How does cryptocurrency lead to crime?

Abstract:

Recently, the high-yield indices of cryptocurrencies have drawn a lot of attention from the public for investments. However, it also attracts criminals, and Gertrude (2020) claims that the losses from the cryptocurrency crimes in 2020 are about $1.9 billion. This literature review analyzes how cryptocurrency leads to crime from introducing the “useful” characteristics and imperfect regulations. Then the review discusses several specific kinds of crimes via cryptocurrency.

1. Introduction

Investing in cryptocurrency has become one of the most profitable approaches to investments since 2020. For example, according to Huobi Global, one of the famous stages to trade cryptocurrencies, the average weekly price of one Bitcoin on March 21st, 2020, was $6715.08. Its weekly price on March 13th, 2021, is $60032.56. Suppose people buy one Bitcoin in March 2020. They, in March 2021, would obtain the revenue increased as high as nine times the original value. Such profit also happened on other cryptocurrencies, like Ethereum, YFI. Therefore, it has dramatically drawn people’s attention.

1.1 Background of Cryptocurrency

According to *Is Cryptocurrency Money?: Three Empirical Studies Analyzing Medium of Exchange, Store of Value and Unit of Account*, Mattke et al. describe a cryptocurrency as “a peer to peer application that stores its transactions on a public blockchain and uses a consensus mechanism to validate and process transactions” (Section 2.1, p. 27). While Mattke et al. described a public blockchain as a “distributed ledger,” people record the transactions in blocks and ensure that each trade has a unique number referring to itself. People could access it without any permission since it is public. And the blocks are claimed to be “cryptographically linked in a temporal order so that a block always has only one predecessor”(Mattke et al., 2020). Cryptocurrencies do not utilize an agent to help check the transactions’ validations since they are built on the consensus mechanism, which means that all the holders or lovers have no disagreements with each transaction.

Some of the famous cryptocurrencies are Bitcoin, Ethereum, XRP, Polkadot. Among those, Bitcoin is the most famous and valuable cryptocurrency. According to CoinMarketCap, the total market value of a Bitcoin's circulating supply on March 23rd, 2021, was about 1.04 trillion dollars. People could obtain cryptocurrencies by either trading or using mining applications. Based on different cryptocurrencies, the mining applications always function with different algorithms to solve complicated math problems. Some mining applications may be various, like the one for Filcoin, which acts via storing a plethora of files rather than solving problems.

1.2 Unknown Problem and Purpose

Nevertheless, cryptocurrencies not only draw attention from people for the potential of investing, but cryptocurrencies also attract criminals. A series of crimes via cryptocurrencies are reported in the news. For example, the U.S. Department of Justice published a piece of information that *South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet*

Child Pornography Website, Which was Funded by Bitcoin on October 16th, 2019. Hence, here comes the question, "how does cryptocurrency lead to crime."

This review paper refers to resources from various disciplines, including law reviews, cybersecurity experts, computer science, conferences, and academic perspectives. The purpose of this paper is to find out the reasons that how cryptocurrency leads to crime and narrate several kinds of crimes via cryptocurrency.

2. Natures of Cryptocurrency

There must be reasons why criminals like to utilize cryptocurrency to address their illicit money rather than any other approach. Certain reasons must correlate with the unique advantages that cryptocurrencies could bring. In this review paper, the two critical advantages for criminals are the cryptocurrencies' function as money and anonymity.

2.1 Function as Money

The first advantage of cryptocurrencies is their function as money. In Is Cryptocurrency Money, Mattke et al. (2020) compare currency like the dollar to cryptocurrency and illustrate the three factors to determine whether something can function like money.

