CERTIK

HACK3D

THE WEB3 SECURITY QUARTERLY REPORT | Q1 2022 EDITION

Securing the Web3 World

EXECUTIVE SUMMARY

1. The amount lost to exploits is up over **8x** from Q1 of last year, setting 2022 on the path to being the most expensive year for web3 on record.

2. The **three** most lucrative exploits all targeted cross-chain bridges, highlighting both the importance and the vulnerabilities of the infrastructure.

3. CertiK Q1 2022 Stats: **807** projects audited, 548 new clients. This is up from 387 projects audited in Q1 of 2021, marking a **109% increase** in the number of projects audited per quarter. This brings the total number of CertiK audited projects to 3702. CertiK also completed KYC verification for 78 projects and onboarded 180 new projects to Skynet.

4. Together, rupgpulls and flash loan attacks make up **75%** of all attacks, making them the most common incidents by far.

5. Further research from governments and central banks into both CBDCs and the creation of regulatory frameworks for crypto assets herald the coming era of governmental involvement in web3.

> ***“ DeFi, has seen an increase in total value locked from $72.6 Billion at the end of March 2021, to $229 Billion at the end of March 2022.***

OVERVIEW

The opening quarter of 2022 was dramatic to say the least, with a total of **$1.3 billion** ($1,297,166,019.19) lost across 82 attacks.

This amounts to over eight times the amount lost in the same quarter of 2021, a staggering increase even when placed in the context of the growth within DeFi, which has seen an increase in total value locked from **$72.6 billion** at the end of March 2021, to **$229 billion** at the end of March 2022.

To put these losses in perspective, $1.55 billion was stolen across the whole of 2021, meaning that 2022 will undoubtedly mark the biggest year of losses for web3 so far.

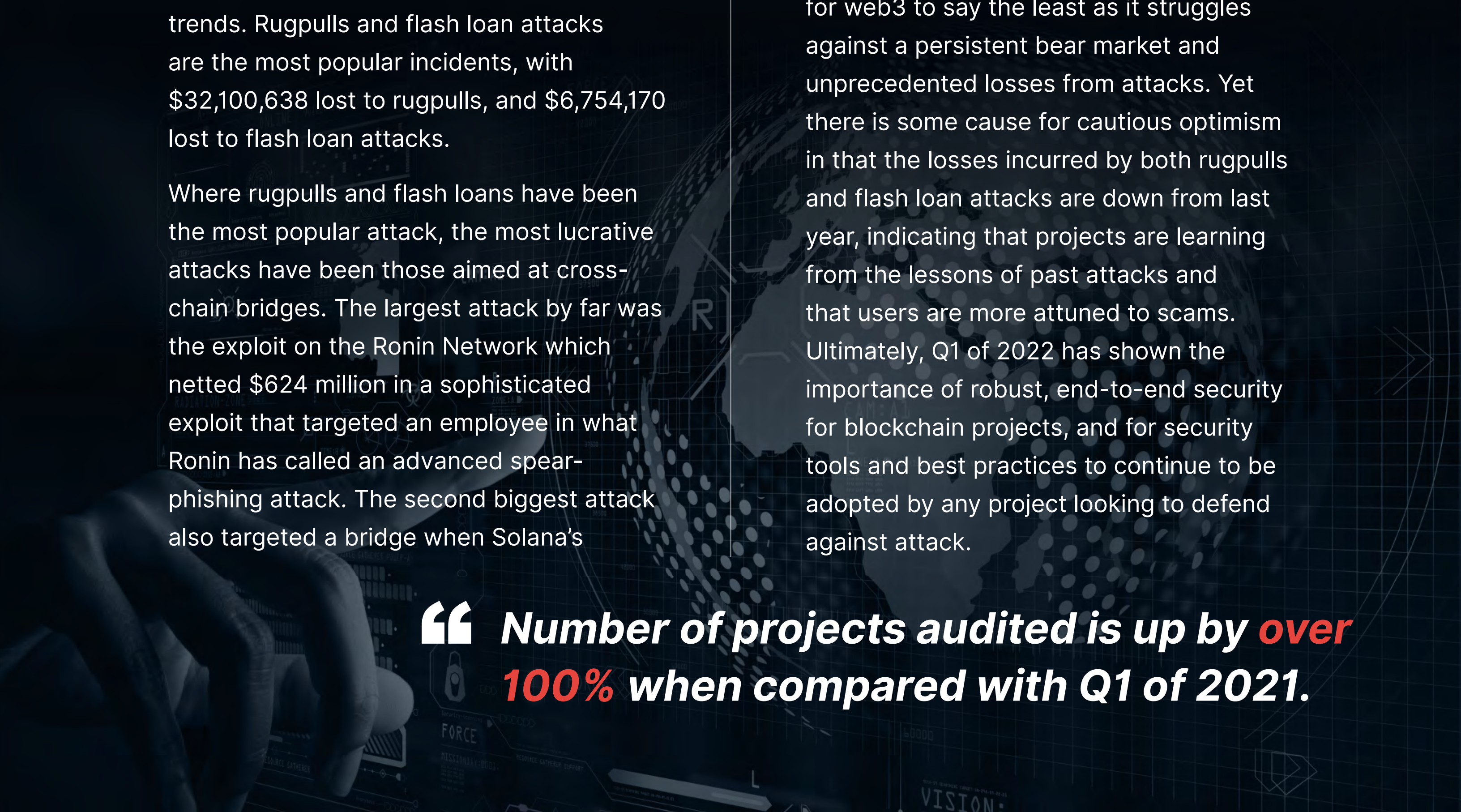
Within this, we are seeing some clear trends. Rugpulls and flash loan attacks are the most popular incidents, with $32,100,638 lost to rugpulls, and $6,754,170 lost to flash loan attacks.

