Cryptocurrency and its Forensic Significance

By

Daniel Gregory

A thesis submitted in fulfilment of the requirements for the degree of

Master of Forensic Science (Professional Practice)

In

The School of Veterinary and Life Sciences

Murdoch University

Supervisors:

Brendan Chapman

John Coumbaros

Semester 2, 2018

MURDOCH
UNIVERSITY
PERTH, WESTERN AUSTRALIA

Declaration

I declare that this thesis does not contain any material submitted previously for the award of any other degree or diploma at any university or other tertiary institution. Furthermore, to the best of my knowledge, it does not contain any material previously published or written by another individual, except where due reference has been made in the text. Finally, I declare that all reported experimentations performed in this research were carried out by me, except that any contribution by others, with whom I have worked is explicitly acknowledged.

Signed:

Daniel Gregory

Acknowledgements

I would like to thank the support of Mr. Brendan Chapman and Dr. John Coumbaros for all their help and guidance throughout this study. This study would not have been as good without their guidance and support.

Table of contents

Part one

Part Two

Part one

Literature Review

Cryptocurrency and its Forensic Significance

Abstract

Cryptocurrency is a relatively new form of investment. Its concept was first introduced in 2009, and has grown ever since. To this day, there are thousands of cryptocurrencies. Just as other currencies, cryptocurrency can be related to a crime. Ever since its introduction nearly a decade ago, there have been crimes where cryptocurrency are related. According to ACIC's crime types, cryptocurrency are related to two crime categories: cybercrime, and illicit drugs. There are also other cases where the type of crimes is not listed as a part of ACIC's. In response to the crimes that have occurred throughout the years, several governments have moved to establish laws regarding cryptocurrency. Some governments chose to ban cryptocurrency completely, whereas others opted for regulation.

Abbreviations

- AUSTRAC: Australia's financial intelligence agency, Anti-money laundering, and Counter-Terrorism financing Regulator
- AML/CTF: Anti-Money Laundering and Counter-Terrorism Finance
- DCE: Digital Currency Exchange
- DFRWS: Digital Forensic Science Workshop
- EAEU: Eurasian Economic Union
- RAM: Random Access Memory

Introduction

Cryptocurrency is a relatively new form of investment. The concept of cryptocurrency was first submitted by Satoshi Nakamoto (46), where it was highlighted that cryptocurrency eliminates the requirement of a middle-man, such as banks, and that users are able to safely and securely conduct transactions.

Cryptocurrency is a form of digital asset, as it does not physically exist in the actual world. Over the years, there has been an increase in the number of cryptocurrencies types, and their number in circulation. More people are starting to invest in them as well. The price of cryptocurrency differs between each type, and the price of a single cryptocurrency coin could be as expensive as $13,000 (bitcoin)(31). Being a currency, cryptocurrency can be used in a crime, or at least a motivation in a crime. There have been reports of cases that are related to cryptocurrency in the last decade since their creation.

The aim of this study is to explain cryptocurrency in great details, including its components, and how they differ from flat currencies such as cash. A few cases that are related to cryptocurrency would also be discussed in order to understand their connection to cryptocurrency.

What is cryptocurrency

Cryptocurrency are digital assets that are designed to work as a medium of exchange, using cryptography to secure its transactions, to control the creation of additional units, and to verify the transfer of assets. Cryptocurrencies can be classified as a subset of digital currencies. What is unique regarding cryptocurrency is that they utilise decentralised system; in decentralised banking system, boards or governments does not hold control over the system. This differs from traditional banking system, which utilises centralised control.

What are some of the terms associated with cryptocurrency

There are a few terms that are closely associated with cryptocurrency. Brief description will be given below, in order to assist with understanding the later contents of this work.

Cryptography

Cryptography is the practice and study of secure communication in the presence of a third party. This also includes construction of protocols that prevent third parties, or the public, from reading private details within a message.

Blockchain

Blockchain is a public transaction database. Blockchain also functions as a distributed ledger which contains list of records called blocks – linked and secured using cryptography. Each block contains a pointer as a link to the previous block, a timestamp, and transaction data.

Decentralised

A decentralised system in economy means that none actually holds control of them system; neither the government, nor the boards. In other words, the government holds no power in setting market cap for cryptocurrencies, or how much a cryptocurrency is in circulation, whereas in the traditional banking system such as cash, the government regulates how much cash are in circulation, and setting the market cap.

Digital asset

A digital asset is anything that exists in binary format, and is able to be used for trade purposes. Digital assets includes, but not limited to: digital documents, audible content, motion picture, and other digital data that can be stored in mediums such as laptop, personal computers, and media players.

Ledger

A ledger is a summary of all amounts entered in supporting journals which list individual transactions by date. The function of a ledger is to record, and total economic transactions.

Volatile

Cryptocurrencies are known to be volatile. A cryptocurrency can have a high value in a moment, and become significantly cheaper the next moment. Such risk is common amongst cryptocurrencies.

Components of cryptocurrency

Cryptocurrency trading involves several key components, in which without would result in failure to trade cryptocurrency. The components are cryptocurrency keys, cryptocurrency wallets, blockchain, and cryptocurrency mining. Details of each component will be discussed below.

Keys

There are two types of keys that are essential in cryptocurrency trading: Private keys and Public keys. A private key is stored in a cryptocurrency wallet, and proves ownership of a public key. A public key is connected to a particular amount of cryptocurrency, and can be used to access that amount. Both the private and public keys are significant tools to maintain the security of crypto-economy.

Private Key

A private key is a sophisticated form of cryptography that allows a user to access his or her cryptocurrency. A private key is an integral aspect of cryptocurrency, and its security helps in protecting a user from theft and unauthorized access to their cryptocurrency.

In cryptocurrency trade, a use is commonly given a public address and a private key to receive cryptocurrency in a form of coins or tokens (20). The private key is made up of 51 alphanumeric characters, which make it hard for a hacker to obtain.

The private key of a user is typically stored in a digital wallet belonging to the same user. When a transaction is commenced, the wallet software creates a digital signature by processing the transaction with the private key. This symbolizes a secure system, since the only way to generate a valid signature for any given cryptocurrency transaction is to use the private key. The signature is then used to confirm that a transaction has come from a particular user, and ensures that the transaction cannot be changed one it has been broadcasted into a blockchain. If a transaction is altered, the signature will change as well.

If the private key is lost, the user can no longer access their wallet to spend, withdraw, or transfer cryptocurrency. Hence, it is imperative that to save the private key in a secure location. Private keys can be stored on paper wallets, or hardware such as smartcards or USB devices. An offline software wallet can also be used to store private keys. This type of wallet has an offline portion for private keys, and an online portion which contains the public key.

In short, a private key is an indispensable component in order to conduct a cryptocurrency transaction. Security measures need to be taken to prevent loss of private key, whether accidental, or theft by hackers.

A solution to cryptocurrency private key security was suggested by WISeKey International Holding Ltd, a leading cyber security and IoT Company in January 2018, about the use of a secure mechanical watch called WIS.WATCH, powered by contactless secure hardware enabled wallet (14). It was designed to offer security and ease to cryptocurrency users. The WIS.WATCH can securely store a user's private key, and allows them to make contactless transactions. Every time a contactless blockchain transaction is initiated, including a bitcoin transaction, the private key must be validated by using the Near Field Technology, before enabling the transaction. While software wallets continue to be vulnerable to hackers, the secure hardware wallets have gained popularity. With the existence of WIS.WATCH, hardware wallets such as USB flash drives are now able to be used without contact, and users can establish multiple private keys into the secure store by using the WISeWallet application, and access these private keys to make transactions (29). The WISeWallet application was said to be compatible with most of the existing blockchain technologies, and works as a part of payment using WISeKey Blockchain-as-a-Service technology offerings. The WIS.WATCH is also said to be able to be used as a unique personal key identifier and trusted device to access smartphones, applications, personal data, and secured cloud storage.

