FAIRYPROOF

Review of Blockchain Security in Q1 2022

Presented by Fairyproof
April 2022

OVERVIEW

After Bitcoin and Ethereum reached their all-time highs at the end of 2021, they both experienced a 50% dip in Q1 2022. So does the whole crypto market. As the market bubble burst, the whole crypto market no longer gains that much traction from investors. However, the crypto ecosystem was still attractive to hackers.

Based on Fairyproof's statistics, there were 75 publicly-reported security incidents taking place in Q1 2022. And more than $1.26 billion of crypto-assets were exploited.

We studied these 75 incidents and compose our findings, analysis, and best practices in this report.

BACKGROUND

Before we proceed, it is necessary to introduce some terms and technologies that we mention in this report.

CCSS

CCSS stands for "centralized crypto custody service". A CCSS refers to a platform or a service that provides crypto-related products or services and is run by a conventional/centralized organization, entity, or company such as conventional crypto exchanges e.g. Coinbase[1] and crypto Fintech companies e.g Stobox[2].

FLASHLOAN

Flash loans were a popular feature that had been utilized by hackers in 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]. 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.

In the past flash, loans were often used to borrow ERC-20 tokens [5] and attack DeFi applications, however in Q1 2022, this feature was utilized to exploit NFT applications [6].

FLASH LOANS IN NFT APPLICATIONS

Right after flash loans were created, they were introduced in NFT-related applications such as NFTX [7], NFT20[8], etc. For an application that has pools of NFTs, users can take out a flash loan on any of the pools and borrow any of the available NFTs locked in the application without collateral and return the NFTs to the pools within a single trading block. If this is completed, the entire transaction will revert.

FOCUS OF THIS REPORT

In this report we list our statistics collected from typical security incidents that happened in the blockchain industry in Q1 2022, give an in-depth analysis of their root causes and present our recommended best practices.

STATISTICS AND ANALYSIS OF SECURITY INCIDENTS OF Q1 2022

We studied 75 publicly-reported security incidents that took place in Q1 2022 and present our statistics and analysis based on the suffering targets and root causes.

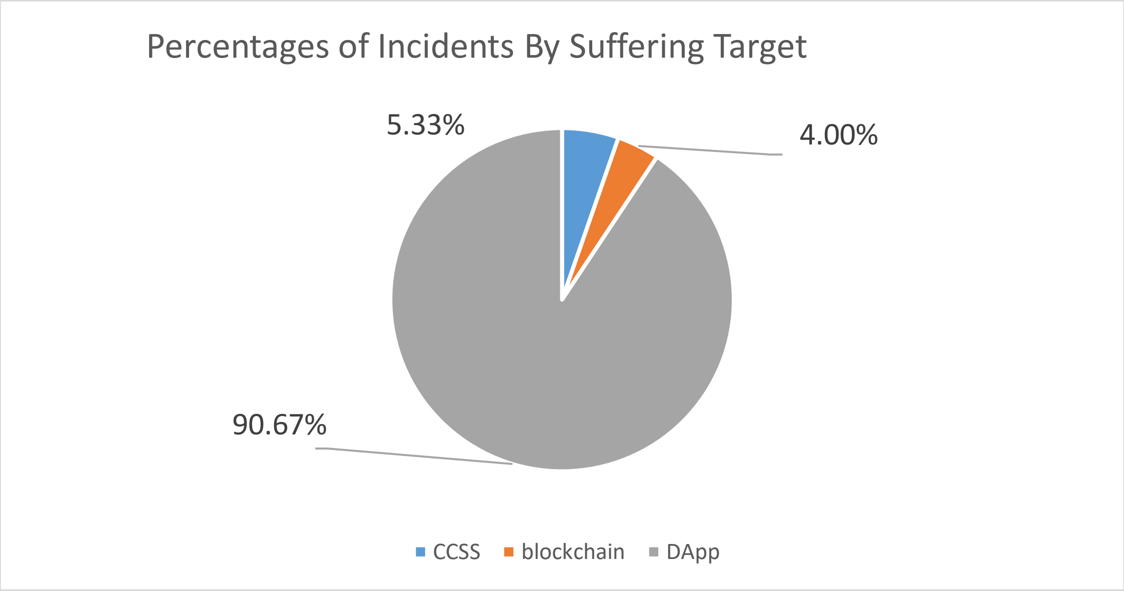
INCIDENTS CATEGORIZED BY SUFFERING TARGET

Based on the type of suffering target, our researched incidents can be categorized into two types: blockchains and DApps.

