ISSN: 2473-3857
v5 n5110

Teaching Cases

Cybersecurity and Cryptocurrencies: Introducing ecosystem vulnerabilities through current events

Anthony Serapiglia
Anthony.Serapiglia@stvincent.edu
CIS Department
St. Vincent College
Latrobe, PA 15650

Abstract

Teaching Cybersecurity is at times a balancing act. It is necessary for students that are involved in cybersecurity education to develop very specific skills and areas of mastery, however, these points of focus must not come at the expense of understanding the greater picture of how everything interacts and affects each other outside of the technical aspects. Introducing students to the kaleidoscope of interrelated topics encompassed by Cybersecurity through a "systems" approach can help to ensure that especially early in the process students learn to appreciate and understand the enormity of possible attack vectors or vulnerabilities of things that they use every day. Utilizing current events and cutting-edge technologies in the classroom is also a minefield of risk vs reward. The world of Bitcoin and Cryptocurrencies has been a fascinating and volatile mix of technology, money, and human nature for the past decade. With multiple cycles of "to the moon" bubbles followed by "falling to zero" crashes, this technology has jumped from being just a "techie" thing to being followed by mainstream media and everyday people across the globe. With the increase value, and the increase in general awareness, Bitcoin and the Cryptocurrency world has invited not just investors to the show, but also all the con-men, tricksters, and thieves that money attracts. This paper will provide three specific cybersecurity vulnerabilities related to Cryptocurrencies and that can be utilized to illustrate to students starting out in the cybersecurity world the intricacies of complex systems and un-foreseen vulnerabilities. These real-life events can be utilized to further research in these areas or to spark ethical discussions in class or through position papers.

Keywords: Cybersecurity, Cryptocurrency, Bitcoin, 51% Attacks, Exit Scams, Attack Vector, SIM Swapping

1. INTRODUCTION

Cybersecurity is at times a balancing act. With the increased focus on cybersecurity education since President Obama's executive order in 2013 on Improving Critical Infrastructure – Cybersecurity (E.O., 2013) the umbrella that encompasses topics and domains of focus within the discipline has grown tremendously. It is necessary for students and practitioners that are involved in cybersecurity to develop very specific skills and areas of mastery, however, these points of focus must not come at the expense of understanding the greater picture of how everything interacts and

affects each other, including non-technical issues. The system is always bigger than we think it is. Being aware of the kaleidoscope of interrelated topics encompassed by Cybersecurity through a "systems" approach can help to ensure that especially early in a cybersecurity degree or career, everyone involved begins to learn to appreciate and understand the enormity of possible attack vectors or vulnerabilities of the things that they use every day.

One of the most publicly hyped and topical areas of technology interest of the past several years has been the rise of cryptocurrencies. The world of Bitcoin, Ethereum, Litecoin, Monero, etc. has crossed from the world of techies and geeks into mainstream media outlets and integrated into economies around the world. During its first ten years of existence, Bitcoin has had quite a journey. The initial paper released by the pseudo-anonymous Satoshi Nakamoto was released in October 2008 (Nakamoto, 2008). The first Bitcoin was mined in January of 2009. What followed saw several cycles of growth and decline, culminating in the peak of hysteria in December of 2017 that found the price of a bitcoin reach approximately $20,000 each. This was just as quickly followed by the "Crypto Winter" of 2018 that saw that price fall to below $3000 at times. Bitcoin and other cryptocurrencies have captured the imagination of millions, spawned new industries, and disrupted multiple established markets and economies worldwide. When money is involved, especially when it appears to the novice that it is money from nothing and lots of it, attention is quickly captured. Naturally, with the rise in value and understanding of the cryptocurrency world so too has come the rise in crime and security concerns around this system.

The ecosystem of cryptocurrencies provides a wide array and variety of vulnerabilities associated at various levels of the system to highlight to Cybersecurity students. Specific topics are many and can be found to fit just about every aspect of the common domains of Cybersecurity focus. Options could run from the technical aspects of software selection in choosing mining programs, securing online accounts, hardening operating systems, two-factor authentication, remote access programs, open source software, even to physical and environmental security in organizing data centers that could generate extreme amounts of heat causing damaged equipment or even fire.

This paper will describe the common cryptocurrency ecosystem from mining through currency exchanges. Following, four specific events will be highlighted that culminated in successful attacks on the cryptocurrency world. For each, an overview will be provides explaining the event and will include multiple links to news articles that provide more detailed coverage. Sample questions are also provided to help spark discussion or further research.

2. A BRIEF BACKGROUND ON CRYPTOCURRENCY

Marshal McLuhan spoke of the Global Village well before the Internet tied the world together. The Internet has grown and matured to become the universal medium that McLuhan predicted would come (McLuhan, 1962). It has broken down barriers between peoples and nations, has crossed the boundaries of politics and religions, and has become a ubiquitous presence in the lives of the vast majority of people on earth. Language barriers have become lessened, machines talk to machines, and physical distance has become almost irrelevant. Where virtual reality was once the cutting edge of technology, the blended augmented reality of today has shown how a mature internet can be utilized to coexist with our physical world to allow for a greater capacity in nearly every aspect of a daily routine.

With the rise of the commercial internet, many traditional industries have seen vast disruptions. Again, McLuhan had promises that, "The next medium, whatever it is – it may be the extension of consciousness – will include television as its content, not as its environment…A computer as a research and

communication instrument could enhance retrieval, obsolesce mass library organization, retrieve the individual's encyclopedic function and flip it into a private line to speedily tailored data of a saleable kind…(McLuhan 1962)" foretelling the subsuming of existing channels into the new medium of the Internet.