Public key

The public key is where cryptocurrency funds are deposited and received. It is a cryptographic code that allows a user to receive cryptocurrencies into their account (21). When a user initiates their first transaction with a cryptocurrency, a unique pair of public key and private key is created. The transaction would also be broadcasted to the network, where distributed nodes confirm the validity of the transaction, before finalising it and recording it on the blockchain. It was noted that before a transaction is broadcasted, it needed to be signed digitally using the private key. The signature would prove the ownership of the private key, but not divulge the details of the private key to anyone.

Since a public key is created based on the private key, the user's public key is used to prove that the digital signature came from their private key. Once the transaction has been verified as valid, the cryptocurrency funds are sent to the recipient's public address.

The public address is a hashed version of a public key. Since the public key is made up of extremely long string of numbers, it needed to be compressed and shortened, hence the creation of public address. In other words, a private key generates a public key, which then generates a public address. When two users agreed to conduct a transaction, they would reveal their public addresses to each other. The sender needs the recipient's public address to be able to send the funds to, which will then be able to spend or withdraw the amount using their private key. The recipient can also verify the sender's batch of cryptocurrency coins using the sender's public address, which is displayed on their screen.

Cryptocurrency wallets

Cryptocurrency wallets are essential component of cryptocurrency. They are digital wallets that are used to store, send, and receive cryptocurrencies. A cryptocurrency wallet is commonly used to store a private key that proves ownership of a public key, which is a public digital code connected to a particular amount of currency.

Types of cryptocurrency wallets

There are several types of cryptocurrency wallets, and each wallet has their advantages and disadvantages. Most cryptocurrency have their official wallet, or a few officially recommended third-party wallets. Typically, no wallet can store many cryptocurrency;

most can only hold one, or two cryptocurrencies. Cryptocurrency users would need to figure out which wallet can store their chosen cryptocurrency.

Cryptocurrency wallets can also be divided into two categories: cold wallet, and hot wallet. A cold wallet is generally considered to be effective for long-term storage of unused funds. A hot wallet is described as a type of wallet that is carried around for immediate use of the funds within. The key difference between hot and cold wallets is that hot wallets are connected to the internet, whereas cold wallets are not. Hot wallets are also considered to be more likely targets from hackers, as they're connected to the internet – cold wallets are offline/not connected to the internet; hence they're safe from hackers. Due to this, it was recommended to have as many layers of protection as possible on hot wallets. Layers of protection can include two-factor authentication, strong password, and security settings. It was also thought to not have many funds in a hot wallet. The reason being that hackers can see how much funds are inside a hot wallet as it's connected to the internet. Lesser funds would naturally mean less appealing target.

However, despite having an offline feature to protect them from online threats, cold wallets are not immune to threats. A study found that a malware can be preinstalled, or pushed in during the initial installation of the wallet (38). Alternatively, it can infect the cold wallet's system when removable media such as USB flash drives is inserted into the wallet's computer in order to conduct a transaction. The study found that these attack methods have been repeatedly been proven feasible in the last decade (1, 23, 44, 50, 54). After obtaining a foothold in the wallet, a hacker can then utilise various air-gap covert channel techniques (39), including physical, electromagnetic, electric, magnetic, acoustic, optical, and thermal techniques. In conclusion, even though cold wallets provide a high degree of isolation, it is still possible for attackers to compromise such wallets and steal private keys from the owners.

Desktop wallet

A desktop wallet is the type that is considered more secure, when compared to both an online and mobile wallet. However, the degree of security is directly related to the quality of the desktop's protection against online threats, such as computer virus, and malware. Examples of desktop wallets are desktop applications, such as Exodus, Multibit, Armory, and Bitcoin Core.

A desktop wallet also has a feature that can identify it as a 'cold' wallet; when not connected to the internet, the desktop wallet is impervious to online threats from hackers, viruses, etc. A cold, desktop storage can be an older laptop that is completely offline, and on a clean operating system install.

Some of the advantages of desktop wallets are that they are easier-to-use cryptocurrency wallet as compared to the others, good cold storage solution, and private keys not stored on a third-party server. It was noted however, that they are only great solution for a cold wallet, only if they have never been connected to the internet before; if they have been connected to the internet, they would obtain an IP address, which hackers can trace and use to access the desktop. Desktops can also store private keys by downloading and storing them - eliminating the need to rely on third-party server.

Disadvantages of desktop wallets include the security concerns, when and if they are connected to the internet. As mentioned before, connecting to the internet would present the desktop with an IP address, which hackers can use to hack the desktop. Being able to or connected to the internet also exposes the desktop to other online threats, such as malware, key loggers, and viruses. Desktops are also not immune to physical damages. Fixing desktops by relying on service of others can expose its contents to them; they can examine the desktop’s contents, potentially obtaining access to cryptocurrency funds of the owner. It was also mentioned earlier that desktops can download private keys into them for storage. This also creates a risk such as that if a backup key/s were not made and the desktop become disabled or inaccessible; the key/s would be lost, and likely impossible to retrieve.

Mobile wallet

Mobile wallet is a type of wallet that is run from a phone application. It provides access to cryptocurrencies via mobile devices and provides additional features via the applications; however, it does create security risks similar to desktop wallets when connected to the internet.

Advantages of mobile wallets include them being practical and easier to use and access than other cryptocurrency wallets; mobile phones can be carried around and accessed anywhere, so long as there’s internet connection. This enables users to accept, or send cryptocurrency payments practically from anywhere. It was also mentioned that mobile wallet have additional features via the applications. One such feature includes QR code scanning to access cryptocurrency funds.

The disadvantage of mobile wallets is the fact that mobile phones in general are incredibly insecure devices; just as desktops, they can also be infected with online threats such as malware and viruses.

Online wallet

Online wallets are commonly cryptocurrency wallets that are accessed via web browsers, which is why they can also be referred to as web wallet.

Advantages of online wallets include the fact that they are the fastest way to complete cryptocurrency transactions, given that there is no lag between locations of the application and server. They are also ideal to hold small amounts of cryptocurrency. This characteristic categorise them as hot wallets, and share their property; ideal for quick, daily transactions that does not involve massive amount of cryptocurrency. Some online wallets are also able to manage multiple cryptocurrencies, transfer between them, or be directly integrated into a cryptocurrency exchange marketplace.

Disadvantages of online wallets include users being susceptible to phishing scams, malware, and insider tracking, and out-dated security measures. The risks mentioned are a part of the hazard of using web browser services, and often out of the user's control. Information relating to user's cryptocurrency details are also out of their control, as in they are stored in a third-party storage, the internet. Use of online wallet requires a desktop, and as mentioned earlier, desktops connected to the internet are at risk from malware, key loggers, and viruses. As such, it is generally not recommended to use services such as internet café, to reduce the risk of information theft.