A blockchain-related incident is one in which a blockchain is attacked by malicious actors from either inside or outside or both such that its operation would go out of order, or a blockchain fails to work properly due to either software issues or hardware issues or both such that attackers would be able to exploit the consensus for profits.

A DApp-related incident is one in which a DApp is attacked or a DApp's daily operation goes out of order such that attackers would be able to exploit users' crypto assets that are under custody of the DApp.

There were 75 incidents in total and here is a figure that shows the percentages of CCSS-related incidents, DApp-related incidents, and blockchain-related incidents respectively.



The above figure shows that the number of DApp-related incidents accounted for more than 90% of the total incidents. Among 75 incidents, 4 were CCSS related, 3 were blockchain-related and 68 were DApp related.

BLOCKCHAIN-RELATED INCIDENTS

Among the incidents that happened to blockchains, we further categorize them into three sub-categories: blockchain main nets, side chains, and layer 2 solutions.

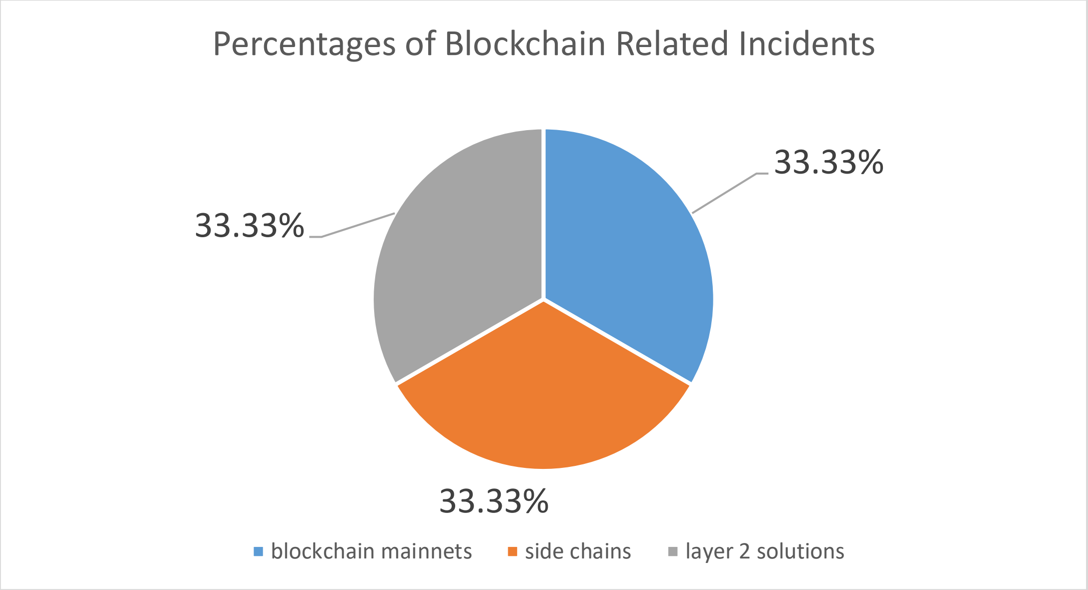
A blockchain mainnet, also known as lay 1 is an independent blockchain that has its network with its protocol, consensus, and validators. A blockchain mainnet can validate the transactions, data, and blocks that are generated in its network by its validators and reach a finality. Bitcoin and Ethereum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

A side chain is a separate blockchain which runs in parallel and independently to a blockchain mainnet. It has its network, consensus, and validators. It is connected to a blockchain mainnet e.g., by a two-way peg [9].

A layer 2 solution refers to a protocol or network that relies on a blockchain as its base layer for security and finality [10]. The base layer is also referred to as layer 1. Layer 2's main purpose is to solve the base layer's scalability issues. A layer 2 solution processes transactions much faster and costs much less compared to its base layer. The Ethereum blockchain, for instance, saw a huge surge in the growth and development of layer 2 solutions about it since 2021.

Both side chains and layer 2 solutions are to solve blockchain mainnets' s scalability issues. The significant difference between a side chain and a layer 2 solution is that a side chain doesn't necessarily rely on its blockchain mainnet for security or finality, but a layer 2 solution does.

There were 3 blockchain-related incidents in total in Q1 2022 and here is a figure that shows the percentages of blockchain mainnets related incidents, side-chain related incidents, and layer 2 related incidents respectively.



The figure shows that the numbers of blockchain mainnet-related incidents, side-chain-related incidents, and layer 2-related incidents each accounted for 33.33% of the total incidents. Blockchain mainnets, side chains, and layer 2 solutions each have 1 incident. Among these 3 incidents, the one that happened to blockchain mainnets happened to Solana [11], the one that happened to side chains happened to the Ronin network [12] and the one that happened to layer 2 solutions happened to Arbitrum One[13].

