American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-10, Issue-12, pp-103-106
www.ajer.org
Research Paper Open Access

Cybercrimeand Cryptocurrency

Samira Ibrahim[1], Daniel Ikechukwu Nnamani[2]Ojeifoh Okosun[3]Olumuyiwa Ezekiel Soyele[4]

[1]*Texas Southern University, Barbara Jordan- Mickey Leland School of Public Affairs, Department of Administration of Justice*
3100 Cleburne Street, Houston, Texas 77004. America, PH- +1 346-401-7062
[2]*Texas Southern University, Barbara Jordan- Mickey Leland School of Public Affairs, Department of Administration of Justice*
3100 Cleburne Street, Houston, Texas 77004. America, PH- +1 832-946-1426
[3]*Texas Southern University, Barbara Jordan- Mickey Leland School of Public Affairs, Department of Administration of Justice*
3100 Cleburne Street, Houston, Texas 77004. America, PH- +1 346-777-0765
[4]*Texas Southern University, Barbara Jordan- Mickey Leland School of Public Affairs, Department of computer sciences*
3100 Cleburne Street, Houston, Texas 77004. America, PH- +1 (281) 713-4740706

Abstract: *Since the mining of the first Bitcoin, thousands of other forms of cryptocurrency have been created. These electronic currencies, in essence, have begun to put the notion that central planning is necessary to the function of an economy to the sword. By their very operation, the traditional administration of money that is mired in a litany of legislative standard and financial policies can be circumvented. Additionally, they operate with features that make financial transactions open-source, decentralized, peer-to-peer, anonymous, and non-demanding of regulatory and time-consuming intermediaries. However, the technicalities of these currencies mean they are a cybercriminal's dream. This study defines cybercrime, traces its evolution to the origins of blockchain technology, and illustrates the technicalities of cryptocurrencies. Finally, it explores some forms of crime facilitated by these currencies.*

Keywords: Anonymity, Blockchain, Cryptocurrency, Cybercrime.

Date of Submission: 08-12-2021 Date of acceptance: 23-12-2021

I. INTRODUCTION

The development of the modern and mobile computer heralded the arrival of a new era of information storage, analysis, dissemination, and computation that was, less than a century ago, the stuff of dreams. Soon, the internet followed, and novel platforms and technologies for unfettered communication began to be developed and to proliferate (Armstrong and Forde, 2003). But as is often the case with every other invention and novel development, a sense of opportunism far beyond the remits of what these iterations were intended for had materialized. For the severe opportunist, this moved far beyond the convenience of networking systems and communication platforms unconstrained by time or spatial reach (Marcum and Higgins, 2019). Almost as soon as these modern technologies were being developed, they were being used for criminal activity. This led to the identification and definition of cybercrime.

II. CYBERCRIME

Simply defined as criminal activity involving computers, networks and networked devices as accessories, weapons or targets, cybercrime comes in many forms today (Scheau and Pop, 2018); some similar to traditional crime types and others entirely novel by virtue of a complete reliance on computer technologies. Generally speaking, the number and sophistication of the forms of cybercrime obtainable today are the result of the steady evolution of these technologies. Prior to the official arrival of the internet in the early 1980s, the main instance of cybercrime obtainable was the unauthorized data and information transfer from computer systems (Marcum and Higgins, 2019). When the internet arrived, cybercrime evolved to computer viruses, denial-of-

service attacks, privacy invasion and business email compromise (BEC) scams, before upgrading to forms such as cyberbullying, cyber terrorism, cyber warfare, wire fraud, identity theft, and credit card fraud (Marsili, 2019; Scheau and Pop, 2018; Tarabay, 2021).

Notably, these developments were generally mirrored by efforts by legal systems to control and mitigate against the proliferation of these offences. Often at the heart of these law-enforcement campaigns were efforts to check and minimize the online anonymity of the perpetrators of these crimes—a feature than enabled them conceal their identities during and after the execution of these offences (Holt, 2018). As difficult as these campaigns had it with the anonymity feature of internet technologies, some successful cases provided hope that law enforcement would not be too far behind the curve of cybercrime sophistication. That was, until the arrival of another novel feature of the internet: cryptocurrencies (Tarabay, 2021).

