Cryptocurrency and Corporate Security

By Anthony J. Ferrante and D. Frank Hsu

This article discusses the foundations of the cryptocurrency landscape including blockchain. It will cover the risks associated with this space and the steps organizations should take to build strength in their security posture as it relates to their use of cryptocurrency.

The movie *In Time,*[1] which depicts a world where time is the universal currency, is an interesting sci-fi spin on the implications that evolving global currency could have on society. While we may not ever buy coffee with literal minutes of our lives, payment methods and the way money flows between entities are changing rapidly. These changes, particularly the growing hype and adoption of blockchain technology and cryptocurrency, have introduced a new dimension of cybersecurity considerations in particular for financial services institutions, e-commerce organizations, and consumers.

This article discusses the foundations of the cryptocurrency landscape including blockchain. It will cover the risks associated with this space and the steps organizations should take to build strength in their security posture as it relates to their use of cryptocurrency.

Blockchain basics

Blockchain has been hailed as one of the most secure technology advancements in history. And while its distributed nature does inherently enable a secure front, it is not without problems.[2] The explosive growth of this technology has made it a prime target for malicious actors looking to exploit it for gain, and researchers have identified that it is indeed vulnerable to theft, network attacks, mining compromises, and fraudulent use.[3] Among the many emerging blockchain networks and solutions, cryptocurrency is the most widely used and most mature application. It is also the most attractive to cyber threat actors, as it provides an anonymous and essentially irreversible channel to steal money or earn it through illicit means.

There are 2,000 different cryptocurrencies[4] and many exchanges and networks currently available around the world, and the list is growing all the time. Like any financial market, the total cryptocurrency market capitalization is constantly fluctuating. Earlier this year, it hit more than $800 billion and has been predicted by some to exceed $1 trillion in 2018.[5] Bitcoin continues to hold the dominant position among all the currencies and tends to be the most targeted by malicious actors.

A study by the US Department of Homeland Security found that between 2009 and 2015 one third of all Bitcoin exchanges had been hacked and about half closed shop during that

1 *In Time*, IMDB.com – https://www.imdb.com/title/tt1637688/.

2 Mauro Conti et al, "A Survey on Security and Privacy Issues of Bitcoin," arxiv.org, Dec. 25, 2017 – https://arxiv.org/pdf/1706.00916.pdf.

3 Ibid.

4 "All Cryptocurrencies," Investing.com – https://www.investing.com/crypto/currencies.

5 Ryan Browne and Arjun Kharpal, "Cryptocurrency Market Will Hit $1 Trillion Valuation This Year, CEO of top Exchange Says," CNBC.com, Feb. 13, 2018 – https://www.cnbc.com/2018/02/13/cryptocurrency-market-to-hit-1-trillion-valuation-in-2018-kraken-ceo.html.

time.[6] The largest of these attacks was against the Mt. Gox exchange, in which hackers stole more than 700,000 bitcoins, valued at about $350 million. The exchange shut down in the wake of the attack, and the losses were absorbed by its investors and account holders.

Beyond the obvious concerns for consumers, the cryptocurrency market presents some serious red flags and considerations for security professionals at e-commerce organizations, financial services institutions, and other corporations. It is critical to become familiar with the landscape and understand the ways in which cryptocurrency is stored, the risks associated with cryptocurrency in a corporate setting, and available means through which cybersecurity practitioners can prevent losses.

The lay of the land

Blockchain is a distributed, peer-to-peer digital ledger in which transactions are recorded chronologically and publicly.[7] It provides a way to account for and openly track transactions between parties, particularly cryptocurrency trades, while masking the identity of the individuals involved. Because it is de-centralized and designed for versatility, blockchain in and of itself is typically secure and difficult to defraud. But we begin to see diverse issues around how various networks and exchanges secure digital wallets, the accounts that store the cryptocurrency. This is a challenge and the root of most breaches of cryptocurrency accounts.