Solana suffered from a DOS attack, Ronin suffered from a 51% attack due to leaking of private keys, and Arbitrum One suffered from a hardware issue.

DAPP-RELATED INCIDENTS

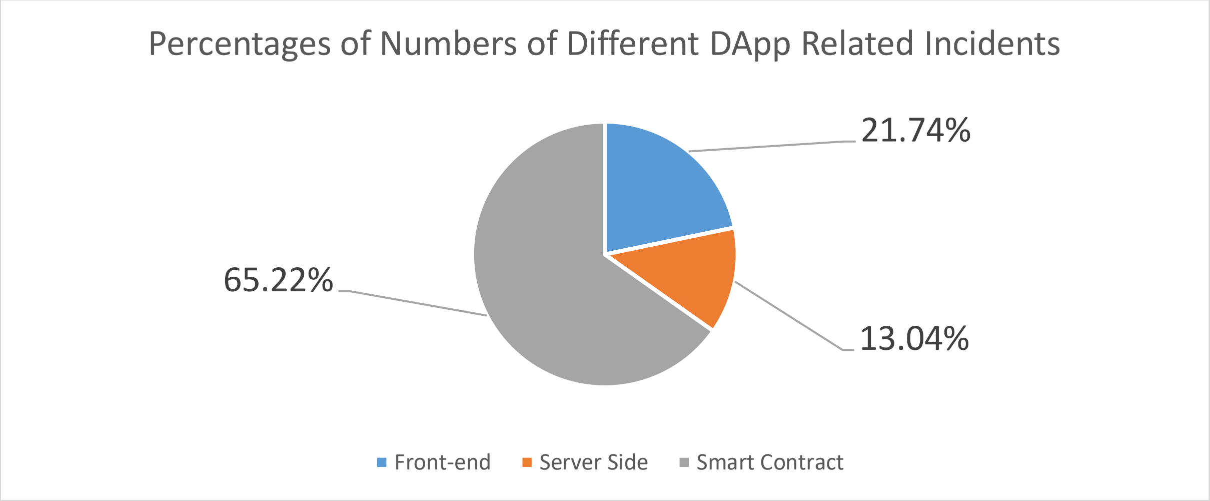
Among the 68 incidents that happened to DApps, 46 were incidents in which DApps suffered from attacks. An attack that targets a DApp can happen to its front-end, server-side, or smart contract(s). Therefore, we further categorize these 46 incidents into three sub-categories: DApp’s front-end, DApp’s server-side, and DApp’s smart contract(s).

DApp’s front-end related incidents are those in which vulnerabilities in the conventional client-side are exploited such that users’ account information and personal details would be stolen and used to exploit users’ crypto assets.

DApp’s server-side related incidents are those in which vulnerabilities in conventional server-side are exploited such that communication between off-chain and on-chain would be hijacked and users’ crypto assets would be exploited.

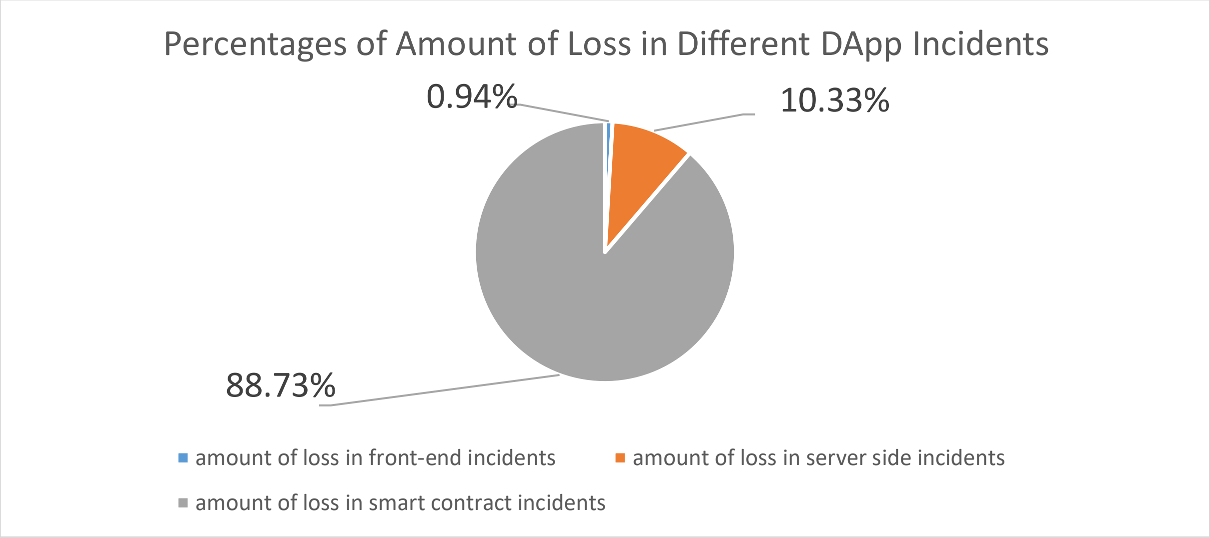
Smart contract-related incidents are those in which vulnerabilities in smart contract design or implementation are exploited such that users’ crypto assets in the smart contracts would be exploited.

