An Overview of DeFi Security In 2022

By Drofa Comms together with HashEx, Beosin, and Apostro

drofa comms HashEx BEOSIN Blockchain Security apostro

About the study participants:

drofa comms

Founded in 2011, Drofa Comms is a finance and fintech PR consultancy with offices in London and Limassol. Being focused on the specific sector, we are deeply emerged into the market.

Our mission is to help top financial and fintech companies grow with care and respect through well-tuned communications with their audience.

#HashEx

Founded in 2017, HashEx brings together a team of experts in blockchain and smart contract auditing, with the mission of providing security in the crypto sector.

Over the course of its history, HashEx has audited and helped launch over 500 DeFi projects and prevented the loss of over $2 billion worth of investor funds.

BEOSIN

Beosin is a Singapore-based leading global blockchain security company co-founded by several professors from world-renowned universities.

With the mission of "Securing Blockchain Ecosystem", Beosin provides integrated blockchain security products and services to one million+ users in global blockchain ecosystem, including Smart Contract Audit, Blockchain Risk Monitoring & Alert, Crypto KYT&KYC, and Crypto Tracing.

apostro

Apostro is a risk management platform that provides economic security for crypto projects by preventing smart contract exploits.

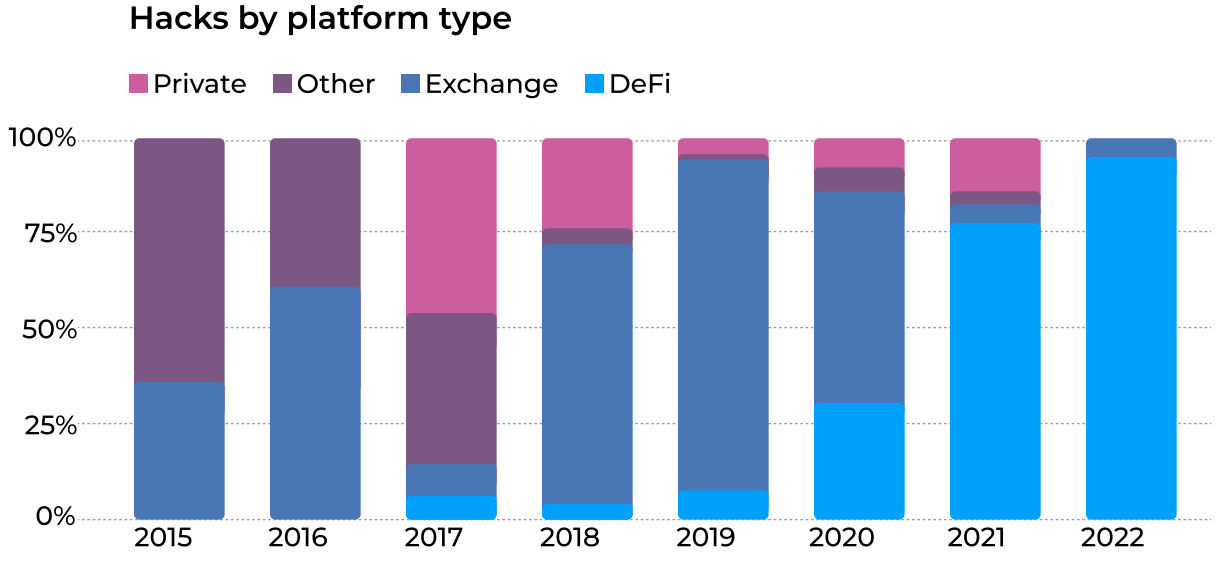
The platform takes risk management methods used in traditional finance and applies them to the crypto industry. Headquartered in Warsaw, Apostro works with DeFi projects, Web3 protocols, DAOs, crypto funds, liquidity providers, developer communities, etc.

2022 Records the Highest Number of Crypto Hacks in DeFi space:

Experts Comment On What It Means for DeFi In the Long-Term

The end of 2022 is approaching, which has already become the biggest year in terms of loss of funds due to hacks in the decentralized cryptocurrency sector according to the current amount of stolen funds for the year.

According to the blockchain analytics firm Chainalysis, since the emergence of the DeFi market, it has attracted more and more attention from hackers every year.