Where rugpulls and flash loans have been the most popular attack, the most lucrative attacks have been those aimed at cross-chain bridges. The largest attack by far was the exploit on the Ronin Network which netted $624 million in a sophisticated exploit that targeted an employee in what Ronin has called an advanced spear-phishing attack. The second biggest attack also targeted a bridge when Solana's Wormhole lost $326 million after a hacker was able to bypass the verification process and mint themselves Wormhole Eth (wETH).

In light of these attacks, it is unsurprising that we are beginning to see further steps toward some long anticipated governmental regulations. Most notably President Biden signed an executive order aimed at research and creation of a regulatory framework for cryptocurrencies, and the progression of the European Union's hotly debated MiCA bill, which proposes 126 articles for the regulation of crypto-assets.

Overall, 2022 has been a rocky start for web3 to say the least as it struggles against a persistent bear market and unprecedented losses from attacks. Yet there is some cause for cautious optimism in that the losses incurred by both rugpulls and flash loan attacks are down from last year, indicating that projects are learning from the lessons of past attacks and that users are more attuned to scams. Ultimately, Q1 of 2022 has shown the importance of robust, end-to-end security for blockchain projects, and for security tools and best practices to continue to be adopted by any project looking to defend against attack.

> ***“ Number of projects audited is up by over 100% when compared with Q1 of 2021.***

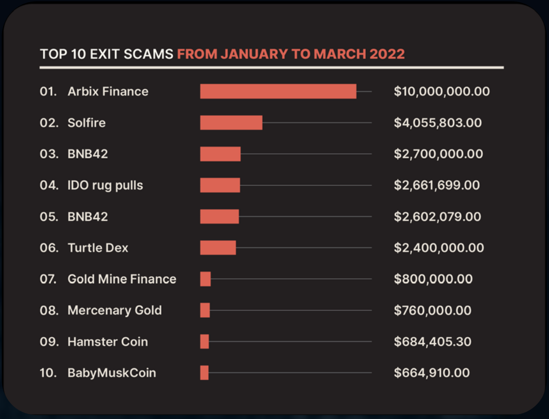


1. RUGPULLS AND FLASH LOAN ATTACKS

The overwhelming majority of attacks during this quarter have been either rugpulls or flash loan attacks, with rugpulls accounting for 50% of the total exploits, and flash loan attacks accounting for 25% of total exploits. Both classifications serve as umbrella terms given the multiple and often ambiguous ways of conducting attacks.

RUGPULLS

A total of $32,100,638 has been lost to rugpulls, this is down significantly when compared to Q1 of last year which saw losses of $2,731,785,937. Whilst heartening to see this decline, we may have the bear market to thank. In bull runs, we see an uptick in retail investors and new money flood the space. Whilst good for the market, these new investors are far more likely to fall prey to bad faith founders who promise the moon only to execute a rugpull or other exit scam. By contrast, those weathering a bear market are battle-hardened and a lot harder to dupe.

