ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 4, No. 2, 402-412 (2019)

www.astesj.com

ASTESJ

ISSN: 2415-6698

Behavioral Analysis of Bitcoin Users on Illegal Transactions

Zuha Samsudeen, Dhanushka Perera, Mgnas Fernando*

University of Colombo School of Computing, 00700, Sri Lanka

ARTICLE INFO

Article history:
Received:19 February, 2019
Accepted:09 April, 2019
Online: 26 April, 2019

Keywords:
Analysis
Behavior
Bitcoin
Blockchain
Illegal

ABSTRACT

Bitcoin is a popular crypto currency that is used as a mode of investment and a medium for trading goods and services. Anonymity, security and decentralization are significant features of Bitcoin. This creates several opportunities for criminals to involve in illegal and fraudulent activities. This research study aimed to automate the process of gaining the interconnected illegal transactions from Bitcoin Blockchain; which also identified the behavioral patterns and significant facts among illegal incidents that are of varied nature.

The motivation for choosing this study was lack of literature that covers illegal incidents that are of various natures. In addition, the lack of literature on spending patterns common to several illegal incidents is also one of the motivations. For this study, an inductive approach was carried out. Initially the illegal incident and transaction data extracted from publicly available sources were parsed into BlockSci. In BlockSci scripts were written to gain the details on related illegal incidents. In visualizing the relationship of derived interconnected transaction indexes, Gephi tool was used in which the most significant indexes were summarized for further interpretation of data. Thereafter, traversing data back in the Blockchain was the method used in deriving patterns and significant facts. Finally, the common patterns obtained were evaluated based on previous findings. Consequently, the study recognized common spending patterns and popular exchanges used.

1. Introduction

Many crypto currencies have come into usage in recent years for multiple purposes. Bitcoin developed by Satoshi Nakamoto came into usage from 2009 [1] and it is the most prominent crypto currency in terms of market capitalization with $250 billion as of January 2018 [2]. Bitcoin is discussed mostly based on its negative aspect [3] since Bitcoin systems are being targeted by hackers and fraudsters [4] thus making it easy to compromise [3, 4]. Among the negative discussion, aspects such as darknet marketplaces [5, 6, 7], Ponzi scheme [8, 9, 10], ransomware [11, 12, 13], Bitcoin Exploits [10, 14], Denial-Of-Service (DOS) attack [15], thefts [14, 16] and Money Laundering [9, 17, 18] have been discussed widely by previous researches and media. These negative aspects can be briefed as illegal activities.

The literature reveals in detail about illegal activities separately based on its nature or as a case study focusing on a single incident. According to careful investigation of the literature, it reveals that there is no or evidences have not been documented properly by analyzing several illegal incidents as a study. Thereby, this study focuses on providing an analysis of different illegal incident categories by highlighting user transactions behavior in dissimilar natured incidents as depicted in Figure. 1. The curves among incidents represent any possible patterns among incidents of dissimilar nature.

This study is important to provide a more comprehensive idea about real-world user behavior of those who involve in illegal transactions which is a real-world requirement. It will specify the view of the relationship among incidents of different nature. In addition, it will mainly assist Bitcoin Miners or protocol designers to make changes in protocol to reduce the illegal activities. In addition, it would assist relevant officials to impose new rules and controls on Bitcoin exchanges or services, Bitcoin users and potential Bitcoin users will become aware of illegal incidents and how related each incident are to another.

The goal of the study is to provide a behavioral analysis of Bitcoin users involving in illegal incidents that are varied in nature.

* Mgnas Fernando, University of Colombo School of Computing,00700, Sri Lanka | Email: nas@ucsc.cmb.ac.lk

The main question to be addressed is 'What are the behavioral patterns among Bitcoin users involving in different types of illegal incidents?' by answering sub-questions such as 'What are the illegal incidents involving Bitcoin and how they can be categorized into various categories?', 'What are the significant facts for each illegal incident?'.

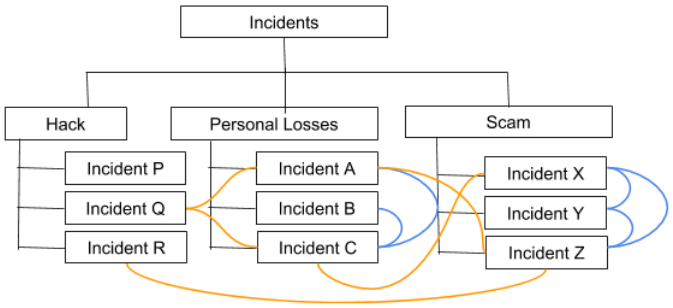

Figure. 1: An example of analysis considering different types of illegal incidents

2. Background

Bitcoin is the crypto currency that works based on the principle of a public ledger called Blockchain [2] which provides security using Blockchain technology [14]. Each Block in Blockchain consists of Bitcoin transactions [1] and information about transactions is publicly visible. The blocks in the Blockchain can be uniquely identified by the block hash or the block height. The Merkle Tree is the data structure which is used to summarize all the Bitcoin transactions in the block [19]. The processing of transactions involves solving a computation problem to put the transactions included in a confirmed block to be included in Blockchain. This is called mining [20]. The transactions between users are registered, validated and maintained via the entire network which is called Bitcoin mining.

The usage of Bitcoin became substantial due to the various reasons such as speed [21], anonymity, security, convenience [22] and decentralization with less transaction cost as there is no middle party involved to control the Bitcoin in comparison to traditional payment methods [1]. But [14] critiques that while Bitcoin exist as a decentralized system; it requires a formal structure, rules and a proper line of communication for better management. But still, Bitcoin is lack of legal interpretation in the Bitcoin user community and Bitcoin exchanges. In addition, there is no coordination among the Bitcoin Exchanges as well [14]. Regardless of several criticisms and concerns on the legality of Bitcoin, currently not only online businesses, but also traditional retailers are also beginning to accept Bitcoins as a payment method [22]. However, Bitcoins have their own risks such as major exchange rate fluctuations and hacking of major Bitcoin exchanges [13].

Bitcoin payments or transfers are carried out by generating transactions. Bitcoin addresses are used in performing transactions [23]. A user generally has hundreds of different Bitcoin addresses which are usually stored in their digital Bitcoin wallet [22, 24]. The addresses that are used only once are termed as disposable addresses. Bitcoin addresses can be reused as well [25]. But, reusing Bitcoin address is traceable because the flow of Bitcoin can be traced from one known or unknown address to another [12] leading to privacy leaks. Therefore, Bitcoin community and previous researches has encouraged using a different Bitcoin address for every transaction [25]. However, if users use strategies such as CoinJoin [12, 25] or Mixing Services or tumblers [12], it is difficult to trace by identifying Bitcoin addresses accordingly. A Bitcoin transaction happens in the form of an input or set of inputs pointing to an output or set of outputs [25]. The total values of the inputs must be distributed to the output. In Bitcoin Blockchain, for a transaction to be valid the total value of the outputs should not exceed the total value of the inputs.

2.1. Bitcoin Exchanges

A Bitcoin exchange is an online platform where anybody can buy and sell Bitcoins using fiat currencies. Some of the exchanges behave like a bank where they offer fixed interest on the customer savings. The exchange creates a wallet for every customer in their system and one can sell or buy Bitcoins with this wallet [20]. But, major risk of hacking Bitcoin exchanges still prevails [13]. However, [14] concludes on recommending exchanges to clearly disclose all the details of the cyber-attacks on them to their customers. Thus, leading to better transparency in the way they operate. Some of the instances for the major attack on exchanges were Mt. Gox attack losing 450 million dollars, attack on Bitfinex exchange leading to reduction in value of Bitcoin by 23% and DDoS attack on Bitfinex and Bitcoin-e Exchanges [14], Bitfloor loss of 24,000 Bitcoins in an attack [20].

