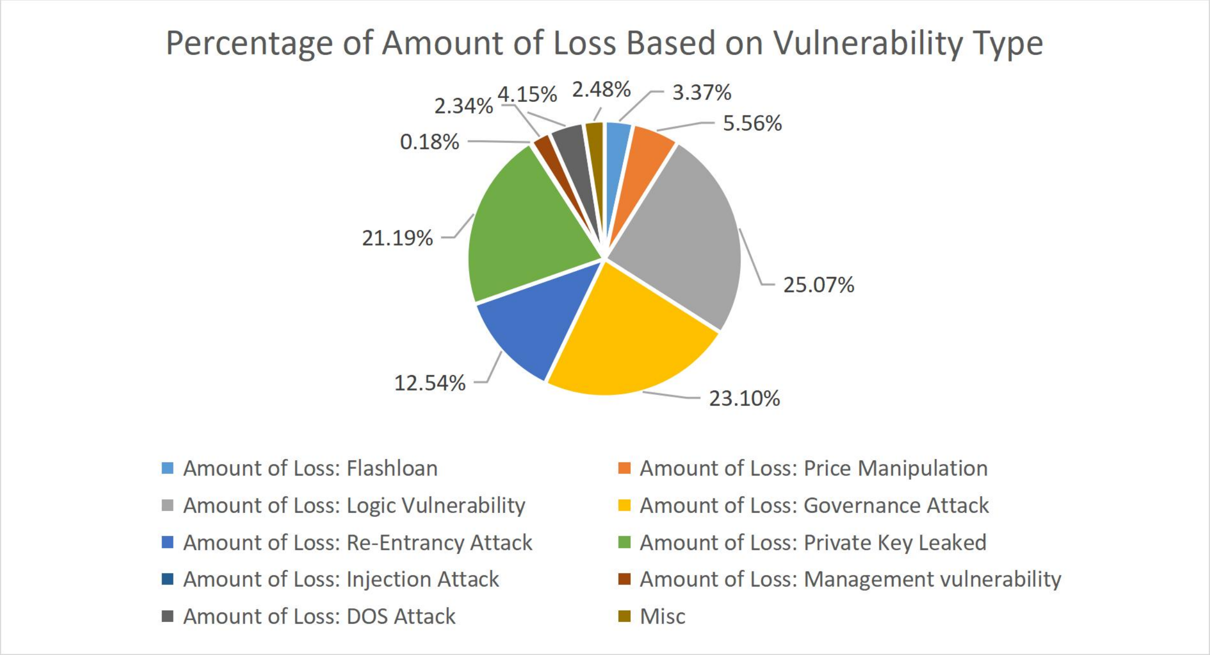
It is clear that smart contract related incidents were the biggest issue. Typical vulnerabilities we found pertaining to smart contracts in 2022 include logic vulnerabilities, private key leaks, flash loans, re-entrancy attacks, and more.

We studied the 132 incidents in which smart contracts were directly attacked and derived the following figure based on vulnerability types:



The figure shows that the number of incidents with the highest percentages were logic vulnerabilities and followed by flashloan attacks. Logic vulnerabilities mainly include missing validations for parameters, missing validation for access control, etc. 51 projects suffered from logic vulnerabilities and 24 suffered from flashloan attacks.

The following figure illustrates the amount of loss for each vulnerability type:



The amount of loss caused by logic vulnerabilities still ranked first. 51 incidents were caused by logic vulnerabilities, totaling a loss of US $205.64 million. This loss accounting for 25.07% of the total loss. The amount of loss caused by governance attacks ranked second. 6 incidents were caused by governance attacks, totaling a loss of US $189.51 million. This loss accounted for

23.1% of the total loss. Meanwhile, 8 incident caused by private key leaks totaled a loss of US $173.85 million and accounted for 21.19% of the total loss, ranking third.