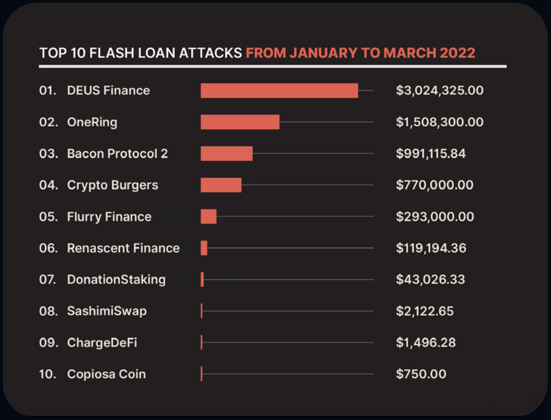


To help stem the losses incurred by rugpulls, CertiK announced their new KYC Verification service for project teams, making them the only major security provider that performs KYC verification in addition to a security audit of the code, as well as continuous monitoring of a project via CertiK Skynet. Team anonymity is a common factor in rugpulls as the lack of accountability allows for high-risk behavior. By conducting thorough KYC checks on a project's team, CertiK KYC helps bolster trust and confidence in project teams and helps users make educated decisions on how to invest.

> ❝ ***A total of $32,100,638 has been lost to rugpulls in Q1***

FLASH LOANS

After rugpulls, flashloan attacks have been the second most popular exploit, an attack which as we have seen this quarter, can be used in numerous ways to exploit De-Fi protocols.



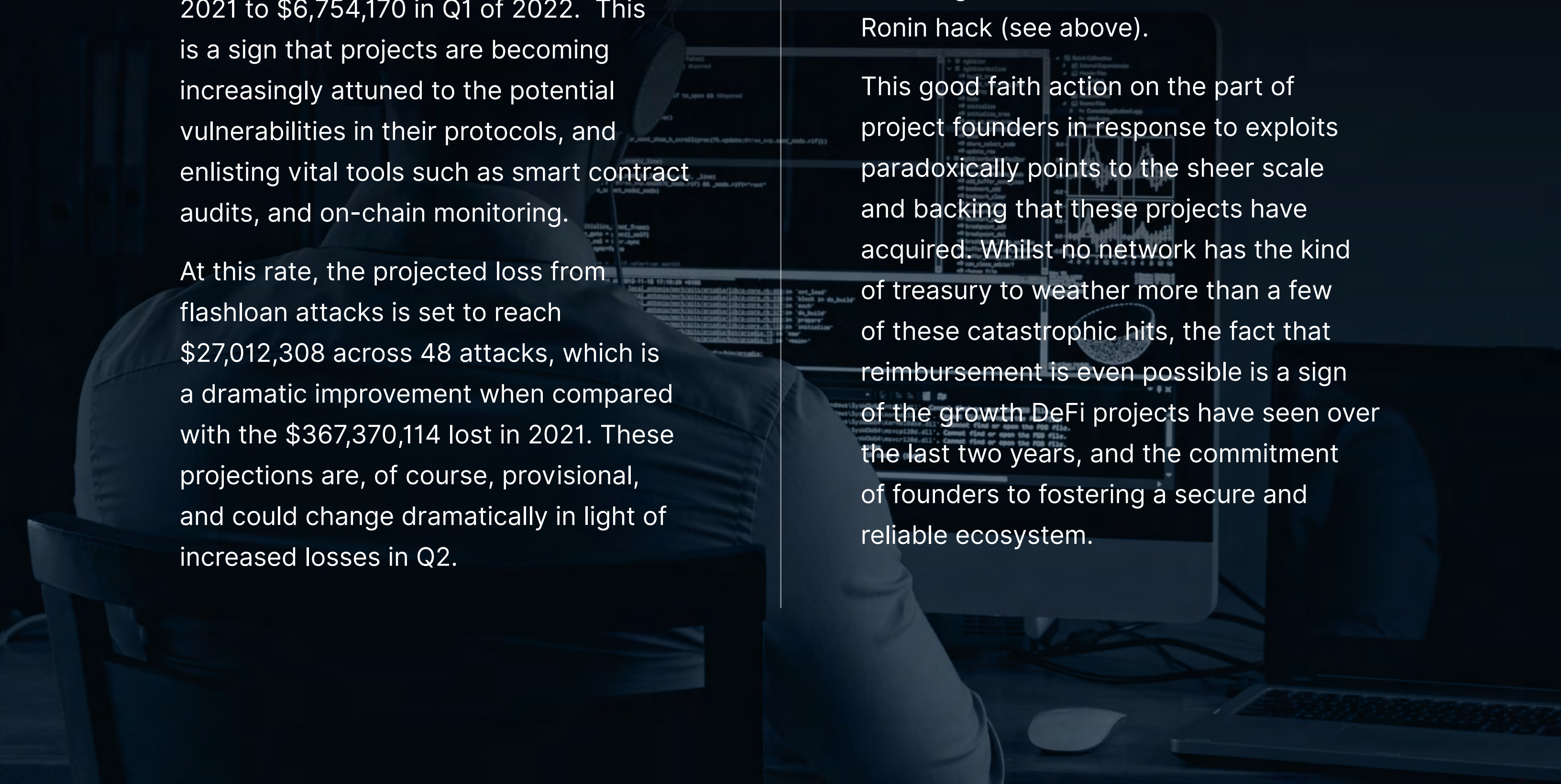
Whilst flash loan attacks are still a favorite of hackers, there is cause for some cautious optimism given that the amount lost to flashloan attacks is down significantly from $176,345,409 in Q4 of 2021 to $6,754,170 in Q1 of 2022. This is a sign that projects are becoming increasingly attuned to the potential vulnerabilities in their protocols, and enlisting vital tools such as smart contract audits, and on-chain monitoring.