Disruptive innovations of the Internet Age have been the catalyst for rapid change in almost every industry. Newspapers and other news mediums have moved to or shifted focus to online editions. Big Data and Data Analytics have allowed competition on equal footing in various markets and industries of e-commerce and services. One of the oldest industries in the world, the financial industry, is currently experiencing what may turn out to be one of the greatest disruptions it has faced in centuries. Though the financial world has seen its fair share of modernization and evolution in the past 40 years. starting with a greater acceptance of credit cards, through ATM cards, to electronic stock trading and the ability to trade stocks as an individual – the financial industry has not seen a disruptive, decentralizing, force like that of cryptocurrencies.

Currency, both physically and intrinsically, has itself undergone change. The advent of the Euro as an idea in 1992, as an accounting currency in 1999, and finally as a physically circulating currency in 2002 was a major event in the history of world currency (Spahn, 2001). The advent of the common currency for the European zone saw the elimination of such venerable currencies as the Greek Drachma, the French Franc, and the Italian Lira amongst the 21 nationalist currencies that it replaced. Still, amongst the most traded currencies in the world: the US Dollar; the Euro; the Japanese Yen; and the English Pound (McFarlane, 2014) – all are what is considered "fiat" currencies.

Fiat money is a currency that is backed by the promise of a nation or entity that it will support the exchange of the physical representation of that money. It is not directly tied to a commodity, such as gold. The idea of the Gold Standard, that each bank note issued by a country is attached to a corresponding holding of physical gold equaling the amount of currency issued in value, has not been a reality for nearly a hundred years. The United States effectively went off the gold standard in 1933 with a permanent detachment in 1971. The Bank of England abandoned the gold standard in 1931. Still, with these changes and others, there existed a backing entity in each currency. The United States backs the Dollar, Great Britain backs the Pound Sterling, and the European Central Bank backs the Euro.

In November 2008, the idea that currency had to be backed by a country or governmental entity began to be challenged in earnest. A paper began circulating on Internet message boards titled, "Bitcoin: A Peer-to-Peer Electronic Cash System" authored by Satoshi Nakamoto (A nom de guerre with the real identity of Satoshi Nakamoto as yet unknown). The paper proposed a "system for electronic transactions without relying on trust" (Nakamoto, 2008). A peer-to-peer network was proposed that would use individual 'mining clients' to perform work that creates a virtual "coin" and verifies the transfer of ownership of these coins (Nakamoto, 2008). The 'work' involves solving encrypted hash blocks, thus the true basis for the coin lies in cryptography. This has led to the use of the term "cryptocurrency" in describing the various forms of currency that have developed utilizing this process.

To prevent inflation and the flooding of the market of coins, the work in solving the encrypted blocks becomes increasingly more difficult and metered by time. The creation, or mining process, does not require a central authority to acknowledge the existence of a coin; records exist as a shared log with all individual clients that are connected to the network. This is referred to as the "blockchain" and it exists as a shared ledger. The crossover between virtual representation and physical manifestation occurs in the exchange of the virtual coins for a currency that is physical, or "real

world". Value is negotiated through markets and currency exchanges that have sprung up with the increasing awareness and popularity of the virtual currency. These exchanges function in much the same way other commodity markets function with direct buy and sell orders exchanged between individuals. However, for much of their history and in much of the world these exchanges are non-regulated and operate outside of the traditional money markets. There is no safety net of law or government. Multiple incidents have occurred of fraud and theft that has become a major hurdle for general acceptance of cryptocurrencies to overcome. The exchange value of all cryptocurrencies has fluctuated wildly based on the smallest pieces of news or rumor. The entire "Crypto-Economy" has gone through several peaks and valleys.

3. THREE TOPICS

"...Because it's where the money is..."
"Someone once asked Slick Willie Sutton, the bank robber, why he robbed banks. Sutton looked a little surprised, as if he had been asked 'Why does a smoker light a cigarette?' 'I rob banks because that's where the money is…' he said (Yoder, 1951)."

By December 17, 2017 the value of a single Bitcoin reached $19,783.21 (Higgins, 2017).

The Cryptocurrency world was certainly where the money was.

For much of the second half of 2017 FOMO (Fear of Missing Out) ran rampant with many looking to get rich quick on the "..to the moon" rocket of rising valuation. And while many developers and implementers were making great strides in evolving a system that could truly change the way industries from the financial world, supply chain management, and e-medical records were handled – many charlatans, hucksters, and just plain old thieves gathered like moths to a flame.

Since its inception, the fundamental code and functioning of the Bitcoin system has never been directly compromised. Even if Bitcoin itself has not been "hacked", many pieces of the system surrounding the core code have been found to be exploitable. The lure of easy money emboldens black hats hackers to leave no stone unturned in looking for a way into a system. In some cases, the perpetrators were never caught and seemingly made off with a significant gain. As time has progressed, law enforcement agencies from around the globe have developed more and more sophisticated ways of tracking cryptocurrencies and have brought some thieves to justice even years after their crimes (Brandom, 2017). Unfortunately, the most affected victim of these attacks, or crimes, is the crypto community itself. These situations lead to the market suffering from price crashes as FUD (Fear, Uncertainty, and Doubt) creep into amateur and professional investors alike.

This paper will highlight several areas in which attackers have been able to take advantage of surrounding technologies or systems to their gain. In covering some of these instances in a cybersecurity classroom, a professor can more clearly show students that seemingly farfetched theoretical attacks can become real. Three categories of instances will be covered: 51% attacks, Exit Scams, and Two Factor Authentication (2FA) SIM Swapping attacks.

51% Attacks
Primary to the functioning of any cryptocurrency is the validation of transactions in the blockchain through the mining process. The system works because any set of transactions must be agreed upon as valid by the rest of the participants before it is accepted into the permanent record of the blockchain. This concept of agreeance is also utilized in signaling acceptance of hard forks and other modifications to the system. When enough participants decide on a path it reaches a consensus and is accepted.

