nccgroup

Illustration of cryptocurrency across the world. Royalty-free stock vector ID: 1034445187.

Sep 29, 2021 13:49 BST

# Securing a growing industry: spotlight on crypto security

Cryptocurrency is growing quickly, with a market capitalisation of $1.92 trillion dollars and the global market for hardware and mining equipment is estimated to hit $4.94 billion by 2030, more than triple its estimated size of $1.49 billion in 2020. This growth has attracted additional institutional interest, with Ernst & Young (EY) announcing this month that it will deploy its own blockchain solutions onto the public Ethereum blockchain ecosystem.

However, it has also attracted the attention of cyber criminals looking to take

advantage. Last month, hackers stole a combined total of around $700m (£506m) in two separate attacks on Liquid Global, a Japanese cryptocurrency exchange and Poly Network, a digital token platform.

With these attacks casting doubt on the security of the market at a pivotal point in its growth, we asked Javed Samuel, Cryptography Services Practice Head, about why cryptocurrency has emerged as a target for hackers, how cyber security can help the industry to build trust with new and existing customers and how cryptocurrency organisations can increase their resilience against cyber attacks.

**Why are hackers targeting cryptocurrency organisations?**

*"The cryptocurrency market is still growing, so organisations can definitely gain a competitive advantage by being the first to launch a new token or innovative product or solution. However, speed mustn't come at the expense of cyber security. For example, many crypto platforms use digital keys and signatures to verify a user's identity when carrying out transactions. If the code and the cryptography behind them is not validated or implemented appropriately, hackers can compromise keys and signatures to generate a fraudulent proof of identity, enabling them to access a user's account or exploit more vulnerabilities in the platform.*

*"The increase in attacks on cryptocurrency organisations is also linked to the rise of ransomware attacks. The liquidity of cryptocurrencies enable ransomware hackers to use them as ransoms before converting them into fiat currency as necessary. These factors, combined with the billions of dollars worth of assets that crypto platforms manage, make the market a natural target for hackers."*

**What tactics, techniques and procedures are hackers typically using?**

*"Typically, hackers attempt to extract and gain control of cryptocurrency by impersonating legitimate users. They use open-source intelligence to discover vulnerabilities on the platform, before using common tactics to exploit those vulnerabilities and gain the permissions required to achieve their goal. For example, this could involve the use of phishing to eventually access a user's keys or wallets where their cryptocurrency is stored, before extracting the assets and removing the legitimate owner's claim to them."*

**How resilient is the industry, and how does it compare to industries such as FinTech?**

*"The cryptography used in cryptocurrency tends to be fairly resilient, but the problems occur when the applications and platforms that leverage implementations are rushed to market without having their security sufficiently tested. This occurs because the market's first mover advantage leads many platforms to adopt a high risk, high reward strategy to ensure that they can innovate quickly, despite the strong possibility of financial and reputational loss in the event of a security breach.*

*"There are parallels between the crypto industry and FinTech, including the number of products available and the need for innovation and agility. However, many FinTechs are driven by institutions and more regulation, making it harder to develop a product without considering security thoroughly from the start of the process. In contrast, we may not know the identity of the developers of many cryptocurrencies, and the industry does not cater solely to institutional investors."*

**Why is cyber security so important for the cryptocurrency industry now?**

*"As the industry matures and consolidates and continues to become intertwined with institutional investment, there will be a natural demand for more risk management and security procedures before institutions get involved in cryptocurrency.*

*Some countries have already started using cryptocurrencies as legal tender, and it's likely that we'll see more regulation as other central banks and government institutions follow suit. From a policy perspective, crypto platforms should remember that they might need to adhere to security regulations that haven't even been developed yet, so it's advisable to begin following best practice now.*

*"We are gathering more and more data to quantify the impact of attacks on the sector, so it will become more important for the big, established players to avoid a security breach. It's important that the industry balances its innovation and agility with security and sustainability to ensure that it takes the next step on its growth journey effectively."*

**How can the industry become more resilient?**

*“Developers need to understand the risks in what they are building, in terms of the design and architecture and how the product could be abused or manipulated. This should involve building security in from the start of the process and thorough threat modelling that considers the ways in which a hacker would be likely to target the product. As the industry grows, companies should also share best practice and experiences with each other to build resilience across the board.*

*“NCC Group has already worked with multiple cryptocurrency companies to review their code, implementation, design and security guarantees against what they promise to their users. Based on the experiences we’ve seen across similar platforms, we provide insight into the potential security challenges that platforms could face now and in the future, and we are trying to encourage cryptocurrency to prioritise cyber security.”*

**ENDS**

---

## About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 14,000 customers to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience, and investment in research and innovation, it is best placed to help organisations assess, develop and manage their cyber resilience posture.

With circa 2,000 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

## Contacts

**NCC Group Press Office**
Press Contact
All media enquires relating to NCC Group plc
press@nccgroup.com
+44 7824 412 405
+44 7976 234 970