INCIDENTS CATEGORIZED BY ROOT CAUSES

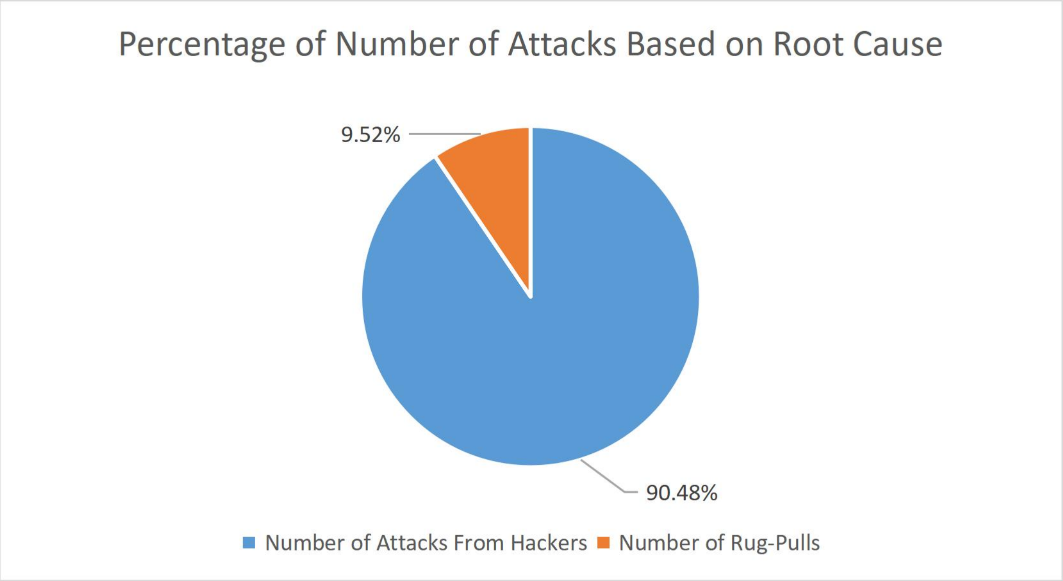
The root cause of these incidents can be categorized into the following:

i. Attacks from hackers

ii. Rug-pulls

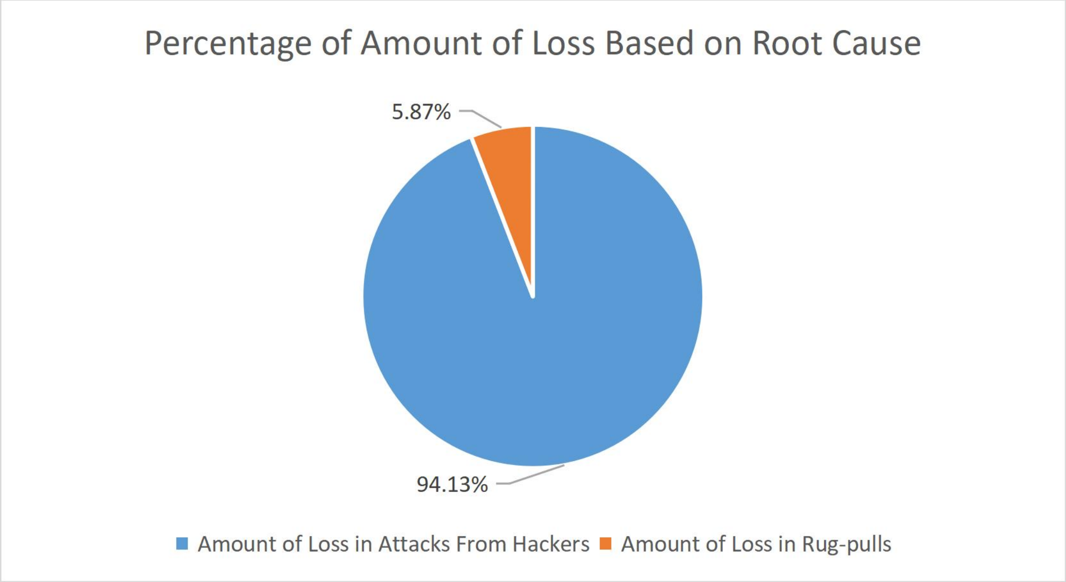
iii. Misc.