2.2. Illegal Activities

The illegal activities related to Bitcoin cover a wide range of crimes such as murders for hire, funding terrorism, drug, weapon, organ trafficking, ponzi schemes, forgeries, unlawful gambling, money laundering, illegal mining, computer hacking, spreading ransomware and outright theft [2, 6, 26].

At least 25% of Bitcoin users and around 44% of Bitcoin transactions are associated mainly with illegal activities as previous researches shows [5]. It is discovered there are 24 million Bitcoin users; use Bitcoin primarily for illegal purposes [5]. Another research [2] said that exactly half of Bitcoin transactions are illegal. However, a study mentioned that Bitcoin will become less used in illegal activities in future as it will be accepted as a common medium in near future since the need for exchanges will be reduced to a certain extent. A recent study [2] reveals that the illegal users tend to transact more in smaller amounts repeatedly with a certain party to avoid getting noticed. In addition, it is noted that the illegal users are holding less Bitcoin due to Bitcoin seizure incidents by FBI [2]. As [5] highlight that the users who are spending Bitcoin on illegal goods had about 25%-45% more Bitcoin (with the 95% confidence interval) than those who doesn't spend Bitcoin on illegal goods [5].

Therefore, it is timely needed to have a look on the illegal activities. Following is a literature review on some major illegal activities which involves Bitcoin.

- *Ransomware*

  Ransomware are similar to other computer virus such as trojan horse, worms and spyware [27, 28] and it is defined as the emergence of cyber hack jacking threat in new form in the cyberspace. Ransomware has become a significant problem

[13] due to its rapid growth in global level [29]. In [30], it mentions one of the main reasons for the growth of ransomware is due to the increasing ease of use of Bitcoin systems for payment purposes. In addition, for example CryptoLocker [11], according to [31], there is an existence of connections between CryptoLocker to Bitcoin services namely Bitcoin Fog and BTC-e, and to the Sheep Marketplace scam happened in 2013. A pattern that has been already revealed is that most ransomware related transactions occur multiple times with the same party and Xapo.com, BTC-e.com, LocalBitcoin.com and Kraken.com are frequently used Bitcoin exchanges. Also, Helix Mixer has been used in purifying tainted coins. A notable finding indicates that some ransomware attackers directly sent the ransom payments received to known parties such as exchange services and gambling [12].

- *Theft*

Over one-third (⅓) of money in the Bitcoin system was lost [14] due to Bitcoin being vulnerable to software hacks and network-based attacks [3]. These attacks are commonly termed as Cyber-Attacks referring to any action that violates the security of the exchange system. Cyber-attacks on Bitcoin wallets can be due to security flaws in system, mistakes of Bitcoin users such as negligence or ignorance and a Denial of Service (DoS) attack [14]. The patterns that have been identified so far related to DOS are; sending Bitcoins in tiny amounts to the same set of addresses and transaction rate attack forming the parasitic worm structures [32]. The studies [3, 8] highlighted that the transactions are not reversible. It is an advantage for criminals because it is impossible to correct errors occurred due to a theft. Thus, allowing funds being stolen or taking without the permission of Bitcoin owners [8].

- *Scam*

Scams based on Bitcoin can be classified into mainly four groups such as high yield investment programs or ponzi scheme, mining investment scams, wallet scams and exchanges scams according to a classification identified by studying 192 scam incidents [10].

- *Darknet*

Darknet refers to a network that is encrypted and existing on internet which can be accessed only by using special browsers [7]. The research [33] proves 57% of content in darknet is illegal, whereas 47% of all Bitcoin transactions involve illegal trading on darknet [2]. So the deeper layers; deep web, dark web and darknet are mainly with the illegal content [33].

As per study of [7], Ross Ulbricht the main operator of Silk Road was traced down and seized by FBI in October 2013. In addition, after the closure, as [7] mention, Silk Road 2.0 emerged, following the darknet marketplaces such as 'The evolution' evolved quickly where in some cases the operators disappeared along with Bitcoins held in escrow.

In studies of [14] and [34], authors highlight that mainly anonymity of Bitcoin transactions give criminals as an enabler tool to operate without getting noticed by legal authorities. Even though numerous real-world incidents prove some criminals use only Bitcoin to conduct illegal activities, [6] says the same will be applicable even for cash transactions conducted using fiat currencies indicating less necessity to implement additional rules and regulations especially for Bitcoin.

2.3. Tainted Coins

Tainted are Bitcoins which has involved in some sort of crime [35]. If a Bitcoin address is tainted, it is visible across the network. This is due to the digital signature mechanism in Bitcoin. The publicly available transaction history can be used to examine how a tainted Bitcoin behave in the network [36]. When a Bitcoin user receive Bitcoins from a sender, the Bitcoin user can check whether the receiving Bitcoins has involved in fraudulent activity in past. Thereafter, determine whether to continue the transaction with accepting Bitcoin or not [35]. An example would be Mt. Gox, a Bitcoin exchange based in Japan locked Bitcoin holder's account with tainted coins after an incident of theft where 43,000 Bitcoins were robbed from another Bitcoin trading platform Bitcoinica [36].

According to [4] the more 'tainted' the chain of transactions is, the stronger the link in between the Bitcoin addresses is. For example, if a wallet is stolen, whenever the robber tries to bank the money at an exchange, they can be arrested as [37] pointed out.

3. Methodology

3.1. Research Design

The research design shows the important stages followed to answer the research problem (Figure. 2). Each block in Figure. 2 represent a main stage in addressing the research problem.

This is a summary how the research was carried out. The incident data was extracted from publicly available data sources whereas transaction data was from the Bitcoin Blockchain. Definition of illegal incident based upon incident data extracted was helpful to categorize the incidents.

During the process of resource setting, Blockchain data was parsed into BlockSci which was imported into Jupyter to run python scripts. The scripts included filtering of non coinjoin incident transactions using heuristic parameter, gaining transaction data using chain classes in BlockSci, gaining significant index details using address classes in BlockSci. Thereafter, through traversing back in the Blockchain the initial data derived from Blockchain was verified. To visualize the data, Gephi was used along with various metrics. The most significant indexes were then summarized for further interpretation of data using Address classes in BlockSci which consisted of addresses and address types. Traversing data back in the Blockchain was the method used in deriving patterns and significant facts. Finally, some of the patterns obtained were evaluated based on previous findings. In addition, new findings were evaluated using user feedback obtained via a survey and some test cases. Let's look at on detailed description on stages.