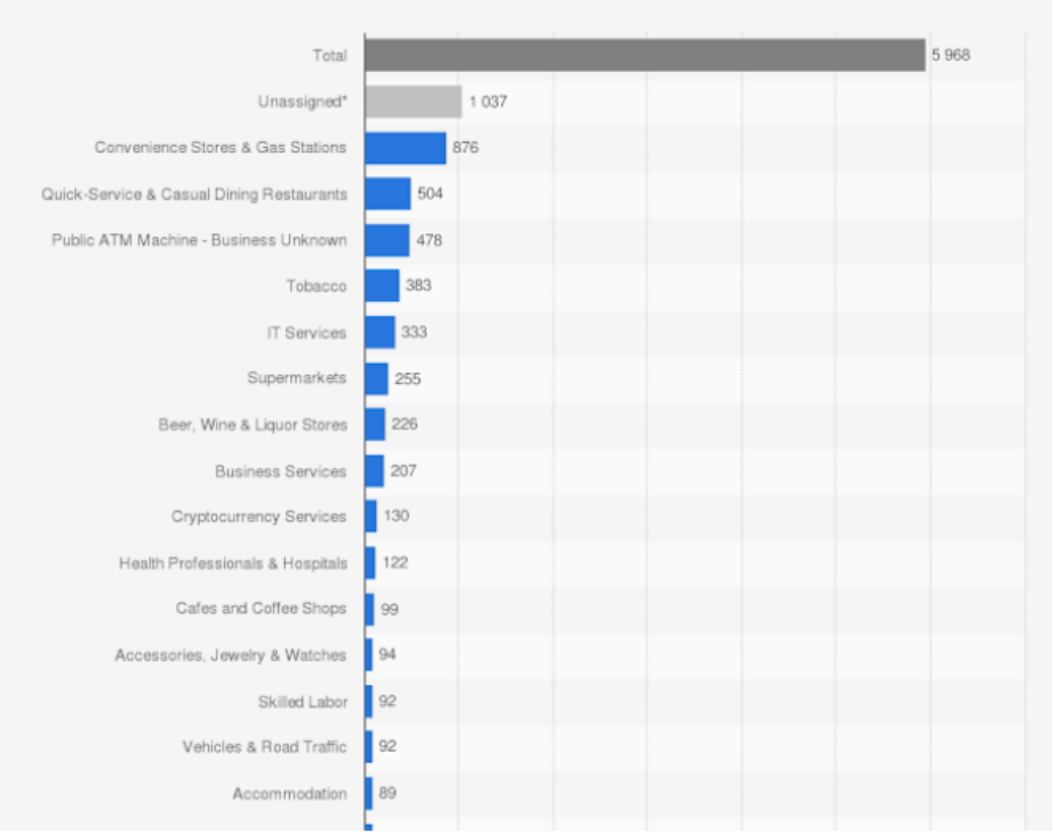
2.1.1 Medium of Exchange

The first factor is the "medium of exchange." In Section 2.3.1, Mattke et al. (2020) illustrate it as the functionality of "an intermediary between the products and services that people want to exchange with each other" as money.

For cryptocurrencies, they fulfill the requirement for being a "medium of exchange." On the one hand, many companies accept cryptocurrency as a way to purchase their products or services. Figure 1 illustrates that a large variety of businesses support virtual currency as a way of payment.

Figure 1

The number of businesses in the United States that supports cryptocurrency as a payment



Note: this figure is from Statista and the data was on March 9, 2021. It supports by either having a cryptocurrency ATM or offering crypto as an in-store payment method.

According to Figure 1, 5968 businesses support utilizing cryptocurrency for trading. In other words, if people live with only the cryptocurrency and do not encounter much trouble. On the other hand, companies like Huobi Global and Coinbase could trade the owners' cryptocurrency for legal tender as Dollar, Pound, Yuan with specific exchange rates. Therefore, it has the quality of "medium of exchange."

2.1.2 Store of Value

Mattke et al. (2020), claim another feature of money: "store of value," and it means that "it needs to enable the maintenance of purchasing power or possible savings" (p. 28). Since cryptocurrencies are always valuable and people could trade them via certain companies for legal tender due to their nature of "medium of exchange," they are equipped with the "maintenance of purchasing power."