To inject changes or to validate improper transactions (double spend, reverse transaction, etc.) no one node would be able get the transaction accepted as many other nodes would see the transaction as invalid

ISSN: 2473-3857
v5 n5110

and reject it. If, however, an organization would be able to command over 50% of the network processing capacity they could conceivably validate their own invalid transaction as they would command the majority of the network. Nodes that would see the new block as invalid and reject it would be outvoted by the majority of corrupted nodes that would validate the transaction.

Given a sufficient number of participants it becomes exponentially more difficult to effectively gain and maintain 51% of the processing (hashing) power of the network. With the Bitcoin hash rate of 73,895,420 terra hashes per second (blockchain.com) in July of 2019 it has effectively become immune to any one entity conceivably gaining control over 51% of that processing power. In May 2019 a study estimated that the cost of such an endeavor to purchase and run enough Bitcoin mining equipment would be in excess of $1.4 billion (HackerNoon, 2019). However, with the fragmentation of the Alt-Coin market, some smaller more obscure cryptocurrencies are susceptible.

Since 2017 the technology of mining equipment and ASIC (Application Specific Integrated Circuit) chips designed precisely for crypto mining has exploded in both power and availability. Many pieces of mining equipment that were profitable to run up through 2017 have become obsolete and unprofitable to run with their return when mining the most popular coins with large networks of extreme hashing power. These older pieces of mining hardware can be found on the market through auction sites and user groups very cheaply. While they might not be profitable for Bitcoin, Litecoin, or Ethereum, they may be put to use, given a cheap enough power source, for smaller community coins or Alt-Coins that have been split from their parent with limited following. Verge, Bitcoin Cash, Bitcoin Gold, and Ethereum Classic have all been hit by a 51% attack at some point.

Here are background articles detailing these attacks:

https://fortune.com/2018/05/29/bitcoin-gold-hack/

https://bravenewcoin.com/insights/etc-51-attack-what-happened-and-how-it-was-stopped

https://cointelegraph.com/news/two-miners-purportedly-execute-51-attack-on-bitcoin-cash-blockchain

https://www.coindesk.com/verges-blockchain-attacks-are-worth-a-sober-second-look

Questions:

- Detail a 51% attack. How can one be carried out?

- What are factors leading to a blockchain being vulnerable to a 51% attack?

- How can a cryptocurrency protect against or defend against a 51% attack?

The Exit Scam

Cybersecurity has always been about more than just technical issues. From origins in Information Assurance and other government and legal efforts, there is a long history of policy, procedure, and regulation topics within the Cybersecurity field.

At the ten-year-old mark, Bitcoin and the Crypto world in general, remains a highly unregulated industry. Several countries, most notably Japan, have been early leaders in developing national governance over the industry. Some countries such as Malta and Barbados have created local laws creating crypto havens to attract investments and gain status in world markets. The United States, amongst other traditional economic powers, have been very slow to create formal laws and regulations. Guidance has been issued by the IRS on how to pay taxes on crypto investments, but formal regulations are still a long way off.

Thus the many warnings and caveats that are delivered to anyone that is looking to invest personally, institutionally, or develop

business models around the crypto industry. People can, and do, lose money.

Many of the same fraud and Ponzi schemes that exist in traditional investment markets also exist in the crypto world. Initial Public Offerings (IPOs) on the stock market can be a huge payday for a startup company to bring in investment capital and prestige to their company. The process is long and highly regulated by the Securities and Exchange Commission (SEC) with penalties and possible jail time for violations. During 2018 the Crypto world had none of those safety nets or guard rails. ICOs (Initial Coin Offerings) became a fertile ground for many scams and outright fraud. According to Coinopsy, a website devoted to tracking dead cryptocurrencies, by June 2018 there were over 1000 dead crypto coin projects with 55%of those listed as failed ICOs from the 2017 bull market (Partz, 2018). Were all of those fails fraud, scams, or Ponzi schemes? Probably not, but several have now been brought into court as fraud cases by the US Department of Justice (USDoJ) and the SEC (Bryanov, 2018).

Exit Scams hold a unique place in the crowd of failed projects, criminal or not. They are unique in their ability to spark imagination and stoke fear. While there may be many variants of the exit scam, a good working definition can be found through Investopedia, "An exit scam is a fraudulent practice by unethical cryptocurrency promoters who vanish with investors' money…" (Investopedia, 2019).

The first and the most influential situation that was labeled as an exit scam was the Mt. Gox disaster. February of 2014 may seem like ancient history in the crypto world, but for those that have been involved long enough, just the mention of Mt. Gox or Mark Karpelés can send chills down a spine. "I got Gox'ed" is still slang for being swindled by an exchange that has suddenly ghosted their depositors and made off with their deposits. The rise and fall of the Mt. Gox exchange was the first real catastrophe of the cryptocurrency world. Its demise sparked the first major sell-off and price crash that for sheer percentage loss is still greater than the cryptowinter of 2018 (Febrero, 2018).

The story of Mt. Gox is long and complicated and may eventually turn out to be a simple case of an incompetent leader in over his head and unwilling to admit it. Mark Karpelés, the head of Mt. Gox, was arrested in Japan in August 2015 and charged with fraud and embezzlement. He was imprisoned until July 2016, when he was released on bail. Closing arguments in his trial were held on Dec 27, 2018. Originally facing up to five years in prison, he was eventually found guilty on lesser charges, fined $33.5 million with a 30 month suspended sentence (Palmer, 2018).

One primary point about the Mt. Gox case is the concentration of power and responsibility in the hands of one person. This is a fundamental red flag in any risk assessment or business continuity/disaster recovery plan. Yet businesses in the crypto world are still able to operate with investor money at risk without outside auditor scrutiny of business practices due to the unregulated world they operate in. While public awareness of signs of professional operation have become more common knowledge to neophyte investors, scams still happen.