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



The above figure shows that the number of smart contract-related incidents, server-side-related incidents, and front-end-related incidents respectively accounted for 65.22%, 13.04%, and 21.74% of the total incidents. Among 46 incidents, 10 were front-end related, 6 were server-side related and 30 were smart contract related.

We went further and studied the amount of loss in these three sub-categories and got the following figure:



In our statistics the amount of loss in front-end related incidents was $5.485 million, the amount of loss in server-side related incidents were $60.44 million and the amount of loss in smart contract related incidents was $519 billion.

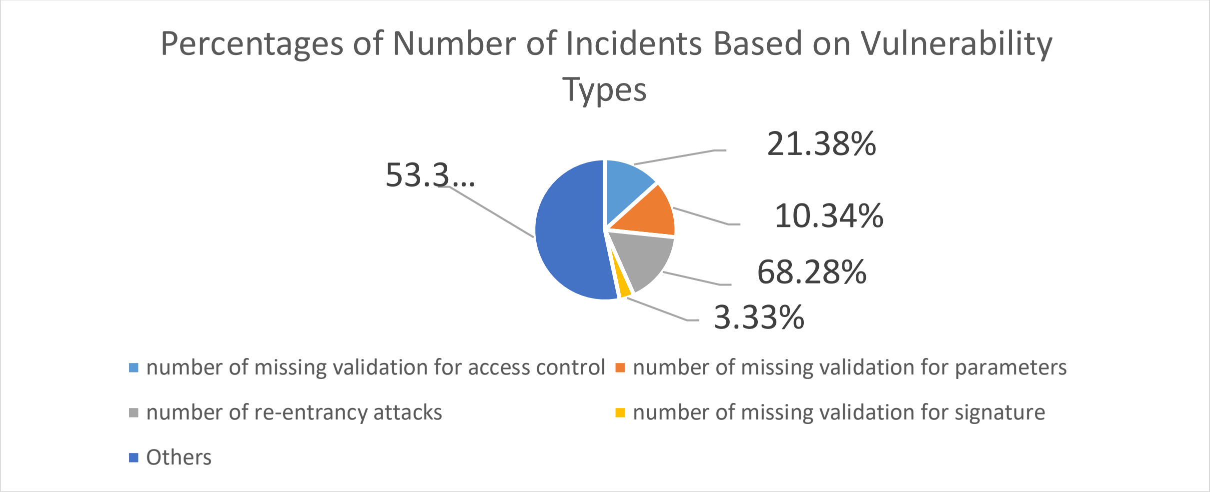
Although the front-end related incidents most of the attackers launched their attacks by sending fishing links on Discord servers.

Clearly smart contract related incidents were the biggest issue. Typical vulnerabilities we found pertaining to smart contracts in Q1 2022 included missing validation for access control [14], missing validation for parameters [15], missing validation for signatures [16], re-entrancy attacks [17], oracle security[18], incorrect LP price algorithm[19], interger overflow/underflow[20] etc.

Quite often, in the incidents that suffered from re-entrancy attacks or oracle security, their losses would be hugely enlarged by hackers' employing of flash loans.

