Westford University College Research Journal
Online ISSN No. 2790 – 3885
Vol. 1 Issue 1

A Systematic Exploration of the Relationship between Cryptocurrency and Cybercrime – An Assessment of the Implications and Issues of Anonymity

Behrang K. Ravari
ORCID No.0000-0003-4579-2390
behrang@ravari.net
UCAM Catholic University of Murcia

Shaa Ista Francke Mukaddam
ORCID No.0000-0002-0467-2408
s.francke@westford.org.uk
Westford University College, United Arab Emirates

Rajesh Chandra Mutah
ORCID No. 0000-0001-5536-7502
rajesh.c@westford.org.uk
Westford University College, United Arab Emirates

ABSTRACT

Cryptocurrencies establish a lot of chances for offenses like money laundering. Cryptocurrencies are not under the control of any government institution. They permit users to anonymously exchange commodities, and they effortlessly transverse frontiers through the Internet. Each of these attributes makes it hard for individual countries to manage cryptocurrencies in seclusion. This research investigates how cryptocurrencies have become a tool and a target for cybercrime. The paper will explores that a relationship exists between cybercrime and cryptocurrencies. Today, cybercrime poses a substantial threat to the global community. It may exploit the CI (Critical Infrastructures) structures that are largely interlinked. Despite the increased interconnectivity enabling easier and more effective communication, it has created vulnerabilities that were not in existence a decade ago. However, not having a standardized definition has made it increasingly complex to establish a policy that will permit more effective interagency cooperation and robust regulations concerning cybercrime. Cybercrime thrives on internet's anonymity with the utilization of certain browsers, for instance, the Onion Router, to gain access to data that cannot be searched within the daily search engines. The proliferation of cybercrime is based on the heightened utilization of peer-to-peer decentralized cryptocurrency. The study utilizes both secondary and primary data gathered to demonstrate whether a relationship exists between cryptocurrency and cybercrime based on the aspect of anonymity that characterizes cryptocurrency. This systematic study aims to determine whether the aspect of anonymity in cryptocurrencies encourages people online to use it as a tool or target for cybercrime. The sample for the study will be broad to allow for a wide scope of information. The participants will encompass participants from companies that have been victims of cybercrime due to cryptocurrencies (10). 60 – 80 participants that are specialized experts in the internet and technology field, and criminologists that have to solve some of these reported crimes. Cyber criminals behind bars, preferably 20 to 30 respondents. Lastly, the researcher recruited 300 students from the university without a specification on discipline to participate in the survey. Participation in the study will be completely voluntary. The researcher anticipates a 85% response rate to meet the required sample size for the study

to draw significant conclusions on the issue. However, a pilot study was deemed necessary before the main study to pre-test the research tools questionnaire and sub structured interview guide. The pilot study encompassed a sample of 20 respondents who will also take part in the main study. Ethical considerations will be observed in the study to increase the validity and reliability of the survey.

Keywords— Cryptocurrency, cybercrime, anonymity, technology

INTRODUCTION

Cryptocurrency is used to refer to a cryptographic string of alphabetical symbols and numbers. The instigation of the cryptocurrencies notion can be attributed to an academic paper publicized by Satoshi Nakamoto in 2008. Since Bitcoin was introduced, a plethora of virtual currencies has risen. After Bitcoin, Litecoin, Ethereum, and Ripple are the three most extensively utilized cryptocurrencies. According to the Coin Market Cap, more than 10,000 kinds of cryptocurrencies are in circulation.

Cryptocurrencies like Bitcoin were initiated to provide an electronic system of payment that was more resistant to fraud and more secure than credit cards, eroding the need for trusted intermediaries like economic institutions. However, cryptocurrencies are not under the regulation of any central institution like a government (or the Central Bank of the Nation) or even an executive non-profit. Hence, they allow for a digital currencies owner to receive gold credibility without the inconvenience of having to transfer a physical item for a transaction to occur. Hence, the reasoning for the existence of cryptocurrencies is based on the argument that the distribution, creation, and regulation of money do not have to get managed by the central banks or state. Therefore, cryptocurrencies challenge the medieval perception that central planning requires money to be in operation. In standard communities, the development, distribution, and control of money are managed by the central banks and state, in the company of a plethora of regulatory standards and monetary policies that users are obliged to.

The ECB (European Central Bank, 2012, p.6) assumed the lead in the classification of cryptocurrencies. Based on the ECB, cryptocurrencies are virtual currencies that encompass the three classifications below:

1. Closed virtual schemes. Game-only (closed virtual currency) schemes, means transactions (the currency obtained from acts within this virtual universe and can only be utilized in purchasing virtual services and goods within this world of gaming) are restricted to the virtual universe. Hence, the scheme on its own fails to have a link in the actual economy on any banking or economic structures. The enrolment requirement for such kinds of schemes is normally a subscription fee. Once the subscription fee has been paid, users choose to earn virtual money based on their virtual acts implemented within these virtual universes. One such currency is WoW (World of Warcraft) Gold. The direct buying of such a currency may be made with the help of official (fiat) currency. The moment it is bought, the currency may not be converted back or exchanged into official currency.