3.2. *Resource Set Up*

The following configurations made the analysis easier: A Cloud Virtual Machine with the specifications of (i) Ubuntu 18.04

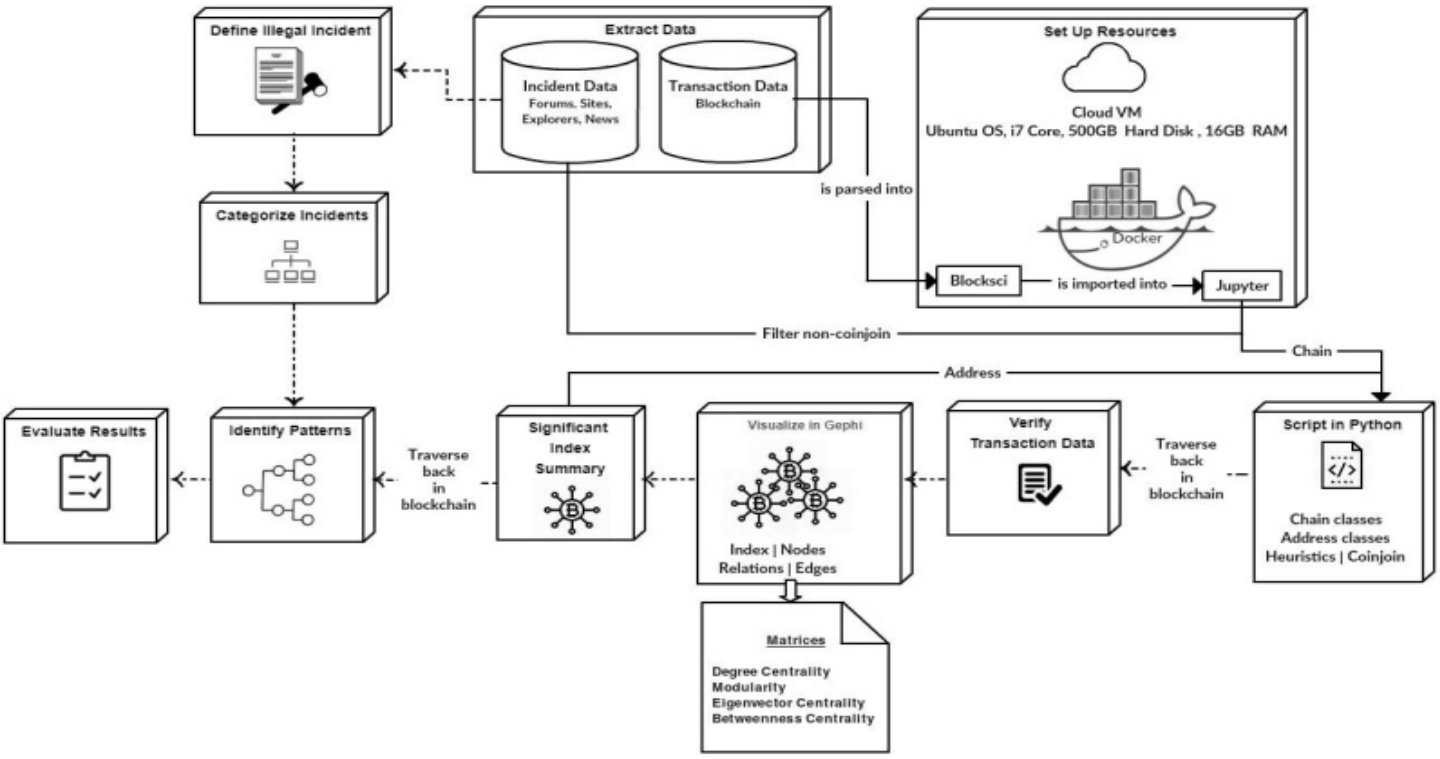

Figure. 2: Research design

LTS Server Version as the Operating System (OS), (ii) i7 as core processor, (iii) 500GB as Hard Disk, (iv) 16GB as RAM and (v) Docker as the OS level virtualization, (vi) Blocksci as Blockchain analysis tool, (vii) Jupyter as Notebook, (viii) Gephi as visualization tool.

3.3. Blocksci

BlockSci is a tool developed with the intention of analyzing the transactions of Bitcoin in Blockchain [38] which was in use at Princeton for research and educational purposes [39]. According to a research paper [40], BlockSci library has used to analyze the Bitcoin Blockchain from 2009 till August in 2017. To examine how the Bitcoin usage has grown over time by the original developer of the tool and to identify whether there is a diverse community present and thereon to investigate whether they differ in important factors. Accordingly, this research study was carried out using the Blocksci tool by parsing transaction data inside it.

3.4. Data Extraction and Pre-processing

Since the Bitcoin Blockchain is decentralized, no authorized party is responsible for reporting illegal endeavors involving bitcoin. So, the publicly available data is the sole data source from where the details of illegal incidents can be obtained. Initially the details such as Incident Name, Date, Value (USD), Coins (Bitcoin), Transaction Id, Bitcoin Address, Nature /Description of Incident, Countermeasures were collected from public data sources via surfing through internet. Among those collected incidents, from 2012 to 2018[1], there were 33 illegal incidents that were available with respective 331 transaction ids which were mandatory in uniquely identifying the incidents. The data for the period from 2012 to 2014 was extracted mostly from publicly available forum called Bitcointalk and prepared to a homogeneous format in an Excel sheet manually. Online forums Bitcointalk, discussion websites, Reddit in [10, 41], blogs, Bitcoinwhoswho Bitcoin Blockchain explorer, Walletexplorer in[12] and additional sites coindesk.com, bleepingcomputer.com in [11] were used to extract data which are mentioned in several previous types of researches and completed the majority of data for the period from 2015 to 2018. Finally, all collected data was cross-checked with multiple sources that were available publicly and confirmed the reliability of data.

Along with that on parallel, Blockchain[2] up to the block height of 514463 (157.3GB as at March 2018) was downloaded to gain internal transaction data related to illegal incidents like input index, output index and unspent index.

3.5. Definition of Illegal Incident

Based on the details of illegal incidents and previous studies, a definition for illegal activity was formulated. It is defined for illegal incident categorization.

"Any activity that involves Bitcoin which brings a financial disadvantage to one or more parties with or without their knowledge while the opposite party gains benefits financially from its outcome with their knowledge is defined as an illegal incident".

[1] https://docs.google.com/spreadsheets/d/1fOUIA9J4-lJKhgXqh2_zH6__t1BBRjaPMExH3GeFi6w/edit?usp=sharing

[2] https://www.blockchain.com/explorer

3.6. Incident Categorization

The incidents those were defined as illegal were categorized into different sub categories based on the nature of incidents referring to the basic categorization of heists in Bitcointalk till 2014 and with further reading on incidents.

3.6. 1. Hack - Wallets owned to an exchange or a platform is hacked by outsiders led to the collapse of the exchange.

3.6.2. Ransomware - Malware is spread to lock or encrypt the database, files, PC or any electronic copy and demand ransoms in Bitcoin to enable access.

3.6.3. Known Theft - Bitcoin holder knowingly sends Bitcoin to criminal because of threatening or blackmail.

3.6.4. Scams - The exchange or the platform steal the users' wallet and disappear by closing their exchange.

3.6.5. Fake Agencies - Scammers pretend to be an already existing popular exchange or government organization and steal Bitcoin either by communicating with customers or pretending to be honest.

The Sub Categories were put into main categories to enable better analysis. It was based on how the financial loss was committed to the other party. That is, whether the dishonest party obtained an advantage by directly dealing with Bitcoin user or via being a third party and another fact considered is whether the Bitcoin user loss his Bitcoins with his knowledge or not.

3.6.6. Hack - Dishonest party comes in between the Bitcoin holder and the exchange as a third party and collapses the exchange. It causes harm to both the Bitcoin holder and exchange without their knowledge.

3.6.7. Personal Losses - Includes subcategories of 'Ransomware' and 'Known Theft' where the effect of the Bitcoin loss is solely for the individual or a group of Bitcoin users committed by a third party with victims' knowledge.