6 Gertrude Chavez-Dreyfuss, "Cyber Threat Grows for Bitcoin Exchanges," Reuters, Aug. 29, 2016 – https://www.reuters.com/article/us-bitcoin-cyber-analysis-idUSKCN11411T.

7 MIT Technology Review Editors, "Explainer: What Is a blockchain? Where It Came from, What It Does, and How You Make One," MIT Technology Review, April 23, 2018 – https://www.technologyreview.com/s/610833/explainer-what-is-a-blockchain/.

Today, there are two storage formats for digital wallets:

Physical storage

Also known as cold storage, this method involves storing cryptocurrency as a digital file on a computer or other hardware (such as an encrypted wallet). The currency is password encrypted and requires a decryption key to access the funds. While this method keeps the control in the hands of the account owner, it can be problematic if the password is forgotten, the computer is lost or compromised, or if a threat actor gains access to the machine and thus the decryption password. With cold storage, if a backdoor Trojan, key logger, or other malware gains access, they would potentially have access to the wallet and its decryption key.

Cloud storage

There are numerous cloud-based cryptocurrency exchanges that allow users to create an account and store their currency. This removes the need to build internal controls to protect physically stored cryptocurrency accounts but comes with the risk that the exchange may experience a breach. If the exchange is not maintaining proper security controls, a threat actor may gain access to any number of the exchange's wallets. And because transactions are anonymous, it is easy to steal money once a wallet is accessed, but nearly impossible to get that money back or investigate the offender. Unlike criminal activity in other arenas, no trail is left behind in cryptocurrency transactions, leaving very little for law enforcement to work with when trying to piece together clues about a theft.

For corporations with cryptocurrency accounts, determining the best storage method involves a few key considerations. Organizations that do not typically rely on third parties for storing their critical data and have robust cybersecurity programs can be good candidates for cold storage. When an or-

ganization has strong methodology in place, with real-time threat monitoring and the experience and personnel to protect critical assets, they can apply those practices to the cryptocurrency accounts and maintain them in-house. However, companies that do not have the resources or know-how to appropriately lock down their assets should store their accounts via a reputable and record-proven exchange.

No central organization exists to protect cryptocurrency, meaning that defrauded parties simply lose their money with little or no recourse, regardless of the storage method they use. Tyler Moore, a University of Tulsa cybersecurity professor and researcher, has been quoted extensively about the vulnerability of the cryptocurrency market. In an interview he said, "I am skeptical there's going to be any technological silver bullet that's going to solve security breach problems. No technology, cryptocurrency, or financial mechanism can be made safe from hacks."[8]

No central organization exists to protect cryptocurrency, meaning that defrauded parties simply lose their money with little or no recourse.

Indeed, the Mt. Gox breach is only one of many instances of cryptocurrency breaches. Malicious actors may use a variety of approaches to gain access to digital wallets through physical storage or exchanges. One study Moore conducted found that in an empirical analysis of distributed denial of service (DDoS) attacks in the Bitcoin ecosystem, there were 142 unique DDoS attacks on 40 Bitcoin services and seven percent of all known operators were victims of these attacks.[9] The research also concluded that the majority of DDoS attacks were against the exchange services and large blockchain mining pools, given the potential monetary gains of breaching these targets.

As cryptocurrencies become more widely used and more valuable, nefarious groups are increasingly motivated to impair transactions and leverage DDoS bots to expose vulnerabilities that may allow them to steal money. *Bitcoin Magazine* recently reported a study from Imperva Incapsula that noted "the cryptocurrency industry continues to be a frequent target of DDoS attacks, more so than many larger industries. Three out of every four bitcoin exchange sites were attacked in Q3 2017."[10] During a DDoS event attackers are working to flood the servers at cryptocurrency exchanges and operators to disrupt service and shut down activity, including delaying transactions or making them unavailable for an indefinite period of time. Given the importance of timeliness in financial trading, this can have serious implications. This activity underscores the importance that organizations trading in or relying on cryptocurrency must understand they are at higher risk to be targeted by this type of attack and must implement standard precautions, such as a combination of cloud and on-premise DDoS defense solutions to mitigate it.