2. Schemes characterized by unidirectional flow make it possible for both in-game buying (virtual) services and goods and purchases in the actual world (the buying of real

services and goods). Nintendo Points and F.B. (Facebook Credits) are examples of the kinds of currencies distinct to such a scheme.

3. When it comes to virtual schemes with the bidirectional flow, users have the freedom to sell and purchase virtual currency based on the official currency exchange. Hence, it can be utilized in the same manner that other convertible currencies are utilized in the actual universe. The two virtual and real services and goods can be purchased using this currency type. Examples of currencies distinct to this kind of scheme encompass Linden Dollars (L$) (the gaming world currency Second Life) and Bitcoin.

Therefore, cryptocurrency is a virtual currencies' sub-set. Despite the taxonomy above, cryptocurrencies were established for the "sole aim of proffering the legal tender competition" (Halaburda and Gans, 2013 p.1). Additionally, the development and technical underpinnings of the cryptocurrency are largely distinct to those of virtual currency. For instance: "A cryptocurrency is based on maths, a decentralized exchangeable cryptocurrency that is safeguarded by cryptography. It encompasses cryptography principles for the implementation of a decentralized, disseminated, secure information economy" (Financial Action Task Force, 2014 p. 5). On the contrary, virtual currencies are grounded on virtual worlds (online gaming). Based on the ECB (2015 p.25), a virtual currency is a valuable computerized rendition that an e-money organization, credit institution, or central bank has not issued.

In some situations, it may be utilized as an alternative money. Below are elements of Bitcoin and other altcoins that are critical for cryptocurrency creation and network functioning.

a. Bitcoin utilizes open-source software. This software does not have any restrictions on who can access it, leaving the network open for any person to take part. This resembles Twitter or Facebook and most infrastructure on the Internet. To be a facet of the network, one ought to begin by installing and downloading the software. The Bitcoin software name is 'Bitcoin core.'

b. Transactions occur in a P2P (peer-to-peer) network that allows for direct communication from a single user to the next. This eliminates the need for intermediaries like financial institutions and payment clearing houses that serve to validate or process finances. For example, when a debit or credit card purchase occurs, the transaction can only be valid when the creating house has cleared it.

c. Although there is an elimination of intermediaries, the transaction still requires validation or clearance. To achieve this, the Bitcoin network utilizes a process of computation referred to as 'mining. Mining serves not simply for the creation of cryptocurrencies but also transaction validation. The moment cryptocurrency is established; it employs an algorithm that is cryptographic to safeguard the integrity of the transactions.

d. Private and public keys are utilized in the transference value from a single individual (or institution) to a second one and have to be signed cryptographically every time transactions occur (there is a transference of keys) PoW (Proof of Work) or SoW (Stake of Work) based on the currency type.

e. The primary technological creativity behind cryptocurrencies functioning is the disseminated ledger technology, known as a blockchain. It encompasses varied blocks generated every time a transaction occurs, hence recording the cryptocurrency's recipient and sender addresses. The address helps in the identification of certain transactions and not Bitcoin.

f. Virtual 'vaults' and 'wallets' are utilized in the storage of the Bitcoin (represented by several alphanumeric codes)

This strategic study aims to show a relationship exists between cryptocurrencies and cybercrime. The secondary aim is to analyse both secondary and primary evidence that will assist in showing if cryptocurrencies' anonymous nature can influence the actions of an individual in their day-to-day exploration of the Internet. Thus, the survey's objectives are designed to uncover a link between cybercrime, anonymity, and cryptocurrency. The objectives for the study are:

1. To determine a link between cryptocurrency and cybercrime;
2. To determine whether the anonymity attribute in cryptocurrencies is responsible for increasing a criminal's or individual's ability to commit a cybercrime; and
3. To determine whether cryptocurrency anonymity increased online criminal activity.

The study will help criminologists, law enforcement officers, and the reader appreciate how people offered a chance to stay anonymous and have resources to do so would participate in acts of crime, varying from PII (Personally Identifiable Information) paying for drugs to illegal downloading. The study will assist in revealing how these cybercrimes are linked to anonymity. There is very limited information gathered regarding the types of cryptocurrencies and the link with cybercrime. Hence, this survey will provide grounds for additional studies in this field. Information will be gathered with regards to whether or not respondents take part in the utilization of cryptocurrencies and if that participant has taken part in any cybercrimes in the past. Cybercrime is linked to any crime that is facilitated via the Internet or computer use. It can vary from buying or downloading pirated software to terrorist acts or acts of hacking.