Hardware wallet

Hardware wallets are dedicated hardware that is built to be able to hold cryptocurrency, and keep it secure. Hardware wallets include USB devices, and external hard disks. These devices are able to go online when connected to desktop, conduct transactions, and taken offline upon completion, for transportation and security. Requiring a desktop and internet connection to conduct transactions relating to cryptocurrency classifies this type of wallet as hot wallet.

Paper wallet

Paper wallets are a medium in which stores information related to both public and private keys. An example of the information stored is QR code that belonged to a private key. Using that QR code, a user can both send, and receive digital currency using a paper wallet. Overall, paper wallets enabled an option of not storing digital data about a user's data, such as private key, by using a paper wallet.

Mining

Cryptocurrency mining is the process of generating new cryptocurrency in the form of coins. Cryptocurrency mining is called such, from to the fact that when transactions are added to the public ledger that is blockchain, new coins is created, or in other word, mined.

Cryptocurrency mining is an integral part of how cryptocurrency functions as a digital currency. The mining network relies on miners to verify and update the public ledger of cryptocurrency transactions, to verify that cryptocurrency users are not trying to cheat the system, and to add newly-discovered coins into the system.

Miners

As explained earlier, miners work together to verify transactions, ultimately mining new coins into the system. But that does not mean that all miners are on the same team. Cryptocurrency miners gets rewarded in the form of some new coins for their hard work in mining coins, but the amount of coins rewarded are directly proportional to the contribution a miner had in the process of generating new coins. Hence, there are competitions amongst cryptocurrency miners in adding new transactions into the ledger as part of generating new coins. To put it simply, the more a miner contribute into adding new transactions into the ledger and generating coins, the more coins the miner obtains as rewards.

Proof-of-Work

In cryptocurrency, proof-of-work is a system that utilises hard-to-compute, but easy-to-verify functions, in order to limit exploitation of cryptocurrency mining by miners.

A proof-of-work system's hash function is the algorithm used to find a solution to the computational puzzle, which is simple to calculate the output is if the input is known. However, it is virtually impossible to calculate an output, if the input is unknown; trying every possible input would be done until the correct input is found. When cryptocurrency miners mine digital coins and add blocks of transactions to a blockchain, they effectively complete a proof-of-work system by using high-powered computers to solve a mathematical problem that is cryptographical puzzle.

One of the most popular proof-of-work functions is called SHA256, a part of the SHA-2 family of Secure Hash Algorithms. It is also the one that is used as bitcoin's proof-of-work. It was first used by Adam Back in 1996 as a way to block spam emails. Recently however, bitcoin started utilising an alternative to proof-of-work, called proof-of-stake (30, 53). It was a new proof-of-work mechanism that improves decentralisation and reduces risk of 51% attack, without increasing the risk of Sybil attack – an attack in which a single node such as a cryptocurrency miner assumed multiple identities (53).

There is a single major flaw to the proof-of-work system, and that is requiring a large amount of computing power, to solve cryptographical puzzle. The proof-of-work system holds no use apart from protecting the validity of cryptocurrency transactions and generally ensuring cryptocurrency system are ran honestly. This would mean that the process of mining cryptocurrency with proof-of-work is horribly wasteful, in terms of energy-use. Given the wasteful energy spent on proof-of-work system, it was not viewed as a long-term for cryptocurrency. Alternatives such as the aforementioned proof-of-stake are seen as a more friendly function.

In short, proof-of-work is indeed designed to be difficult, in order to prevent malicious behaviour, such as a miner trying to add fake transaction block into a blockchain to get reward coins. Proof-of-work would not only protect digital currency such as cryptocurrency from malicious miners, but also prevent a single person from assuming control over which transaction block to next be added into the blockchain.

How cryptocurrency are mined

In order to add transactions into a blockchain, all miners collect all transactions that were recently broadcasted by cryptocurrency users, verify the transactions, and compile them down into a transaction block – a condensed record of all transactions for that period of time.

It is possible for a miner to simple create a fake transaction block and adding it into the blockchain. Due to this, the cryptocurrency algorithm was designed to make cryptocurrency mining difficult. To prevent a miner from adding a transaction block at their will, they have to solve a difficult computational puzzle – a proof-of-work scheme. The proof-of-work scheme was designed to provide solutions that are easy to verify, but difficult to find.

In short, cryptocurrency miners compete against each other to see who can solve a difficult, cryptographic puzzle first. As one miner found the solution, they broadcast the solution to all the other miners, for them to verify that the solution is correct. If the solution is indeed correct, the network adds the successfully-mined transaction block to the accepted blockchain permanently.

The miner who was the first to successfully solve the cryptographic puzzle of transaction block is the rewarded for their effort, by receiving new coins – the amount of coins differs and depends on the transaction block size. The possibility of reward acts as an incentive for cryptocurrency miners to keep investing in computational time and effort into mining new cryptocurrency coins. The process of rewarding cryptocurrency miners with coins for their hard work of solving cryptographic puzzle also contributes to the overall cryptocurrency coins supply.

Where cryptocurrencies are mined

It was explained that cryptocurrencies are mined by miners, in which they solve cryptographical puzzle to add transactional blocks into a blockchain, creating new coins as a result. As such, cryptocurrency mining can be done from practically everywhere, providing that the miner have access to a computer with sufficient computing power.

It was also explained that mining cryptocurrency with proof-of-work in place would require a large amount of energy. This raised a concern such as carbon footprint (34). It was estimated that the combined electricity consumption for bitcoin and ethereum mining, which represented as high as 88% of the total cryptocurrency market capitalisation (36), had already reached a staggering 47 terawatt-hours yearly, and is on the rise. In terms of perspective, Greece's population of 11 million consumed close to 57 terawatt-hours annually; the consumption of energy to mine bitcoins and ethereum coins alone nearly require as much energy as Greece, a nation.

A vast majority of cryptocurrency mining (48%) was done in China, and is typically powered by coal plants (34). With the use of life-cycle impact-assessment methodology, it was estimated that the annual carbon footprint for bitcoin and ethereum mining was comparable to that of some 6.8 million average European inhabitants; hence the conclusion of the study being that the cryptocurrency industry was in need of reform to be more environmentally sustainable.

However, despite the claim that cryptocurrency mining was environmentally hazardous, a different study found that findings to be economically unsound. In a review, Stuart Wimbush mentioned a possible fault in the claim of the combined annual electricity consumption due to bitcoin and ethereum mining was 80% that of Greece (56). It was found that Bitcoin and ethereum generated a total wealth of US$275 billion in 2017, whereas the 11 million inhabitants of Greece generated a total wealth of approximately US$205 billion in the same year. Given that Greece generated less wealth than cryptocurrency mining, and would have consumed much more than simply electrical energy in the process, it was thought that the mining of cryptocurrency seemed to be considerably less wasteful.

In summary, even though there are valid claims that cryptocurrency mining is environmentally hazardous, it was theoretically impossible for it to be so, given that Greece, a nation, generated less wealth than cryptocurrency mining, and yet consumed much more than simply electrical energy in the process. In other words, it was natural for cryptocurrency mining to have consumed as much power (electrical) in order to generate a large amount of wealth. It was also suggested for nations to transit from using fossil-fuel-based electricity generation, to nuclear or other sustainable alternatives (56). This would allow generation of a large amount of wealth such as from cryptocurrency mining, and using a large amount of sustainable energy.

Blockchain

In terms of cryptocurrency, a blockchain is a public ledger of all a cryptocurrency's transaction. As new transactions are made, they are compiled into blocks, which will be added into the sequential blockchain. In order for a transaction to be considered successful, it has to be added into the blockchain. Once a transaction block is added into a blockchain, it will remain there permanently and are considered as public record.