3.6.8. Scams - Includes subcategories of 'Scam' and 'Fake Agencies' where frauds are done by exchange or platform itself or by a scammer. Exchange would purposefully close by issuing a notice by falsely claiming that they were hacked. Sometimes the exchange would make their website unavailable either by issuing a notice or without issuing a notice. This would lead to the financial loss to the Bitcoin holders of that exchange without their knowledge.

The following Table 1 summarizes the main similarities and differences of Main Categories.

3.7. Main Scripts

The n-ary tree chart as in Figure 3 represents how transactions are interconnected and it led to try out scripts. For an example, in T2 169...Tig address sends 5 Bitcoins to 1DV...NQs address holding the transaction id 118du….2a8u7. In T3 1DV...NQs address sends 4.52809038 Bitcoins to 1Nc...ytD address holding the transaction id 7d5uc….5c2e1 and sends 1.28 Bitcoins to 1xt...vsn address holding the transaction id 1frtu….. ud2e1. Every output address can spend its Bitcoins like in T5, T6, T7 and T8 or else it can keep Bitcoins unspent as in T9 (Figure. 3).

Table 1: Summary of main categories

Main Category	***Sub Category/ies***	***Attacker***	***Victim***	***Knowingly happened?***
Hack	Hack	Third Party	Bitcoin Holder + Exchange	No
Personal Loss	Ransomware Known Theft	Third Party	Bitcoin Holder	Yes
Scam	Scam Fake Agencies	Exchange	Bitcoin Holder	No

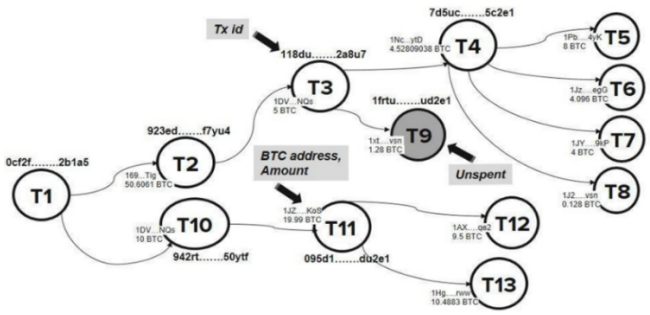

Figure. 3: N-ary tree chart for bitcoin transactions

The n-ary tree chart triggered to use recursion in the scripts to get chained transaction data. First the focus was on the circulation of the illegal input addresses and output addresses inputting illegal transaction ids. The results come out from the script were computationally expensive because these illegal transaction ids often result out ScriptHashAddress along with wrapped_addresses with different types of address requirements. One such example is represented in Table 2.

When a result was with a ScriptHashAddress, only the first address was needed. The rest was an additional security for the transaction. So as the next effort, it was considered to output related transaction ids. But still transaction ids resulted out 256-bit hash which had longer number of digits leading to slow up of results. So, the circulation of the input and output indexes was created as the solution. The index was a few digits number (lesser than 9 digits in this dataset). It was more convenient in terms of consumption of computing resources.

3.8. Data Processing

Pseudocode 1 was used to automate gaining related illegal input and output indexes after the data processing for a given transaction id.

Table 2. Different Address Types

	Output Address
Result Obtained	ScriptHashAddress(344...1Md[3], wrapped_address=MultisigAddress(2 of 4 multisig with addresses 13d...Vrc[4], 1Da...SbB[5], 1Gv...WbU[6], 18V...BAJ[7]))
Result Expected	344p...1Md (Recipient Address)

Pseudocode 1: Related illegal input and output indexes for a given transaction id

Input: Transaction id related to illegal incident; txid

Output: Related index details to a given txid; input index, output index, unspent index

01. Extract details from chain tx
02. Define results (tx)
03. If any tx has output:
04. for each output:
05. If any output is spent:
06. Write input index, output index
07. Do results recursively for every output
08. Else:
09. Return unspent index
10. Else:
11. Return unspent index

Each transaction id under main categories was input to the script. It resulted out the details i.e. input index and output index of the transaction undertaken or unspent index in a state of unspent.

The script extracted data from stored Blockchain transaction data considering the hash value for a given transaction id. Then the function 'results' was called. In this function, simply there was an initial selection construct identifying whether there were outputs i.e. whether the transaction was continued. If so, for those each output, script checked whether the resulting outputs of first if condition were also spent through the use of second if statement. If, then a file was appended with the details of input and output index pairs, according to the outcome of secondary condition of 'if'. Here, two selections were used to prevent the repetition of the records appended in the file while maintaining the connectivity of the transaction chain. Then the function was recursively called for each output index identified in both first and second selections. Recursion got terminated when the transaction had no more transaction relationship further as denoted in T9 as "Unspent" (Figure. 3). Approximately 1 million records on input-output indexes were obtained per each illegal transaction id. There was a variable number of transaction ids per incident considered in inserting into the script according to the availability of extracted transaction ids in dataset.

3.9. Transaction Data Verification

The output transaction data from the script was verified by traversing back in the Blockchain and sketching up an n-ary tree manually for the chain.

3.10. Data Visualization

Gephi[8] considered 'indexes' as the nodes, the 'relationships between indexes' as the edges and 'directed' as graph type. The noisy data was removed through filters considering the degree range under topology. The ForceAtlas 2 layout was chosen. It is a continuous graph layout algorithm suitable for handy network visualizations as recommended in study [32]. Fruchterman-Reingold layout improved the viewing and the perception of the network [42]. Thereon, metrics in statistics such as Degree Centrality, Modularity, Eigenvector Centrality and Betweenness Centrality were computed to obtain further insights [42, 43].

In the graphs, the Degree represents the number of direct or 'one hop' connections each index has to other indexes which also considered as illegal under Poison heuristics i.e. the related party are also considered as illegal meaning all the outputs are completely tainted by all illegal inputs. The size of the node denotes the strength of the connectivity meaning the total number of input and output indexes that is linked with. Modularity in the study measures how well the network decomposes into modular communities of illegal Bitcoin users. Eigenvector Centrality measures the importance of an index in terms of connectivity of other indexes. For instance, an index with high eigenvector score is connected to many indexes who themselves have high number of connections. Betweenness Centrality measures how often an index is required to go to another index. If an index is with a high betweenness, it often appears on shortest paths between indexes in the network. If the high betweenness indexes are removed, the graph may cut into multiple unconnected components losing the connectivity.

As a summary, these metrics demonstrated the connectivity of the illegal indexes i.e. degree and eigenvector score represent the number of direct and indirect connections respectively, modularity measures number of modular communities of illegal Bitcoin users, betweenness represents how an index is needed to maintain the connectivity. So, indexes scored higher for the above metrics were taken into consideration as the most significant indexes in the graph. Then corresponding Bitcoin addresses were output for those indexes through scripts and started investigation of those addresses in the Blockchain and obtained the results as explained in results section.

[3] 344pUP56enuGjbPdyubYEqoxB6VaFmD1Md
[4] 13dCNU7T38Ca3zp4mMBSmP6FGyBzq6vVrc
[5] 1DayuQZkBCt4MYYA5Hr8awXvmJDXLndSbB
[6] 1GvFkgaLV69PtrTcMC9XznqcXZxRHWvWbU
[7] 18VibwUc5CNG8TFZNRMSY6LMadED3qGBAJ
[8] https://gephi.org/

3.11. Justification for Methodology

The motivation for choosing this study was lack of literature that covers analysis for patterns and significant facts in patterns on illegal incidents of various nature. Since the inductive approaches usually focus on exploring new phenomena that have not been investigated or previously explored, it was best suited to this research. To identify new patterns based on the information, detailed data on each illegal incident was gathered and preliminary patterns from separate incidents were obtained first. Once the data analysis has been completed for each incident, generalized conclusions were produced based on the patterns and facts derived from the analyzed individual cases. It required extensive and repeated sifting through the data and analyzing and re-analyzing multiple times to identify new patterns.