Literature Review

Cryptocurrency was instigated in 2014 in tandem with the FinTech ideal. It is currently a facade of the greater process of digitization. In 2018, literary texts revolved around the idea of diversity categorization and cryptocurrency. After 2018, writers are now open to existing niches in the literary texts. The effect of cyber-crime on cryptocurrency or cryptocurrency on cyber-crime and the economy in its entirety has been examined in several recent articles. Visual currencies have established themselves in current years both as a tradable resource utilized for risk-cushioning aims (Bouri et al., 2017) and a fiat money alternative (Yermack, 2018). Hence, given their rising significance, several surveys have been undertaken to analyse the primary attributes of these novel established markets.

These studies include risk and returns (Tsyvinski and Liu, 2018; Balcair et al., 2017), efficiency in the market (e.g., Bariviera, 2017; Urquhart, 2016; Chu and Nadarajah; 2017) and anomalies (Carporalie and Plastun, 2019), illegal acts (Li et al., 2018; Foley et al., 2018), hedging properties (Baur et al., 2018), the initial offering of coins (ICO) (Howell et al., 2018), the impact of cyber-attacks (Shanaev et al., 2020), and financial effects of the rise of a novel kind of asset (Dwyer, 2015) (in Guglielmo Maria Caporale, 2020).

The effect of cyber-crime on the economy and cryptocurrency markets in its entirety has been examined in several current articles. For example, Benjamin et al. (2019) approximated that cyber-attacks from offenders in operation in the underworld web communities like Darknet have led to approximated yearly losses amounting to $445 billion for the universal markets (Graham, 2017). Bouveret (2018), another fascinating survey, utilized a VaR (Value-at-Risk) model to examine the risk of cybercrime and the resultant losses in several nations.

Corbet et al. (2019) delineated Bitcoin and other altcoins as a monetary resource. The article described a literature appraisal from a verifiable standpoint of the features linked with cryptocurrencies as a monetary asset because of their face. The writer picked a cryptocurrency subject on the grounds of the past articles due to its existing queries on bubbles of asset pricing, market efficiency, volatility clustering or decoupling hypotheses, and contagion. Digital currencies are located at the convergence between regulatory mistakes and the probability of illegal utilization via its anonymity inside a youthful underdeveloped framework of exchange. This youthful underdeveloped framework is characterized by violations in the infrastructure affected by the rise of cyber offenses and cryptocurrencies contribution has been confirmed to be under the influence of all these. Further, Bouri et al. (2019) examined related cryptocurrency exchanges. Bitcoin was picked as the currency for study and they uncovered the concurrent movements' presence of 12 other kinds of cryptocurrencies. As grounds for the study, they utilized day to day information on the cryptocurrencies value. The survey uncovered that the exchanges involving a single cryptocurrency dictate, in a huge percentage, the exchanges of other cryptocurrencies in a similar direction. The procedure is referred to as co-jumping. The survey assumed that their merchandising capacity denoted the cryptocurrency levity.

Chu et al. (2019) examined the hypothesis on the flexible market with regards to the markets of two famous cryptocurrencies (Ethereum and Bitcoin) in opposition to the U.S. Dollar

and the Euro. The findings were correlated with the supposition. The scholars also delineated that occurrences could co-occur with substantial alterations in-market effectiveness. This market efficiency attributes sentiment was verified using sample analysis to examine whether these acts influenced market inefficiency/efficiency. The core is that occurrences and sentiment may not be a substantial attribute in influencing the efficiency of cryptocurrency markets. The gathered information encompassed hours logged with elevated–frequency in Ethereum and Bitcoin cost as opposed to the USD and the Euro. It ensued transactions outlined on the cryptocurrency known as Kraken conversion commencing at 11 a.m. on July 1, 2017, up to noon on September 1, 2018. The distinct period was chosen to analyse the intervals because it is when the costs of the two altcoins endured immense increases (before January 2018) and falls (after January 2018). Although the outcomes seemed to show consistency with the supposition, the market effectiveness differed over time.

Zhang et al. (2018), in their report, delineated the 'conventionalized facts.' Cryptocurrencies were examined as an economic resource. They examined the conventionalized reality based on the Hurst advocate by utilizing the DFA (Detrended Fluctuation Analysis) and R/S Analysis of the famous cryptocurrencies positioned on the grounds of their market subsidization. The repositories had archival high–frequency costs of those altcoins as compared to the U.S. Dollar, starting on February 25 to August 17, 2017. The top four picked altcoins for the study's assessments encompassed Ethereum, Bitcoin, Litecoin, and Ripple. The survey was undertaken on high-frequency turnover information with distinct lags. It is equally reflected on attributes of subservience between the distinct cryptocurrencies. These attributes offer industrial practitioners and academics information on the attributes and structure of these four famous digital currencies and can equally be significant in the development of pricing cryptocurrencies.