Other uses for blockchain

Aside from cryptocurrency, there are emerging theories in ways to utilise the blockchain technology. Amongst them are medicines, gun control, stock exchange, and other investments such as gold.

Medicine

A use of the blockchain ledger system was suggested by M. Hoy in medicines (42). It was suggested to tie everything from medical records to library checkouts using a blockchain ledger containing verifiable time-stamped records of creation and ownership. The system can also potentially prevent changes in documents, and data tampering.

Gun control

It was suggested by Thomas F. Heston that the blockchain used for effective gun control (40). The blockchain protocol can be used to keep track of gun flow from manufacturer to end user, and track sales from a gun owner to another. The blockchain's anonymity feature would also allow better privacy than existing background check systems, and simultaneously link ownership of a particular gun to an individual in an immutable manner.

Stock Exchange

In December 2017, it was announced that ASX, Australia’s main stock exchange, would start using blockchain technology to process its equities transactions (2). ASX would begin replacing its current system, CHESS, with the distributed ledger technology to help manage the clearing and settlement for buying and selling stocks. ASX chief executive at that time, Dominic Stevens, stated that the change into using blockchain technology would put Australia at the forefront of innovation in the financial markets.

Other investments – Gold

It is apparently possible to implement the blockchain system onto other types of investment. An article was published about Australia’s biggest gold refiner, Perth Mint, developing their own blockchain-based gold products, as a response to the threat posed by the increasing in popularity of Bitcoin and other cryptocurrencies (37). Richard Hayes, chief executive of Perth Mint at that time, commented that the underlying blockchain technology behind cryptocurrencies presented an opportunity for Perth Mint to develop new products with greater security, and traceability.

In summary, blockchain has features that are beneficial to many fields. Such features include anti-tempering, as all records added into a blockchain are final, anonymity, and continual records to keep updated about a matter.

How to trade cryptocurrency

Trading cryptocurrency requires having good background knowledge, and the components needed to trade cryptocurrency. The two main components a user needed to start trading cryptocurrency are cryptocurrency wallet, and cryptocurrency exchange. In terms of having good background knowledge, there are several notes to consider. First, a beginner should choose a trading company with a good reputation that offers an exchange and a wallet. A beginner should also trade prominent coins, as starter. Bitcoin and Ethereum are two of the most prominent coins as of June 2018 (31, 49).

How to spend cryptocurrency

One of the major concerns regarding cryptocurrency is finding ways to spend it. Conducting a search using a search engine was thought to be one of the best ways to look for ways, or merchants who accepts cryptocurrency. Gambling is also a way to spend cryptocurrency (51)

Spending cryptocurrency is not always possible, as some countries have banned trading of cryptocurrency. Some countries opted for a compromise in the form of regulations. Government regulations will be discussed in more detail in a later section.

How cryptocurrencies differ from flat currencies

As explained earlier, cryptocurrency differs from regular, flat currency. The difference lies in two major ways. Cryptocurrencies are only accepted as payment by other users – if no one accepts it, then it is considered worthless. Flat currency however, will always be accepted as payment by the government, at the very least. The second major difference is that cryptocurrency token supply is not managed by a central authority, whereas flat currency is managed by the government and can lead to either inflation, or deflation.

Popular cryptocurrencies (latest price)

There are thousands of cryptocurrency. It can be hard to determine which cryptocurrency is the best, or worst. There are several parameters that can be used to rank cryptocurrency: their price, market cap, supply rate, and existing volume in circulation. In terms of price, the four highest-ranked cryptocurrency as at June 2018 are Bitcoin, Bitcoin Cash, Mixin, and Ethereum (31).

Crime types in Australia

The types of crimes in Australia will be listed, and matched with some of the cases related to cryptocurrency discussed below. The types of crime happened in Australia according to Australian Criminal Intelligence Commission (ACIC) are illicit drugs, fraud, financial crimes, illicit firearms, money laundering, cybercrime, identity crime, exploitation of business structures, public sector corruption, and violence (10).

Some of the most recent crimes in relation to cryptocurrency

To understand more as to how cryptocurrency can be related to crimes, various case involving cryptocurrency in general, or a particular cryptocurrency such as bitcoin, various case that occurred in the last decade will be discussed below. Swoop for cases that occurred in the last decade was decided, as cryptocurrency, or at least the proof-of-concept, was published in 2009 by Satoshi Nakamoto (46).

6 December 2017 – Hacking of NiceHash

One of the case examples to be explained is the cyber-attack against Nicehash. The crime happened on the 6th of December 2017, where NiceHash, a crypto-mining company based in Slovenia, reported that their system was breached in a cyber-attack(6).

NiceHash is known as the world's largest crypto-mining marketplace, and was created based on the concept of a shared economy. They were founded on the 24th of March 2014, and has grown to exponential heights ever since, and harboured 160,000 cryptocurrency miners daily on average (47). NiceHash is different from any crypto-mining marketplace in that they applied a new system to cryptocurrency mining that resolved around the relationship between cryptocurrency sellers and buyers. NiceHash users upon registration are presented with three options. The first option would be that users can choose to sell their hashing power generated from their mining hardware to receive earnings. The second option would be that investors can choose to buy a package to mine a particular cryptocurrency at a designated set pool with the support of crypto-algorithm. The last option would be to be a combination of a buyer, and a seller via NiceHash.

On more detail about the case, it was reported on Newstex Finance & Accounting Blogs that about 4,700 bitcoins were stolen (3). The approximate worth of those stolen bitcoins was $70 million. It was reported earlier that day, that the price of bitcoins was at a record-high of more than $14,000 (6). The record-high price of the bitcoin was very possibly be the motive of the crime, or at least tempted them to steal bitcoins.

In terms of bitcoin-theft, the case was not the first reported case in the field. In February 2014, Mt. Gox, a bitcoin exchange based in Japan, reported a theft of 850,000 coins (17). Those bitcoins were worth nearly $500 million at that time. Mt. Gox were shut down not long after the case (19), and filed for bankruptcy protection in Japan, later that year (5). A study of this case found that a meteoric rise in price and rapid growth were associated with cryptocurrency, particularly bitcoin – this also attracted thieves/hackers (32).

In regards of the aftermaths of the case about NiceHash, the CEO of NiceHash at that time, Marko Kobal, had resigned following the incident (55), and reimbursements were carried out by the company. On the 31st of January, nearly two months after the hacking of bitcoins, the company announced that they are going to reimburse their service users that were affected by the security breach that occurred on 6th of December 2017 (18).

The reimbursement program is called the Repayment program, and thus far consisted of four stages: the first was carried out on the 2nd of February (18), the second on the 1st of March (22), the third on the 3rd of April (27), and the latest stage, fourth stage, was done on the 7th of May (12). It was also reported along with the fourth stage, that 30% of the old balance amount was already reimbursed to all users that were impacted by the security breach. More details about the program are unknown, or if there will be any more, but given that there are four stages thus far and 30% of the stolen amount reimbursed, it can be predicted that there will be about seven more stages of reimbursements, with each stage reimbursing approximately 10% of the stolen amount.