However, the few patterns that were discovered so far in literature also got confirmed in this study. Since deduction begins with expected patterns (already defined patterns in prior researches in this study) and is able to test them against observations, this study is following deductive approach too. Thus, a combination of inductive and deductive approaches was practiced in this research study.

4. Results

In this study, 10 illegal incidents were analyzed thoroughly, and results were obtained. The results are shown below in incident wise along with its main category.

4.1. NiceHash / Hack

NiceHash, is a cryptocurrency mining marketplace. During the early December 2017, NiceHash has been hacked due to a security breach, causing a loss of 4,736.42 bitcoins[9] [46].

The analysis of results shows that the illegal party has been transferring in small amounts to new wallets and different addresses in subsequent transactions. Thereafter, subsequently Bitcoins are being sent out to an exchange or a service.

The Bitcoins have been distributed in a constant amount or by a percentage. For instance, 100 of Bitcoins are sent constantly whereas the rest to another wallet and to fresh wallets simply for transacting in small amounts.

4.2. Shapeshift.io / Hack

Shapeshift.io is a Switzerland based cryptocurrency exchange service that offers trading cryptocurrencies through its website and its API globally. On 7th April 2016, it faced a security breach which compromised on the server infrastructure of platform[10].

The analysis of results shows that the illegal party has been transferring in small amounts to new wallets and different addresses in subsequent transactions. Thereafter, subsequently Bitcoins are being sent out to an exchange or a service. The transactions traversed indicate that Bitcoin services such as Helix Mixer, Polenix.com and Bittrex have been used to cash out. In addition, one of the significant results is that next transaction that comes out from exchange has been made with the address 344...1Md[11] that has been tagged in 'Richest Bitcoin Address'. In addition, we can identify an address 1DU…. Uru[12] tagged as sixth richest on the Tether crypto list has also been involved in transaction traversal.

4.3. Gatecoin / Hack

Gatecoin is an exchange established in Hong Kong, mainly facilitating services for Bitcoin and Ethereum tokens. The hackers accessed the hot wallets of both Bitcoins and Ethereum stealing 250 Bitcoins and 185,000 ethers[13].

As per the analysis, a major portion of the immediately sent inputs is still unspent. Due to that reason, a clear insight on the tainted Bitcoin circulation cannot be obtained. However, the minor number of Bitcoins that were spent indicates that mostly Poloniex.com, OKCoin.com, Bter.com, Xapo.com have been used very commonly to cash out immediately.

4.4. WannaCry / Personal Losses

WannaCry Ransomware is a type of malicious software. According to statistics of this attack 300,000 computers including entities such as hospitals, companies, universities and government organization across 150 countries had a loss of hundreds of millions to billions of dollars [47].

The analysis of results shows that the illegal party has been transferring in small amounts to fresh wallets in subsequent transactions. Thereafter subsequently Bitcoins are being sent out to an exchange or a service.

In addition, the transaction traversal shows that there are few popular Bitcoin services that have been commonly used. They are Poloniex.com, Bittrex.com, HaoBTC.com, BTC-e.com, Xapo.com, CoinGaming.io and bitfinex.com.

Another notable result would be that there are addresses in their respective wallets have involved in conjoin transactions to mix their coins which is usually used to makes it harder for outside parties to determine which party or parties were making a particular transaction.

4.5. CryptorLocker / Personal Losses

CryptorLocker Ransomware started spreading since September 2013 that encrypted files and demanded ransom. This created almost USD 519,991 of direct financial impact. CryptoLocker opened the gates to many other ransomware variants [12].

In the study of the incident Cryptor Locker, it could be discovered that one single wallet has been used to obtain and transfer Bitcoins. Thereafter, gambling services such as SatoshiDice.com and LuckyB.it has been used to cash out. In addition, the results also indicate that an address 121...PM4[14] has obtained Bitcoins from Agora and Evolution darknet market and paid in the medium of Bitcoins to Agora market and Black bank

[9] https://bitcointalk.org/index.php?topic=2535366.0;all
[10] https://news.bitcoin.com/looting-fox-sabotage-shapeshift/
[11] 344pUP56enuGjbPdyubYEqoxB6VaFmD1Md
[12] 1DUb2YYbQA1jjaNYzVXLZ7ZioEhLXtbUru
[13] https://news.bitcoin.com/gatecoin-official-statement-hot-wallet-breach-losses-estimated-2m-usd/
[14] 121dBo5epQEDJZVpZDuBYBwV5Y2xeXTPM4

market. Thereby, it is possibly a wallet belonging to a darknet market supplier.

4.6. VenusLocker / Personal Losses

VenusLocker is a ransomware type virus which was spreader via an infectious email letter [47]. The analysis of results shows that the illegal party has been transferring in small amounts to fresh wallets in subsequent transactions. Thereafter subsequently Bitcoins are being sent out to an exchange or a service.

In addition, the transaction traversal shows that there are few popular Bitcoin services that have been commonly used. They are Poloniex.com, Luno.com, korbit.co.kr, Xapo.com and HelixMixer.

4.7. Blackmail / Personal Losses

Several people received different versions of emails claiming that the recipient's computer has been used to create a video of adult websites that the recipient visiting and threaten that it will be sent to recipients' contacts if they do not pay $200-$400 in BTC within 20-24 hours[15].

As per analysis, it can be noted that majority of the transactions have been performed directly through exchanges such as Poloniex.com, Matbea.com, Cubits.com. Among the blackmail incidents, it is significant that the Bitcoins are immediately cashed out via exchanges since the money received on blackmailing is not relatively a notable large Bitcoin amount.

4.8. BTGwallet.com / Scam

Bitcoin Gold (BTG) is one of the forks of Bitcoin which was released on 24th October 2017 [16]. MyBTGwallet.com is an online wallet creator that only stores data on the browser. This website cheated investors out of $3.3 million in November 2017 by promising to allow them to claim their Bitcoin Gold[17].

The analysis of results shows that the illegal party has been transferring in small amounts to fresh wallets in subsequent transactions. Thereafter subsequently Bitcoins are being sent out to an exchange or a service. The results of transaction traversal show that, there are few popular exchanges such as Bittrex and Bitflyer.jp that are involved in the transactions. In addition, the results highlight that there have been continuous transactions from the exchange 'hitbtc.com' to another address 3Jj...4FC [18] belonging to wallet [457b8ced80]. From further analysis, it was evident that this is another incident where a malware was installed in Hitbtc website which automatically changed the Bitcoin addresses of users to another address when an address was copied from Hitbtc.com.

4.9. Fake Agency Support / Scam

This includes a Coinbase support phone scam where a phone number '1-888-455-1155' which is not a real Coinbase support number were shown up in a lot of web search results. When users search in Google typing "coinbase phone support" they obtained a phone number from Google search results that leads them to this scam in which an operator tells them to send money in Bitcoin[19] .

The analysis reveals that the transactions have been performed directly through exchanges such as Cex.io, Luno.com and Bittrex.

4.10. Alphabay / Scam

AlphaBay Market operated in Thailand was an online darknet market which was launched in December 2014. It operated under an escrow system which paved the way for the scam. Alpha Bay went offline due to a scam with 1,479 Bitcoins transferred from a Bitcoin wallet which were identified to be used by those behind the darknet site to other Bitcoin wallets. During that period, there are numerous orders pending in its escrow system. It was shut down by 13th July 2017 [20].