We studied these incidents and got the following figure.



The above figure shows that the number of attacks from hackers and rug-pulls incidents accounted for 90.48% (342) and 9.52% (36) of the total incidents respectively.

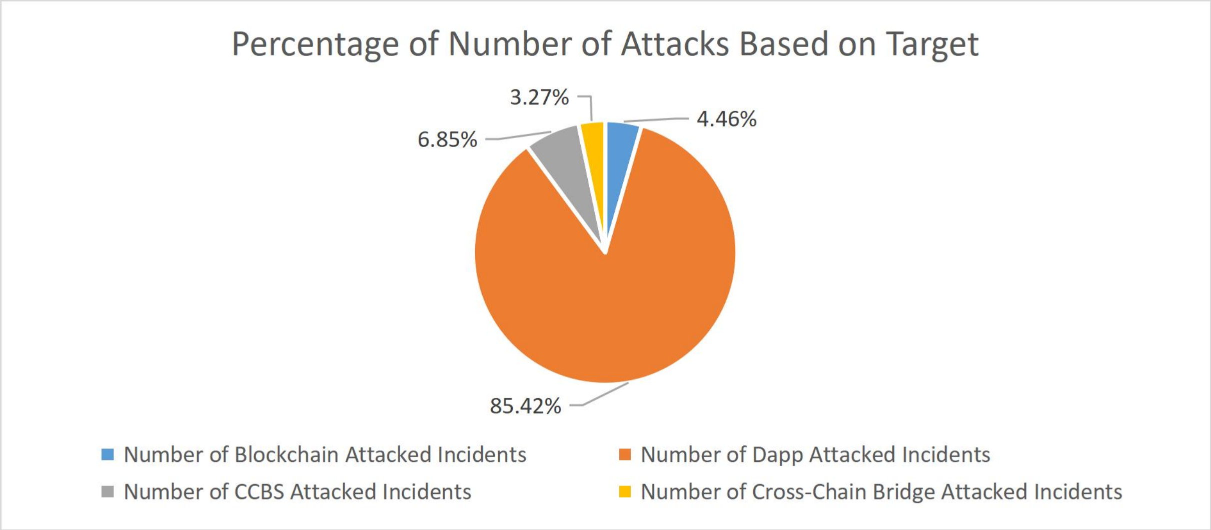
We studied the amount of loss of each category of incidents based on the root cause and got the following figure:



The above figure shows that the amount of loss in the incidents that suffered from attacks and the amount of loss in rug-pull incidents each accounted for 94.13% and 5.87% of the total loss respectively. The amount of loss in the incidents that suffered from attacks was US $2.37 billion and the amount of loss in rug-pull incidents was US $0.15 billion. This reveals that attacks from hackers posed the largest threat to the whole crypto ecosystem in 2022.