III. CRYPTOCURRENCIES

Origins

The concept of cryptocurrencies was first introduced in an original publication by Satoshi Nakamoto in 2008(Reddy and Minnaar, 2018; Nakamoto, 2008). Defined simply as currencies in a digital format, cryptocurrencies were intended to be operationalized as a means of electronic payment. But unlike the equally revolutionary movement of funds electronically, between traditional financial institutions or for payment purposes, this form of electronic transfer would be more secure and fraud-proof, and would not need the role of trusted intermediaries like banks (Nakamoto, 2008; Stroukal, 2016). In fact, most of these currencies would be free from deflationary forces and from the control of a central institution—such as a central bank or national government—and their transfer would eliminate roadblocks that would otherwise arise from the exchange of physical currency (Nakamoto, 2008). When the first cryptocurrency—Bitcoin—was mined, its features generally lived up to what was promised in Satoshi's whitepaper. This began to inspire calls for the reevaluation of the notion that the creation, control and distribution of finances required the agency of government institutions(Reddy and Minnaar, 2018). Unfortunately, it also manifested features that meant that major roadblocks faced by cybercriminals could be obliterated (Higbee, 2018).

Technicalities of Cryptocurrencies

Notably, it is generally accepted that the main aim of the invention of cryptocurrencies is completion with established legal tenders (Bray, 2016; Foley, Karlsen and Putnins, 2019; Nakamoto, 2008). For a revolutionary edge, these electronic monies run on an analytic and decentralized system of cryptography. This technology enables electronic cash to be transferred online and peer-to-peer (P2P) (Nakamoto, 2008). The major cryptocurrencies operate via an open-source system; a framework where there are generally no restrictions on who may gain access into the software (Custers, Oerlemans and Pool, 2020). This technology is similar to that employed in social media platforms, which means it is also P2P. The P2P capability of cryptocurrencies like Bitcoin means it can be traded directly between two parties who desire to make the transaction in question, without the interference of an intermediary party such as a credit card company (Reddy and Minnaar, 2018). The clearance feature of traditional transactions is, in cryptocurrency transfer, replaced by a process of mining where peers validate transactions using algorithms that maintain their integrity (Nakamoto, 2008; Stroukal, 2016).

Cryptocurrency and Cybercrime

Facilitation of Money Laundering and BEC scams

The technology behind these digital currencies incorporate private and public key features that enable the transfer of value between two entities in transaction and mandate its signing to show Proof of Work (PoW). This key transfer feature is enabled by an integrated distributed ledger function comprised of numerous blocks of data; each of which is created for every single transaction made and where the records of the transaction (such as the addresses of the transacting parties) are recorded (Nakamoto, 2008; Tarabay, 2021). A sequence of block-recorded data is known as a blockchain. Several virtual vaults and wallets are finally linked to these blockchains, and allow holders store their cryptocurrencies (Reddy and Minnaar, 2018). Comprehensively, these features and functions make up a system of financial ownership and transfer that is transparent but secure, decentralized and well distributed, fast, and not in need of traditional intermediaries (Nakamoto, 2008). Notably though, a feature of the blockchain technology is anonymity (Armstrong and Forde, 2003; Bray, 2016). Despite its transparency, users can operationalize its speed and the lack of regulatory intermediaries to perform a series of maneuvers that would obscure the trail of the illegal movement of large amounts of money offshore by mixing digital funds in a pool of other users' holdings (Tarabay, 2021). These features of blockchain technology are also perfect for the perpetuation of other forms of cybercrime like BEC scams and advance-fee fraud, as they guarantee the hitch-free transfer of proceeds from these endeavors (Bray, 2016; Marcum and Higgins, 2019).

Hacking and Ransomware Attacks

Ransomware attacks are generally pulled off through a process wherein cybercriminals gain access into an organization's system and swiftly take over its processes. By the time the attack is detected by the organization, preset overrides would be powerless as the site would be inaccessible (Tarabay, 2021). A ransom demand would then be sent by the hackers, usually via email, containing descriptions about how a ransom should be paid by the organization in exchange for access to their account. Prior to cryptocurrency technology, ransom payments were demanded through money transfer institutions—such as Moneygram—and in the form of wire transfers (Reddy and Minnaar, 2018). The fact that these processes usually revealed the identity of the owners of the accounts into which ransoms were paid meant ransomware attacks were dangerous and often fruitless. But if ransomware attacks were fairly commonplace in the 2010s, they have certainly been turbocharged by the evolution and adoption of cryptocurrency technology (Reddy and Minnaar, 2018; Tarabay, 2021). Now, hackers simply input cryptocurrency addresses in their ransom messages and run their ill-gotten proceeds through pre-developed cryptocurrency mixers to obscure their trail, from any location, without revealing their identity (Higbee, 2018). A report from crypto analysis firm Chainanalysis places the cost of cryptocurrency-enabled ransomware attacks at over $400 million in 2020 (Custers, Oerlemans and Pool, 2020).

