CRYPTO SECURITY REPORT

MARCH 2019

BitIRA

Altcoin Security Woes

Ethereum and especially Ethereum Classic have been weathering a rocky few months due to security concerns (and breaches) surrounding hard fork events. For instance, fake "hard fork" coins called Ethereum Nowa and Ethereum Classic Vision were attempting to scam people out of ETC and ETH. Ethereum Classic suffered more blows to its reputation after a likely 51% attack had reorganized blocks on its blockchain, causing Coinbase to suspend trading of the coin and the Gate.io exchange to lose 54,200 ETC to theft. These breaches have caused some to reevaluate the security vulnerabilities of proof-of-work (PoW) algorithms.

Other altcoins have unearthed security vulnerabilities recently, but these were luckily caught in time to prevent hacks. Zcash, a privacy coin, discovered a problem in the code that may have allowed an infinite amount of counterfeit ZEC coins to be produced by an attacker. Zcash quietly fixed the issue in a patch and then notified the community about it. EOS, another altcoin, got ahead of security risks by offering bounties for ethical hackers to find weaknesses in its blockchain code. Five such critical vulnerabilities were found by ethical hackers, to whom EOS.io awarded $40,750.

Security Threats ‘Fatal’ to Blockchain – How Likely Are They?

Crypto hacks of varying degrees have been an ongoing problem since Bitcoin was launched in 2009, and the issue still plagues the young industry. A recent report that rated major cryptocurrency exchanges on their security only gave A or A- ratings to 16% of them (none received an A+). One such exchange, Cryptopia, was hacked earlier in January, resulting in “significant losses”. Although the MIT Technology Review predicted that 2019 will be the year that blockchain technology becomes ubiquitous, it also recently published an article arguing that the market currently underestimates security threats to the technology, calling it “under certain conditions… quite vulnerable.”

But most of these hacks don’t rise to the level of systemic threats that could take down an entire blockchain. One such existential risk for a blockchain is the 51% attack, where hackers take control of more than half of the computing power in a network to manipulate the whole blockchain, potentially fatally. Ethereum Classic recently suffered such an attack, and one crypto developer and CEO even thinks that such attacks will greatly increase this year (though measures could be taken to prevent this, he notes).

Another less-discussed threat that could potentially unravel a blockchain is quantum computing. In January, IBM launched the world’s first commercially-available quantum computer, which can solve algorithms much faster than regular PCs. Can such quantum computers, in hackers’ hands, crack the very encryption behind blockchain? Most agree, though, that this threat is currently very minor and almost purely theoretical. Plus, if quantum computers become available to everyone at the same time, then blockchain networks can preemptively adapt to quantum computing power and fix any weaknesses in encryption.

More Top Brands Targeted by Cybercriminals

A recent report showed that $1.7 billion was stolen by crypto criminals in 2018, including $950 million taken from crypto exchanges alone. Most of the attacks on exchanges do not happen by lone individuals with a laptop in their basement but rather by sophisticated, criminal enterprises. Two hacking groups in particular, a recent report by Chainalysis suggests, are responsible for a whopping 60% of all attacks on crypto exchanges. The report called the groups Alpha and Beta, one a “giant organization partly driven by nonmonetary goals” and the other a “smaller organization absolutely focused on the money”.

Besides attacking exchanges, a trend is emerging of hackers targeting large corporations’ web properties or brands. In February, Microsoft removed eight Windows 10 applications from its app store because they were found to be utilizing users’ computing resources to mine Monero (XMR), a scheme called cryptojacking. Another scam earlier in the year involved the creation of a spoof website made to look like BBC News that would then send users to exploitative affiliate sites. Such high-profile attacks will possibly put even more pressure on governments to regulate the crypto space.