The analysis reveals that the transactions have been performed directly through exchanges such as Bitstamp.net, Xapo.com, Bitfinex.com

Accordingly, the analysis reveals that the incidents which are of high number of users involved have high severity. Since, it would create panic situations among the Bitcoin community. During these incidents, we can observe, the illegal users tend to cash out the tainted Bitcoins indirectly through an exchange. Whereas, the incidents that had affected fewer users tends to be with less severe. Thus, enabling illegal users to cash out directly via an exchange. However, one exception would be the incident Alphabay. Even though, it had affected large user base and created a tense situation; it had been cashing out directly through an exchange.

A summary of incident results is depicted in Table 3 based on the common factors identified in all incidents.

Table 3: Summary of Incident Results

	Direct to Exchange / Mixer	Indirectly to Exchange / Mixer	Small Amount	New wallets
NiceHash		✓	✓	✓
ShapeShift		✓	✓	✓
Gatecoin				
WannaCry		✓	✓	✓
CryptoLocker				
Venuslocker		✓	✓	✓
Blackmailing	✓			
BTGwallet		✓	✓	✓
Fake Agency	✓			
AlphaBay	✓			

[15] https://bitcoinwhoswho.com/blog/2017/10/09/blackmail-scam-run-on-russian-wallet-matbea/#more-540

[16] https://99bitcoins.com/the-bitcoin-gold-hard-fork-explained-coming-october-25th/

[17] https://news.bitcoin.com/bitcoin-gold-wallet-stole-private-keys-scooped-3-3-million/, https://bitcointalk.org/index.php?topic=2412182.0, https://www.reddit.com/r/CryptoCurrencies/comments/7db42c/httpsmybtgwallet com_seems_to_be_scam/

[18] 3JjPf13Rd8g6WAyvg8yiPnrsdjJt1NP4FC

[19] https://bitcoinwhoswho.com/blog/2017/12/17/fake-coinbase-support-phone-number-1-888-455-1155/, https://www.reddit.com/r/Bitcoin/comments/77hxl0/my_bitcoin_at_coinbase_got_hacked/

[20] https://www.reddit.com/r/AlphaBay/comments/6lbu32/alphabay_down_shit_vendor_review_as_well_buyer/, https://news.bitcoin.com/major-darknet-marketplace-alphabay-goes-down-exit-scam-speculations-arise/

5. Discussion

The findings of this study reveal that there are common patterns that can be identified among different illegal incidents. The study highlights novel findings along with validation previous studies result. The discussion section highlights the previous study findings and novel key findings from this study by comparing both.

According to previous study [12], It has been identified that "Ransomware criminals' cash out via a Bitcoin services, gambling and mixing services".

According to this study, it has been revealed that "criminals" cash out via a Bitcoin services, gambling and mixing services. But, when they are cashing out there are mainly two ways, as

- Illegal users directly transfer illegally obtained Bitcoins to exchanges
- Another way is that, criminal will not directly transfer illegally obtained Bitcoins to exchanges or mixtures. But, they would first transfer to several other unidentified Bitcoins address and later they would transfer exchanges or mixtures"

The next discussion point would be that according to previous study, it was recognized that "Generally users have hundreds of different Bitcoin addresses [22, 44].

Whereas, according to this study, the notable novel finding is that "Illegal users do not only have hundreds of different Bitcoins addresses but they also create new wallets to transfer their tainted Bitcoins'.

In addition, another discussion fact would be that according to previous study,

Illegal users "Transact more in smaller amounts" [12, 32].

According to this study, it is revealed that illegal users do not only transfer in small amounts, but they transfer the small amounts in constant or in a certain proportion in the subsequent transactions".

In addition, the final discussion point is that the previous studies have recognized exchanges such as Xapo.com, BTC-e.com, LocalBitcoin.com, Kraken.com as popularly used by Ransomware attackers. The studies also reveal the mixing services Helix Mixer has been repetitively used by illegal users. [12, 45].

According to this study, it has identified additional exchange services such as Poloniex.com, Bittrex, Cex.io, Bitfinex and Helix Mixer being popular used across illegal users.

6. Evaluation

As in [48], it has been highlighted that many of the proposed solutions in Blockchain related researches are lack of solid evaluation on their effectiveness. However, recent researches in [49], [50], [51] has used deep neural network and unsupervised feature learning approach to evaluate the results obtained.

As in recent research study [49], on Bitcoin address linking; authors used deep neural network for testing the efficiency of the method used. In addition, as in [50] and [51], for frauds detection in Bitcoin network, a feature learning approach of K-means has been used. Whereas in [52], feature learning approach along with performance measures and validation techniques have been used for evaluation.

But, accordingly the approach of machine learning cannot be implemented as only few results can be tested using some features. Therefore, in this study two evaluation methods were used for testing the results obtained. The two techniques were obtaining feedback from real Bitcoin users regarding the Bitcoin usage. The next approach is by using a sample test dataset to evaluate the results instead of a machine learning approach.

6.1. User Feedback

This approach is to obtain feedback from real Bitcoin users about their spending patterns of Bitcoins by issuing an online survey. This technique assumed all the survey respondents are legal. The Survey targeted on validating the findings from this study. This was posted to Bitcoin forum using the username "Rosecuppy123". There were about 27 complete responses for the survey.

The user feedback highlights that frequent users send Bitcoins to their own addresses in existing wallets before sending someone else. In addition, over 75% of respondents use 2 to 5 wallets for the security purposes. But, they do not create new wallets for every single transaction unlike illegal users. Thus, confirming that illegal users create several new wallets, addresses to spread their tainted coins.

Generally, an illegal person can pretend to be a legal individual and can provide feedback which can mislead. Most of the respondents were not willing to provide reliable information. Therefore, this approach was not productive.

Due to the lack of reliability in user feedback evaluation technique, another evaluation technique of using sample test incident dataset was used.

6.2. Test Cases

Sample incidents were tested to check whether the same patterns are resulted out for each main category. Sample hack incident called Linode repeated the pattern of transferring in small amounts to new wallets alike in NiceHash, ShapeShift hacks. Samsam ransomware replicated the same pattern as in WannaCry, Venuslocker; ransomwares which were analysed in the study. Btc-e is also used in this incident as in WannaCry. TradeRoute scam also transacted directly through several exchanges and Bitfinex.com was popular as in Alphabay. Fake Coinbase scam replicated the same pattern as was in Fake Agency, AlphaBay. Bittrex exchange was popular same as BTGwallet, Fake Agency scams.

7. Conclusion

Bitcoin is a crypto currency that is being used by millions of people for both legal and illegal intentions. The decentralized and anonymized feature of Bitcoin has drastically increased the rate of Bitcoin being misused, particularly its involvement in illegal activities. This triggered to conduct a comprehensive analysis of several illegal incidents of different nature. The aim of study is to identify behavioral patterns among illegal incidents that are dissimilar in nature.

Based on the results, it can be identified that there are mainly three patterns identified as,

1. Illegal users directly use exchanges to cash out tainted Bitcoins as shown in Figure. 4.

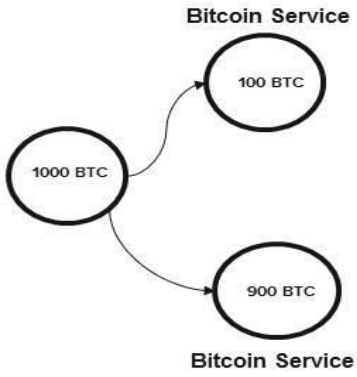

Figure. 4: Use exchange directly

2. Illegal users cash out tainted Bitcoins after sending to intermediate addresses in small amount as shown in Figure. 5.

