Why is Bitcoin used in cybercrime money laundering and ransom payments?

Brandon Z. Pearson

School of Cybersecurity, Old Dominion University

IDS 300W: Interdisciplinary Theory & Concepts

Dr. Kat LaFever

December 3, 2022

Introduction

This paper addresses the rising use of cryptocurrency and the potential it has to be used for cybercrimes. Focusing on how it can be used for money laundering and the possible way it can be recovered. Why is Bitcoin used in cybercrime money laundering and ransom payments? This paper will employ the use of three separate disciplines to address the research question. The disciplines that will be viewed are economics, political science, and computer science. Each discipline is being used to dissect the question to come to a comprehensive understanding among the three disciplines. The economics discipline is used to understand how Bitcoin impacts the market. It is used to determine how wide of a range of incidents involving ransom have impacted the market. Economics allows for the ability to see what economic factors are being impacted due to the money laundering of Bitcoin. The discipline explores concepts and ideas that further why someone commits crimes. Political science is used to understand what laws are being impeded on to commit the act of money laundering. Political science is also used to see the relationship between the government and an individual. Lastly, the discipline of computer science is used to understand the fundamentals of Bitcoin and how money laundering is committed on a virtual landscape. Computer science is a key discipline to use to understand the technological side of this paper. An interdisciplinary approach helps accomplish many outcomes when it comes to writing. Interdisciplinarity allows for a more integrated understanding when it comes to analyzing multiple perspectives on a topic. Incorporating this type of research in this paper helped me understand how disciplines are similar and different in many ways. This allowed me to know what to research and how to analyze the research correctly. Determining how to gather the concepts, methods, phenomena, epistemology, and assumptions from each discipline. Drastically improving the takeaways from each source due to understanding the views

of each discipline. The justification for this paper is due to it relates to my major as a cybersecurity major. Researching this topic furthered my experience and understanding of different cyber crimes. Teaching me about how technology is being used and exploited in today's world. This question deserves to be looked into further because of the importance of limiting the ability of cyber criminals can get away with cybercrimes. Creating a better understanding of how money laundering works within cryptocurrencies attempts to do so.

Key Terms

The key terms that are discussed in this paper are money laundering, blockchain, bitcoin, ransom, and cybercrime. Each of the terms is used frequently in the paper and is foundational to understanding the premise of the paper. According to Cornell University, *money laundering* "refers to a financial transaction scheme that aims to conceal the identity, source, and destination of illicitly-obtained money" (University C.). Within money laundering the term *dirty money* is used to signify money that is illegally obtained. Money laundering is an extensive process to make dirty money into clean money. *Clean money* refers to money that would pass as if it was obtained legally. According to the United States Government Accountability Office, *blockchain technology "*combines several technologies to provide a trusted, tamper-resistant record of transactions by multiple parties without a central authority such as a bank. Blockchain can be used for a variety of financial and non-financial applications, including cryptocurrency, supply chain management, and legal records" (2022). *Bitcoin* is a "convertible virtual currency. Virtual currency is a digital representation of value that functions as a medium of exchange, a unit of account, and/or a store of value." (U.S. Commodity Futures Trading Commission). *Ransom* refers to a request of payment or action typically by a criminal for the release of information or

items. *Cybercrime* refers to any criminal acts that take place in cyberspace. This involves the use of a computer or access to a network.

Economics Discipline Contribution

Over the years with the rapid development of technology, many new crimes have come about. The rapid and ever-changing landscape of technology creates the problem of attempting to maintain its security. Technology can be used to enable malicious acts for individuals who choose to commit such acts. A large reason someone may commit cybercrimes is in an attempt to gain financial benefit. In many cases, bitcoin is compared to gold. This is due to the limited quantity of bitcoin that can be mined (Yan, et al, p.1). In recent years bitcoin has launched in price. Not only does the rise of bitcoin in itself bring many eyes towards it but its capabilities do as well. Individuals with malicious intent saw the potential that bitcoin could be used for money laundering. According to the United States, Treasury Department in 2020 self-reported losses exceeded 4.1 billion when it came to cyber crimes (National, p.17). These losses have a lasting effect on the economic market. Leaving individuals with less money to spend in the free market due to being a victim of cyber crimes. One such cybercrime is a ransom attack, cyber criminals request bitcoin for payment. In turn, promoting the use of Bitcoin and making the Bitcoin currency appear to be more in demand. Ultimately, the money that is taken from the ransom attacks has to be laundered in order to clean the money.