2.1.3 Unit of Account

The last factor Mattke et al. (2020) convey to their audience in the "Is Cryptocurrency Money?" is the "unit of account", which means that "money must make it possible to show the real economic value relations between two goods or services" (p. 29). It is not hard to prove this characteristic. Since cryptocurrency has the characteristics of "medium of exchange" and "store of value," they could quickly be conversing with specific legal tender with special exchange rates. Meanwhile, people know that legal tender like the Dollar can show the "real economic value relations between two goods or services."

2.2 Anonymity

Another outstanding characteristic is cryptocurrencies' anonymity. Amarasinghe et al. (2019) have conducted "A Survey of Anonymity of Cryptocurrencies" based on the *Australasian Computer Science Week Multiconference Proceedings*. In their survey, there are seven different attributes of anonymity (p. 3).

- unlinkability: with two transactions, people could not conclude that they are for the same user.
- recipient anonymity: people could not build the connection between the transaction and the recipients' identities.
- untraceability: people could not build the connection between the transaction and the senders' identities.
- fungibility: the unit for each virtual currency should be the same so that every currency has the same right.
- confidentiality: after analyzing the transaction flow pattern, people could transfer the value to other addresses.
- unlinkability of metadata: After analyzing the IP address of the transaction, the identity information might be revealed.
- deniability: the user has the right to deny that they have once participated in a certain transaction.

For Bitcoin, they suggest that it should be "pseudonymous rather than anonymous since public keys represent users instead of their real identities," and Bitcoin's anonymity focuses more on the "ownership rather than the coins themselves" (p. 4).

In addition to Bitcoin, other cryptocurrencies also have the trait of anonymity. For each virtual currency, there is a kind of wallet that could store the currency without any information to register and the wallet consists of a series of random numbers. When people want to trade that virtual currency, they just need the address of the recipient rather than any other specific information like Government ID to transfer their currency to the recipient, which follows the "recipient anonymity". The transaction will only show two wallet addresses and the amount of the virtual currency. Therefore, the real identity information of the sender and recipient would be hidden, which confirms the "untraceability" and "unlinkability".

In contrast, the traditional approach of trade could be traced. Taking online banking transfer as an example, the bank account carries the identity information of people, and once a transaction is considered a crime, the police could get all the information of the criminals and chase them.

Some attempts have been made to reduce anonymity. Most companies of trading cryptocurrencies, like Huobi Global and Coinbase, need people to offer their identity information when registering the account, so that police could obtain the criminals' information as well as a transaction is considered a crime. This reduces the "unlinkability of metadata" aspect of anonymity.

However, criminals could transfer their illicit virtual currency to other innocent people and force them to register accounts and do the legal tender trade, so that the criminals increase the difficulty to trace their identities.

Overall, the anonymity of cryptocurrencies mainly reflects on the transactions with the only information of wallets, which do not have the users' identity information.

3. Imperfect Regulation

In addition to cryptocurrencies' outstanding and unique characteristics, the government's imperfect regulation becomes the integral part that attracts criminals to trade. Zaytoun (2019) has written a comment on "Cyber Pickpockets: Blockchain, Cryptocurrency, and the Law of Theft" and discussed how certain crimes via cryptocurrency are not suitable or adaptable with current laws.

For the stolen situation, it means some criminals may steal, in a physical way, the private keys for the wallet of cryptocurrencies and transfer the currency to the criminals' wallet. Under such a situation, people may refer to the National Stolen Property Act. However, Zaytoun states that the law

would not apply to the “act of taking an individual's private key” due to the disagreement of considering cryptocurrencies as tangible goods merchandise (p. 18).

The fraud and abuse represent that the crime of hacking computers to get illicit cryptocurrencies, and people would refer to the Computer Fraud and Abuse Act at that time. Nevertheless, with prosecution under such statute, the difficulties are “the act’s breadth, attributable to both statutory amendments and court interpretation, leaving prosecutions under the CFAA susceptible to vagueness attacks” and “whether Bitcoin meets the definition of anything of value" (p. 21).