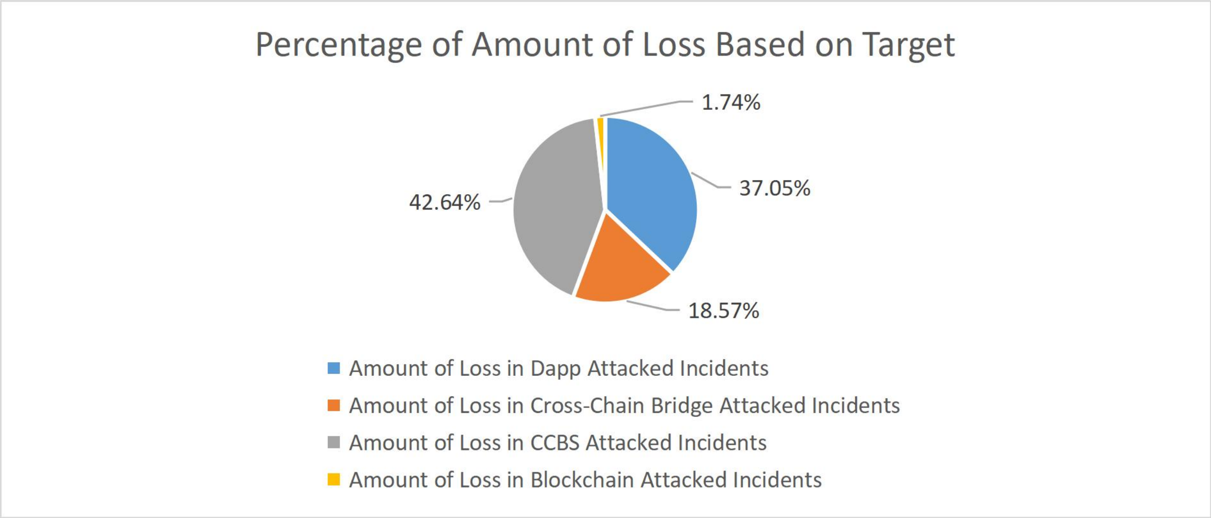
ATTACKS FROM HACKERS

We studied the targets the hackers attacked and got the following figure:



The figure above shows that the number of attacks on dApps, CCBSs, blockchains and cross-chain bridges accounted for 85.42% (287), 6.85% (23), 4.46% (15) and 3.27% (11) respectively.

After we studied the amount of loss in each of them we got the following figure:



The amount of loss in attacks on cross-chain bridges, dApps, CCBSs and blockchains were 42.64%, 37.05%, 18.57% and 1.74%, resulting in a loss of US $1.01 billion, US $873.95 million, US $438.06 million and US $40.95 million respectively.

RUG-PULLS

The rug-pulls that happened in 2022 were against dApps or CCBSs. 1 was a CCBS rug-pull and 35 were dApp rug-pulls. There were 36 incidents totaling a loss of US $147.85 million which were not as severe as losses caused by attacks.

RESEARCH FINDINGS

dApps were the most prominent target for attacks in 2022 as the most number of attacks were against them. However the amount of loss caused by cross-chain bridge attacks ranked first totaling a loss of US $1.01 billion and accounting for 42.64% of the total loss that suffered from attacks from hackers. This reveals that the overall security situation of the existing cross-chain bridges is a big concern for the whole crypto space.

Hackers proved to remain as the main threat to the crypto industry, accounting for more than 90% of all the number of incidents and more than 94% of the total loss. It far surpassed any other root causes such as rug-pulls, etc.

Both the number of attacks on layer 2 solutions and the amount of loss in these attacks increased dramatically in 2022 compared to those of 2021. We think this will be an irreversible trend because layer 2 solutions have and will keep emerging drastically in the following years.

A dApp consists of three parts: a front-end, a server-side and smart contracts. Either one or multiple parts are targeted during dApp attacks. According to our statistics, smart contract(s) accounted for an extraordinarily high percentage of attacks compared to the front-ends or server sides with regard to both attack frequencies and amount loss in 2022. This shows that attacks on smart contracts still posed as the biggest threat to dApps.

Most of the rug-pulls in 2022 were dApps accounting for 97.22% of the total number of rug-pulls and 78.36% of the total loss in rug-pulls.

Finally, for smart contract related incidents, we found the number of attack sub-categories (except the misc incidents) to be ranked as the following:
Rank 1: Logic vulnerability
Rank 2: Flash-loan
Rank 3: Price manipulation.
And the amount of loss in the incidents that suffered from logic vulnerabilities far surpassed any one of these ranks.

TENTATIVE THOUGHTS

In addition, more project teams rushed to or planned to jump in Zero Knowledge (zk) related applications including zk-rollup solutions for Ethereum, zk related social applications, and more. We think there will be an increasing demand for audits of zk related applications.

Both the number of attacks on cross-chain bridges and the amount of loss in these attacks in 2022 far surpassed those of 2021.