Political Science Contribuiton

When it comes to money laundering there are many laws and policies that have been set in place to prevent it. Anti-Money Laundering or AML is the proper set of rules that are supposed to be followed to help deter money laundering. The issue comes with the development of cryptocurrencies. Cryptocurrencies such as Bitcoin offer a way for an individual to be

anonymous within a transaction. This essentially makes it impossible to track down the individual. Therefore, allowing the individual to bypass many of the AML policies. “Moreover, the aforementioned characteristics of cryptocurrency are pushing lawmakers all over the world to unify the legislative system regarding utilizing cryptocurrency as a means of payment.” (Dyntu, V., & Dykyi, O. p.79). Employing the use of a cost-benefit analysis, the government would see the benefit of doing something about the crypto market. Cracking down on the crypto market or developing a way to determine when money is being laundered through Bitcoin. This would, in turn, reduce the number of ransom attacks that take place because attackers would have a harder time cleaning the money through Bitcoin. The largest ransom attack that was paid was the United States Colonial Pipeline incident being known for having paid $4.4 million in ransom (Connolly, A. Y., & Borrion, H. p.1). The U.S. government does not want to be a part of another incident like this one. Not only due to the negative attention it brings to the U.S. but the effects it has on the economy.

Computer Science Contribution

The reason cryptocurrencies such as bitcoin attract criminals is due to many reasons. One of the most appealing factors about Bitcoin is its ability to provide some sort of anonymity. This is due to the blockchain technology that Bitcoin operates on. The blockchain creates a ledger of transactions that take place between exchanges of Bitcoin. It keeps all the transactions that take place in chronological order. It keeps the Bitcoin address of the user showing from what address the transaction originated to what address received it. This allows for monitoring of the integrity of the blockchain. If a previous block in the chain fails to match with the current it shows that it has been tampered with. Now for a criminal having all the transactions that take place tracked would be a negative. This is why when it comes to money laundering criminals have to go

through extraneous processes to clean the money. This is done by displacing Bitcoin across multiple transactions to broaden where the original money came from. This further complicated the ability to accurately track it. Furthermore, the criminal can transfer the money out of Bitcoin into other cryptocurrencies or more private coins. When it comes to being able to recover ransom the blockchain presents the means to do so. Due to the transaction that takes place already being ledged down in the blockchain, it allows the government to attempt to follow where it goes. This by no means is an easy task to conduct but it can be done to recover some of the ransom that has been sent. One proposed way to initiate an investigation is "To investigate the ransoms extorted by a ransomware, we first identify the Bitcoin addresses linked to the ransomware. Then, we obtain the transaction history of these addresses. Finally, we distinguish the transactions associated with the ransom payments." (Conti., et al, ch. 4). Attempting to conduct this process could lead to more ransoms being recovered.

Common Ground

There are three significant findings disclosed by the interdisciplinary research. First, the discipline of economics and political science both believe that individuals' place in society dictates their involvement in particular hobbies. People's social status or rank is a factor in the choices that they potentially make. Secondly, modernist economists and modernist political scientists are under the same assumption that people act in their own self-interest (Repko, A. F. & Szostak, R. p.55). Relating back to why individuals may commit crimes. The third finding is between economics and computer science. The two disciplines both have a similar belief on how economic systems function. Both disciplines employ the use of Game Theory to help assist in understanding how things interact. Without using interdisciplinary research these findings may

have not been disclosed. Doing interdisciplinary research allowed for a more comprehensive understanding of each discipline to determine where the disciplines overlapped.

Identifying Conflicts

The conflict that persists between the three disciplines is a major ethical one. Computer science believes that Bitcoin was created to be a decentralized currency. Established to be separate and not burdened by any one government. This creates a concern if it's ethical to monitor individuals and what they do with Bitcoin. Whereas economists and political science would rather be able to intervene or have some presence. All the disciplines want to come to a solution for the issue of ransom and money laundering. The difference is how it could be done ethically. “We must consider the impact on victims before taking down ransomware infrastructure.” (Huang et al., 2018).

Constructing a More Comprehensive Understanding or Theory

In order to create a more comprehensive understanding of how Bitcoin is used to launder money requires integrating concepts, theories, and assumptions from each of the three disciplines. All of the disciplines in this paper utilize a form of Game theory that is slightly modified for each individual discipline. Each discipline has its assumptions about life and how reality is perceived. Game theory comes into play to further support ways to analyze and come to an understanding of why people do what they do. Integrating each discipline's version of Game theory into one would allow for a more efficient way to address the issue. This would create a common understanding among the disciplines. This theory would be used to analyze how individuals decide what actions to take when in a certain situation. Secondly, it would be used to determine what actions would strategically and statistically make sense to make. Establishing a uniform approach when it comes to analyzing the next step a criminal might take based on what

action law enforcement had previously taken. This creates a game of trying to stay multiple steps ahead of criminals by attempting to determine what actions a criminal may take based on the actions of law enforcement.