At this rate, the projected loss from flashloan attacks is set to reach $27,012,308 across 48 attacks, which is a dramatic improvement when compared with the $367,370,114 lost in 2021. These projections are, of course, provisional, and could change dramatically in light of increased losses in Q2.

Only flashloan attacks that have reached a threshold of being profitable attacks, over $100k or against a highly visible or popular protocol, have been included in this report. Many attacks resulted in small losses, and many losses or attacks are lost in the noise of simple arbitrage farming by bots. It is also worth noting that flashloan attacks are rarely “just” flashloan attacks, they often involve manipulation of price oracles, bridge vulnerabilities, liquidity pair pools, and many more exploits.

Interestingly, this quarter also marks an increase in the number of projects reimbursing their communities for any funds lost. Deus Finance, the protocol hit hardest by a flash loan attack this quarter with $3 million lost, reimbursed all user funds from their personal and DAO treasuries. Similarly, Axie Infinity said it was committed to restoring user funds after the $600 million Ronin hack (see above).

This good faith action on the part of project founders in response to exploits paradoxically points to the sheer scale and backing that these projects have acquired. Whilst no network has the kind of treasury to weather more than a few of these catastrophic hits, the fact that reimbursement is even possible is a sign of the growth DeFi projects have seen over the last two years, and the commitment of founders to fostering a secure and reliable ecosystem.



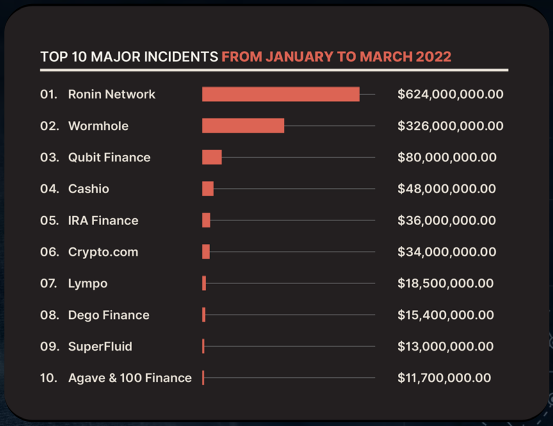
2. WEAK BRIDGES: RONIN, WORMHOLE, QUBIT FINANCE

Despite the preponderance of rugpulls and flashloan attacks, the three most lucrative attacks this quarter have targeted cross-chain bridges-infrastructure which enables the transfer of cryptocurrencies from one blockchain to another.

As noted by CertiK’s CEO and Co-Founder Ronghui Gu, the prevalence of these attacks highlights two key points. Firstly, cross-chain bridges are a critical piece of infrastructure that addresses a real need in web3; the fact that a single bridge held over $600 Million USD as in the case of the Ronin hack, is a testament to the market for users who want to explore and share assets across multiple ecosystems.

Secondly, cross-chain bridges are extremely vulnerable to attack. As shown in the hacks this quarter, the complexity of cross-chain bridges introduces more attack vectors than would normally exist on a single chain. Indeed, we may be seeing proof of Vitalik Buterin’s prediction at the start of this year that “the future will be *multi-chain*, but it will not be *cross-chain*: [as] there are fundamental limits to the security of bridges that hop across multiple “zones of sovereignty”.

Either way, there is a clear tension here between the flaws in the current cross-bridge architecture and the high demand from users for cross-chain functionality. As it stands, the current vulnerabilities in the cross-chain system cannot continue indefinitely, as there are only so many times trading firms will backstop hundreds of millions of liquidity in order to keep a blockchain alive.