This has raised a big concern to the whole crypto space. Quite a few teams have been exploring various new solutions to improve the security of the existing cross-chain bridge solutions. The MPC technology is one of the promising solutions. We think more mature and affordable solutions based on the MPC technology will emerge in the following years. And there will be an increasing demand for audits of MPC related applications and solutions.

BEST PRACTICES TO PREVENT SECURITY ISSUES

In this section we present some best practices to help both blockchain developers and users manage the risks posed by the incidents that happened in 2022, and support coordinated and efficient response to crypto security incidents. We would recommend both blockchain developers and users to apply these practices to the greatest extent possible based on the availability of their resources.

Note: “Blockchain developers” refers to both developers of blockchains and developers of dApps, and blockchains or systems pertaining to crypto cyrrencies. Here, “blockchain users” refer to everyone that participates in activities pertaining to crypto system’s management, operation, trading, etc.

FOR BLOCKCHAIN DEVELOPERS

Developers of cross-chain bridges need to pay closer attention to the bridges’ security as cross-chain transactions become increasingly popular. Cross-chain bridge solutions include handling of operations – not only on-chain but also off-chain. Naturally, the off-chain part would be more vulnerable to attacks. Hence, security solutions for cross-chain bridges should be particularly capable of handling off-chain activities safely and securely.

Awareness of security for layer 2 solutions should still be kept even though attacks on them were few with negligible losses as more layer 2 solutions will emerge in the coming years. Research and development for solutions to tackle security challenges in this area must be prompt.

A step to transfer an admin’s access control to a multi-sig wallet or a DAO to manage access control to crypto assets or critical operations is a must-have.

Attackers would employ flash loans to maximize their exploits when they detect vulnerabilities in smart contracts, including issues of re-entrancy, missing validations for access control, incorrect token price algorithm, and more. Proper handling of these issues should have the highest priority for a smart contract developer when designing and coding a smart contract.

Our statistics show that an increasing number of hackers have been using social media tools – especially Discord – to launch phishing attacks. This persisted through the whole year of 2022 and will very likely persist in 2023. Many users have suffered huge losses. Project developers and managers are advised to prioritize safely and securely managing social media accounts and finding security solutions for them on top of project implementation.

FOR BLOCKCHAIN USERS

More users are varying their crypto portfolio across different blockchains. The demand for cross-chain transactions is rapidly increasing. Whenever a user participates in a cross-chain transaction, the user will have to interact with a cross-chain bridge – a popular target among hackers. Hence, before starting a cross-chain transaction, users are advised to investigate the bridge's security condition and ensure they use a reliable, safe and secure bridge.

While it is necessary to pay great attention to the security for smart contracts when interacting with a dApp, the importance to also pay attention to the security of the user interface while exercising caution to detect suspicious messages, prompts, and behavior presented by the UI is increasing.

We strongly urge users to check whether a project has audit reports and read these reports before proceeding with further actions.

Use a cold wallet or a mutl-sig wallet where possible to manage crypto assets that are not for frequent trading. Be careful about using a hot wallet and make sure the hardware in which a hot wallet is installed is safe and secure.

Be cautious of a dApp where its team members are unknown or lack reputation. Such dApps may eventually be rug-pull projects. Be cautious of a centralized exchange which has not established a reputation or does not have tracked transaction data on third party media as it may also eventually prove to be rug-pull projects.

REFERENCES

[1] zero-knowledge proof. https://en.wikipedia.org/wiki/Zero-knowledge_proof

[2] MPC. https://en.wikipedia.org/wiki/Secure_multi-party_computation

[3] Aave. https://aave.com/

[4] Flash-loans.. https://aave.com/flash-loans/

[5] ERC-20 TOKEN STANDARD. https://ethereum.org/en/developers/docs/standards/tokens/erc-20/

[6] Sidechains. https://ethereum.org/en/developers/docs/scaling/sidechains/

[7] Layer-2. https://academy.binance.com/en/glossary/layer-2

[8] Loopring. https://loopring.org/#/

[9] zkSync. https://zksync.io/

[10] Optimism. https://www.optimism.io/

[11] Arbitrum. https://arbitrum.io/