Blockchain-related – Child pornography

In a report published in March 2018, German researchers found about 1,600 files of non-financial data, some linking to, or actually containing child pornography, and other objectionable materials, on the blockchain system that stores bitcoin transactions (52). It was concluded that users of blockchain are able to add non-financial data for purposes such as describing a transaction’s purpose, and insert benign messages or record information for other financial services. The objectionable contents were found to be imbedded in such data, and given that blockchain are viewable by practically all users, the data would be downloaded and persistently stored by them.

This discovery would place certain users of the bitcoin network in legal difficulties. The researchers also mentioned that this discovery could pose an obstacle for greater adoption and mainstream acceptance of bitcoin and other cryptocurrencies. Upon further analysis, the researchers found that most of the files were harmless, but some of the files contained copyright violations and the disclosure of the people’s identifiable information, and at least eight files were said to containing sexual content (33). Amongst the child pornography materials, two files were found to contain 274 links to child pornography websites, and a file depicting a nude image of a minor.

Experts said that the files were likely to be downloaded as a part of notes to transactions, or inserted as the transactions themselves. Users of blockchain are able to add non-financial data for purposes such as describing a transaction's purpose insert benign messages, or record information for other financial services – anyone with access to bitcoin software such as miners, exchanges, and traders, have the ability to upload any content into the blockchain.

Arbitrary data insertion methods for bitcoin's blockchain

As explained before, aside from recording financial transactions, Bitcoin's blockchain are also able to be filled with non-financial data. Non-financial data can take a form of short messages via special transaction types, or even complete files. To add complete files into a blockchain, arbitrary data has to be encoded as standard transactions. There are two insertion methods for non-financial data: low-level insertion methods, and content insertion services.

Benefits and risks of arbitrary blockchain content

Bitcoin's blockchain design included several ways to insert arbitrary, non-financial data into its blockchain, both intentionally, and unintentionally. Potential benefits of engraving arbitrary data into the bitcoin's blockchain and the risks associated with them will be discussed further below.

Benefits

Bitcoin offered Coinbase, a digital currency exchange headquarters, and OP_RETURN, a special transaction template that allows one small data chunk as an attachment onto a transaction, as explicit channels to insert small chunks of non-financial data into their blockchain. The benefit of using OP_RETURN is that different services use OP_RETURN to link non-financial assets such as vouchers, to bitcoin's blockchain. Coinbase differ from OP_RETURN in those only miners who dedicate significant computational contribution to maintain the blockchain, to be able to add extra chunks of data into the new transaction blocks.

Risks

There are several risks associated with adding data into blockchain content. Some of them are copyright violations, malware, privacy violations, politically sensitive content, and illegal & condemned content. As the blockchain are akin to file-sharing networks, pirated data can be distributed as part of a transaction block. Malware is also a threat, as they can be inserted as an attachment, and if downloaded and opened, can cause cataclysmic damage onto the system or device. Governments have valid concerns regarding a leakage of classified information. If such classified information is added into a blockchain, it would mean that more than a single user having the file, and the ability to access it, potentially exposing sensitive information about a government.

In short, there are ways for someone to add an objectionable content into a blockchain, and cause harm if possessed or accessed by other users. Unlike systems such as social media platforms, file-sharing networks, and online storage systems, contents that are stored in a blockchain can be do so while remaining anonymous, making it hard to trace the culprit.

Examining the data (non-financial data)

There are three methods to examine non-financial data in a blockchain: low-level insertion methods detectors, and service detectors, and suspicious transaction detectors.

Low-level insertion method detectors

The low-level insertion method detectors were designed to match individual transactions that are likely to contain non-financial data. They detect manipulated financial transactions, as well as OP_RETURN, non-standard, and Coinbase transactions.

Service detectors

The service detectors enabled the detection and extraction of files based on the service' protocols, and also tracking of data used in service-created transactions.

Suspicious transaction detectors

The suspicious transaction detectors examine standard transactions that are likely to carry non-financial data, but were not detected. For a transaction to be examined by this method, it has to have at least 50 suspicious outputs.

Illegal drugs

There was a reported case in India about a drug trade related to cryptocurrency (11). An arrest was made by the police against two university students that were caught purchasing drugs using cryptocurrencies. The duo would purchase an amount of drug, and then have it transported into a particular place where it'll be picked up.

It was not the first case where cryptocurrency was used to purchase drugs. There was a case in 2011, where a university student sold/auction drugs via an online drug marketplace called 'Silk Road' (41). The student had created a fake profile and auctioned drugs online, where customers would buy, and have it delivered to an address of their choice. The method of payment was cryptocurrency, with different drugs cost different amount of coins. The case was ultimately solved when police made an arrest of the student in a public library, where he logged in into his Silk Road profile.

9 March 2018

In a newspaper article published on March 2018, it was announced that Pavel Lerner, a cryptocurrency businessman, was kidnapped in Ukraine by armed assailants, and was forced to pay $1 million ransom in the form of bitcoins from his digital wallet (45). The case led to demands being made to the government to clamp down on cryptocurrency crime. It was mentioned that every month, the Ukrainian police would raid the Kvazar semiconductor plant in Kiev, and seize millions of pounds in form of computer equipment, which were claimed to be taken by Russians and used to finance the separatist regions of Donetsk and Lugansk.

Base on the case examples below, in terms of type of crimes in Australia by ACIC, cryptocurrency had been used in two categories of crimes: illicit drugs (Silk Road), cybercrime (hacking of NiceHash). Child pornography and kidnapping did not quite fit into the crime categories listed, but they are serious crimes, nonetheless.

Government regulations

In response to several concerns such as environmental impacts of cryptocurrency mining and the risks of owning cryptocurrency, several governments had decided to take actions against cryptocurrency. Actions taken include total banning, and putting regulations in place.

China

China as of February 2018 had completely banned cryptocurrency trading within their country. The process actually started from September 2017, where it was announced that Chinese regulators declaring initial coin offerings illegal (7). This meant that cryptocurrency owners are not allowed to promote, much less sell, their cryptocurrency to anyone in the country. The regulatory action was said to be caused by growing fear from initial coin offerings, which caught investors' imagination that further leads to phishing activities.

Ultimately, cryptocurrency was banned in total starting February 2018. It was announced in an article that was published by Financial News, a publication company that is affiliated with the People's Bank of China, that the Chinese government's recent attempts to stamp out digital currency trading by shutting down domestic cryptocurrency exchanges were not successful in completely eradicating cryptocurrency trading, and that the government will strengthen measures, to thoroughly remove any onshore or offshore trading platforms related to virtual currency trading (8).

South Korea

South Korea is another country that moved to regulate cryptocurrency. Initially, it was reported that South Korea planned to ban cryptocurrency trading, in light of cryptocurrency abuse. South Korea's justice minister at that time, Park Sung-Ki, mentioned there being great concerns regarding virtual currencies (26, 35). However, as at mid-January 2018, a ban had not been placed, but instead considered taxing cryptocurrency transactions, according to the South Korean finance minister at that time, Kim Dong-Yeon (25). Later in the month, raids were conducted by the country's police and tax agencies on major cryptocurrency exchanges for alleged tax evasion. Aside from alleged tax evasion case, the police were also looking for a Seoul-based cryptocurrency exchange, over possible gambling allegations.

Ultimately, the South Korean government officially banned anonymous cryptocurrency trading commencing at the end of January 2018 (24). This would mean that cryptocurrency traders could only make cryptocurrency transactions from bank accounts set up under their real names.