Ultimately, money is the digital asset within cryptocurrency and should be treated like any other financial system. It will continue to be targeted by actors looking to steal it by exploiting the blockchain and intercepting fund transfers, or engineering funds out of wallets. To this end, according to data from BAE Systems, there have also been increases in bitcoin-stealing malware tools with attacks aimed at digital wallets, the compromise of private keys, and malware that hijacks computing resources for mining bitcoins.[11] Routing attacks[12] and phishing campaigns have also been identified as key threats targeting the cryptocurrency industry. Trojans that can gain access to copy or view information from computers through a backdoor are also threats to cold storage accounts. Threat actors are continually evolving and becoming more sophisticated, and what doesn't exist today may exist tomorrow. We will likely see new approaches that decrypt digital wallets and attack exchanges.

Cybersecurity strength for cryptocurrency assets

Today, the most common business users of cryptocurrency are e-commerce organizations that offer bitcoin and other currencies as a way to pay for products or services and financial services institutions that are looking to take advantage of blockchain technology and cryptocurrency to enable high-speed trades and other transactions. More and more enterprises are beginning to integrate cryptocurrency into their businesses and will need to address security accordingly.

Ultimately, cybersecurity is about insuring the critical and financial assets that drive value for the organization are protected. These are what the malicious actors will target. Today, and for a growing number of organizations, cryptocurrency has become another valued asset. To put the proper controls in place around these assets, security practitioners first need to examine what kind of storage and the type of exchange the organization is using for its cryptocurrency. With that as the foundation, teams can build a holistic and sound defense to ensure that the infrastructure around their accounts is protected with cybersecurity best practices.

Organizations using cold storage need to put proper in-depth security controls around their digital wallets. These controls are the same as those used to protect the organization's other assets. Implementing an incident response plan, leveraging leading-edge security technology, patching systems, monitoring threats, defending infrastructure, and intelligence gathering are among the best practices that should be exercised. Without proper security controls, teams will not have

8 Gautham, "Security Issues Plague All Financial Platforms," News BTC, August 29, 2016 – https://www.newsbtc.com/2016/08/29/security-issues-plague-all-financial-platforms-not-just-the-bitcoin-ones/.

9 Marie Vasek, Micah Thornton, and Tyler Moore, "Empirical Analysis of Denial-of-Service Attacks in the Bitcoin Ecosystem," – https://tylermoore.ens.utulsa.edu/bitcoin14ddos.pdf.

10 Giulio Prisco, "Bitcoin Exchanges Are Favorite Targets of Global DDoS Attacks: Report," Bitcoin Magazine, Dec. 5, 2017 – https://bitcoinmagazine.com/articles/bitcoin-exchanges-are-favorite-targets-global-ddos-attacks-report/.

11 "Cryptocurrencies Changing the Risk Landscape," BAE Systems – https://www.baesystems.com/en/cybersecurity/managing-the-risks-of-cryptocurrency#.

12 Maria Apostolaki, Laurent Vanbever, Aviv Zohar, "Hijacking Bitcoin: Routing Attacks on Cryptocurrencies," – https://btc-hijack.ethz.ch/.

ISSA
Information Systems Security Association

October 17–18, 2018
Georgia World Congress Center
Co-located with Cyber Security Atlanta

2018 ISSA International Conference

SECURING TOMORROW TODAY

ISSA's eighth annual flagship conference is a world class event bringing together cyber, information, software, and infrastructure security professionals from 92 countries around the world. This two-day conference delivers practical sessions and no-nonsense insights that give cybersecurity professionals the tools to strengthen their security without restricting their business.

