RESHAPING CYBERCRIME WITH CRYPTOCURRENCIES

Introduction

Today's digital transformation lets us turn any car into a taxicab and any house into a hotel. Likewise, it creates boundless opportunities for agile companies and startups alike to build new offerings for customers and improve operating efficiencies. But what are the risks when traditional money transforms into digital cryptocurrencies?

Individuals and businesses are using cryptocurrencies like Bitcoin—with a current market capitalization of over $125 billion[1]—and hundreds of other digital currencies for money transfers, payment systems, raising capital to support business growth, and as hybrid securities for investing. As each of us is likely to be affected either directly or indirectly by cryptocurrencies, now is a good time to understand them and their cyber security risks.

As cryptocurrencies grow in usage and in number, they have also reshaped trends in cybercrime. To understand the risks, it helps to understand how each element that makes up a cryptocurrency can be a potential target for cybercrimes.

[1] Nathan Reiff, Top 5 Cryptocurrencies by Market Cap - Investopedia, June 25,2019.

Is Malware in the Money?

A cryptocurrency is built on a digital ledger called a blockchain that contains public addresses. Each public address stores users' balances of cryptocurrency units, for example 2.0003 BTC (Bitcoins). You can think of a public address as a transparent safe that lets everyone see how much money it contains, but not who owns or interacts with the money. To move money out of a safe, you need the safe's private key. When you "own some bitcoin," you actually own a private key to a public address that contains a record of your balance of bitcoins. Making a transaction means changing the cryptocurrency balances of those involved in the transaction and recording all changes in the blockchain ledger.

You call a cryptocurrency unit the name its issuer gives it such as a bitcoin issued by Bitcoin. More generally we refer to a cryptocurrency unit as a token or an altcoin (alternative to bitcoin). Tokens can either be intrinsic or asset based. Intrinsic tokens contain their own value like dollars or euros. In contrast, asset-based tokens have a claim on an asset such as a business. Security Tokens are asset-based tokens which provide many of the same benefits and regulatory safeguards as traditional securities such as stocks and bonds.[2] In addition, some issuers like Bitcoin simply provide tokens, while other issuers such as Ethereum provide tokens and "smart contracts" that are executable applications optimized to run on a distributed peer-to-peer blockchain computer network.

As tokens are virtual numbers entered in a blockchain and are not entities independent of a blockchain, users don't send tokens to other users' wallets. Tokens are not in a form that can be compromised to infect their owners' computing devices. Blockchain technology that underlies cryptocurrencies is a different story however.

[2] Toshi Times, 6 Cryptocurrency Trends For 2019 September 9, 2019, https://toshitimes.com/6 cryptocurrency-trends-for-2019.

Blockchain: Distribution and Encryption as Safety Measures

Blockchain acts as the bank vault that stores tokens and the ledger that records transactions. A blockchain is a series of lists—the blocks. Blocks contain data and pointers that link one block to the previous block. This creates a record of transactions through time that can't be altered. The reason that a blockchain can't be altered is Blockchain is a distributed software system. This means that similar copies of blockchain software and the data they hold reside on many computers connected to each other through a peer-to-peer network.

According to a Check Point analyst, there are several different software versions just for bitcoin. The computers on the network use a consensus protocol to confirm the records of verified transactions and verify new transactions in the blockchain. To steal tokens or otherwise alter a blockchain, criminals would have to compromise many hundreds or thousands of distributed computers at the same time. Blockchain's decentralized structure and use of computer-intensive encryption makes cryptocurrencies resistant to tampering. However, there are weaknesses in blockchains.

Bitcoin is an open system which means a community of developers creates updates for Bitcoin's software. Members of Bitcoin's blockchain-processing community (called coin miners or operators) choose whether or not to install these updates on their computers. On one hand, there isn't a process for making automatic software updates that attackers could use to install malware throughout the network. On the other hand, if researchers find a vulnerability in Bitcoin software, the computers are using several versions of the software, which could make patching difficult. In addition, all Bitcoin operators might not install patches in a timely manner, leaving computers on the network vulnerable to exploitation.