Funding of Terrorism and Facilitation of the Drug Trade

The main reason for the invention of cryptocurrencies—use as a digital legal tender—makes it suitable for the financing of illegal activities, including terrorism (Bray, 2016; Nakamoto, 2008). Prior to the proliferation of cryptocurrencies, the movement of funds for terrorism support came in the forms of wire transfers, currency exchange services and physical cash drop-offs; processes that were either too tedious or that could reveal the identity of owners of the sending and receiving accounts (Marsili, 2019). Today, all a terrorism financer has to do is obtain the blockchain address of a terror organization and, through a digital blockchain application, transfer the desired amount of cryptocurrency. This system is also useful for the purchase of weapons, narcotics and illegal equipment on the Dark Web (Reddy and Minnaar, 2018). Traders on this corpus of websites generally accept cryptocurrencies as exchange for goods today (Stroukal, 2016), as the trail of transaction records generated by this process can easily slip into the distributed ledger system and be masked by several other legal transaction records on the blockchain.

IV. DISCUSSION AND CONCLUSION

Since the mining of the first Bitcoin, thousands of other forms of cryptocurrency have been created. These electronic currencies, in essence, have begun to put the notion that central planning is necessary to the function of an economy to the sword. By their very operation, the traditional administration of money that is mired in a litany of legislative standard and financial policies can be circumvented. Additionally, they operate with features that make financial transactions open-source, decentralized, peer-to-peer, anonymous, and non-demanding of regulatory and time-consuming intermediaries. These features have attracted millions of investors—institutional and retail—to the cryptocurrency market. However, the technicalities of these currencies mean they are a cybercriminal's dream. The forms of crime boosted by cryptocurrencies and explored in this study are money laundering, terrorism, drug trade, hacking and ransomware attacks. But by no means is this list exhaustive. Other potential forms facilitated by this technology are Ponzi schemes, crypto jacking, pyramid schemes, initial coin offering (fraud), phishing, and cyber extortion (Higbee, 2018; Reddy and Minnaar, 2018). Like the computer and the internet, the invention of cryptocurrencies and blockchain technology had a noble intent; but has since served to propagate ugly behaviors. In general, the financial costs of these crimes are staggering and remain on the rise.

REFERENCES

[1]. Armstrong, H. L., & Forde, P. J. (2003). Internet anonymity practices in computer crime. *Information management & computer security*.

[2]. Bray, J. (2016). *Anonymity, Cybercrime and the Connection to Cryptocurrency* (Doctoral dissertation, Eastern Kentucky University).

[3]. Custers, B., Oerlemans, J. J., & Pool, R. (2020).Laundering the Profits of Ransomware: Money Laundering Methods for Vouchers and Cryptocurrencies. *European Journal of Crime, Criminal Law and Criminal Justice*, *28*(2), 121-152.

[4]. Foley, S., Karlsen, J. R., &Putniņš, T. J. (2019). Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?. *The Review of Financial Studies*, *32*(5), 1798-1853.

[5]. Higbee, A. (2018). The role of crypto-currency in cybercrime. *Computer Fraud & Security*, *2018*(7), 13-15.

[6]. Holt, T. J. (2018). Regulating cybercrime through law enforcement and industry mechanisms. *The ANNALS of the American Academy of Political and Social Science*, *679*(1), 140-157.

[7]. Marcum, C. D., & Higgins, G. E. (2019).Cybercrime.In *Handbook on crime and deviance* (pp. 459-475).Springer, Cham.

[8]. Marsili, M. (2019).The war on cyberterrorism. *Democracy and security*, *15*(2), 172-199.

[9]. Nakamoto, S. (2008). Re: Bitcoin P2P e-cash paper. *The Cryptography Mailing List*.

[10]. Reddy, E., &Minnaar, A. (2018). Cryptocurrency: A tool and target for cybercrime. *ActaCriminologica: African Journal of Criminology &Victimology*, *31*(3), 71-92.

[11]. Șcheau, M. C., & Pop, Ș. Z. (2018). Cybercrime evolution. *ISSN 1843-682X*, *24*(1), 225.
[12]. Stroukal, D. (2016, November). Bitcoin and other cryptocurrency as an instrument of crime in cyberspace.In *Proceedings of Business and Management Conferences* (No. 4407036).International Institute of Social and Economic Sciences.
[13]. Tarabay, J. (2021, July). How Cryptocurrency Turbocharged the Cybercrime Racket. Bloomberg.Accessed August 21, 2021.https://www.bloomberg.com/news/articles/2021-07-03/how-cryptocurrency-turbocharged-the-cybercrime-racket-quicktake

Samira Ibrahim, et. al. "Cybercrimeand Cryptocurrency."*American Journal of Engineering Research (AJER)*, vol. 10(12), 2021, pp. 103-106