Conference Highlights

- 1000+ attendees spanning all levels of IT and InfoSec
- Expert Key Note Program
- Latest Information Security trends and techniques
- Intimate roundtables and panel discussions
- Networking lunches, general sessions, and evening receptions and award parties
- Career center
- VIP Lounge

Topics

- Application & Data Security
- Cloud Security
- Security Awareness
- Security & Privacy Collaboration
- Governance, Risk & Compliance
- Email & Endpoint Security
- Professional Development
- Threat Intelligence
- Emerging Technologies
- Bridging the Business Gap

The Expo floor will now feature more than 50+ leading technology companies

For registration and more information, visit www.issa.org

visibility into the cyber threats that pose the biggest risks to their cryptocurrency accounts.

For example, an e-commerce website that accepts bitcoin as a method of payment and is using cold storage should be diligent about protecting the wallet. In some cases, the wallet may be located on the same server as the website's payment gateway, which is an Internet-facing server and therefore a prime target for infiltration. Internet-facing web servers are compromised all the time, and if the digital wallet is stored on it, it can be easily stolen. Further, even if the wallet is stored on an internal network, protections against lateral movement must be put into place. Any open points on the network must be secured so that an actor who gains access through the web server or other methods like spear phishing can't find the lateral channels to the server where the wallet is stored.

When using cloud storage, organizations should be very mindful of which exchanges they use, as these are the most targeted by threat actors. When choosing an exchange, the security team should be involved in conducting a well-rounded, third-party threat-assessment program. This exercise should be done for all outside partners with which data is shared to evaluate their cybersecurity fortitude and ensure their standards meet the organization's requirements on all fronts. Assessments should examine whether the exchange has a robust cybersecurity program that aligns with industry best practices.

In most ways, securing cryptocurrency is like securing any other critical asset or currency. Generally, the best practices that should be examined and implemented are the same as any that would be utilized to ensure a secure network. The CryptoCurrency Security Standard[13] is one entity that has recently emerged to help standardize security techniques and methodologies specific to cryptocurrency systems. The standards are currently in their nascence, but as they develop they may help organizations fine tune their cybersecurity posture relating to securing their wallets and blockchain implementations.

Conclusion

Cybersecurity is not a nebulous practice, and blockchain is no longer nebulous either. It is being used increasingly in all kinds of business practices, and its application will continue to proliferate. Cryptocurrency and blockchain technology use must be viewed as any other corporate critical asset or intellectual property and be protected accordingly. By treating crypto accounts as high-value assets, teams can build holistic cybersecurity methodologies that proactively defend against known and anticipated threats, and enable rapid response and eradication of threats that are discovered. Then they can learn from new intelligence and leverage it to further strengthen defenses across the overall network. As one academic paper put it, cryptocurrency accounts should have, "layers and layers amounting to metaphorical armed guards defending iron gates with vaults deep underground behind a thousand doors."[14]

The views expressed herein are those of the authors and not necessarily the views of FTI Consulting, Inc., its management, its subsidiaries, its affiliates, or its other professionals.

About the Authors

Anthony J. Ferrante is the global head of cybersecurity and a senior managing director at FTI Consulting. Mr. Ferrante has more than 15 years of top-level cybersecurity experience, and maintains first-hand operational knowledge of more than 60 criminal and national security cyber threat sets and extensive practical expertise researching, designing, developing, and hacking complex technical applications and hardware systems. He may be reached at Anthony.ferrante@fticonsulting.com.

D. Frank Hsu, PhD, is the Clavius Distinguished Professor of Science and a professor of computer and information science at Fordham University in New York, NY. He has published over 200 technical papers and co-authored/co-edited over 40 books and book chapters. He has extensively used data analytics, micro- and macro-informatics, AI, and combinatorial fusion in the study of biomedicine, health care, virtual screening, target tracking, cognitive neuroscience, market segmentation, and cybersecurity. He may be reached at hsu@cis.fordham.edu.

13 "Crypto Currency Security Standard (CCSS)," Crypto Currency Certification Consortium – https://cryptoconsortium.org/standards/CCSS.

14 Mauro Conti et al, "A Survey on Security and Privacy Issues of Bitcoin," arxiv.org, Dec. 25, 2017 – https://arxiv.org/pdf/1706.00916.pdf.