CRYPTO SECURITY REPORT

NOVEMBER 2018

BitIRA

Government and Cryptocurrency – Problems and Solutions

Regulatory agencies, especially in the United States, have been busy. Cryptocurrency crime poses a special problem for them, and the U.S. Commodity Futures Trading Commission (CFTC) said in early October that prosecution of such cases has increased dramatically in the last fiscal year. Up to $900 million was collected by the agency in fines alone.

As governments ramp up enforcement efforts, the allure to criminals of cryptocurrency's supposed anonymity is fading. A director at U.S. Immigration and Customs Enforcement testified to Congress on October 3 that trades from cryptocurrency to fiat money can now be traced. Every time such a transaction is made, he said, it creates a "vulnerability" which law enforcement can use to trace the source.

In an ironic twist, though, a federal agency has inadvertently fueled crypto crime. Cryptojacking—installing malware that hijacks a PC's resources to mine cryptocurrency—has increased a whopping 459% this year. This surge was made possible in part by sophisticated new tools for cyberattacks that were stolen from none other than the U.S. National Security Agency (NSA). The agency was developing the software to conduct its own cyberattacks.

Governments' use of cyberwarfare for their own ends should not be surprising. A study published on October 16 suggested that a staggering 65% of all crypto theft can be attributed to North Korean-sponsored hacks. Government hacking or surveillance of cryptocurrency will likely not affect the vast majority of crypto investors in North America. Still, Cointelegraph has published a useful guide for how citizens can avoid government surveillance of their digital assets.

Busting Bitcoin Myths

One reason for the increase in cryptojacking is the rise in amateurs getting in on the game. In one case, this is literally true as there have been reports of malware targeting players of the video game Fortnite. Cryptojacking malware, now available on underground forums, can be utilized for profit by even inexperienced hackers.

Nevertheless, there are some indications that the trend is reversing. In its Q2 2018 report, Malwarebytes noted a drop in mining malware detections from March to June and predicts that "cryptocurrency miners may be going out of style".

There have been other interesting reports published recently that challenge conventional wisdom. Due to the way Bitcoin was adopted in its early days, about 1,000 people own 40% of all existing bitcoins. Called "whales", this elite of concentrated crypto wealth has been blamed for much of the volatility in the digital currency markets. A new study, though, suggests that the $6.3 billion in wealth held and traded by "whales" has not caused price volatility.

Another reason popularly cited for price volatility has been that the issuance of tether (USDT), another digital currency, pumps up the price of bitcoin and vice versa. A study published in the October 2018 issue of Economics Letters suggests that this is not the case. The authors found that "the impact of tether grants on bitcoin returns were not statistically significant, and therefore tether issuances cannot be an effective tool for moving bitcoin prices."

Hacking the Unhackable

On September 20, Bitcoin Core developers disclosed to the public that a potentially disastrous vulnerability was discovered in the Bitcoin code that could have allowed hackers to create fake bitcoins and devalue the digital currency. Luckily, this weak link has not been exploited and the vulnerability was fixed in a recent upgrade.

Some believe that large-scale hacks such as this against a cryptocurrency pose a serious threat to digital assets. One of the most critical types of hacks is called a 51% attack. In such a hack (which requires enormous computing resources), a miner dominates the computing power on a blockchain network to influence outcomes. Bitcoin has never been attacked in this way, but five less popular coins fell prey to this malicious method in June alone. Even this vulnerability, though, is being addressed, with one possible solution involving penalizing the creation of delayed blocks necessary for a 51% attack.

New security measures of all sorts are being brought to market in 2018, including even the faithful high-security vault for offline storage. When all else fails and one's digital wallet falls victim to ransomware, services even exist that will negotiate on your behalf with cyber criminals to get your digital assets back. Traditional investors may be suspicious of the crypto market being able to scale if institutional investment increases, but BitGo foresees a time when securing a "Trillion Dollar Wallet" can be a reality. For now, the average crypto investor can learn a lot from previous hacks of crypto exchanges to be proactive about securing their own digital coins.