Attackers have compromised Bitcoin's blockchain at least twice so far. The first attack used Bitcoin's network to distribute child abuse materials. The second attack took over operators' computers to illicitly mine Monero cryptocurrency and perpetrate other malicious acts after becoming infected with Glupteba malware.[3]

[3] Billy Bambrough, Warning Issued After Malware Is Found To Have Hijacked Bitcoin Blockchain, Forbes, Sep 7, 2019, https://www.forbes.com/sites/billybambrough/2019/09/07/serious-malware-warning-over-bitcoin-blockchain/#7c59ff6d7c28

For some time, criminals have attacked blockchains in other ways. A "51% attack" happens when a miner or group of miners control over 50 percent of a network's computing power or "hash rate." Controlling the majority of a network's computing power could let an attacker monopolize the recording of new blocks and prevent other miners from completing blocks. This lets the attackers receive all of the mining rewards and can block other users' transactions. Or, the attacker could send a transaction, then reverse the transaction to make it appear they still own the coins they spent. In January 2019, Etherium's blockchain suffered a 51% attack in which at least seven instances of double spending occurred.[4]

Another possibility is an "eclipse attack." Nodes on the blockchain must remain in constant communication in order to compare data. An attacker who manages to take control of one node's communications and fool it into accepting false data that appears to come from the rest of the network can trick it into wasting resources or confirming fake transactions. Similarly, researchers at Cornell University have discovered how to subvert blockchains using less than 50 percent of a cryptocurrency's mining power. Using their method, a "selfish miner" can trick other computers on the network into wasting time decrypting transactions that have already been decrypted while the selfish miner reaps the rewards of processing new transactions.[5] Looking beyond infrastructure, there are many examples of cyber-attacks that steal, extort or scam using cryptocurrencies.

A "51% attack" happens when a miner or group of miners control over 50 percent of a network's computing power or "hash rate."

[4] Gareth Jenkinson, Etherium Classic 51% Attack – Reality of Proof-of-Work, Cointelegraph, January 10, 2019. https://cointelegraph.com/news/ethereum-classic-51-attack-the-reality-of-proof-of-work

[5] Mike Orcutt, How Secure is Blockchain? MIT Technology Review, April 25, 2018. https://www.technologyreview.com/s/610836/how-secure-is-blockchain-really/

Crypto-crime Does Pay

COIN MINERS AND CLAIM JUMPERS

When a computer in a blockchain network processes an encrypted transaction, it adds the details of the transaction to a block. In return for this participation, the cryptocurrency's decentralized mining application creates a block that contains a reward for the participant that all the networks' computers validate. Processing transactions to receive tokens is called mining. However, not all mining is performed legally or ethically. In one attack, cyber criminals infected over 50,000 computers with cryptomining malware using highly sophisticated methods. Called the "Nansh0u campaign," this attack impacted organizations in healthcare, telecoms, media and IT industries.[6]

The owners of the compromised computers paid for the electricity and processing power needed to make blockchain transactions, but received no compensation.

Using a different method for illicit crypto-coin mining, a company called Coinhive, provided an in-browser cryptomining service. Coinhive software let websites such as Showtime, Salon.com and The Pirate Bay, to receive revenue by tapping into visitors' computers to mine Monero tokens. As the mining was done without visitors' knowledge or permission, the ethics of Coinhive's service was murky at best. When criminal hackers started using Coinhive to mine tokens using thousands of websites and hundreds of thousands of unpatched IoT devices they had taken over illegally, the service crossed over into enabling illegal activity. Coinhive shut down March 8, 2019.[7]

[6] Benedict Alibasa, Hackers Infect 50,000 Servers With Sophisticated Crypto Mining Malware, Coindesk, June 3, February 28, 2019. https://www.coindesk.com/hackers-infect-50000-servers-with-sophisticated-crypto-mining-malware

[7] Graham Cluley, Coinhive, the in-browser cryptomining service beloved by hackers, is dead, Tripwire, https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/coinhive-browser-cryptomining-service-dead/

ATTACKING EXCHANGES

Exchanges are websites where members of the public can buy, sell and trade cryptocurrencies. Exchanges present several possible points of compromise. Recently Bitpoint, a cryptocurrency exchange in Japan, lost $32 million worth of cryptocurrency when thieves attacked Bitpoint's hot wallet, which is an application that is connected to the Internet.[8] In a combined data-theft and phone scam, criminals stole bitcoins from customers of a bitcoin exchange called Bithumb located in South Korea. They started the attack by stealing the personal data of 31,000 customers from a Bithumb employee's computer. The criminals used the stolen data for a social engineering campaign in which a phone scammer tricked Bithumb customers into divulging their wallet credentials, which the criminals used to steal the victims' bitcoins.

Another way for criminals to make money is by launching distributed denial-of-service (DDoS) attacks against exchanges to manipulate the value of cryptocurrencies. Since the price of a crypto currency is set by several exchanges around the world, denying access to one or more exchanges could let a complicit trader take advantage of price differences.