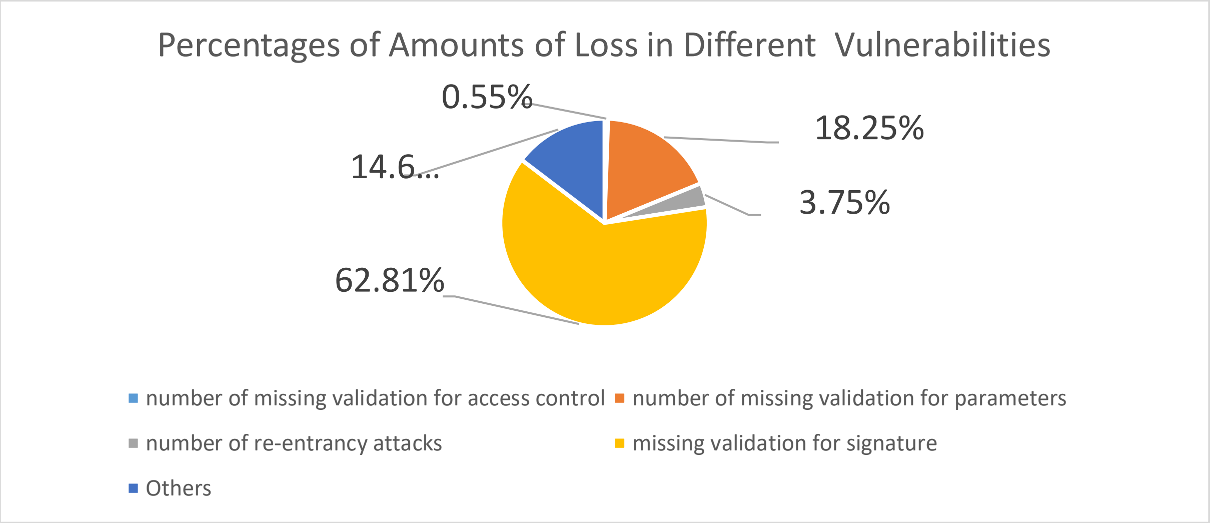
We studied the 30 incidents in which smart contracts were attacked and got the following figure based on the **vulnerability**

types:



The figure shows that the number of incidents that suffered from re-entrancy attacks ranked No. 1 among all smart contract-related incidents and it was followed by the number of incidents that suffered from missing validation for access control and the number of incidents that suffered from missing validation for parameters. 5 suffered from re-entrancy attacks, 4 suffered from missing validation for access control, 4 suffered from missing validation for parameters, and 1 suffered from missing validation for signatures.

After we studied the amount of loss in each of the vulnerability types and got the following figure:

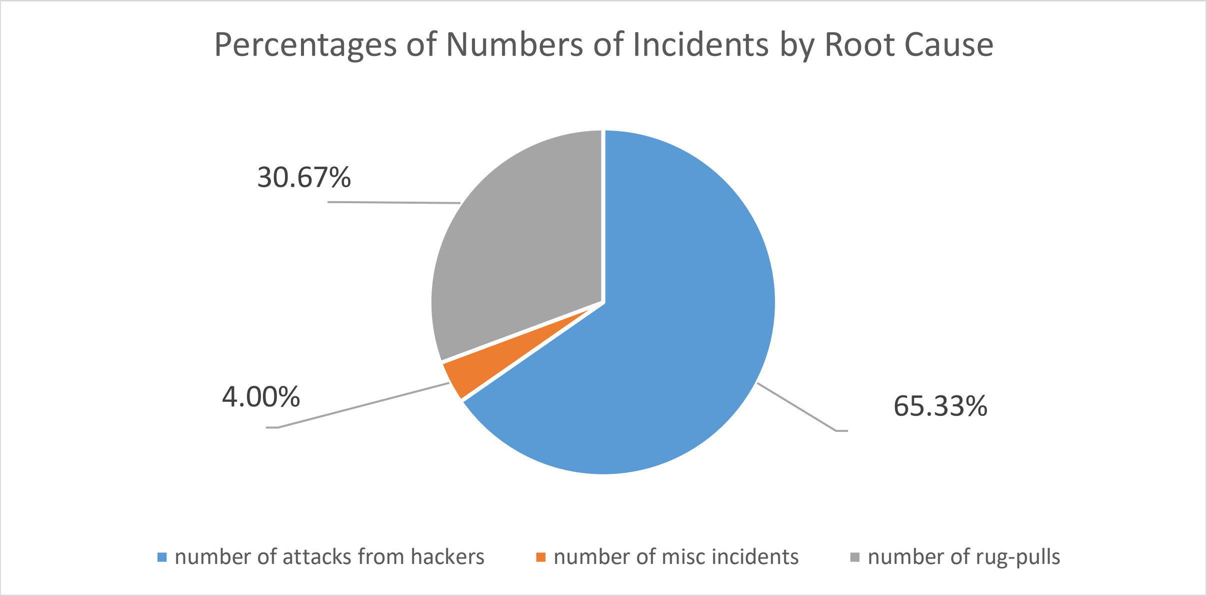


The interesting thing that the figure shows is that although the number of incidents that suffered from missing validation for signatures was neglectable, the amount of loss it caused was far more than any single type. There was one incident that was caused by this. It happened to a DApp deployed on Solana and it caused a loss of $326 million [16].