Other scholars like Xu et al. (2019) have examined the VaR (value at risk) for all cryptocurrencies by utilizing past approaches. They approximated the VaR (value at risk) for every digital currency by utilizing quantile regression, often known as the TENET (Tail-Event Driven NETwork model). Based on this survey, the researchers recognized that a substantial risk overflow impact subsists and that the extent of the complete interconnection of all the digital currencies selected gradually soared over time. Bitcoin appeared to be the most substantial strategic recipient of risk, and Ethereum the greatest strategic emitter of risk. Like Bouri, Grobys equally came up with a survey in Grobys, Ahmed, and Sapkota rooted on the day-to-day information on the value of cryptocurrencies. At that moment, their processing encompassed the determination of the moving mean merchandising approaches that are employed. The 11 most merchandised currencies between 2016 and 2018 were utilized for this goal. The outcome showed that the moving average of a variable approach is triumphant when utilizing a moving average of 20 days' approach of merchandising. Moreover, the outcomes illustrated that cryptocurrency markets were effective.

Corbet et al. (2020), in another survey, depicted the destabilizing impacts of cyber criminality and cryptocurrency. The article aims to discover the rage of economic market impacts of current cybercrimes, particularly those linked to cryptocurrencies. Corbet utilized

information from the Bitfinex conversion at constancy of one hour for the eight most fragile digital currencies. The outcomes concluded that hacking occurrences also raised both the volatility of the price of the cryptocurrency targeted and cross–cryptocurrency correspondence. Furthermore, cybercrime situations lower the value finding sourced in the course of the hacked currency commensurate to additional cryptocurrencies. Koerhuis et al., (2019) undertook a forensic examination of privacy-oriented digital currencies. They uncovered that offenders exploited digital currencies because they possessed build-in privacy and anonymity attributes making them extremely hard to track down finances back to a certain user in distinct types of money laundering malware. The scholar examined Verge and Monero and examined the precious forensic artefacts that these digital currencies software abandoned on the computer structure. Distinct sources of probable facts were explored in this paper (Koerhuis et al., 2019).

Caporale et al. (2019) explored the issue of cyber-attacks, non-linearities, and digital currencies. For this aim, he utilized a specification of the Markov-switching to undertake an analysis of the impacts of cyber-attacks on four cryptocurrencies returns from 2015 to 2019. The analyses are perceived as cyber-attacks, and they target cryptocurrencies. The outcomes imply substantial adverse impacts of cyber-attacks on the cryptocurrency likelihood staying in a regime of reduced volatility. This shows the significance of understanding the way to deal with cybercriminals for the prevention of market disruptions.

Baron et al. (2015) undertook a meta-analysis to examine the non-state actors' feasibility of increasing their financial and political power by deploying virtual currencies (V.C.) for their utilization in regular financial transactions. They note that the national security policy impacts for the virtual currency technology rise has been subjected to a lot of debate lately. There has been a certain focus on the V.C.s (like Bitcoin) potential anonymity in addition to the likelihood of insurgent groups or terrorists using it in a resilient way against actions by the international and local law enforcement, intelligence organizations, and the military (encompassing the ones in the U.S.) to undertake a survey. The report aimed to enrich the conversation on policy by exploring the technical matters linked with virtual currencies. The scholar examines the matter of the deployment of V.C. from both the political-economic and technological perspectives, focusing on the difficulties facing non-state actors that try to deploy V.C.s. These difficulties inform how the United States, its allies, and additional cyber actors may respond to a V.C. deployment of this nature if it was a threat to their interests in national security. To date, a case of such a non-state actor deployment has been missing. The report highlights those primary issues that may act as political-economic and technological hindrances to comprehend why such deployment can increase its feasibility and are advantageous in the future for the non-state actor.

Casino et al. (2019), in their study, insist that cryptocurrencies have the anonymity attribute that increases their favorability by criminals both as a tool and as a target for cybercrime, the blockchain technology that it uses favors the law enforcements' ability to track down and capture these offenders. The study avails a strategic literature review of blockchain-based applications across various sectors. The scholars' goal was to examine the present state of blockchain technology and its applications and delineate how certain attributes of this

troublesome technology may revolutionize practices of "business-as-usual." The study included hypothetical prop up of various studies publicized in top-ranked scientific journals in the past decade. It also included various accounts from grey literature as a way of rationalizing the appraisal and seizing the growing blockchain sector that is incorporated in this appraisal. It is from this structure that a strategic appraisal of thematic content appraisal of the literature uncovered shows a comprehensive categorization of applications that are blockchain-enabled across varied domains like enterprise, supply chain, medical care, enterprise, privacy, IoT, and management of data. The scholars delineate the key trends, themes, and emerging study areas. The study also denotes the limitations identified in the relevant literary texts, especially the limitations presented by the blockchain technology and the way such limitations spawn across varied industries.

In contrast, Scheau et al. (2020) conduct a meta-analysis that tries to inquire into the global activities linked to digital currencies as an aspect of the general occurrence and also lay bare several interlinks with cybercrime. The study insists that one of the primary attributes of digital currencies – total anonymity and pseudo-anonymity – can be viewed as a bridge to the domain of criminality, and cybercrime to be specific. Haken is a negotiating corporation that engages in the audit of blockchain structures and more in discovering fraud with various packages that cover a greater array of what a client wants. After appraisal, an outline of important value frauds linked to medieval and novel ICOs is publicized on the online column. Monero, being among them due to its dark web trades, utilizes a kind of cipher that in theory provides for 100% anonymity. The articles provide examples of cybercrimes where cryptocurrency was utilized as both a tool and target for cybercrime. This helps to depict that indeed the aspect of anonymity in cryptocurrencies sets a favorable climate for cybercrime to occur.