Recently Bitpoint, a cryptocurrency exchange in Japan, lost $32 million worth of cryptocurrency when thieves attacked Bitpoint's hot wallet, which is an application that is connected to the Internet.[8]

[8] Shane Hickey, $32m stolen from Tokyo cryptocurrency exchange in latest hack, The Guardian, July 12, 2019. https://www.theguardian.com/technology/2019/jul/12/tokyo-cryptocurrency-exchange-hack-bitpoint-bitcoin

Who's In Your Wallet?

Crypto wallets are different than digital wallets. A digital wallet holds digital versions of credit cards, bank cards, and other standard payment methods. In contrast, crypto wallets are software applications that hold the owners' public and private encryption keys and interact with blockchains. These wallets let users make transactions and keep track of their tokens stored on the blockchain. Wallets' main risk factor depends on the whether they are hot wallets that are connected to the Internet or cold wallets that are not connected. Experts generally consider cold wallets to be much more secure.

In addition, a wallet's security depends on its owner not divulging the wallet's credentials to attackers in a phishing attack. Your wallet's security depends on the malware resistance of the device that keeps the wallet. A crypto wallet kept on your computer or smartphone can be compromised if attackers steal your wallet credentials using malicious apps, spyware, phishing, and other standard cyberattack methods.

RANSOMWARE

Perhaps cryptocurrencies' most prominent contribution to global cybercrime is its use as the payment method of choice in ransomware attacks. Declining in 2018, ransomware attacks have shown a resurgence, doubling in 2019.[9] Ransomware encrypts files stored on a victim's computer and demands a ransom payment to unlock the victim's files. Researchers at Check Point have reported threat actors scaling back banking Trojan attacks and increased ransomware attacks. A reason behind the changeover was that banks have put in place safeguards that block suspicious money transfers. This made banking Trojan attacks less likely to succeed. Also, bank transfers are easier for law enforcement agencies to trace. In addition, ransomware attacks are simpler and less costly to produce and operate than banking Trojans.

In contrast, ransomware payments made in cryptocurrency tokens are much harder to trace and the transactions can't be blocked.

Due to growing interest by government regulators and security analysts, cryptocurrencies and exchanges are becoming less anonymous payment methods for cyber criminals. Despite this, 98 percent of ransomware payment requests are for bitcoins.[10] Criminals maintain complete privacy by quickly converting bitcoins into untraceable cryptocurrencies such as dash and Monero.

---

[9] Jessica Davis, Ransomware Attacks Double in 2019, Brute-Force Attempts Increase, HealthITSecurity, September 3, 2019. https://healthitsecurity.com/news/ransomware-attacks-double-in-2019-brute-force-attempts-increase

[10] Marie Huillet, Bitcoin Accounts for 98% of Crypto-Denominated Ransomware Payments, Study, Cointelegraph, April 19, 2019 https://cointelegraph.com/news/bitcoin-accounts-for-98-of-crypto-denominated-ransomware-payments-study

FEASTING ON ICOs

To raise startup capital, some entrepreneurs issue their own asset-based cryptocurrencies. Investors buy the newly issued tokens in events called initial coin offerings (ICOs). Besides legitimate investment opportunities, ICOs can create opportunities for scammers and thieves. Scammers who want to raise money by holding an ICO can simply pretend to issue a cryptocurrency and instead set up a Ponzi scheme. Because Etherium's platform makes it easy for legitimate entrepreneurs to issue their own crypto coins to raise capital through ICO's, Etherium has also become a favorite platform for scammers setting up Ponzi schemes or simply raising money and disappearing.[11]

A different group of attackers found a simple way to use an ICO to steal tokens. When a trading platform for an ether-based cryptocurrency named Coindash held their ICO, cyber criminals took over Coindash's website and replaced Coindash's ether wallet address with their own wallet address. Before Coindash discovered the attack, investors sent $7.4 million worth of ethers to the criminals' wallet. For unknown reasons, a year later the attacker returned 20,000 of the Eths stolen during Coindash's ICO.[12]

Asset-based Security Token Offerings (STOs) are expected to overtake ICOs as a means for raising capital as STOs are more highly regulated in the USA and have limited exchange platforms.[13]

PUMP-AND-DUMP FRAUD

Like shares of stock, the value of tokens can quickly vary. This makes them, like shares of stock, subject to pump-and-dump fraud schemes in which a scammer makes misleading statements that cause a token's price to rise. The scammers sell their tokens at the inflated price.

