“Cryptocurrency: Why Should Small-to-Medium Businesses Be Aware of What’s at Stake?”

Written by Matthew Butterman and Eric Powell for Rylet Industries, LLC

This is the first of a three-part series on cryptocurrencies, how it relates to modern banking, and the common security issues that small-to-medium business leaders should be aware of surrounding this new technology.

In this first part, we want to introduce our readers to the basic terminology and ideas surrounding this exciting new development in our digital world. This is will not be an exhaustive text that will cover all the aspects of this topic. This is simply a primer to assist you with understanding the “big picture”.

WHAT’S ALL THE FUSS ABOUT?

By now, you may have heard a lot about the volatile digital asset or cryptocurrency called, “Bitcoin”. (1) If you haven’t bought any yet, you may also be wondering what all the fuss is about. So, today, we’re going to try to shed some light on what Andreas Antonopoulos purports in his book, “The Internet of Money” as the “next layer of the internet”. (2)

Starting with Bitcoin, it is a person-to-person (P2P) financial network that was launched in 2009 by an unknown computer genius, referred to as “Satoshi Nakamoto”. When individuals run computers that help to sustain the network, (i.e. miners) they are rewarded for their efforts with “bitcoins”. On many of the websites and applications that you can buy, sell, or trade bitcoins, it’s commonly denoted by the three-letter symbol, “BTC”. (1)

As the first of its kind, it is also the most valuable and prevalent form of cryptocurrency. Currently, there are over 1,400 projects running their own cryptocurrency networks with associated coins. Likewise, other networks also have their own coins. For example, the Ethereum network rewards its miners with coins referred to as “Ether”. (3)

WHAT’S WRONG WITH MY GREENBACKS?

It’s safe to assume that you’re very familiar with using some form of *fiat currency* such as the U.S. Dollar, the E.U.’s Euro, the Chinese Yuan, and many others. Processing transactions with fiat currencies requires a third-party intermediary - typically a bank. The global banking system runs on a system of networks that facilitates the movement of over $74 Trillion US Dollars per year. (4)

In addition to banks, there are several global payment processors such as VISA ®, MasterCard ®, American Express ®, PayPal ®, Venmo®, and many others. All of these entities work together to track the value of currencies and verification of the identities of senders and recipients. This system, requiring fixed or “centralized” points of reference and control, for fiat transactions is technically referred to as *centralized banking*.

These intermediaries are necessary to commerce because the validity and security of bank transactions must be constantly verified and cross referenced to the identities of both the senders and recipients. Furthermore, in the case of international banking, volatile currency exchange rates add entirely different layer of complexity to the mix. Hence, centralized banks and the transactions they process rely on ledger systems to check value and identity at every step of the way. For these reasons, the banking system relies heavily on human capital despite the use of modern computer technology. There are literally armies of accountants, law firms, and other support personnel to facilitate the "magic" that goes on behind the scenes of bank terminals and ATMs.

The complexity of steps in a centralized transaction means there are a number of "way stations" in the process. Because of this, there are several opportunities for security breaches to occur. Just think about the number of verifications that are made in the typical credit card transaction: the identity of the cardholder, the current value of the account, the card's credit limit, the identity of the merchant, and many more. With all of these checks taking place, it's no wonder that transactions may be declined or accounts frozen because of security concerns. In fact, it's truly a modern marvel that it doesn't happen more often than it actually does. So, the next time you pay bank fees, keep in mind that the banks are paying a lot in labor and security costs to process even simple transactions.

THE BLOCKCHAIN WILL CHANGE THE FUTURE OF CENTRAL BANKING

Today, our civilization relies on central banks, fiat currencies, and fractional reserve banking. In this system, a central bank, controlled by several member banks, create money that is backed by their associated sovereign government. These fiat funds along with deposits are then lent to consumers in the form of loans. These loans are then repaid with interest over a period of time. For at least the last two hundred and fifty years, this has worked very well to stimulate incomprehensible amount of wealth in several capitalist societies such as the United States. However, cryptocurrencies threaten to disrupt this paradigm via its use of blockchain technology. (5)

Blockchain technology decentralizes and, to an extent, anonymizes financial transactions between two parties. This decentralization means that there is no central reference point or banking institution to verify value and the identities of senders and recipients. Instead of using a centralized ledger and armies of support staff, the blockchain uses a distributed ledger system running complex mathematical encryption to confirm transactions between two parties. (2)

What's even more remarkable is that cryptocurrencies use open-source software. This software is available for anyone to examine, contribute to, and even use for their own purposes. This openness, counterintuitively, makes cryptocurrency networks more secure than fiat currencies. It achieves this high level of invulnerability because any manipulation of the code (e.g. backdoors, viruses, malware) are relatively easy to spot and correct by community contributors.

> Note: Although, people have lost coins by fraud, thefts, or hacks, the actual Bitcoin network itself has never been hacked in its nine-year history. Now, think about how many times you've heard of banks being hacked in the last year alone.