INCIDENTS CATEGORIZED BY ROOT CAUSE

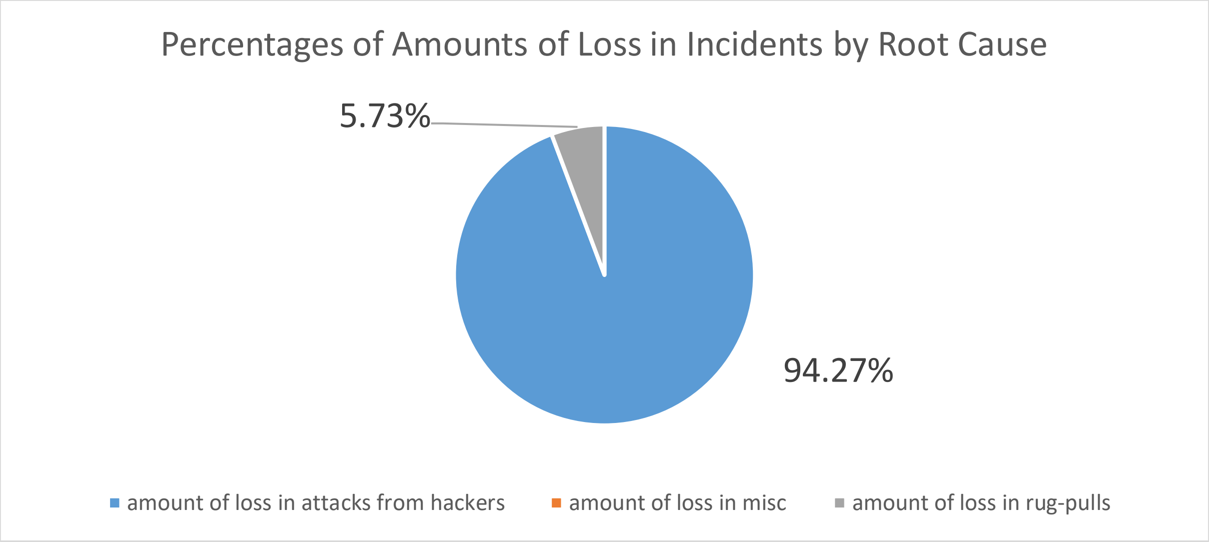
Based on the root cause we categorize these incidents into three categories: attacks from hackers, rug-pulls, and misc.

We studied the incidents and got the following figure.



The above figure shows that the number of attacks from hackers, the number of rug-pulls, and the number of misc incidents accounted for 65.33%, 30.67%, and 4% of the total incidents respectively. 49 suffered from attacks from hackers, 23 were rug-pulls and 3 were misc incidents.

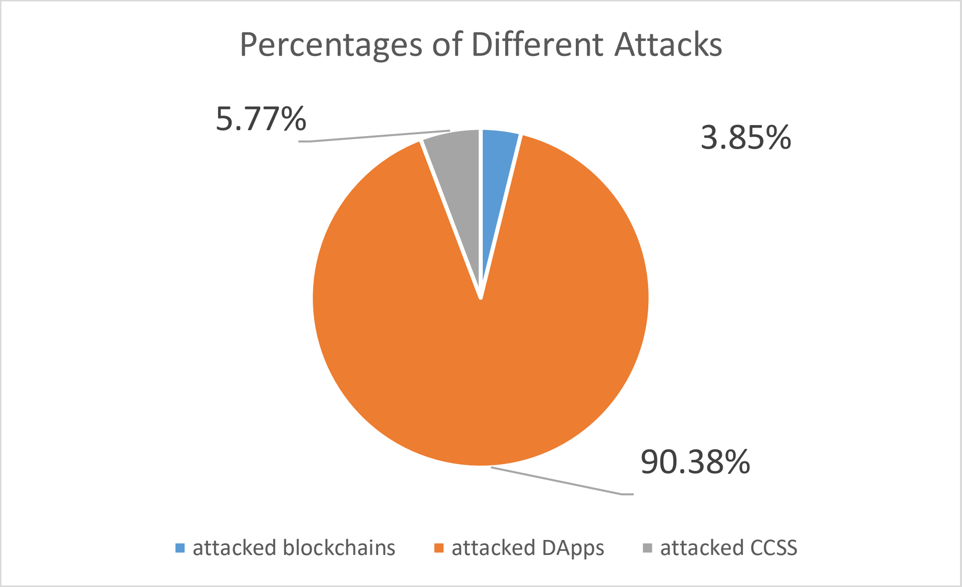
We studied the amount of loss of each category of incidents based on the root cause and got the following figure:



The above figure shows that the amount of loss in the incidents that suffered from attacks and the amount of loss in rug-pulls each accounted for 94.27% and 5.73% of the total loss respectively. That amount of loss in the incidents that suffered from attacks was $1.19 billion and the amount of loss in rug-pulls was $72.6 million. This reveals that attacks on smart contracts were the biggest threat to the whole crypto ecosystem.