Conti et al. (2017) present a strategic survey that covers the privacy and security attributes of Bitcoin. The study delineates an overview of the Bitcoin protocol, its primary constituents and their interactions and functionality within the structure. Next, the scholars review the pre-existing vulnerabilities in Bitcoin and its root technologies like PoW and blockchain grounded consensus protocol. This vulnerability results in the execution of varied security threats to the customary bitcoin functionality. The article then delineates the robustness and feasibility of state of the art solutions in security. More importantly, the scholars examine the present anonymity and privacy-associated threats to those using bitcoins. They also include an appraisal of the pre-existing solution and ways to preserve the solutions. Virga (2015) provides a report that asserts that there is a robust need for global regulations of cryptocurrencies to prevent crime and fraud. Therefore, as it is, the article asserts that the privacy and anonymity features increase the susceptibility of cryptocurrencies being used as both a target and tool for crime. The article provides background information on the reason virtual currencies, particularly global regulation, are substantial. The scholar starts with a brief description of the types of virtual currencies and then delineates current law enforcement acts led by varied countries to close operations by utilizing virtual currencies to finance acts of crime. Finally, the article stresses that global regulation on cryptocurrencies is critical to curbing the continuing exploitation of the currencies in cybercrime.

In their article, Clouston, Hashofer, and Dupont (2019) present a data-driven approach for identifying and gathering data on transactions involving bitcoin associated with illicit acts on the grounds of footprints left on the blockchain of the popular Bitcoin. The researchers implement an approach on top of the GraphSense opensource platform and empirically examine transactions linked to 35 families of ransomware. The article approximates that the lower bound direct economic effect of every ransomware family and uncovers that, between 2013 and mid-2017, the ransomware payment markets has a minimum worth of 12,768,536 USD. The article also stresses that the market is expansively skewed, with just several players responsible for most of the payments. Based on these study outcomes, law enforcement agencies and policymakers can utilize the statistics outlined in the article to comprehend the magnitude of the illegal market and make informed resolutions on the best way to respond to the threat.

From the extensive studies discussed above, it is clear that cryptocurrencies and the continued thrive in cybercrime have been very critical. In the example of the U.S., the specific concern has been the utilization of cryptocurrencies in preventing sanctions. Some scholars have gone a step further to suggest that a task force encompassing agencies from State, Treasury, Defence, and Justice ought to be established to concentrate particularly on cryptography's blockchain system to trace transactions. A knowledge gap still exists as none of the surveys above has considered the extensive array of cyber-attacks in distinct classifications and their impacts on the peril-adjusted returns and volumes of cryptocurrencies trading and varied sectors in the cybersecurity presence. The study responds to all these aspects utilizing an appropriate empirical framework that generates informative novel results on the efficacy of cybersecurity and distinctions in the behavior of trading of Ethereum, Bitcoin, and Litecoin. The study also examines the minds of criminals behind bars for cryptocurrency-related cybercrimes and get the perspective of those organizations that have been victims of cybercrime for using cryptocurrency as the preferred mode of payment. The study is interested in examining whether the victim and the criminal consider the privacy and the anonymity aspect and the steering forces for using cryptocurrency as a tool and target for cybercrime.

Methods

There is a wide array of data regarding anonymity, cryptocurrency, and its link to cybercrime; very limited studies on cybercrime are in existence. The scarcity of studies on the subjects leaves a gap in comprehending the risk and security that come with the use of cryptocurrencies. The law enforcement agents and the intelligence community also lack enough knowledge of the criminal's mind in this aspect to be able to offer guidance on the matter. This limited information gives criminals and hackers an opportunity for circumventing authorities and later attacking and stealing personal and classified data.

Therefore, this multidimensional, descriptive survey aims to determine if or not anonymity as an attribute of cryptocurrency impact the acts of individuals while using the internet. The study provides grounds to start to comprehend if an individual given a chance to stay anonymous and resources to participate in acts of crime would engage in crime, varying from personal Identifiable Information (PII) purchasing to drug or illicit downloading. The survey assists in revealing these acts that are linked with anonymity.

Methodology

This observational and qualitative (multifaceted) survey utilizes primary data gathered by the researchers to rule out any link between cybercrime, anonymity, and cryptocurrency. Data collection is dependent on both primary and secondary data. The primary data were obtained from the study participants, while secondary data is gathered from reliable websites. The survey was disseminated via email, and Zoom was used to hold interviews with technical respondents. The study encompasses semi-structured interview questions and closed and open-ended questions for the survey. Participants were requested to take about 10 to 15

minutes to complete the survey. To make sure participants responded to the questions honestly, the participants were informed that no personally identifiable data would be gathered and that all the answers for the study would stay anonymous. The participants were sent the questionnaire via mail, and the survey would run for 60 days from June 1, 2021, to July 31, 2021, to give room for participants to respond to the questions and manage to reach 85% of the study sample. Once all the data had been collected, it was cleaned so that it would leave room for coding and data analysis.