Ukraine & Kazakhstan

Ukraine had started to intensify the search for methods to regulate cryptocurrencies, due to growing concerns in their capital, Kiev, that exploitation of the digital assets by criminals and geopolitical adversaries presented a growing national security risk (48). Ukraine's national security and defence council chief, Oleksandr Turchynov, warned that the current legal vacuum posed a threat to the economy and security of the state. He also mentioned that given the rapid development of cryptocurrencies around the world, the issue could not be left out of attention, hence the plans to develop regulations. The soaring prices of cryptocurrency have made the market an increasingly lucrative target for cyber criminals. There was also a growing concern among regulators and governments that cryptocurrency could be used by organised crime-groups for money laundering (4, 43), and other criminal activities.

In a response to growing concerns of cryptocurrency being used, or simply being related to crimes, The Kazakhstan Association of Blockchain and Cryptocurrency submitted a proposal to the Eurasian Economic Union (EAEU) to create an advisory board on blockchain and cryptocurrency (15). The proposal was submitted during the Cryptoconference 2018 in Almaty, and had gathered some support for governments to adopt legislation to regulate the cryptocurrency market. Conference participants were pushing for the adoption of cryptocurrency laws within the EAEU in order to protect the best interests of all market from third parties such as cryptocurrency exchange marketplace. The regulation also aimed to prevent the use of cryptocurrency as a tool for illegal transactions, the legalisation of proceeds from crime, and the financing of terrorism.

Australia

As of April 2018, new laws for digital currency exchange (DCE) providers operating in Australia were implemented by AUSTRAC, Australia's financial intelligence agency, anti-money laundering, and counter-terrorism financing regulator (AMF/CTF) (16). The new laws would cover regulation of service providers of cryptocurrency, such as cryptocurrency exchange marketplace.

The AUSTRAC CEO, Nicole Rose, announced that the new laws would strengthen the agency's compliance and intelligence capabilities to help DCEs implement systems and controls that can minimise the risk of criminals using them for purposes such as money laundering, terrorism financing, and cybercrime.

With the new laws in place, DCEs with a business operation located in Australia must now register with AUSTRAC, and meet the government's AML/CTF compliance and reporting obligations. The transition period were run until May 2018, to allow DCEs time to register them.

Corporate regulations

Countries are not the only one capable of banning, or at least regulating cryptocurrencies. It was found that massive corporations such as Google, and Apple, have also moved to regulate cryptocurrency – cryptocurrency mining, to be exact.

Google

On the 3rd of April 2018, it was reported that Google had decided to start cracking down on malicious cryptocurrency mining via extensions on their website platform, Google

Chrome (9). Until that period, Google Chrome's web policy had been permitting cryptocurrency mining in their extensions, providing that cryptocurrency mining was indeed an extension's single purpose of use, and that the user is adequately informed of the cryptocurrency mining behaviour.

Unfortunately, it was found that approximately 90% of extensions with cryptocurrency mining scripts that developers have attempted to upload to the Chrome Web Store failed to comply with Google Chrome's policies (13). That resulted in their rejection or removal from the store, according to James Wagner, Extensions Platform Product Manager, explained in a blog post. It was then decided that Chrome Web Store would no longer accept extensions that mine cryptocurrency. However, the currency existing extensions with blockchain-related purposes other than cryptocurrency mining would still continue to be permitted in the Web Store.

Apple

Apple is one of the latest companies to ban cryptocurrency mining on their devices (28). It began with the release of a new set of developer guideline updates. Virtual currencies such as cryptocurrency heavily rely on cryptocurrency mining to sustain their existence. The process required using a computer's processing power in order to obtain fractions of coins – this consumes an incredible amount of power. The power drains could potentially end up leading to a higher electricity bill, surpassing the price of what are mined. It could also put a significant burden on the mining device. The reason of Apple banning cryptocurrency mining seemed to be caused by the latter concern, as they banned cryptocurrency mining on their devices due to power consumption, and the potential of the process to put unnecessary pressure on the devices.

In summary, some countries actively ban cryptocurrency, while others opted to compromise by placing regulations in place. Concerns regarding cryptocurrency being used for crime seemed valid, but with regulations such as the new law implemented by Australia's AUSTRAC would ensure transparency of DCEs, and assist in solving crimes by having DECs registered in the system, and keeping track into their activities. The new law would also help in monitoring DECs for any sign of criminal activities.

Conclusion

In conclusion, cryptocurrency indeed have a relation to crimes. There have been cases where cryptocurrency was used to commit a crime such as purchasing a drug, kidnapping a person and demand ransom in the form of cryptocurrency, and hacking into a cryptocurrency marketplace to steal cryptocurrency. Based on the crime types listed by ACIC, two crime categories have been proved to be related to cryptocurrency: cybercrime, and illicit drugs. In response to crimes related to cryptocurrency being committed, laws were put in place in several countries. Some laws were implemented to ban cryptocurrency completely such as in China, whereas others such as South Korea and Australia opted to regulate cryptocurrencies as opposed to completely banning them. As cryptocurrency are able to continue to rise, so too are the number of people that accept them as payments – this can be a cause for a crime. In this study, there was no search conducted on the relation between cryptocurrency against other crime types such as violence and arson. A future study concerning the relation between cryptocurrency and other crime types, including the lesser ones, would be helpful in identifying more ways cryptocurrency can be used, or related to a crime – this can help in placing laws, or create methods to counter, or solve those crimes.

References

1. 25 Percent of New Worms in 2010 Are Designed to Spread Through USB Devices, According to PandaLabs. NewsRX LLC; 2010. p. 22.

2. Australia's main stock exchange to use blockchain. Global Banking News (GBN) 2017.

3. Bezinga [Internet]. United States, Chatham: Newstex Finance & Accounting Blogs. 2017 2017-12-07. [cited 2018]. Available from: http://libproxy.murdoch.edu.au/login?url=https://search-proquest-com.libproxy.murdoch.edu.au/docview/1973499126?accountid=12629.

4. Benzinga: Today In Cryptocurrency: Japan Money Laundering Crackdown, Market Flooded With ICOs. Chatham: Newstex; 2018.

5. Bitcoin fallout: Mt Gox files for US bankruptcy protection. Money Life. 2014 2014/03/11/.

6. Bitcoin marketplace NiceHash hacked, over $60 mn lost. The Day After 2017.

7. China bans cryptocurrency "initial coin offerings". China Economic Review - Daily Briefings 2017.

8. China to completely ban cryptocurrency trading, SCMP says. The Fly 2018:0.

9. Chrome Web Store bans extensions mining cryptocurrency. Asian News International 2018.

10. Crime types: Australian Criminal Intelligence Commission 2018 [Available from: https://www.acic.gov.au/about-crime/crime-types.

11. Cryptocurrency drug trade, 2 held. The Times of India. 2018.

12. Fourth reimbursement of the Repayment program Ljubljana: NiceHash; 2018 [updated 2018-05-01. Available from: https://www.nicehash.com/news/fourth-reimbursement-of-the-repayment-program.

13. Google bans cryptocurrency mining extensions on Chrome. The Day After 2018.

14. InvestorIdeas.com: WISeKey's (SIX: WIHN) WIS.WATCH powered by VaultIC Semiconductor and NFC Technology designed to secure #cryptocurrency private keys is now available. Chatham: Newstex; 2018.

15. Kazakhstan Blockchain Association calls for cryptocurrency regulation in EAEU. Interfax : Central Asia General Newswire 2018.