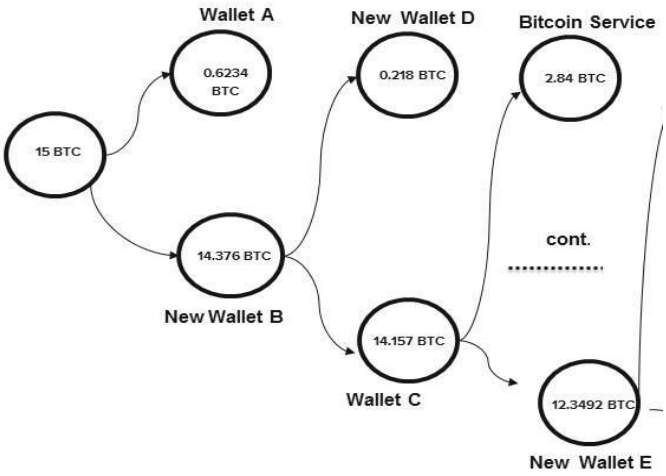

Figure. 5: Use intermediate addresses

3. Illegal users cash out tainted Bitcoins by transferring to new wallets in small amount as shown in Figure. 6.

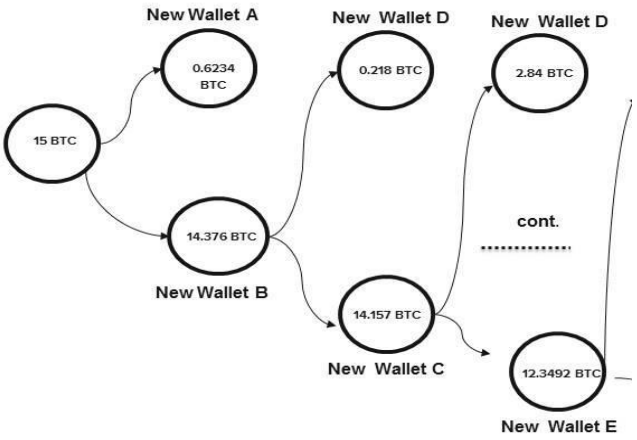

Figure. 6: Use new wallets

Accordingly, the two findings 1 and 2 validate with previous researches. The novel finding of this study is that illegal users "create new wallets to transfer the tainted Bitcoins before sending to an exchange or a service". The study also revealed significant exchanges from the analysis. The Evaluation techniques results also indicate similar patterns as the analysis.

Thereby, it can be concluded that "The behavior of an illegal user in spending tainted Bitcoins can generalized among different natured incident". However, "The patterns tend to vary when the 'severity' of the illegal incident differs". However, this study has been limited to certain limitations in scope and implementations.

7.1. Delimitations

In this research, the illegal incidents considered were limited to the definition of 'Illegal Activity' (i.e. this study does not consider every single illegal activity defined in accordance with general definition of law authorities).

In addition, specific country rules will not be considered because legality of Bitcoin is different according to the country law. For example, some countries consider Bitcoin as legal or illegal or restricted whereas some other countries are neutral on legality status of Bitcoin.

7.2. Contributions

The main contributions of this study are the novel findings from the analysis of illegal incidents regarding the spending behavior patterns of illegal users. The novel findings from this study are that the Illegal users send tainted Bitcoins in mainly two ways, as

2.Using intermediate addresses and then transferring Bitcoins to exchanges or mixtures. While they are transferring Bitcoins, Illegal users create new wallets to transfer their tainted Bitcoins.

In addition, the study also highlights popular exchanges or services used across illegal users such as Poloniex.com, Cex.io, Bittrex, Bitfinex and Helix Mixer.

In addition, a major contribution to the research community would be the illegal Incident data collection for 33 incidents along with 331 transaction id[21].

References

[1] Nakamoto, S., 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/en/bitcoin-paper (accessed 7 February 2018).

[2] Foley, S. M., Karlsen, J. R. M., Putniņš, T. J. M., 2018. Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies? SSRN Electronic Journal.

[3] Spagnuolo, M., Maggi, F., Zanero, S., 2014. BitIodine: Extracting Intelligence from the Bitcoin Network. 18th Conference on Financial Cryptography and Data Security. 457-468.

[4] Raeesi, R., 2018. The Silk Road, Bitcoins and the Global Prohibition Regime on the International Trade in Illicit Drugs: Can this Storm Be Weathered? Glendon Journal of International Studies. 8, 1.

[5] Bohr, J., Bashir, M., 2014. Who Uses Bitcoin? An Exploration of the Bitcoin Community. 2014 Twelfth Annual International Conference on Privacy, Security and Trust.

[6] Janze, C., 2017. Are Cryptocurrencies Criminals Best Friends? Examining the Co-Evolution of Bitcoin and Darknet Markets. Proceedings of the Americas Conference on Information Systems (AMCIS). https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1041&context=amcis2017 (accessed 10 August 2018).

[7] Kethineni, S., Cao, Y., Dodge, C., 2017. Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes. American Journal of Criminal Justice. 43, 2, 41-157.

[8] Moore, T., Christin, N., 2013. Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk. 18th Conference on Financial Cryptography and Data Security. 25-33.

[9] Vasek, M., Thornton, M., Moore, T., 2014. Empirical Analysis of Denial-of-Service Attacks in the Bitcoin Ecosystem. 18th Conference on Financial Cryptography and Data Security. 57-71.

[10] Vasek, M., Thornton, M., Moore, T., 2015. There's No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scam. 18th Conference on Financial Cryptography and Data Security. 44-61.

[11] Huang, D., Aliapoulios, M., Li, V., Invernizzi, L., Bursztein, E., McRoberts, K., Levin, J., Levchenko, K., Snoeren, A., McCoy, D., 2018. Tracking Ransomware End-to-end. 2018 IEEE Symposium on Security and Privacy (SP).

[12] Paquet-Clouston, M., Haslhofer, B., Dupont, B., 2018. Ransomware Payments in the Bitcoin Ecosystem. https://arxiv.org/abs/1804.04080 (accessed 15 August 2018).

[13] Richardson, R., North, M., 2018. Ransomware: Evolution, Mitigation and Prevention. Scholars' Press. http://scholarspress.us/journals/IMR/pdf/IMR-1-2017.%20pdf/IMR-v13n1art2.pdf (accessed 12 August 2018).

[14] Marella, V., 2017. Bitcoin: A Social Movement Under Attack. Selected Papers of the IRIS - European Journal of Philosophy and Public Debate. http://aisel.aisnet.org/iris2017/1/ (accessed 17 August 2018).

[15] Karami, M., McCoy, D., 2018. Understanding the Emerging Threat of DDoS-as-a-Service | USENIX. https://www.usenix.org/conference/leet13/workshop-program/presentation/karami (accessed 12 August 2018).

[16] Barber, S., Boyen, X., Shi, E., 2012. Bitter to Better—How to Make Bitcoin a Better Currency. Financial Cryptography and Data Security. 399–414.

[17] Bryans, D., 2018. Bitcoin and Money Laundering: Mining for an Effective Solution. Digital Repository @ Maurer Law. https://www.repository.law.indiana.edu/ilj/vol89/iss1/13/ (accessed 12 August 2018).

[18] Gifari, A., Anggorojati, B., Yazid, S., 2017. On preventing bitcoin transaction from money laundering in Indonesia: Analysis and recommendation on regulations. 2017 International Workshop on Big Data and Information Security (IWBIS).