The main study was preceded by a pilot survey which is a small-scale trail run of all the steps scheduled to be used in the main study inquiry. It helped in establishing a core aspect of the research process. It involved the pretesting of the research tool by administering it to a smaller number of individuals who have similar characteristics to the target population. It assists the scholar in fine-tuning the study for the main inquiry and it utilizes similar subjects as the ones in the final study. It is for this rationale that the research instrument was used, the semi-structured interviews, and the survey questionnaire was pilot tested. The pilot testing of the instrument was deemed necessary to assist in enhancing the data collecting tools' quality and to make sure that the content in the questionnaire was clear. The pilot study encompassed I.T. experts, criminologists who have handled cybercrimes, an anonymous representative from an organization that has endured cybercrime, and several students. The pilot study questionnaire was modified or adapted to meet the needs of the data sought. The pilot study assisted in enhancing the order of the questions, filter the layout of the questionnaire and the questions used. Data collected from the pilot study sample – in addition to fine-tuning the instruments used in the main study – also cleared my perception of people's outlook on the issue of cryptocurrency, cybercrime, and the attribute of anonymity. The questionnaire was administered to 20 respondents. The technical respondents (I.T. Expert and Criminologist), through zoom, responded to the semi-structured interview questions, and the rest of the respondents filled in the open and close-ended questionnaire.

Data Analysis

The researcher would start with the extraction of descriptive statistics from the data collected with the inclusion of standard deviation and average. The demographics descriptive statistics were gathered and statistics on the awareness and utilization of cryptocurrency in respondents. A Likert Scale was utilized in measuring the degree of agreement with stipulated close-ended questions by availing responses of 1= being strongly disagreed and 5 = strongly agree. A neutral choice was permitted for respondents with indecision or uncertainty. Other queries were permitted for participants to answer no/yes or assess all that apply. The open-ended questions were clustered together, and themes derived from responding to research questions. Return log was used in the analysis of secondary data. Descriptive statistics include frequency distributions and averages. Group comparisons fell under the normal variables and were accomplished with the help of the chi-square test for determining the extant association in contingency tables. Microsoft Excel was used in undertaking the data analysis; a 0.05 alpha level was utilized as the significance standard.

Although the pilot study was used as a critical prerequisite primarily aimed at examining the feasibility of the generated information, the information generated can be incorporated into the main study. One of the aims of the qualitative constituent of this study is to determine whether the anonymity attribute in cryptocurrencies is responsible for increasing a criminal's or individual's ability to commit a cybercrime. The researchers began by debriefing the participants on the aim of the study and getting them to sign a consent form as proof that they were taking part in the survey voluntarily. The consent form also made it clear to the client that they were allowed to discontinue the study at any point they no longer desired to continue with it.

The pilot study focused on the following research questions:

1. What is your definition of cryptocurrencies?
2. What is your definition of cybercrime?
3. Would you say that cryptocurrencies have an anonymity attribute?
4. Since the introduction of cryptocurrencies, has there been an increase in cases of cybercrime?
5. Are most of the cybercrimes reported recently directly linked to cryptocurrencies?
6. What are some of the cybercrimes mostly linked to cryptocurrencies?
7. Given a chance would you engage in cybercrime, where cryptocurrencies are involved now that the probability of being caught is reduced?
8. Do you believe that state regulation of cryptocurrencies is necessary to lower the threat of cybercrime?

While analysing the information gathered from the pilot study, the researchers were cautious of the limitations that come with utilizing a questionnaire, especially when it is individually filled and via the internet. One such limitation is not being truthful. This encompasses participants deliberately giving inaccurate responses, either to paint a largely negative picture of the situation or to please the researcher. Either way, the pilot study provided an opportunity to gather some critical information concerning cybercrime and cryptocurrencies.

Results

The 20 participants completed the pilot study for the research. More than half (55%) of the participants were male while 45% were female. The students who participated cut across the psychology, computer science, and education disciplines while the rest of the participants were in the workforce (law enforcement, IT expert, and employees in organizations). Most (90%) of the respondents could provide an accurate definition of cryptocurrencies and went ahead to give examples like Bitcoin. Most (92%) of the participants could accurately define cybercrime. However, when it came to the question of whether they believed that cryptocurrencies have an anonymity attribute, only 75% of the participants affirmed this statement. Few (10%) of the respondents were not sure while 15% said no. This brings out the perception that not everyone is aware that cryptocurrencies are largely anonymous which increases its preference as a tool for exchange.