On December 9th 2018 Gerald Cotton died while on a combined mission trip/honeymoon to India. Cotton had been the founder and CEO of QuadrigaCX, the largest cryptocurrency exchange based in Canada. One safety net Quadriga had instituted that had become standard at exchanges post-Gox was to have a hot wallet/cold wallet setup. This means that hot wallets attached to the front end of the website based exchange, and cold wallets to store the primary assets of the company and its investors. What was unusual is that the only person who had access to the cold wallets on an encrypted hard drive was Gerald Cotton. With his passing no one could access what was valued at over $190 million and constituted over 90% of the assets of the company and its clients.

ISSN: 2473-3857
v5 n5110

In the subsequent months, what began as a sad tragedy of the death of a charismatic leader with a heart towards charity, became labeled as possibly the largest exit scam ever. A suspicious death certificate, a recently updated will, and a court mandated audit that showed assets moved into private accounts and even used in personal trades at other exchanges painted a vastly different picture. As investigations continue through 2019, much has yet to be settled as to the ultimate fate of Gerald Cotton or QuadrigaCX.

Here are background articles detailing the QuadrigaCX situation:

https://coolwallet.io/quadriga-ceo-exit-scam-5-years-since-mt-gox-hack-have-crypto-exchanges-learned-anything/

https://economictimes.indiatimes.com/magazines/panache/a-crypto-millionaire-loose-ends-a-dead-end-a-consignment-of-teddy-bears-before-gerald-cotten-died/articleshow/68804401.cms?from=mdr

https://www.coincola.com/blog/what-happened-to-quadrigacx-how-to-avoid-it/

Questions:

- From a business continuity/disaster recovery perspective, detail steps that should be taken by any crypto exchange or ICO that could prevent a QuadrigaCX/Mt. Gox event from happening again.

- Research the current state of SEC advisories on ICOs. Are they currently regulated? To what extent?

- Are there any protections for individual investors in the crypto world? How does this differ from the FDIC system in the United States? Could something similar be developed for the Crypto world?

SIM Swapping

Strong authentication methods have been a moving target for generations of systems even before the internet. Effectively and efficiently validating the identity of an object, user or system, is always a challenge. A standard modern way of hardening authentication has been to incorporate Two Factor Authentication (2FA). This forces users to provide two forms of verification from three categories: something you know (password), something you have (a hardware device), and something you are (biometric, fingerprint, face ID, retina scan, etc.). One of the more popular combinations has been to utilize passwords combined with one-time use access codes either sent to a phone number or e-mail address, or a one-time code generated by an application such as Google Authenticator or an RSA key fob. However, the two are very different in the level of security they can ensure.

A downfall of onetime passcodes sent through SMS texting systems is that while a user may believe that they are in possession of the physical phone, that does not necessarily mean that they are in possession of the phone number. The phone number is assigned to the phone through the Subscriber Identity Module (SIM) card which has a small chip that is utilized in mobile networks to identify and authenticate subscribers. These chips can be re-programed remotely and the phone number for a subscriber attached to a new or different SIM card. This is a normal process that allows a person to purchase a new phone and to transfer their existing number to the new device. However a relatively new threat has appeared and has grown in popularity and significance in the past several years as SMS texting has become more relied upon as a second piece in the 2FA process.

SIM Swapping relies primarily on a series of identity theft, impersonation, and social engineering attacks. The threat agent begins in a traditional identity theft methodology by gathering as much information about a potential victim as possible. Open Source Intelligence gathering has made this a much easier proposition. This information is then used to execute the SIM Swap by impersonating the target with their phone

ISSN: 2473-3857
v5 n5110

carrier to convince the carrier to port the target's phone number to the attackers SIM. Once executed, all SMS messages and voice calls will then be received by the attacker. Thus, any one-time passwords or phone calls with codes needed to change authentication for login purposes to any accounts that rely on 2FA such as crypto exchange or bank accounts will be received by the attacker.

SIM Swapping began to appear in the wild around 2014, but instances of this attack greatly rose in 2017 with increased attacks on cryptocurrency holders. Two notable cases saw arrests made during the summer of 2018. In July 2018, Ricky Joseph Handschumacher of Port Richey, FL was arrested and charged with grand theft and money laundering. Investigators allege Handschumacher was part of a group of at least nine individuals scattered across multiple states who for the past two years had drained bank accounts via SIM Swapping (Krebs, August 2018).

Investigations into this group continued, and as of May 2019 nine have been formally charged in relation to their participation with "The Community" a gang that realized more than $2.4 million through stealing cryptocurrencies and extorting people for restoration of social media accounts that they had hijacked through SIM swapping (Krebs, May 2019). A separate criminal complaint was also brought against three former employees of mobile phone providers who collaborated with the gang in helping to effect the SIM swapping.

In a separate SIM Swapping case, an arrest was made in California. On July 12, 2018 police arrested a college student accused of being part of a group of criminals who hacked dozens of cellphone numbers to steal more than $5 million in cryptocurrency. Joel Ortiz, a 20-year-old from Boston, allegedly hacked around 40 victims with the help of still unnamed accomplices, according to court documents (Franceschi-Bicchierai, August 2018). The Ortiz arrest was the first against someone using the SIM Swapping attack. Investigators accuse Ortiz of being a prolific SIM hijacker who mainly targeted victims to steal their cryptocurrency but also to take over their social media accounts with the goal of selling them for Bitcoin. According to the investigators, as well as people in the SIM swapping community, Ortiz was a member of OGUSERS, a website where members trade valuable Instagram or Twitter accounts. In one of at least three attacks that happened during Consensus, a major conference of the blockchain and cryptocurrency community, Ortiz allegedly stole more than $1.5 million from a cryptocurrency entrepreneur, including nearly $1 million that he had crowdfunded in an ICO (Franceschi-Bicchierai, July 2018)

Here are background articles regarding SIM swapping:

https://www.wired.com/story/sim-swap-attack-defend-phone/

https://krebsonsecurity.com/2019/05/nine-charged-in-alleged-sim-swapping-ring/

https://securelist.com/large-scale-sim-swap-fraud/90353/

https://www.zdnet.com/article/wave-of-sim-swapping-attacks-hit-us-cryptocurrency-users/

Questions:

- What is Open Source Intelligence? How is it used? Is it legal?