16. Media Release: New Australian laws to regulate cryptocurrency pr. MediaNet Press Release Wire 2018.

17. Mt. Gox finds 200,000 missing bitcoins. Management Compass. 2014 19 May 2014.

18. NiceHash will fully reimburse its users Ljubljana: NiceHash; 2018 [updated 2018-01-31. Available from: https://www.nicehash.com/news/nicehash-will-fully-reimburse-its-users.

19. . United States, Chatham: Newstex. 2015-04-21. [cited 2018]. Available from: http://libproxy.murdoch.edu.au/login?url=https://search-proquest-com.libproxy.murdoch.edu.au/docview/1674518473?accountid=12629.

20. Private Key: Investopedia; 2018 [DEFINITION of 'Private Key']. Available from: https://www.investopedia.com/terms/p/private-key.asp.

21. Public Key: Investopedia; 2018 [DEFINITION of 'Public Key']. Available from: https://www.investopedia.com/terms/p/public-key.asp.

22. Second reimbursement of the Repayment program Ljubljana: NiceHash; 2018 [updated 2018-02-28. Available from: https://www.nicehash.com/news/2nd-reimbursement-of-the-repayment-program.

23. ShadowPad: How Attackers Hide Backdoor in Software Used by Hundreds of Large Companies Globally. Business World 2017.

24. South Korea bans anonymous cryptocurrency trading. Al Jazeera America 2018.

25. South Korea Considers Taxing Cryptocurrency Transactions – Finance Minister. Sputnik 2018.

26. South Korea Plans to Ban Cryptocurrency Trading. Business World 2018.

27. Third reimbursement of the Repayment program Ljubljana: NiceHash; 2018 [updated 2018-04-02. Available from: https://www.nicehash.com/news/third-reimbursement-of-the-repayment-program.

28. ValueWalk: Apple Bans Cryptocurrency Mining On Devices. Chatham: Newstex; 2018.

29. WISeKey's WIS.WATCH powered by VaultIC Semiconductor and NFC Technology designed to secure cryptocurrency private keys is now available. NASDAQ OMX's News Release Distribution Channel 2018.

30. Bentov I, Lee C, Mizrahi A, Rosenfeld M. Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake [Extended Abstract]y. ACM SIGMETRICS Performance Evaluation Review. 2014;42(3):34-7.

31. Brauneis A, Mestel R. Price discovery of cryptocurrencies: Bitcoin and beyond. Economics Letters. 2018;165:58-61.

32. Cheung A, Roca E, Su J-J. Crypto-currency bubbles: an application of the Phillips–Shi–Yu (2013) methodology on Mt. Gox bitcoin prices. Applied Economics. 2015;47(23):2348-58.

33. English C. Bitcoin kiddie porn: rpt. New York Post (New York, NY). 2018.

34. Foteinis S. Bitcoin's alarming carbon footprint. Nature. 2018;554(7691):169.

35. Gambe RL. South Korea planning ban on cryptocurrency trading. SNL Asia-Pacific Financials Daily 2018.

36. 2017 Global Cryptocurrency Benchmarking Study [Internet]. SSRN. 2017 [cited 30-06-2018]. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2965436#

37. Garvey P. Blockchain-backed gold: Mint’s answer to bitcoin. The Australian. 2018.

38. Guri M. BeatCoin: Leaking Private Keys from Air-Gapped Cryptocurrency Wallets. 2018.

39. Guri M, Elovici Y. Bridgeware: the air-gap malware. Association for Computing Machinery, Inc; 2018. p. 74-82.

40. Heston TF. A blockchain solution to gun control. PeerJ PrePrints 2017.

41. Hout MCV, Bingham T. 'Silk Road', the virtual drug marketplace: A single case study of user experiences. International Journal of Drug Policy. 2013;24(5):385-91.

42. Hoy MB. An Introduction to the Blockchain and Its Implications for Libraries and Medicine. Medical Reference Services Quarterly. 2017;36(3):273-9.

43. Jacquez T. Cryptocurrency the new money laundering problem for banking, law enforcement, and the legal system: ProQuest Dissertations Publishing; 2016.

44. Langner R. Stuxnet: Dissecting a Cyberwarfare Weapon. IEEE Security & Privacy. 2011;9(3):49-51.

45. Mowat L. Cryptocurrency shock as blockchain crime 'used to finance terrorism' in Ukraine. Express (Online). 2018.

46. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System2009.

47. Norge K. NiceHash crypto mining review from an expert Medium: Medium; 2018 [updated 20 May 2018. Available from: https://medium.com/coinmonks/how-to-make-35-usd-per-day-without-work-best-crypto-mining-11ef148f7ef7.

48. Olearchyk R, Murphy H. Ukraine steps up effort to regulate cryptocurrencies. FTcom 2018.

49. Phillips RC, Gorse D. Cryptocurrency price drivers: Wavelet coherence analysis revisited. PloS one. 2018;13(4):e0195200.

50. Pichel A. TrendLab Security Intelligence Blog [Internet]: Trend Micro. 2013 25-12-2013. [cited 2018]. Available from: https://blog.trendmicro.com/trendlabs-security-intelligence/new-cryptolocker-spreads-via-removable-drives/.

51. Roose K. Kodak’s Dubious Cryptocurrency Gamble. The New York Times. 2018.

52. Shaban H. People are using bitcoin’s system to share child pornography, researchers say: Bitcoin's blockchain offers a permanent tamper-proof record of financial transactions, but researchers say illegal content stored there can also pose a risk to users. Washington: WP Company LLC d/b/a The Washington Post; 2018.

53. Shi N. A new proof-of-work mechanism for bitcoin. Financial Innovation. 2016;2(1):1-8.

54. Smith M. Attackers hack Linux Mint website to add ISO with backdoor. Network World (Online) 2016.

55. Suberg W. NiceHash CEO Quits After 4,000 BTC Hack, Service To Continue Work. Cointelegraph. 2018.

56. Wimbush S. Cryptocurrency mining is neither wasteful nor uneconomic. Nature. 2018;555(7697):443-.

Part Two

Manuscript

Cryptocurrency and its Forensic Significance

Abstract

Cryptocurrency is a relatively new form of investment. Its concept was first introduced in 2009, and has grown ever since. To this day, there are thousands of cryptocurrencies. Just as other currencies, cryptocurrency can be related to a crime. Ever since its introduction nearly a decade ago, there have been crimes where cryptocurrency are related. According to ACIC's crime types, cryptocurrency are related to two crime categories: cybercrime, and illicit drugs. There are also other cases where the type of crimes is not listed as a part of ACIC's. To forensically examine exhibits related to digital crime involving cryptocurrency, tools such as Tableau Imager 3.1.2, EnCase 6.19.7, Internet Evidence Finder 6.2.3, and Winen.exe are available to assist in examination. Results obtained from such examination include includes identity of the owner or user of an account or device that was used in a crime, and matching address of a particular account to a transaction, including "criminal" transaction. One of the flaws of the mentioned tools was they were tested and proven in a study that was centred around Bitcoin and not cryptocurrency in general. Future studies can include testing the tools or similar tools, on other cryptocurrencies such as Ethereum, Bitcoin Cash, and Mixin.

Keywords: Cryptocurrency, Forensic, Crime, Tool, Case.

Introduction

Cryptocurrency is a relatively new form of investment. The concept of cryptocurrency was first submitted by Satoshi Nakamoto (39), where it was highlighted that cryptocurrency eliminates the requirement of a middle-man, such as banks, and that users are able to safely and securely conduct transactions.