Data from Chainalysis

According to blockchain security company Peckshield, $1.55 billion was stolen from the DeFi sector in 2021, which looks catastrophic. However, according to quarterly reports from Certik, one of the largest blockchain security companies, almost $1.3 billion was already stolen in the first quarter of 2022 alone.

Rugpulls and flash loan attacks are the most popular incidents of embezzlement, but not the biggest in terms of the amount of money. The most lucrative attacks have been those aimed at cross-chain bridges.

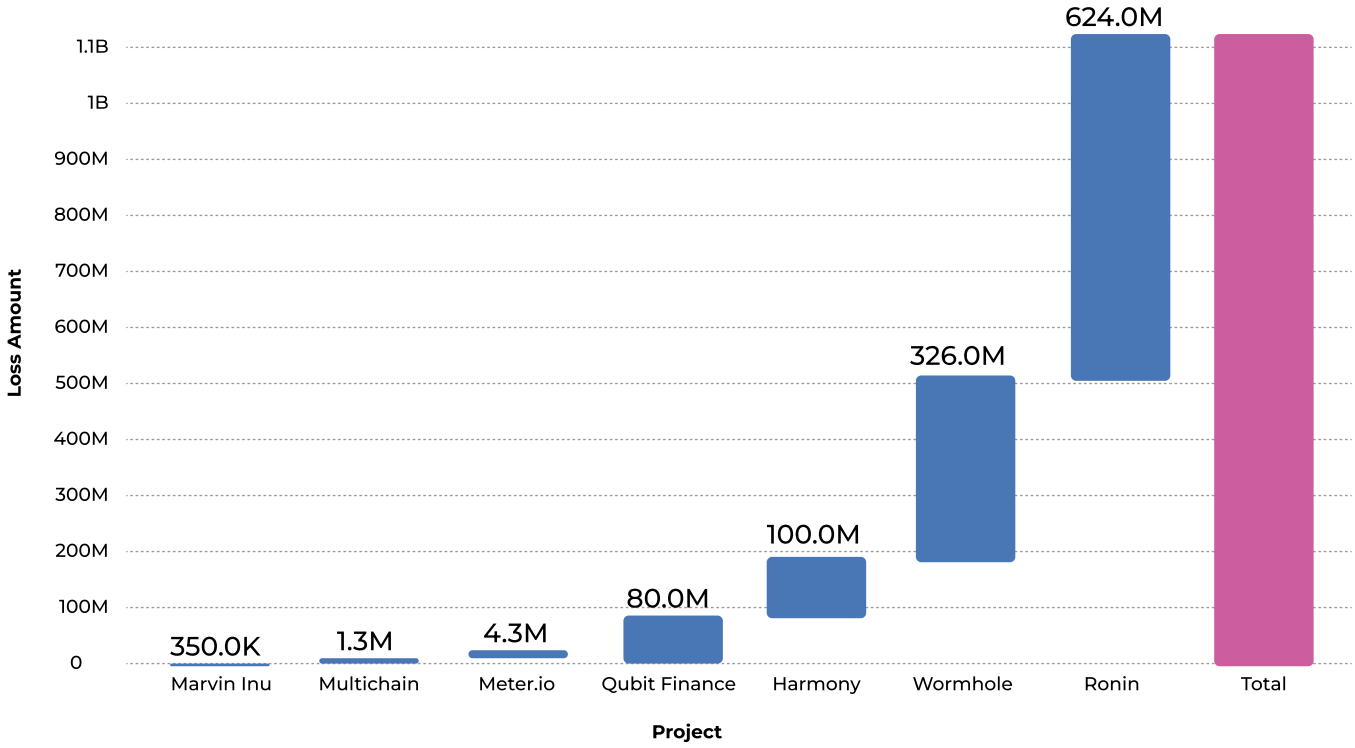
The two largest cross-chain bridge exploits in the first quarter of 2022 are the $624 million Ronin Network exploit, which was an advanced phishing attack, as well as an attack on Solana Wormhole, which is valued at $326 million. The hacker was able to bypass the verification process and illegally receive a large amount of Wormhole Eth (wETH).

Attacks on cross-chain bridges are becoming more and more popular because they contain a lot of liquidity, which attracts hackers, and also have a rather complex system of interaction between interfaces and smart contracts, which makes it hard to provide full service protection.