[19] Gipp. B., Meuschke, N., Gernandt, A., 2015. Decentralized Trusted Timestamping using the Crypto Currency Bitcoin. iConference 2015, Newport Beach, CA, USA.

[20] 20*Bhaskar, N., Chuen, D., 2015. Bitcoin Exchanges. Handbook of Digital Currency, pp. 559-573.

[21] Trautman, L., 2014. Virtual Currencies Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox. Richmond Journal of Law and Technology. 1-108.

[22] Ly, M., 2014. COINING BITCOIN'S "LEGAL-BITS": EXAMINING THE REGULATORY FRAMEWORK FOR BITCOIN AND VIRTUAL CURRENCIES. Harvard Journal of Law & Technology. 27, 2.

[23] Androulaki, E., Karame, G., Roeschlin, M., Scherer, T., Capkun, S., 2013. Evaluating User Privacy in Bitcoin. Financial Cryptography and Data Security. 34-51.

[24] Karame, G., Androulaki, E., Capkun, S., 2012. Double-spending fast payments in bitcoin. 2012 ACM conference on Computer and communications security - CCS '12.

[25] Barcelo, J., 2018. User Privacy in the Public Bitcoin Blockchain. https://pdfs.semanticscholar.org/549e/7f042fe0aa979d95348f0e04939b2b451f18.pdf (accessed 15 August 2018).

[26] Hurlburt, G., Bojanova, H., 2014. Bitcoin: Benefit or Curse? IEEE Computer Society.

[27] Pathak, P. B., 2016. A Dangerous Trend of Cybercrime: Ransomware Growing Challenge. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET). 5(2). http://ijarcet.org/wp-content/uploads/IJARCET-VOL-5-ISSUE-2-371-373.pdf (accessed 12 August 2018).

[28] Upadhyaya, R., Jain, A., 2016. Cyber ethics and cybercrime: A deep dwelved study into legality, ransomware, underground web and bitcoin wallet. 2016 International Conference on Computing, Communication and Automation (ICCCA).

[29] Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., Kirda, E., 2015. Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks. Detection of Intrusions and Malware, and Vulnerability Assessment. 3-24.

[30] Everett, C., 2016. Ransomware: to pay or not to pay? Computer Fraud & Security. 4, 8-12.

[31] Liao, K., Zhao, Z., Doupe, A. Ahn, G., 2016. Behind closed doors: measurement and analysis of CryptoLocker ransoms in Bitcoin. 2016 APWG Symposium on Electronic Crime Research (eCrime).

[32] McGinn, D., Birch, D., Akroyd, D., Molina-Solana, M., Guo, Y., Knottenbelt, W., 2016. Visualizing Dynamic Bitcoin Transaction Patterns. Big Data. 4, 2.

[33] Weimann, G., 2015. Going Dark: Terrorism on the Dark Web. Studies in Conflict & Terrorism. 39, 3, 195-206.

[34] Ron, D., Shamir, A., 2018. How Did Dread Pirate Roberts Acquire and Protect his Bitcoin Wealth?

[35] Fromknecht, C., 2015. One-Time, Zero-Sum Ring Signature. https://scalingbitcoin.org/papers/one-time-zero-sum-ring-signature-conner-fromknecht-2015.pdf (accessed 15 August 2018).

[36] Gervais, A., Karame, G., Capkun, S., Capkun, V., 2014. Is Bitcoin a Decentralized Currency? IEEE Security & Privacy. 12, 3, 6-7. https://eprint.iacr.org/2013/829.pdf (accessed 13 August 2018).

[37] Anderson, R., Shumailov, I., Ahmed, M., Making Bitcoin Legal. https://www.cl.cam.ac.uk/~rja14/Papers/making-bitcoin-legal.pdf (accessed 13 August 2018).

[38] Kalodner, H., Goldfeder, S., Chator, A., Möser, M., Narayanan, A., 2017. BlockSci: Design and applications of a blockchain analysis platform. https://arxiv.org/abs/1709.02489 (accessed 12 August 2018).

[39] Reid, F., Harrigan, M., 2012. An Analysis of Anonymity in the Bitcoin System. Security and Privacy in Social Networks. 197-223.

[40] Stanford, G., Stanford, T., 2018. Cointopia: Blockchain Analysis using Online Forums. https://web.stanford.edu/class/cs224w/projects/cs224w-87-final.pdf (accessed 12 August 2018).

[41] Böhme, R., Christin, N., Edelman, B., 2015. Bitcoin: Economics, Technology, and Governance. Journal of Economic Perspectives. 213-238.

[42] Rodrigues, M., Gama, J., Ferreira, C.A., 2012. Identifying Relationships in Transactional Data, in: Pavón, J., Duque-Méndez, N.D., Fuentes-Fernández, R. (Eds.), Advances in Artificial Intelligence – IBERAMIA 2012. Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 7637.

[43] Rojas, E., Gorton, D., Axelsson, S., 2015. Using the RetSim simulator for fraud detection research. International Journal of Simulation and Process Modelling. 10, 2.

[44] Rose, C., 2015. The Evolution of Digital Currencies: Bitcoin, A Cryptocurrency Causing A Monetary Revolution. International Business & Economics Research Journal (IBER). 14, 4, 617.

[45] Hong, Y., Kwon, H., Lee, S., Hur, J., 2018. Poster: De-mixing Bitcoin Mixing Services. https://pdfs.semanticscholar.org/5425/fb2c0a039bc16e5a4fe31a1b493094631462.pdf (accessed 22 August 2018).

[46] CoinDesk. (2017, Dec. 6). Cryptocurrency Mining Market NiceHash Hacked [Online]. Available: https://www.coindesk.com/62-million-gone-cryptocurrency-mining-market-nicehash-hacked [Accessed: Oct. 18, 2018].

[47] M. Conti, A. Gangwal, and S. Ruj, ―On the Economic Significance of Ransomware Campaigns: A Bitcoin Transactions Perspective, ‖ Computers & Security, vol. 79, pp. 162-189, 2018. doi: 10.1016/j.cose.2018.08.008

[48] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, ―Where Is Current Research on Blockchain Technology? A Systematic Review, ‖ PLoS ONE, vol. 11, no. 10, 2016. doi: 10.1371/journal.pone.0163477

[49] W. Shao, H. Li, M. Chen, C. Jia, C. Liu, and Z. Wang, ―Identifying Bitcoin Users Using Deep Neural Network, ‖ in: J. Vaidya, and J. Li (eds), Algorithms and Architectures for Parallel Processing, ICA3PP 2018. Lecture Notes in Computer Science, Springer, Cham, 2018, vol. 11337, pp. 178-192.

[50] V. R. Patil, A. P. Nikam, J. S. Pawar, and M. S. Pardhi, ―Bitcoin Fraud Detection using Data Mining Approach, ‖ Journal of Information Technology and Sciences, vol.4, no. 2, 2018.

[51] D. Zambre, and A. Shah, ―Analysis of Bitcoin Network Dataset for Fraud, ‖ 2013. [Online]. Available: http://snap.stanford.edu/class/cs224w-2013/projects2013/cs224w-030-final.pdf [Accessed: Oct. 21, 2018].

[52] M. Bartoletti, B. Pes, and S. Serusi, ―Data mining for detecting Bitcoin Ponzi schemes, ‖ 2018. [Online]. Available: https://arxiv.org/pdf/1803.00646 [Accessed: Oct. 21, 2018].