Overall, these features have both positive and negative aspects. One positive is that cryptocurrency blockchains are less prone to manipulation and human error by central actors. For example, fiat currencies can be affected on a macro level by currency manipulations committed by a central bank, a banking meltdown like the one that occurred in 2009, or any number of instances of wholesale fraud. In the case of human error, valuations can be incorrectly entered into centralized ledgers with fiat currencies, purely by chance human error. By eliminating the need to rely on centralized institutions, cryptocurrencies are

less prone to human error and geopolitics. Conversely, because cryptocurrencies don't rely on centralized institutions and preserve a higher level of anonymity, one alleged downside is that they may facilitate criminal activities. For these reasons, cryptocurrencies are looked upon by government agencies with skepticism and banks with generalized fear. In its 2017 Annual 10-K Report, Bank of America® wrote:

> *"In addition to non-U.S. legislation, our international operations are also subject to U.S. legal requirements. For example, our international operations are subject to U.S. laws on foreign corrupt practices, the Office of Foreign Assets Control, know-your-customer requirements and anti-money laundering regulations. Emerging technologies, such as cryptocurrencies, could limit our ability to track the movement of funds. Our ability to comply with these laws is dependent on our ability to improve detection and reporting capabilities and reduce variation in control processes and oversight accountability. "(6)*

IN SUMMARY

Cryptocurrencies and the blockchain technology they're built on may be the biggest innovation to the financial world that we've seen in our lifetimes. Not only does it have the power to free consumers from centralized bankers, it also provides a level of institutional security and privacy not seen in decades. The day is rapidly approaching where small-to-medium businesses will need to know and understand how this new technology works. There will be new threats to securing business transactions and data. These threats will range from simple theft to compliance with more aggressive government scrutiny. In our next installment, we'll cover some of the most notorious cybersecurity incidences involving businesses and cryptocurrency technologies.

SOURCES

(1) Bitcoin.org. Retrieved from https://bitcoin.org/en/

(2) Antonopoulos, AM. "The Internet of Money: A Collection of Talks". Merkle Bloom, LLC. Oct 1st, 2017.

(3) Ethereum.org. Retrieved from https://www.ethereum.org/

(4) Desjardins, J. The $74 Trillion Global Economy in One Chart. http://www.visualcapitalist.com/74-trillion-global-economy-one-chart/

(5) Structure of the Federal Reserve System. Federal Reserve.gov. Retrieved from https://www.federalreserve.gov/aboutthefed/structure-federal-reserve-system.htm

(6) Bank of America SEC 2018 10-K Annual Filing. Feb 28, 2018. Retrieved from http://investor.bankofamerica.com/phoenix.zhtml%3Fc%3D71595%26p%3Dirol-sec#fbid=1MuYFvZHryB

PART II

Continuing our earlier discussion on cryptocurrencies and blockchain technology, we'll focus in Part II on the various security threats to this emerging financial technology.

THE EXCHANGE TRAP

One chief threat is online storage of cryptocurrency. Cryptocurrency can be stored in "wallets", otherwise known as "exchanges", and exchanges are the closest thing to an online or virtual bank that exists in this new financial paradigm. Exchanges are considered the most vulnerable to security breach in the world of cryptocurrency, and there have been a number of hacks by cyber criminals at exchanges - a sort of information age bank heist. The most infamous hack took place at the Mt. Gox bitcoin exchange in 2014, and it resulted in $400 million of stolen currency for about 25,000 bitcoin owners. Unlike banks, which are insured and regulated (and bank deposits in the U.S. are backed up through the FDIC), bitcoin exchanges are the wild west of the financial world, uninsured and unregulated, and therefore there was no recourse for the many thousands of people who were stolen from. Also, the anonymous encryption of cryptocurrency, although ostensibly more secure, means that it's much harder to trace hackers, and indeed the perpetrators of the Mt. Gox heist have never been identified.[4]

THE SOFT TARGET OF SOCIAL MEDIA

Another successful tactic for hackers has been to use people's social media accounts. Many social media users have not adequately hidden their email addresses and mobile phone numbers from savvy online predators. The hackers will then call your mobile phone service provider and request that the number be ported over to their own device. Once they have the number on their device, your name and email address, it can be relatively easy to access your bitcoin exchange and transfer currency to the hacker's wallet. It can then be converted to fiat currency before the digital trail can be traced, if it ever can. One way to avoid this theft is to call your cell provider and put a "do not port" status on your account.[4]

RANSOMWARE AND MALWARE CRYPTOJACKING

Ransomware is a security threat for all computer systems users, but cryptocurrency plays an interesting role here. Ransomware attacks your system, encrypts data and demands a ransom payment to release your system from attack. Traditional currency ransoms have been possible to trace to the criminal, but cryptocurrency ransoms are nearly impossible to trace due to the inherent anonymity of decentralized cryptocurrency. As with other hacks using cryptocurrency, the perpetrators can take the cryptocurrency ransom and convert it to traditional currency, and in turn, cash, without leaving a cyber trail of identity.[4]

The unwanted downloading of malware represents another significant security concern. In a process dubbed "cryptojacking", a computer user can unwittingly download malware from an infected website, and the cybercriminal can use the computing power of your device to mine bitcoin. Because the mining of bitcoin is profitable for the miner, if a website is infected, it can be used to mine bitcoin from tens of thousands of users, resulting in a huge windfall. Unfortunately, some unscrupulous websites know that they have been infected with mining malware but reach a deal with the hackers to share in the profits, making their website visitors clueless abettors to a criminal enterprise. The profits from mining malware can far exceed revenue from traditional advertising sources for the website owners.[4]

IN SUMMARY

The bottom line is that the world of cryptocurrency and blockchain technology already has and will

continue to revolutionize the way we do business. It's not a passing fad. With the premium it places on technology, it offers significant security and cost advantages over traditional bank-based currency. The security challenges that do exist are being met by cybersecurity and cyber-resilience companies like Rylet, and if cybercriminals show their tech-savvy and ingenuity, it is being addressed and greatly surpassed by the innovative work of the cybersecurity industry.

Sources

1. https://www.thelawyersdaily.ca/articles/5147/cryptocurrency-and-cybersecurity-a-primer
2. https://www.investopedia.com/terms/c/cryptocurrency.asp
3. https://www.roguemoney.net/blog/2016/01/21/20160121crypto-currencies-kryptonite-of-the-banksters
4. https://www.thelawyersdaily.ca/articles/5250/cryptocurrency-and-cybersecurity-the-implications