In addition, due to the current situation with centralized exchanges, the credibility of which was undermined due to the collapse of the FTX – one of the largest centralized exchanges, and one-by-one verification of the asset backing of all major centralized exchanges, users are increasingly using decentralized platforms. This means that cross-chain bridges are in demand more than ever, and this is just the beginning.

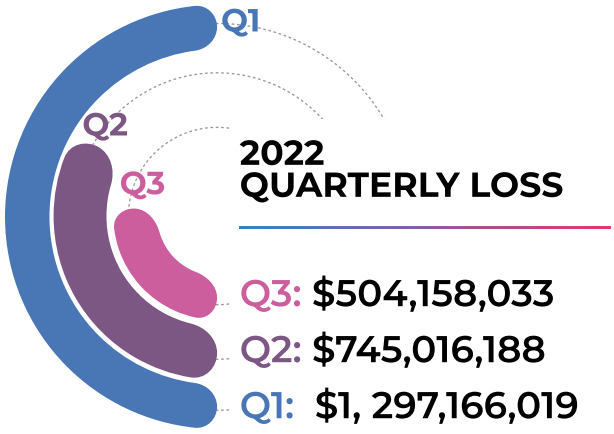
According to the Beosin H1 security research, in the first half of 2022, seven cross-chain bridge attacks occurred resulting in a total loss of approximately $1.1 billion, accounting for 59% of total losses in the first half of the year.

H1 Attacked Bridges by Loss Amount



Data from Beosin H1 2022 security research

According to Certik, there were various attacks on the decentralized finance market worth $2.546 billion from January to October 2022.



Data from Certik 2022 Q3 report

Peckshield stated that 53 DeFi protocols lost $760 million from about 44 attacks in October, which makes this month one of the scariest months in terms of numbers.

As of November, blockchain security firm HashEx is reporting over $530 million worth of attacks and exploits, given the FTX centralized exchange incident, which has invested heavily in the DeFi market.

Thus, at the beginning of December 2022, the decentralized finance sector suffered more than 3.8 billion dollars, which is more than 2 times the amount of losses in 2021.

What has led to such a significant increase in financial losses in the decentralized finance sector, and what can we expect from the crypto industry in the future?

To better understand the real picture and get a deeper insight into the issue, we posed five questions to three industry experts:

Dmitry Mishunin, founder and CEO of HashEx, a DeFi security and analytics company

Tommy Deng, Managing Director of Beosin, a Web3 security firm based in Singapore

Tim Ismiliaev, co-founder of risk management platform Apostro

1

What is the reason for such a significant increase in the number of DeFi hacks?

Responding to this question, Dmitry Mishunin, the founder and CEO of HashEx stated, “It’s down to a couple of reasons. Firstly, the hackers have gotten smarter, gained more experience, and learned how to look for bugs. The crypto industry is still relatively new, and everyone is growing with each other, so it’s difficult to get too far ahead of bad actors.”

“Secondly,” he added, “the amount of money put into DeFi projects has made the industry very attractive to bad actors.”

According to the data from DeFiLlama, the total value of cryptocurrency assets locked in DeFi at present time stands at $41,5 billion. This demonstrates an almost four-times-growth compared to the $11 billion, recorded in November 2020. This rapid growth made the DeFi space a lucrative avenue to explore, thus attracting the attention of all manner of hackers and fraudsters.

In response to Mishunin’s point, Tommy Deng, the Managing Director at Beosin, introduced another angle – the proliferation of new projects in the crypto sector that don’t go through exhaustive security testing and verification. To that point, Deng mentioned that “DeFi is growing at a very rapid rate, and many new protocols are emerging. Unfortunately, many of these projects don’t go through complete security testing before going live. Additionally, many projects have started to explore new areas, such as cross-chain bridges, that need a lot more areas to be protected, including the contract level, the private key level, and the relay level. And as has been documented, cross-chain bridges are the most common target for exploits because of their many vulnerabilities.”

2

We have been witnessing that after each hack, lots of auditors publish reports and analytics explaining ways to prevent the hack. However, it doesn't seem to change the tendency itself. Why do you think that is the case?

Dmitry Mishunin connects this phenomenon with the way PR and mass media work: "Most of these reports and "overviews" are published for the sake of PR. Journalists write about things that interest their audience, and the people that read such analyses are average investors that are concerned about their money. Actual blockchain developers are too busy coding; they don't have time to read stuff like that. In my opinion, this channel of information remains out of the view of its actual target audience. As auditors, we get to read about other people's hacks, but this increases our own expertise. It does not, unfortunately, have a direct influence on the expertise of the developers who are actually building DeFi protocols."