- What is 2FA? Clearly define categories of "factors" that can be utilized for 2FA. Detail strengths and weaknesses of each.

- How are you securing your most valuable accounts? Do you use 2FA? What are the reset e-mail addresses associated with these accounts? How strongly secured are those accounts? Perform a risk assessment of your authentication methods…

4. Conclusion

The world of Bitcoin and Cryptocurrencies has been a fascinating and volatile mix of technology and money for the past decade. With multiple cycles of "to the moon" bubbles followed by "to zero" crashes, this technology has jumped from being just a "techie" thing to being followed by mainstream media and everyday people. With the increase in values, and the increase in general awareness, Bitcoin and the Cryptocurrency world has invited not just investors to the show, but also all the con-men, tricksters, and thieves that money attracts.

While Bitcoin itself has proven to be strong against attack, and has stood up without compromise for ten years, various components of the cryptocurrency eco-system surrounding it have proven less bullet-proof.

This paper has provided several specific cases related to Cryptocurrencies and cybersecurity that can be utilized to illustrate to students starting out in the cybersecurity world the intricacies of complex systems. Each nook and cranny must be hardened and observed, lest it become the vulnerable point that leads to compromise. From afterthought IoT devices, to assumed safe 2FA systems, thieves will find a way to get at money. It's what they do.

The stories/cases described here are only a tip of the iceberg. New attacks are being devised, new vulnerabilities are being discovered, new lines of social engineering are being developed every moment. As a domain of current events and new technologies, the world of Cryptocurrencies can and should be leveraged as a topical, popular, and multidimensional hook for professors to capture the interests of students and point to real life scenarios where the unimaginable comes to life. If the last ten years of Bitcoin are any indication, this area will remain an evergreen source of material for a long time to come.

5. REFERENCES

Assolini, F., & Tenreiro, A. (2019, April 11). Large-scale SIM swap fraud. Retrieved June 1, 2019, from https://securelist.com/large-scale-sim-swap-fraud/90353/

Barrett, B. (2018, August 17). How to Protect Yourself Against a SIM Swap Attack. Retrieved November 11, 2018, from https://www.wired.com/story/sim-swap-attack-defend-phone/

Boddy, M. (2019, May 25). Two Miners Purportedly Execute 51% Attack on Bitcoin Cash Blockchain. Retrieved June 10, 2019, from https://cointelegraph.com/news/two-miners-purportedly-execute-51-attack-on-bitcoin-cash-blockchain

Brandom, R. (2017, July 26). Bitcoin exchange chief arrested amid new questions about Mt Gox theft. Retrieved December 14, 2018, from https://www.theverge.com/2017/7/26/16035702/btce-arrest-bitcoin-alexander-vinnik-mt-gox-theft-suspect

Charles, R. X. (2019, February 07). Against Illegal Content on the Blockchain. Retrieved July 13, 2019, from https://blog.moneybutton.com/2019/01/31/against-illegal-content-on-the-blockchain/

Child abuse images hidden in crypto-currency blockchain. (2019, February 06). Retrieved July 13, 2019, from https://www.bbc.com/news/technology-47130268

Cimpanu, C. (2019, June 03). Wave of SIM swapping attacks hit US cryptocurrency users. Retrieved June 15, 2019, from https://www.zdnet.com/article/wave-of-sim-swapping-attacks-hit-us-cryptocurrency-users/

Constantin, L. (2014, June 17). Hacked Synology NAS systems used in high-profit cryptocurrency mining operation. Retrieved December 22, 2018, from https://www.pcworld.idg.com.au/article/547666/hacked_synology_nas_systems_us

ed_high-profit_cryptocurrency_mining_operation/

Cuen, L. (2018, March 29). Child Porn On Bitcoin? Why This Doesn't Mean What You Might Think. Retrieved July 14, 2019, from https://www.coindesk.com/child-porn-bitcoin-blockchain-what-it-means

Ehrenkranz, M. (2019, February 06). Someone Uploaded Child Pornography to a Blockchain Ledger, and It's Almost Impossible to Delete. Retrieved February 10, 2019, from https://gizmodo.com/someone-uploaded-child-pornography-to-a-blockchain-ledg-1832398480

Exec. Order No. 13636, 3 C.F.R. 22391-22397 (2013).

Febrero, P. (2018, November 25). Bitcoin Op-Ed: Welcome Darkness, My Old Friend. Retrieved December 14, 2018, from https://www.ccn.com/bitcoin-op-ed-welcome-darkness-my-old-friend/

Franceschi-Bicchierai, L. (2018, July 30). 'TELL YOUR DAD TO GIVE US BITCOIN:' How a Hacker Allegedly Stole Millions by Hijacking Phone Numbers. Retrieved December 20, 2018, from https://motherboard.vice.com/en_us/article/a3q7mz/hacker-allegedly-stole-millions-bitcoin-sim-swapping

Franceschi-Bicchierai, L. (2018, August 22). Alleged 19-Year-Old SIM Swapper Used Stolen Bitcoin to Buy Luxury Cars. Retrieved from https://motherboard.vice.com/en_us/article/wjka95/sim-swapper-arrest-bitcoin-luxury-cars

Hash Rate. (n.d.). Retrieved July 15, 2019, from https://www.blockchain.com/en/charts/hash-rate