> ***The three most lucrative attacks this quarter have targeted cross-chain bridges.***

3. THE CENTRAL BANK IN THE DECENTRALIZED ECOSYSTEM

This quarter we have seen the continued rise in interest from nations researching, testing, and piloting their own central bank digital currency (CBDC) projects, with over 87 countries (representing over 90 percent of global GDP) exploring a CBDC.

In keeping with this growing interest, this quarter also saw further signs of future governmental regulation on the web3 space. This corollary between the development of a CBDC project and movement toward regulation is most visible in the U.S, with Q1 seeing both the first report on the Digital Dollar entitled ‘Project Hamilton’, and President Biden’s executive order which asks government agencies to form committees, research cryptocurrencies and work toward creating a regulatory framework for crypto-asset markets.

The European Union’s MiCA Bill proposes 126 articles designed to provide a regulatory framework for crypto assets. Within these, the most controversial article aimed to ban assets that use proof-of-work in an attempt to stem energy consumption. In what came as good news to many in the crypto community, in March MiCA Bill moved forward without the proof-of-work limiting provision, however it is likely there will be some stipulations on energy consumption in the final bill.

Most people agree that regulation and CBDCs are inevitable, with the two likely to come in tandem. What they don’t agree on is whether this is a good or bad thing for the space, with one side welcoming the increased stability and protections that regulatory measures would provide, and others seeing them as a death knell for cryptocurrencies and a fundamental betrayal of the technology’s founding ethos. Ultimately, this all depends on what both the CBDC and the regulations will look like, about which there is scant information.

What is clear is that any regulation will include some form of KYC and AML checks at the very least, and looking at the data for the hacks in this year alone, it is easy to see why. At CertiK we believe that a proactive attitude is the best way to prepare for and anticipate incoming regulations. CertiK’s new KYC checks introduce verification for project teams and are designed to deanonymize project teams and create greater accountability through a rigorous vetting process.

CONCLUSION

Overall Q1 of 2022 shows a dramatic increase in the amount lost to attacks when compared with the same quarter of last year. Even when taking the astronomical attacks against the Ronin Network and Qubit Finance into consideration, this data suggests that 2022 will be the worst year for web3 financial security on record. The surge in web3 growth over the last year has outstripped the growth of the blockchain security and auditors industries, meaning that projects are left vulnerable as there are not enough auditors to secure them.

What is clear is that **the battle for web3 security is now greater than ever**. To win it, projects need to treat their security as an ongoing concern rather than a one-time check. Think of its as akin to washing your hands or brushing your teeth; if you do it only once, you can expect bad consequences. To that end, it is crucial that projects take an end-to-end approach to security through tools such as smart contract security auditing, KYC checks, and on-chain monitoring. As Q1's losses show, it is far better to plan ahead than pay the price of a hack down the line.

In fighting to secure web3, CertiK provides a number of tools designed to help projects take an end-to-end approach to their security.

The CertiK Security Leaderboard – with a total of 1956 completed and on-boarded projects at the end of 2021 – allows web3 users to leverage the expertise of our auditing and security teams in order to equip themselves with a deeper knowledge of security risks. These users push the whole ecosystem to new heights, while we provide the data that helps them make informed decisions.

Skynet actively monitors hundreds of web3 platforms in real-time, using a combination of on-chain transaction monitoring and off-chain data such as social sentiment to ultimately arrive at a comprehensive security analysis. Skynet Premium – unveiled in 2021 – integrated continuously-evolving machine learning to grow in lockstep with the constantly shifting smart contract risk environment, getting more and more advanced as it encounters new threats and vulnerabilities. The Premium platform includes an analytics dashboard which enables enterprise clients to monitor and manage their risk in real-time.

CertiK's Security Oracle allows developers to leverage real-time security scores provided by a decentralized network of nodes to ensure that their contract's interactions with other smart contracts meet an acceptable level of security. This allows developers to take advantage of the powerful interoperability of web3 while protecting their own contracts against failures of third-party dependencies.

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

CertiK KYC provides identity verification for project teams which includes an ID authenticity inspection using AI-based detection systems, as well as liveness checks to ensure the individual is indeed real and matches the ID. In addition to a liveness check during the ID verification process, CertiK will also do a live video call with each team member to verify their identity and other parameters as needed. As team anonymity increasingly enables high-risk behaviors, CertiK KYC helps to build accountability around projects to enable investors to move forward in trust.

Securing the **Web3** World