In continuation of Mushunin's statement, Tommy Deng then highlighted the limited scope of auditor reports and the unique experiences of each crypto project that make such reports unhelpful to developers. He said, "The analysis reports given for each attack are basically event-based vulnerabilities and related recommendations. Such vulnerabilities generally exist in specific projects. This means that while other projects might avoid the problems that have been highlighted in those audit reports, they may still encounter their own unique problems due to the characteristics of their respective protocols. That said, usually, after the emergence of general vulnerabilities, the DeFi projects tend to do a good job of ramping up protection. For instance, the reentrancy vulnerabilities are now not as common as they used to be."

3

What is your forecast for the future — is the number of hacks likely to grow in the upcoming year, or will the market shift to a safer side?

Responding to this question, Tommy Deng said, “I think there is no absolute security. As long as there is interest in the crypto market, the number of hackers will not decrease.”

However, Deng believes companies like Beosin and HashEx could play key roles in securing the crypto sector against such bad actors. He added, “From another point of view, the decentralised ecosystem will continue to strengthen and improve security construction. With the support of security companies such as Beosin and the concerted efforts of various allied projects, we believe the entire crypto market will cut down the number of exploitable vulnerabilities and move in a more secure direction.”

Tim Ismiliaev, co-founder of Apostro, supported Deng’s hopeful take on the future of DeFi, saying, “I expect that the DeFi space will mature over the next five years, and new best practices for securing decentralised finance protocols will emerge. Some companies are already making innovations in that direction. For example, Wormhole recently introduced daily withdrawal limits for its users. Other protocols are leaning towards isolating lending markets.”

Dmitry Mishunin was however more cautious, stating, “In my opinion, the number of hacks is only going to grow going forward, and these attackers will not be stealing only from DeFi projects. They are also likely to target crypto exchanges and banks that will inevitably enter this market as more secure solutions for storing digital assets.”

4

What advice can you give to DeFi companies to prevent hacks before they happen?

In response to this question, Tommy Deng said, “Firstly, I’d recommend that DeFi companies introduce a secure development process to ensure a high level of security when the protocol is implemented. Then, I’d advise them to do a thorough job of testing their security before going live. Finally, I’d recommend introducing a professional auditing company to conduct security audits on the project. When the DeFi project finally goes live, I advise the team to monitor it in real-time. If they encounter an attack, they can always contact security companies like Beosin for patching, vulnerability analysis, and other follow-up services such as tracking stolen funds.”

Tim Ismiliaev then reiterated Deng’s point, stating, “In addition to the obvious security audits outlined by my colleague, I would advise DeFi companies to hire firms that specialise in conducting formal verifications. These firms provide a systematic approach to preventing a wide range of endogenous risks related to bugs in smart contracts.”

Additionally, Ismiliaev pointed out that regardless of the security measures put in place, DeFi projects still needed to have structures in place to counter the effects of attacks. “No platform can be completely hacker-proof; therefore, DeFi companies should prepare themselves for the worst and have specific mitigation mechanisms in place. But in my opinion, the most effective solutions for deterring hacks are daily withdrawal limits and active threat detection systems,” he said.

Dmitry Mishunin wrapped up the question by championing the education of stakeholders in the DeFi space, saying, “I’d tell them to have their best people take a programmer training course. A few months of classes and they will have learned to think in terms of a decentralised development paradigm. For example, at HashEx we have an Academy certification for DeFi developers and auditors, designed with just that idea in mind.”

He further restated the need for DeFi projects to not only empower their in-house security specialists but to go a step further and bring in additional help from outside the project.“My best advice to DeFi companies is for them to either increase their expertise or simply hire experts. Or better yet, do both,” he said.

In addition, Dmitry said that he finds the subscription audit format interesting. Choosing such a tariff, the project will be constantly under the supervision of an auditing company, which will significantly increase the level of protection.

5

Do you consider DeFi safe overall?