[11] Gareth Jenkinson, From Ponzi Schemes to ICO Exits, Ethereum's Blockchain Has Been the Platform of Choice for Scammers, Cointelegraph, February 4, 2019 https://cointelegraph.com/news/from-ponzi-schemes-to-ico-exits-ethereums-blockchain-has-been-the-platform-of-choice-for-scammers

[12] Charlie Osborne, Hacker returns 20,000 ETHs Stolen During Coindash ICO, ZDNet, Feb 26 2018. https://www.zdnet.com/article/hacker-returns-20000-eth-stolen-during-coindash-ico/

[13] Tom Wilson, Explainer: 'Privacy coin' Monero offers near total anonymity, Reuters, May 14, 2019, https://www.reuters.com/article/us-crypto-currencies-altcoins-explainer/explainer-privacy-coin-monero-offers-near-total-anonymity-idUSKCN1SL0F0

MONEY LAUNDERING

Money laundering makes "dirty money" derived from illegal activities appear to be legal or "clean." Cryptocurrencies are ideal for laundering money. Despite the transparency of bitcoin transactions, the transactions don't capture personally identifiable information (PII), which gives users anonymity. To launder money, criminals can buy tokens with dirty money, then quickly make transactions among several wallets, purchase goods through participating merchants, turn their tokens back into regular money, or shift them to other cryptocurrencies at one or more exchanges.

Regulators and private security companies that analyze bitcoin transactions have taken notice. As bitcoin comes under increased scrutiny, Monero, sometimes called a "privacy coin" because it conceals nearly all details of users' transactions, has become popular for illegal money transfers.[13] Monero has grown the 12th largest cryptocurrency with a market capitalization of roughly $1.4 billion.[14]

Traditional banks have largely avoided cryptocurrencies as their use could cause problems complying with money-laundering regulations such as the Bank Secrecy Act (BSA) and the Anti-Money Laundering (AML) Act. Also, the hundreds of blockchains now running and new ICOs make investigations into money laundering more difficult for law enforcement agencies.

Traditional banks have largely avoided cryptocurrencies as their use could cause problems complying with money-laundering regulations such as the Bank Secrecy Act (BSA) and the Anti-Money Laundering (AML) Act.

[13] Tom Wilson, Explainer: 'Privacy coin' Monero offers near total anonymity, Reuters, May 14, 2019, https://www.reuters.com/article/us-crypto-currencies-altcoins-explainer/explainer-privacy-coin-monero-offers-near-total-anonymity-idUSKCN1SL0F0

[14] Op Cit, Toshi Times

What It All Means

Cryptocurrencies create risks whether you are a player on the field or sit on the sidelines. Businesses must be aware that processing blockchain transactions to receive coin mining rewards is expensive for miners due to the high cost of computing resources and the electricity it takes to run and cool them. These high mining costs make it worthwhile for criminals to hijack large numbers of computers from legitimate businesses and the public to mine tokens. Having computing resources hijacked for mining is especially risky for organizations that use scalable virtual machines in a lightly protected public cloud environment in which costs can quickly soar. Whether your IT program uses a business network or a public cloud, you must protect your computing resources with advanced threat prevention and anti-bot security technology or risk paying a high price for mining someone else's tokens.

Currency miners should also protect their computers with advanced threat prevention to protect their computing resources from being hijacked, protect their computing assets against denial-of-service attacks and prevent computers from becoming infected with malware.

Exchanges should protect their user's cryptocurrency by using cold storage to store users' funds. This involves moving private keys to offline devices. In addition, for stronger hot storage security, exchanges should use multi-signature (multisig) wallets that use more than one key to authorize transactions. Exchanges should protect their core networks against denial-of-service and advanced threats to prevent manipulation of currency prices. To prevent exposing customer data to criminals, exchanges must also protect the endpoint computers employees' use.

If you're a personal user of cryptocurrencies, the emphasis moves to your own security practices. The best way to do this is to store cryptocurrency on special hardware wallets that are not connected to the Internet. If you continue to use your current devices for your crypto wallet, be sure you at least have security installed on your devices including anti-virus and advanced mobile threat prevention on your smartphone and laptop. Never give out your wallet credentials to anyone. Preventing spyware and phishing attacks from stealing your wallet's credentials is your responsibility. Cryptocurrencies offer great opportunities for decentralizing transactions of many kinds, but, they still have some work to do before you can feel completely secure using them.

[10] "Code Spaces Forced to Close its Doors After Security Incident," by Steve Ragan, CSO Online June 18 2014

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com