Consequently, 80% of the respondents affirmed that since the introduction of cryptocurrencies, the rate of cybercrime has significantly risen. However, they went on to insist that this was not necessarily a result of the cryptocurrencies but largely because of the digital disruption. Most of the technical experts insisted that cryptocurrencies were introduced in an era of digitization which hinders and counters efforts put in place to nub the offenders. Once the offenders realize that law enforcement agents are utilizing blockchain analysis to numb them, they evolve to make the process even harder. This retaliates the assertion by Reddy and Minnar that the offenders' methods evolve once their old channel is deciphered. For instance, after the Darknode Forum was shut down, the primary purpose of the Darknode service was soon updated and reactivated, featuring the proponents of the blockchain for the main aim of making sure that users were not law enforcement agents. The creation of the Darknode and its recreation in a manner that more sophisticated precisely depicts that criminal will always get methods of countering internet security controls, and that is one of the primary challenges that investigative authorities, regulators, and cybersecurity specialists keep on encountering while attempting to curb cybercrime (Reddy and Minnaar 2018, p.76).

Half (50%) of the respondents agreed that the recent cases of cybercrimes are directly linked to cryptocurrencies, 25% were not sure, while 25% clearly stated that there was no direct link. However, they went on to state that cryptocurrency is being used as a tool to facilitate cybercrime which depicts their agreement on the danger posed by cryptocurrencies. Many (87%) of the participants were able to list some of the cybercrimes directly linked to cryptocurrencies and they included phishing (Bossler & Berenblum 2019, p.497), hacking, ransomware, group contribution, and money-laundering. However, when asked whether given the assurance that the aspect of anonymity in cryptocurrencies would protect them from being caught, if they would engage in cybercrimes, most of the respondents responded not sure. This means that when probed it would have either been a yes or no and this was not possible with the respondents filing their questionnaires. This means that in the main study there is a need to revamp wording or add a probing question to get better resonates on the matter. However, people enjoy anonymity because it puts them at free will to do as they please with the reduced probability of getting apprehended. Lastly, when asked whether state regulation was necessary to curb the vice, the technical experts were in full support of the measure while the rest of the respondents (50%) said not sure. This made it hard to decide whether or not to make it a recommendation or reword the question in the main study to ensure the respondents feel free to clearly articulate their thoughts.

Discussion

The pilot study widely depicts that the utilization of cryptocurrency lies in the facilitation of varied cybercrimes that utilize cryptocurrency exchange blockchain technology (transactions anonymity) and many more cyber - vulnerabilities in the process. It is evident from the study that a link does indeed exist between cryptocurrencies and cybercrime. Cryptocurrencies use blockchain technology that enables anonymity, which makes it an ideal tool for cybercrime and becomes an attractive tool for cybercriminals. The pilot study lays the foundation that will be

built on in the main study and depicts the gaps in the literature that the main study ought to fill to contribute to the field of study. Moreover, the literature review in the pilot study denotes research methods that previous scholars have utilized while conducting the study that the researcher can also use to gather the data required to respond to the study question or improve on the research method to avoid limitations that the scholars encountered while conducting their studies.

Conclusion

The findings of the pilot study suggest that there is a need for more robust cybersecurity. More robust cybersecurity is primarily efficient in increasing the risk-adjusted returns of cryptocurrencies which is the main study interested in studying and trading activities even when cyber-attacks are present. Hacking seems to be the leading threat for cryptocurrency investors. Moreover, cyber-attackers targeting cryptocurrency exchanges have a high probability of attacking other sectors like industry, government, and finance. It is from this information managed to pick the sectors to be studied when it comes to gathering the secondary data. The pilot study sets the variables and measures to be studied in the main study. For instance, the scholar realizes that yes, no, and not sure did not give a determinative figure and there was need to replace with more distinct values like strongly agree, agree, neutral, disagree, and strongly disagree. More importantly, the study depicts pitfalls that the researcher may encounter when gathering primary and secondary data and stipulating the measures available to the researcher to overcome the limitations. Additionally, by reviewing the literature, the researcher is aware of probable outcomes and data collection and analytical tools that have effectively collected and analyzed data. More importantly, the study provides guidelines on ethical considerations when dealing with human participants and sampling methods that can be used to target the preferred study sample. Hence, the pilot study will help to shape the main study.

Limitations and Future Studies

The pilot study depicts that this is a novel topic where very limited research has been completed by this moment. Additional studies ought to encompass the deviant history of persons as this may be a better predictor of future illicit activity or cybercrimes. The scholars of the reviewed studies recommend that future studies in the field ought to concentrate on distinct regions within the U.S. in addition to socio-economic classes. Further surveys should concentrate on the use of cryptocurrencies themselves and what is getting bought will all virtual currency. The scholars recommend that further studies in the field attempt to explore the dark web and discover the goods and services that can be purchased and how cryptocurrency criminal proceeds are transacted. The currencies are laundered on the site.

References

Baron, J., O'Mahony, A., Manheim, D., and Dion-Schwarz, C. (2015). National Security Implications of Virtual Currency: Examining the Potential for Non-State Actor Deployment. Santa Monica: RAND Corporation.