The last one is wire fraud, and when people experience that, they need to refer to 18 U.S.C. § 1343 and other relevant mail fraud provisions. However, “no one has been convicted of theft of crypto-assets. Prosecutors seem to prefer to charge the effects of theft--money laundering of proceeds derived from selling stolen Bitcoin--by waiting until the thief converts Bitcoin to cash”(p. 25).

For each case above, there would be troubles executing the laws to the crimes via cryptocurrency since the laws need to be updated.

4. Crimes

After analyzing those “useful” characteristics of cryptocurrency, this literature review will move to three crimes commonly committed via cryptocurrencies: illegal mining applications, ransomware payments, and dark web crimes. The last crime belongs to the area of money laundering since, according to the journal “Cryptocurrency: The New Face of Cyber Money Laundering,” Sagwadi Mabunda defines money laundering as “ the process of concealing proceeds of illicit or illegal activities to obscure the link between the original criminal activity” (p. 1). In other words, money laundering means criminals execute specific methods to hide their illicit revenue.

For all three crimes, once the criminals gain their illicit revenue via cryptocurrencies, they will rely on some companies, like Liberty Reserve, to exchange legal tender with cryptocurrencies. However, those companies may not need “any supporting documents to verify the legitimacy of the identifying information, such as an official identification document” (Mabunda, 2018). Moreover, Liberty Reserve allows the users to pay a 75 cent ‘privacy fee’ to hide their transactions, and even Liberty Reserve itself would not have a record of those transactions. Hence the illicit revenue would be completely hidden and untraceable.

4.1 Illegal Mining Applications

As analyzed in the background section, there are two approaches to access cryptocurrencies: mining and trading. In contrast, mining means that participants should use specific scripts to solve complex math problems to gain valuable cryptocurrency. However, Higbee, Aaron, a cybersecurity expert, conveys to the audience in “The role of crypto-currency in cybercrime” two ways of mining crimes.

One of them is that the criminals utilize “phishing emails to share a compromised link that directs users to a website domain that allows hackers to run a short script designed to begin the mining” (p. 14). Another crime is adding the mining plugins to websites so that once victims visit the website, the mining script will operate without any notifications to the users. And through this way, not only will those criminals hack people’s computers. But also their phones for mining.

4.2 Ransomware Payments

Another crime is ransomware payments, and like its name, criminals will hack victims’ computers and threaten them to pay by cryptocurrency for their valuable files. With the anonymity of the cryptocurrency, those illicit payments are untraceable as law enforcement could not obtain the

identifying information of the criminals based on the wallet of cryptocurrency. The WannaCry, in Higbee, Aaron's journal, is the "largest ransomware attack in history" (p. 14), and Felix Richter's study, on the scope of the ransomware WannaCry, argues that over 220,000 systems in 150 countries were affected, and WannaCry forced each victim to pay $300 for the ransom.

4.3 Dark Web Crimes

The dark web crime is the primary type of corruption in the money laundering area via cryptocurrency. In the study, "Measuring dark web marketplaces via Bitcoin transactions: From birth to independence," Hiramoto, N. & Tsuchiya, Y. refers the dark web to the content of the World Wide Web but requires "special software and communication methods," and the dark web offers the anonymity for themselves (p. 2). Hiramoto, N. & Tsuchiya, Y. show the avenues for some famous dark web in their study (p. 6):

> The total sales volumes of the dark web marketplaces are 192.7 million USD between June 2012 and October 2013 on Silk Road, and 166.0 million USD between December 2014 and February 2016 on AlphaBay. The corresponding figures are 112.9 million USD on Silk Road 2.0, 220.7 million USD on Agora, 69.7 million USD on Evolution, 88.3 million USD on Nucleus, and 35.6 million USD on Abraxas for their entire lifetime.

The dark web provides many illegal goods or services, including fake ids, drugs, sexual transactions, and even murder and the dark web prefers Bitcoin as the first cryptocurrency for trading.