Hertig, A. (2019, May 25). Bitcoin Cash Miners Undo Attacker's Transactions With '51% Attack'. Retrieved June 1, 2019, from https://www.coindesk.com/bitcoin-cash-miners-undo-attackers-transactions-with-51-attack

Hertig, A. (2018, June 09). Blockchain's Once-Feared 51% Attack Is Now Becoming Regular. Retrieved December 20, 2018, from https://www.coindesk.com/blockchains-feared-51-attack-now-becoming-regular

Hertig, A., & Kim, C. (2018, November 09). Bitcoin Cash Declares War: Why Coming Hard Fork Could Mean Another Split. Retrieved December 20, 2018, from https://www.coindesk.com/bitcoin-cash-declares-war-why-this-could-mean-another-split

Higgins, S. (2017, December 30). From $900 to $20,000: Bitcoin's Historic 2017 Price Run Revisited. Retrieved December 12, 2018, from https://www.coindesk.com/900-20000-bitcoins-historic-2017-price-run-revisited

Jenkins, N. (2018, September 19). They're Drinking Your Milkshake: CTA's Joint Analysis on Illicit Cryptocurrency Mining. Retrieved December 29, 2017, from https://www.cyberthreatalliance.org/joint-analysis-on-illicit-cryptocurrency-mining/

JimiS. (2019, May 27). Blockchain: How a 51% attack works (double spend attack). Retrieved July 10, 2019, from https://medium.com/coinmonks/what-is-a-51-attack-or-double-spend-attack-aa108db63474

Krebs, B. (2017, August 7). Florida Man Arrested in SIM Swap Conspiracy. Retrieved December 13, 2018, from https://krebsonsecurity.com/2018/08/florida-man-arrested-in-sim-swap-conspiracy/

Krebs, B. (2018, March 30). Coinhive Exposé Prompts Cancer Research Fundraiser. Retrieved December 12, 2018, from https://krebsonsecurity.com/2018/03/

Krebs, B. (2019, May 10). Nine Charged in Alleged SIM Swapping Ring. Retrieved from https://krebsonsecurity.com/2019/05/nine-charged-in-alleged-sim-swapping-ring/

Leilacher, A. (2019, January 14). ETC 51 % attack – what happened and how it was stopped. Retrieved June 28, 2019, from

https://bravenewcoin.com/insights/etc-51-attack-what-happened-and-how-it-was-stopped

Li, K. (2019, January 30). The Blockchain Scalability Problem & the Race for Visa-Like Transaction Speed. Retrieved June 12, 2019, from https://medium.com/@wandererli/the-blockchain-scalability-problem-the-race-for-visa-like-transaction-speed-5cce48f9d44

Litke, P. (n.d.). Hacker Hijacks Synology NAS Boxes for Dogecoin Mining Operation. Retrieved December 22, 2018, from https://www.secureworks.com/blog/hacker-hijacks-synology-nas-boxes-for-dogecoin-mining-operation-reaping-half-million-dollars-in-two-months

Madore, P. H. (2018, November 26). Numerous Bitcoin Wallets May Have Been Compromised by Rogue Dev. Retrieved December 20, 2018, from https://www.ccn.com/breaking-numerous-bitcoin-wallets-may-have-been-compromised-by-rogue-developer/

McFarlane, G. (2014, June 26). The 6 Most-Traded Currencies and Why They're So Popular. *Investopedia*. Retrieved Dec 12, 2018, from http://www.investopedia.com/articles/general/022814/rewrite-6-mosttraded-currencies-and-why-theyre-so-popular.asp

McLuhan, M. (1962). *The Gutenberg galaxy: the making of typographic man*. Toronto: University of Toronto Press, Scholarly Publishing Division.

Memoria, F. (2018, November 15). Bitcoin Cash SV Supporter CoinGeek Hit With DDoS Attack Ahead of Hard Fork. Retrieved January 1, 2018, from https://www.cryptoglobe.com/latest/2018/11/bitcoin-cash-sv-supporter-coingeek-hit-with-ddos-attack-ahead-of-hard-fork/

Muslimi, M. (2019, March 21). Cryptojacking in 2019 is not dead - it's evolving! Retrieved June 10, 2019, from https://hackernoon.com/cryptojacking-in-2019-is-not-dead-its-evolving-984b97346d16

Nadeau, M. (2018, December 13). What is cryptojacking? How to prevent, detect, and recover from it. Retrieved June 10, 2019, from https://www.csoonline.com/article/3253572/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html

Nakamoto, S. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Web: www.bitcoin.org.

Narayanan, A., Werbach, K., & Grimmelman, J. (2018, March 29). Why Porn on the Blockchain Won't Doom Bitcoin. Retrieved July 10, 2019, from https://www.wired.com/story/why-porn-on-the-blockchain-wont-doom-bitcoin/

Newman, L. H. (2018, December 22). The Year Cryptojacking Ate the Web. Retrieved March 29, 2019, from https://www.wired.com/story/cryptojacking-took-over-internet/

Nguyen, C. (2018, December 04). Cryptojacking Malware Now Infects More Than 415,000 Routers Globally. Retrieved December 29, 2018, from https://www.digitaltrends.com/computing/415000-routers-globally-infected-with-cryptojacking-malware/

Norry, A. (2018, November 19). The History of the Mt Gox Hack: Bitcoin's Biggest Heist. Retrieved December 28, 2018, from https://blockonomi.com/mt-gox-hack/

Ou, M. (2019, February 07). Quadriga CEO "Exit Scam": 5 Years After Mt. Gox, Have Crypto Exchanges Learned Anything? Retrieved February 8, 2019, from https://coolwallet.io/quadriga-ceo-exit-scam-5-years-since-mt-gox-hack-have-crypto-exchanges-learned-anything/

Palmer, D. (2018, December 27). Mt Gox CEO Mark Karpeles Claims Innocence as Trial Nears End. Retrieved December 29, 2018, from https://www.coindesk.com/former-mt-gox-ceo-mark-karpeles-claims-innocence-as-trial-nears-end