Benjamin, V., Valacich, J., and Chen, H. (2019). DICE-E: a framework for conducting Darknet identification, collection, evaluation with ethics. MIS Quarterly, 1 - 22.

Bossler, A. M., and Berenblum, T. (2019). Introduction: New directions in cybercrime research. Journal of Crime and Justice, 495 - 499.

Bouveret, A. (2018). Cyber risk for the financial sector: a framework for quantitative assessment. IMF Working Paper no. 18/143.

Caporale, G. M., young, K. W., Spagnolo, F., and Spagnolo, N. (2019). Non-Linearities, Cyber Attacks, and Cryptocurrencies. Finance Research Letters.

Casino, F., Dasaklis, T. K., and Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification, and open issues. Telematics and Informatics, 55 - 81.

Chu, J., Yuanyuan, Z., and Stephen, C. (2019). The Adaptive Market Hypothesis in the High-Frequency Cryptocurrency Market. International Review of Financial Analysis, 221 - 231.

Clouston, M. P., Hashofer, B., and Dupont, B. (2019). Ransomware Payments in the Bitcoin Ecosystem. Journal of Cybersecurity, 1 - 11.

Conti, M., E., S. K., Lal, C., and Ruj, S. (2017). A Survey on Security and Privacy Issues of Bitcoin. Arxiv, 1 - 36.

Corbet, S., Charles, L., and Lucey, B. (2020). The Contagion Effects of the COVID-19 Pandemic: Evidence from Gold and Cryptocurrencies. Finance Research Letters.

Corbet, S., Cumming, D. J., Lucey, B. M., and Maurice, P. (2019). The Destablishing Effects of Cryptocurrency Cyber criminality. Economics Letters, 191.

European Central Bank. (2012). Virtual Currency Schemes: 2012. Retrieved June 5, 2021, from European Central Bank: https://www.researchgate.net/deref/http%3A%2F%2Fwww.ecb.europa.eu%3Avirtualcurrencyschemes2012en.pdf

European Central Bank. (2015). Virtual currency schemes: A further analysis. Retrieved June 5, 2021, from ECB: https://www.researchgate.net/deref/https%3A%2F%2Fwww.ecb.europa.eu%2Fpub%2Fpdf%2Fother%2Fvirtualcurrencyschemesen.pdf

Financial Action Task Force (FATF). (2014). Virtual currencies: Key definitions and potential AML/CFT risks (S.I.): FInancial Action Task Force. Retrieved June 5, 2021, from Financial Action Task Force (FATF): https://www.researchgate.net/deref/http%3A%2F%2Fwww.fatf-

gafi.org%2Fmedia%2Ffatf%2Fdocuments%2Freports%2FVirtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

Gans, J., and Halaburda, H. (2013). Some economics of private digital currency. Bank of Canada, Working Paper. Retrieved June 5, 2021, from Bank of Canada: https://www.researchgate.net/deref/http%3A%2F%2Fwww.bankofcanada.ca%2Fwp-content%2Fuploads%2F2013%2F11%2Fwp2013-38.pdf

Graham, L. (2017). Cybercrime costs the global economy $450 billion: CEO. CNBC.

Grobys, K., Ahmed, S., and Sapkota, N. (2019). Technical Trading Rules in the Cryptocurrency Market. Finance Research Letters.

Guglielmo Maria Caporale, W.-Y. K. (2020). Cyber-Attacks, Cryptocurrencies, and Cyber Security. CESifo Working Papers, 1 - 52.

Koerhuis, W., Tahar, K., and Nhien-An, L.-K. (2019). Forensic Analysis of Privacy-Oriented Cryptocurrencies. Forensic Science International: Digital Investigation.

Kopp, E., Kaffenberger, L., and Wilson, C. (2017). Cyber risk, market failures, and financial stability. IMF Working Paper no. 17/185.

Matthews, O. (2017, September 18). Bitcoin and Blockchain: A Russian Money Laundering Bonanza? Newsweek.

Mieghem, V. V., and Pouwelse, J. (2015). Anonymous online purchase with exhaustive operational security. Arxiv.

Reddy, E., and Minnaar, A. (2018). Cryptocurrency: A Tool and Target for Cybercrime. Southern African Journal of Criminology, 71 - 92.

Scheau, M. C., Craciunescu, S. L., Brici, I., and Achim, M. V. (2020). A Cryptocurrency Spectrum Short Analysis. Journal of Risk and Financial Management, 1 - 16.

Tsyvinski, A., and Liu, Y. (2018). Risks and returns of cryptocurrency. NBER Working Paper No. 24877, 1 - 25.

Virga, O. M. (2015). International Criminals and their Virtual Currencies: the Need for an International Effort in the Regulation of Virtual currencies and combating Cyber Crime. Criminosos Internacionais e as suas Moedas, 1 - 16.

Xu, Q., Yixuan, Z., and Ziyang, Z. (2019). Tail-Risk Spillovers in Cryptocurrency Markets. Finance Research Letters.