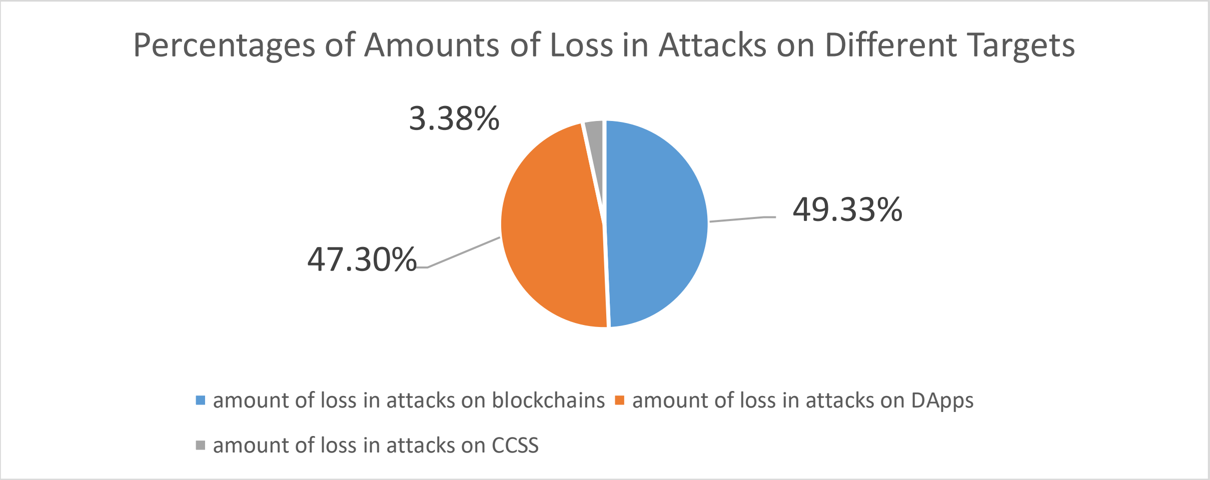
ATTACKS FROM HACKERS

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



The above figure shows that the number of attacks on DApps, CCSS, and blockchains accounted for 90.38%, 5.77%, and 3.85% of the total attacks respectively. The number of attacks on DApps, CCSS, and blockchains was 47, 3, and 2.

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



In contrast to the previous figure, this figure shows that although the number of attacks on blockchains was far less than the number of attacks on DApps. The amount of loss in attacks on blockchains was more than the amount of loss in attacks on DApps. The amounts of loss in attacks on blockchains, DApps, and CCSS were $610 million, $585 million, and $41.74 million.

The reason why the amount of loss in attacks on blockchains was so big is that the loss in the Ronin Network incident was big. The loss in this case alone was $610 million.

RUG-PULLS

The rug pulls that happened in Q1 2022 were all DApps. There were 23 incidents, and the total amount of loss was $72.63 million.

RESEARCH FINDINGS

Regarding attacks on blockchains, 51% of attacks were still the biggest threat to blockchains in Q1 2022. The 51% attack on a side chain (Ronin Network) caused a loss of $610 million. This loss surpassed any loss among all our studied cases.

Incidents about blockchain mainnets still happened in Q1 2022, however, incidents of layer 2 solutions and side chains emerged and the numbers gradually caught up in Q1 2022.

In regard to the suffering types including attacks, rug-pulls, and misc incidents, attacks from hackers were still the main threat to the whole crypto industry, which accounted for 65.33% of all incidents.

The three types of incidents that a DApp suffered from were front-end related incidents, server-side related incidents, and smart contract related incidents. Based on the number of incidents and the amounts of loss in the incidents, smart contract-related incidents accounted for a far more percentage than the other two in Q1 2022. With regard to the number of incidents, smart contract-related incidents accounted for 65.22% of the total, followed by the front-end related incidents which accounted for 21.74%, and then the server-side related incidents which accounted for 13.04%. In relation to the amount of loss in the incidents, smart contract-related incidents accounted for 88.73% of the total, followed by server-side related incidents which accounted for 10.33%, and then by the front-end related incidents which accounted for 0.94%.

Front-end incidents happened increasingly often in Q1 2022. Most of the attacks on the front end were carried out in Discord servers and targeted NFT projects.