Roberts, J. J. (2018, May 29). Bitcoin Spinoff Hacked in Rare '51% Attack'. Retrieved June 10, 2019, from https://fortune.com/2018/05/29/bitcoin-gold-hack/

Sedgwick, K. (2018, March 21). No, There Isn't Child Porn on the Bitcoin Blockchain. Retrieved June 13, 2019, from https://news.bitcoin.com/no-isnt-child-porn-bitcoin-blockchain/

Shaikh, R. (2017, October 13). The Pirate Bay Is Cryptojacking Its Visitors' Computers to Mine for Monero. Retrieved December 22, 2018, from https://wccftech.com/the-pirate-bay-cryptojacking-mine-monero/

Smith, K. (2018, October 14). Attacker pledges to make 51 percent attacks a spectator sport. Retrieved June 15, 2019, from https://bravenewcoin.com/insights/attacker-pledges-to-make-51-percent-attacks-a-spectator-sport

Spahn, H. (2001). *From gold to euro: on monetary theory and the history of currency systems*. Berlin: Springer.

Sparling, A. (2018, November 20). Issue #116 · dominictarr/event-stream. Retrieved December 19, 2018, from https://github.com/dominictarr/event-stream/issues/116#issue-382854428

Stubbs, J. (2017, July 27). U.S. indicts suspected Russian 'mastermind' of $4 billion bitcoin... Retrieved December 29, 2018, from https://www.reuters.com/article/us-greece-russia-arrest/u-s-indicts-suspected-russian-mastermind-of-4-billion-bitcoin-laundering-scheme-idUSKBN1AB1OP

Viewnodes. (2019, May 6). The history of 51% attacks and the implications for Bitcoin. Retrieved from https://hackernoon.com/the-history-of-51-attacks-and-the-implications-for-bitcoin-ec1aa0f20b94

What Happened to QuadrigaCX $190 Million Exit Scam & How to Avoid It. (2019, March 07). Retrieved July 10, 2019, from https://www.coincola.com/blog/what-happened-to-quadrigacx-how-to-avoid-it/

Wilhelm, A. (2014, July 16). Popular Bitcoin Mining Pool Promises To Restrict Its Compute Power To Prevent Feared '51%' Fiasco. Retrieved December 22, 2018, from https://techcrunch.com/2014/07/16/popular-bitcoin-mining-pool-promises-to-restrict-its-compute-power-to-prevent-feared-51-fiasco/

Wilmoth, J. (2018, June 04). ZenCash Latest Altcoin to Suffer 51 Percent Attack. Retrieved December 29, 2018, from https://www.ccn.com/zencash-latest-altcoin-to-suffer-51-percent-attack/

Yoder, R. M. (1951, January 20). Someday They'll Get Slick Willie Sutton. *The Saturday Evening Post*, *223*(30).

Yong, J. (2019, February 22). Exit Scam or Mismanagement? Coinbase Digs Into QuadrigaCX's '$150 Million Loss'. Retrieved February 22, 2019, from https://www.ccn.com/exit-scam-coinbase-on-quadrigacxs-loss-of-150-million/

Young, M. (2018, November 15). BCH Fight: Bitcoin Cash Bashing Heats Up, Rivals Duke It Out Ahead of Hard Fork. Retrieved December 14, 2018, from https://www.newsbtc.com/2018/11/14/forking-around-bitcoin-cash-bashing-heats-up-as-rivals-duke-it-out/

Zmudzinski, A. (2018, December 15). Cryptojacking Overtakes Ransomware as Top Malware in Some Countries. Retrieved December 20, 2018, from https://cointelegraph.com/news/cryptojacking-overtakes-ransomware-as-top-malware-in-some-countries

ISSN: 2473-3857
v5 n5110

Appendix A

Cryptojacking

If 2017 was the year of Ransomware, 2018 has seen Cryptojacking take over as the most prevalent form of Malware attack for general consumers with a reported increase of 459% by the Cyber Threat Alliance (Jenkins, 2018). Cryptojacking is the unauthorized use of another's hardware to mine cryptocurrency. This attack first appeared around October of 2017 with The Pirate Bay often credited as the originator of the idea (Shaikh, 2017). In most cases, malicious code is injected through an ad which then utilizes a host's CPU for mining. Monero has been the primary target for this mining as it is a coin that has been very protective of continuing to keep its mining process within reach of CPU mining and blocking attempts at chip manufactures in producing ASIC (Application Specific Integrated Circuit) miners. Monero also claims to be a more anonymous system than Bitcoin, washing transactions through multiple cycles leaving them very hard to trace. Coinhive has become the focus of the rise in Cryptojacking. By March of 2018 the Coinhive code for Monero mining through websites was the top malware threat tracked by multiple security firms (Krebs, March 2018).

Some legitimate news content sites even experimented with the business model of asking consumers if they would rather pay a subscription fee or allow the site to use their CPU for mining in exchange for access to content. With the continued drop in value of Monero, and the increased amount of antivirus and protection programs flagging these programs, many have backed away from this model.

Before cryptojacking was given its label with the latest outbreak of browser-based malware, the original case of utilizing other's resources for mining occurred in 2014. In a precursor to later compromises of Internet of Things (IoT) devices, an estimated 1 million Synology NAS (Network Attached Storage) devices were compromised to mine Dogecoin. As headless devices, this attack was very hard to recognize or spot. It was estimated at the time that the attacker managed this botnet to mine over 500 million Doge, worth over $620,500 at that time (Constantin, 2014).

Currently, as more AV and other malware detection programs are stopping cryptojacking at the operating system level, this approach of infecting lower powered IoT type devices has spread again. According to one recent study, upwards of 415,000 consumer grad routers have been infecting with cryptojacking malware (Nguyen, 2018).