Reflecting On, Testing, and Communicating the Understanding or Theory

To further the understanding of this theory incorporating additional disciplines could address more aspects of the issue. Employing the use of the sociology discipline could address how society plays a part in the creation of crimes. Possibly looking into how the rapid development of technology has impacted society. Looking into how the social science principle of relativism could explain why criminals exist in society. Overall, this would allow for a deeper look into the issue of how society plays a part in the creation of someone who commits crimes.

Conclusion

When it comes to addressing the vast amount of cybercrimes there are many different approaches that can be taken. Making use of an interdisciplinary approach is an effective way to integrate multiple perspectives to be able to connect to a wider audience. Exploring the topic of Bitcoin and its use in cyber money laundering has drastic impacts on various aspects of society. It is clear that the use of Bitcoin provides criminals with a way to launder money in today's society. It is also clear why Bitcoin is the chosen cryptocurrency for ransom payments. The use of Bitcoin provides a level of anonymity and the ability to work around laws. The relative newness of cryptocurrencies has allowed criminals to exploit the lack of government understanding and supervision in their favor. With this, all being said something should be done to address the ability criminals have to launder money via Bitcoin. Cracking down on these criminals will lead to positive effects on the economy as well as prevent potential victims from ransom attacks. This can be done by incorporating multiple disciplines and fields of study

together to create a better understanding of how to address these crimes. One such solution would be to increase the laws around cryptocurrency. Making it easier for the government or law enforcement to be able to monitor the market. Another route that can be taken is attempting to understand how a cybercriminal thinks in order to prevent crimes. Overall, putting more resources towards understanding this issue will protect many individuals, as well as the government from the loss of significant amounts of money.

References:

Blockchain. NIST. (2022, January 4). Retrieved November 17, 2022, from https://www.nist.gov/blockchain

Connolly, A. Y., & Borrion, H. (2022). Reducing Ransomware Crime: Analysis of Victims' Payment Decisions. Computers & Security, 119, 1. https://doi.org/10.1016/j.cose.2022.102760

Conti, M., Gangwal, A., & Ruj, S. (2018). On the economic significance of ransomware campaigns: A Bitcoin transactions perspective. Computers & Security, 79, 162. http://proxy.lib.odu.edu/login?url=https://www.proquest.com/scholarly-journals/on-economic-significance-ransomware-campaigns/docview/2133398730/se-2

Dyntu, V., & Dykyi, O. (2018). CRYPTOCURRENCY IN THE SYSTEM OF MONEY LAUNDERING. *Baltic Journal of Economic Studies*, *4*(5), 75-81. https://doi.org/10.30525/2256-0742/2018-4-5-75-81

D.Y. Huang, D. McCoy, M.M. Aliapoulios, V.G. Li, L. Invernizzi, E. Bursztein, K. McRoberts, J. Levin, K. Levchenko, A.C. Snoeren Tracking Ransomware End-to-end 39th IEEE S&P (2018), pp. 1-14 Retrieved November 19, 2022, from https://ieeexplore.ieee.org/abstract/document/8418627

National Money Laundering Risk Assessment - home.treasury.gov. (n.d.). Retrieved November 19, 2022, from https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment.pdf?5c22b0df_page=1

Repko, A. F. & Szostak, R. (2021). Interdisciplinary research: Process and theory (4th ed.). SAGE Publications, Inc.

U.S. Commodity Futures Trading Commission | CFTC. (n.d.). Bitcoin Basics. Retrieved November 18, 2022, from https://cftc.gov/sites/default/files/2019-12/oceo_bitcoinbasics0218.pdf

U.S. Government Accountability Office (U.S. Gao). (2022, March). Retrieved November 18, 2022, from https://www.gao.gov/assets/gao-22-104625.pdf

University , C. (n.d.). Money laundering. Legal Information Institute. Retrieved November 17, 2022, from https://www.law.cornell.edu/wex/money_laundering

Yan, Y., Lei, Y., & Wang, Y. (2022). Bitcoin as a Safe-Haven Asset and a Medium of Exchange. Axioms (2075-1680), 11(8), N.PAG. https://doi-org.proxy.lib.odu.edu/10.3390/axioms11080415