After we studied the smart contract-related incidents we found out that the number of incidents that suffered from re-entrancy attacks ranked No 1, both the number of incidents that suffered from missing validation for access control and the number of incidents that suffered from missing validation for parameters ranked No 2. The number of incidents that suffered from missing validation for signatures was neglectable. But in contrast, with respect to the amount of loss, the amount of loss in the incidents that suffered from missing validation for signatures far surpassed anyone and ranked No 1. And this missing validation for signatures happened to a DeFi application on Solana [16].

The rug-pulls in Q1 2022 were all DApps.

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 Q1 2022 and support coordinated and efficient responses to crypto security incidents. Both blockchain developers and users are recommended to apply these practices to the greatest extent possible based on the availability of their resources.

Note: the blockchain developer here refers to not only developers of blockchains but also every developer that participates in the development of DApps, blockchains, or systems of cryptocurrencies. The blockchain user here refers to everyone that participates in activities on the crypto system's management, operation, trading, etc.

FOR BLOCKCHAIN DEVELOPERS

Awareness of security with both side chains and layer 2 solutions should be raised as more side chains and layer 2 solutions will emerge and develop in the coming years. Solutions to tackle the security challenges in this new area need to be researched and developed promptly.

With regard to a DApp's security, the security of its smart contracts still has the highest priority but the security of its front-end and service side needs increasingly more awareness. Audit of a DApp's front-end and server-side shouldn't be ignored.

It should be a must-have 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.

A flash loan is often employed to enlarge the loss in an incident in which the attacked smart contracts have vulnerabilities including re-entrancy issues, missing validation for access control, oracle security issues, incorrect token price algorithm, etc. Proper handling of these issues should have the highest priority for a smart contract developer when designing and coding a smart contract.

FOR BLOCKCHAIN USERS

A vital practice to maintain and run a DPoS-based blockchain's security is to deploy a safe and secure system to manage each validator's private key and to make sure each validator is run by its specified operator.

Both side chains and layer 2 solutions are young, immature, and not immune to security issues. It would be better to check a side chain or a layer 2 solution's security status before participating in activities on top of it.

When interacting with a DApp, while it is still necessary to pay great attention to its smart contracts' security, it is increasingly more important to pay attention to the security of its user interface and be cautious about any suspicious messages, prompts and behavior presented by the user interface.

It is strongly suggested users should check whether a project has audit reports and should read its audit reports before proceeding with further actions.

Use a cold wallet 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 about a DApp whose team members are unknown, unheard of, or lack reputation since such a DApp may eventually be a rug-pull. Be cautious about a centralized exchange that hasn't built a reputation or doesn't have tracked transaction data on third-party media since it may eventually be a rug-pull as well.

REFERENCES

[1] Coinbase. https://www.coinbase.com/

[2] Stobox. https://stobox.io/

[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] How Someone Made $820K From ApeCoin’s Airdrop Via Flashloan. https://cryptopotato.com/how-someone-made-820k-from-apecoins-airdrop-via-flashloan/, March 18, 2022

[7] NFTX. https://nftx.io/

[8] NFT20. https://nft20.io/

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

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

[11] Solana. https://solana.com/

[12] Ronin. https://bridge.roninchain.com/

[13] Arbitrum One. https://portal.arbitrum.one/

[14] Crypto Burgers Hacked: 770K USD Lost. https://coincodecap.com/crypto-burgers-hacked January 17, 2022

[15] DeFi Protocol Qubit Finance Exploited for $80M. https://www.coindesk.com/markets/2022/01/28/defi-protocol-qubit-finance-exploited-for-80m/ January 28, 2022

[16] Solana loses $320M in ETH from the ‘Wormhole’ DeFi token bridge. https://coingeek.com/solana-loses-320m-in-eth-from-wormhole-defi-token-bridge/ February 4, 2022

[17] DeFi Protocols Agave, Hundred Finance Hacked: Attacker Steals $11M Worth of Crypto. https://cryptopotato.com/defi-protocols-agave-hundred-finance-hacked-attacker-steals-11m-worth-of-crypto/ March 16, 2022

[18] $3 Million in DAI and ETH Stolen From Deus Finance in the Latest DeFi Hack. https://cryptopotato.com/3-million-in-dai-and-eth-stolen-from-deus-finance-in-the-latest-defi-hack/ March 15, 2022

[19] Fairyproof’s Analysis of the Attack on OneRing Finance. https://medium.com/coinmonks/fairyproofs-analysis-of-the-attack-on-onering-finance-94d25b66f63c March 22, 2022

[20] Weekly Blockchain Security Report by Fairyproof- Mar 14 to Mar 20. https://www.linkedin.com/pulse/weekly-blockchain-security-report-fairyproof-mar-14-20-?trk=organization-update-content_share-article March 21, 2022