5. Conclusion

This literature review has explored how cryptocurrencies lead to crime from their unique natures, such as money and anonymity and imperfect regulation. And this literature review also points out several types of crimes in the money laundering area with those characteristics. In order to reduce or eliminate those crimes, security software like McAfee and 360 need to improve their capabilities to monitor those safeguards, notifying the phishing link and ransomware to the users before accessing. For the crimes on the dark web, law enforcement may act undercover and is supposed to catch the website's builders as soon as possible. However, above all, the relevant law needs to be updated or public new regulations for the cryptocurrency so that the situation, that a criminal cannot be accused of due to the lack of strict provisions, can be avoided.

References

Amarasinghe, N., Boyen, X., & McKague, M. (2019). A Survey of Anonymity of Cryptocurrencies. *Proceedings of the Australasian Computer Science Week Multiconference*, 1–10. https://doi.org/10.1145/3290688.3290693

Bitcoin price today, BTC live marketcap, chart, and info. (n.d.). CoinMarketCap. Retrieved March 23, 2021, from https://coinmarketcap.com/currencies/bitcoin/

Chavez-Dreyfuss, G. (2021, January 28). *Cryptocurrency crime drops in 2020 but "DeFi" breaches rise, study finds*. U.S. https://www.reuters.com/article/idUSL1N2K2098

Henry S, Z. (2019, January). Cyber Pickpockets: Blockchain, Cryptocurrency, and the Law of Theft [Comment on the article "North Carolina Law Review"]. LexisNexis. https://advance-lexis-com.ezproxy.neu.edu/document/?pdmfid=1516831&crid=18567adf-75eb-42a5-9c2e-34678276c72a&pddocfullpath=%2Fshared%2Fdocument%2Fanalytical-materials%2Furn%3AcontentItem%3A5VBY-FC10-02BN-00MV-00000-00&pdcontentcomponentid=7349&pdteaserkey=sr0&pditab=allpods&ecomp=7bq2k&earg=sr0&prid=8ff6e200-b696-4165-bc3c-33291b908b28

Higbee, A. (2018). The role of crypto-currency in cybercrime. Computer Fraud & Security, 2018(7), 13–15. https://doi.org/10.1016/s1361-3723(18)30064-2

Hiramoto, N., & Tsuchiya, Y. (2020). Measuring dark web marketplaces via Bitcoin transactions: From birth to independence. Forensic Science International: Digital Investigation, 35, 301086. https://doi.org/10.1016/j.fsidi.2020.301086

Huobi Global. (2013). *BTC/USDT Bitcoin Exchange | Huobi Global - Huobi.com*. Huobi Global. https://www.huobi.com/en-us/exchange/btc_usdt/

Mabunda, S. (2018). Cryptocurrency: The New Face of Cyber Money Laundering. 2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (IcABCD), 1. https://doi.org/10.1109/icabcd.2018.8465467

Mattke, J., Maier, C., & Reis, L. (2020). Is Cryptocurrency Money? *Proceedings of the 2020 on Computers and People Research Conference*, 26–35. https://doi.org/10.1145/3378539.3393859

Morris, L. (2015). Anonymity Analysis of Cryptocurrencies (Order No. 1586752). Available from ProQuest One Academic. (1679278024). https://link.ezproxy.neu.edu/login?url=https://www-proquest-com.ezproxy.neu.edu/dissertations-theses/anonymity-analysis-cryptocurrencies/docview/1679278024/se-2?accountid=12826

Richter, F. (May 15, 2017). 200,000+ Systems Affected by WannaCry Ransom Attack [Digital image]. Retrieved March 26, 2021, from https://www-statista-com.ezproxy.neu.edu/chart/9399/wannacry-cyber-attack-in-numbers/

South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, Which was Funded by Bitcoin. (2019, October 16). U.S. Department of Justice. https://www.justice.gov/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-largest-darknet-child

Statista. (2021, March). *Number of businesses in the United States that either have a cryptocurrency ATM or offer crypto as an in-store payment method as of March 9, 2021, by industry*. https://www-statista-com.ezproxy.neu.edu/statistics/1223053/firms-with-crypto-payment-solutions-industry-usa/