Here are background articles regarding Cryptojacking:

https://www.engadget.com/2017/09/16/pirate-bay-hijacks-cpus-for-digital-currency-mining/

https://www.csoonline.com/article/3253572/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html

https://www.wired.com/story/cryptojacking-took-over-internet/
https://hackernoon.com/cryptojacking-in-2019-is-not-dead-its-evolving-984b97346d16

Questions:
- What is malvertising? Explain it's origins and evolution. Is this still a threat? Why?

- What are the economics of browser mining. What is a possible ROI?

- There had been an initial attempt by a handful of pay-walled sites to allow access to subscriber sections if readers allowed browser mining. Debate this idea. Could this be a legitimate revenue stream for content providers?

APPENDIX B

Illegal content on the Blockchain

In February of 2019 headlines appeared with very ominous headlines for a crypto community that was already suffering through the extended long "crypto winter" of 2018. "Child abuse images hidden in crypto-currency blockchain" (BBC, 2019) was just one example. The ramifications of this, if true, were far reaching and possibly disastrous for an already hurting crypto world.

All was not exactly as it seemed from the inflammatory headlines, though. As explanations and details came to light, it was not exactly child pornography that existed on the blockchain, and in the most recent case, it was not even the bitcoin that had been possibly compromised.

The early 2019 report detailed a possible compromise of the Bitcoin Satoshi Vision (BSV) ledger. BSV is an Alt-Coin that that is a controversial fork of a fork of Bitcoin that came into existence only on November 15, 2018 and was a fork out of Bitcoin Cash and was intended by I's founder and community to most closely adhere to the true vision of Satoshi Nakamoto and the foundation of the original Bitcoin White Paper.

One of the most important issues surrounding Bitcoin is the problem of scaling. The capacity of the Bitcoin network is essentially small compared to that of any major credit card system. With a limit of one block committed to the blockchain every ten minutes, and a limited size of 1MB per block, the transaction processing capacity maximum as estimated using an average or median transaction size is between 3.3 and 7 transactions per second. This compares to a reported 1,700 transaction per second on the VISA credit card network (Li, 2019). Many solutions have been proposed to expand the capacity of the bitcoin network, with many creating very contentious debates within he community. Some have gained enough support to drive their supporters to create hard forks off of the bitcoin blockchain to implement these changes into new alt-coins. Many of the proposed ideas for increase capacity involve an increase in block size.

One aspect of an increase in block size is more room within a transaction line item in the leger to include unstructured content. In January of 2019 a Bitcoin SV developer announced that he and other miners had increased data limits on transactions to 100KB, meaning that individuals can now store webpages, images, and video in just one transaction (Ehrenkranz, 2019).

According to payment service MoneyButton, on January 30, 2019 someone utilized their app to create a transaction that contained illegal content. They shared information about the transaction and their response on the company's public blog:

> Yesterday, an anonymous user posted illegal content to the blockchain using Money Button. Money Button does not provide any mechanism to interpret or display this content, but BitcoinFiles.org does. BitcoinFiles.org received a notice from their local authorities about the nature of the illegal content viewable on their website. BitcoinFiles.org removed the content from their website and then contacted us suspecting that Money Button may have been the tool the criminals used to write this content to the blockchain. We have confirmed that was the case and we have banned the user responsible for creating those transactions.
>
> We believe it is important to be proactive about moderating content. Now that Bitcoin SV has the ability to write large amounts of data to the blockchain, it is likely that criminals will continue to attempt to abuse this technology for illegal purposes. We have updated our Terms of Service to explicitly clarify that Money Button cannot be used to write illegal content to the blockchain, and users who attempt to do so will be banned and reported to the authorities.
>
> Furthermore, we are collaborating with other businesses to create protocols and tooling for sharing blacklisted transactions and addresses. BitcoinFiles.org and others are helping to create protocols we can use, including the possibility of writing this information to the blockchain in authenticated way. If illegal content continues to be an issue, we can build moderation tools into the blockchain. Businesses and users will be able opt-in to blacklists from trusted businesses and authorities. (Charles, 2019)

ISSN: 2473-3857
v5 n5110

Many of the stories covering this event turned to extreme consequences for the crypto world as a result. From the speculation, two very serious questions for consideration emerged – If everyone that ran a full node wallet by nature holds a full copy of the blockchain, does this mean that by extension would they also be in possession of illegal materials? And, if one of the primary values of the blockchain is irreversible transactions, meaning once something is written to the blockchain it can never be erased, does that mean illegal content written to the blockchain can never be removed?

Legally, some answers do exist. Laws related to possession of illegal content do change and are inconsistent across the globe. Especially in light of the intent of the person in possession, and the state in which the illegal content exists. As such, the digitized and encrypted links within a blockchain is not directly displayable and there are many and complex steps someone would have to go through to produce viewable images from anything that would could be displayed. Thus intent would be clearly identifiable. This interpretation of legality is not universal, however, and just focused on United States laws and precedent.

While this issue is still waiting for a full test in legal circles across the globe, the crypto community has marched on seemingly oblivious to a possible self-destructing nuclear time bomb within it…

Here are background articles regarding illegal content on the blockchain:
https://www.bbc.com/news/technology-47130268?ocid=socialflow_twitter

https://gizmodo.com/someone-uploaded-child-pornography-to-a-blockchain-ledg-1832398480

https://fc18.ifca.ai/preproceedings/6.pdf
https://www.wired.com/story/why-porn-on-the-blockchain-wont-doom-bitcoin/

Questions:
- Is this an existential crisis facing any blockchain?

- Research legalities associated with this topic. What are relative laws in the United States? European Union? Japan? South Korea? Others?

- Even if you would not be criminally liable, how would you feel about running a local wallet that held a full copy of a blockchain that may contain illegal materials?