To this final question, Apostro's Tim Ismiliaev contended that it was much easier to fix DeFi's security issues than it was to deal with the problems afflicting traditional finance. "I would compare DeFi's safety with the biggest risk in traditional finance. Traditional finance has significant transparency issues; for example, look at the recent FTX bankruptcy; that kind of situation cannot be mitigated by regulation. In contrast, DeFi's security risks can be greatly reduced by proper risk management and monitoring tools. So, I believe that DeFi will be more secure in the next five years."

Tommy Deng was, however, slightly less upbeat, stating the following: "Compared to the previous two years, DeFi is currently safe in general, and there is a trend that ecological security is slowly building up. However, looking at the current ecosystem alone, DeFi is not safe. There have been numerous hacking incidents that have resulted in quite severe losses. According to our Beosin EagleEye platform for security risk monitoring and blocking, more than25 major security incidents occurred in October, with a total loss of $737 million, the highest loss in the blockchain field this year. So, I'd say that although DeFi has improved its security compared to the past, it still faces a serious security situation and needs the joint efforts of the entire blockchain ecosystem."

Dmitry Mishunin had an even more succinct outlook, and ended the interview by saying, "I would go for 'no' rather than 'yes.' Generally speaking, the percentage of hacks will probably become lower as it will become more difficult to find vulnerabilities in DeFi protocols. But at the same time, the amount of money in the industry will increase. To put it another way, the chances of pulling off a hack will drop, but the reward a hacker stands to gain, if successful, will increase."

Conclusion

The statistics in this article show that the world of decentralized finance is plagued by security issues and endless attacks by hackers. This means that DeFi projects should conduct a thorough audit of their smart contracts, especially those that fall into highly vulnerable areas such as bridging. In addition, it is essential that most DeFi companies apply industry best practices to secure their platforms. They also need to engage security experts to investigate, consult, and fix vulnerabilities in their smart contracts and create contingency plans in the event of a breach. The main message of our panel of experts is that the DeFi market is evolving and growing, and the amount of exploits is growing along with this market, but the top companies and experts in the field are also developing every day, which should ultimately lead to a decrease in the number of stolen funds in the future, and increase investors confidence in the industry.

Appreciation

We want to thank the following for their participation in preparing this material:
Dmitry Mishunin, founder and CEO of HashEx;
Tommy Deng, Managing Director of Beosin;
and Tim Ismiliaev, co-founder of Apostro.

The following sources were used in preparing this material:

- Beosin Blockchain Security (2022) [Twitter] 30 November: https://twitter.com/Beosin_com/status/1597891053310210048
- Beosin (2022) H1 2022 Web3 Security Research: https://beosin.com/resources/Beosin_H1_2022_Web3_Security_Report.pdf (Accessed 30 October 2022)
- Browne, Ryan and Sigalos, MacKenzie (2022) Hackers have stolen $1.4 billion this year using crypto bridges. Here's why it's happening, CNBC, 10 August: https://www.cnbc.com/2022/08/10/hackers-have-stolen-1point4-billion-this-year-using-crypto-bridges.html (Accessed 30 October 2022)
- CertiK(2022) CertiK Resources: https://www.certik.com/resources/blog (Accessed 29 November 2022)
- CertiK(2022) HACK3D - Q3 Report Infographics: https://www.certik.com/resources/blog/5LrhUKkvoXsWTEiXF4MtCG-hack3d-q3-report-infographics (Accessed 30 October 2022)
- CertiK(2022) HACK3D: The Web3 Security Quarterly Report - Q1 2022: https://www.certik.com/resources/blog/4ssW3zl1e2N3tO4kgVXy2O-hack3d-the-web3-security-quarterly-report-q1-2022 (Accessed 29 November 2022)
- Chainalysis (2022) [Twitter] 12 October: https://twitter.com/chainalysis/status/1580312145451180032
- DefiLlama(2022): https://defillama.com/
- HashEx(2022) Scam Report: November 2022: https://blog.hashex.org/scam-report-november-2022-dd09ada1a9dd (Accessed 1 December 2022)
- PeckShieldAlert (2022) [Twitter] 31 October: https://twitter.com/PeckShieldAlert/status/1587112410082512897
- PeckShield (2022) Latest Security Research: https://peckshield.com/#research
- Sherman, Natalie and Tidy, Joe (2022) Crypto giant FTX collapses into bankruptcy. BBC.com. 11 November: https://www.bbc.com/news/business-63601213 (Accessed 30 November 2022)