Cryptocurrency is a form of digital asset, as it does not physically exist in the actual world. Over the years, there has been an increase in the number of cryptocurrencies types, and their number in circulation. More people are starting to invest in them as well. The price of cryptocurrency differs between each type, and the price of a single cryptocurrency coin could be as expensive as $13,000 (bitcoin)(22). Being a currency, cryptocurrency can be used in a crime, or at least a motivation in a crime. There have been reports of cases that are related to cryptocurrency in the last decade since their creation. As such, there is a need to be able to forensically examine the items related to such crimes.

The aim of this study is to explain cryptocurrency in details, including its components, and how they differ from flat currencies such as cash. A few cases that are related to cryptocurrency would also be discussed in order to understand their connection to cryptocurrency. The study is also aimed to explore the tools to forensically examine exhibits related to digital crime involving cryptocurrency.

What is Cryptocurrency?

Cryptocurrency are digital assets that are designed to work as a medium of exchange, using cryptography to secure its transactions, to control the creation of additional units, and to verify the transfer of assets (21). Cryptocurrencies can be classified as a subset of digital currencies. What is unique regarding cryptocurrency is that they utilise decentralised system; in decentralised banking system, boards or governments does not hold control over the system (21). This differs from traditional banking system, which utilises centralised control.

Components of cryptocurrency

Cryptocurrency trading involves several key components, including cryptocurrency keys, cryptocurrency wallets, blockchain, and cryptocurrency mining.

Keys

There are two types of keys that are essential in cryptocurrency trading: Private keys and Public keys. A private key is stored in a cryptocurrency wallet, and proves ownership of a public key (14). A public key is connected to a particular amount of cryptocurrency, and can be used to access that amount (15).

Private Key

A private key is a sophisticated form of cryptography that allows a user to access his or her cryptocurrency. In cryptocurrency trade, a use is commonly given a public address and a private key to receive cryptocurrency in a form of coins or tokens. The private key is made up of 51 alphanumeric characters, which make it hard for a hacker to obtain (14).

The private key of a user is typically stored in a digital wallet belonging to the same user. When a transaction is commenced, the wallet software creates a digital signature by processing the transaction with the private key. The signature is then used to confirm that a transaction has come from a particular user, and ensures that the transaction cannot be changed one it has been broadcasted into a blockchain. If a transaction is altered, the signature will change as well (14).

If the private key is lost, the user can no longer access their wallet to spend, withdraw, or transfer cryptocurrency (14). Hence, it is imperative that to save the private key in a secure location.

Public key

The public key is where cryptocurrency funds are deposited and received. It is a cryptographic code that allows a user to receive cryptocurrencies into their account (15). When a user initiates their first transaction with a cryptocurrency, a unique pair of public key and private key is created. The transaction would also be broadcasted to the network, where distributed nodes confirm the validity of the transaction, before finalising it and recording it on the blockchain. It was noted that before a transaction is broadcasted, it needed to be signed digitally using the private key. The signature would prove the ownership of the private key, but not divulge the details of the private key to anyone.

Since a public key is created based on the private key, the user's public key is used to prove that the digital signature came from their private key. Once the transaction has been verified as valid, the cryptocurrency funds are sent to the recipient's public address.

The public address is a hashed version of a public key. Since the public key is made up of extremely long string of numbers, it needed to be compressed and shortened, hence the creation of public address. In other words, a private key generates a public key, which then generates a public address. When two users agreed to conduct a transaction, they would reveal their public addresses to each other. The sender needs the recipient's public address to be able to send the funds to, which will then be able to spend or withdraw the amount using their private key. The recipient can also verify the sender's batch of cryptocurrency coins using the sender's public address, which is displayed on their screen.

Cryptocurrency wallets

Cryptocurrency wallets are essential component of cryptocurrency. They are digital wallets that are used to store, send, and receive cryptocurrencies. A cryptocurrency wallet is commonly used to store a private key that proves ownership of a public key, which is a public digital code connected to a particular amount of currency.

Categories of cryptocurrency wallets

Cryptocurrency wallets can be divided into two categories: cold wallet, and hot wallet. A cold wallet is generally considered to be effective for long-term storage of unused funds. A hot wallet is described as a type of wallet that is carried around for immediate use of the funds within. The key difference between hot and cold wallets is that hot wallets are connected to the internet, whereas cold wallets are not (5). Hot wallets are also considered to be more likely targets from hackers, as they're connected to the internet – cold wallets are offline/not connected to the internet; they are safe from hackers (5, 24).

However, despite having an offline feature to protect them from online threats, cold wallets are not immune to threats. A study found that a malware can be preinstalled, or pushed in during the initial installation of the wallet (30). Alternatively, it can infect the cold wallet's system when removable media such as USB flash drives is inserted into the wallet's computer in order to conduct a transaction. The study found that these attack methods have been repeatedly been proven feasible in the last decade (1, 16, 37, 42, 45). After obtaining a foothold in the wallet, a hacker can then utilise various air-gap covert channel techniques, including physical, electromagnetic, electric, magnetic, acoustic, optical, and thermal techniques(31). In summary, even though cold wallets provide a high degree of isolation, it is still possible for attackers to compromise such wallets and steal private keys from the owners.

Mining

Cryptocurrency mining is the process of generating new cryptocurrency in the form of coins. Cryptocurrency mining is called such, from to the fact that when transactions are added to the public ledger that is blockchain, new coins is created or in another word, mined (36).

Miners

As explained earlier, miners work together to verify transactions, ultimately mining new coins into the system. But that does not mean that all miners are on the same team. Cryptocurrency miners get rewarded in the form of some new coins for their hard work in mining coins, but the amount of coins rewarded are directly proportional to the contribution a miner had in the process of generating new coins (36). Hence, there are competitions amongst cryptocurrency miners in adding new transactions into the ledger as part of generating new coins.

How cryptocurrency are mined

In order to add transactions into a blockchain, all miners collect all transactions that were recently broadcasted by cryptocurrency users, verify the transactions, and compile them down into a transaction block – a condensed record of all transactions for that period of time. Cryptocurrency miners compete against each other to see who can solve a difficult, cryptographic puzzle first. As one miner found the solution, they broadcast the solution to all the other miners, for them to verify that the solution is correct. If the solution is indeed correct, the network adds the successfully-mined transaction block to the accepted blockchain permanently.

Where cryptocurrencies are mined

It was explained that cryptocurrencies are mined by miners, in which they solve a cryptographical puzzle to add transactional blocks into a blockchain, creating new coins as a result. As such, cryptocurrency mining can be done from practically everywhere, providing that the miner has access to a computer with sufficient computing power (20).

Blockchain

In terms of cryptocurrency, a blockchain is a public ledger of all a cryptocurrency's transactions. As new transactions are made, they are compiled into blocks, which will be added into the sequential blockchain. In order for a transaction to be considered successful, it has to be added into the blockchain. Once a transaction block is added into a blockchain, it will remain there permanently and is considered as public record (34).

How to trade cryptocurrency

Trading cryptocurrency requires having good background knowledge, and the components needed to trade cryptocurrency. The two main components a user needed to start trading cryptocurrency are cryptocurrency wallet, and cryptocurrency exchange. In terms of having good background knowledge, there are several notes to consider. First, a beginner should choose a trading company with a good reputation that offers an exchange and a wallet. A beginner should also trade prominent coins, as starter. Bitcoin and Ethereum are two of the most prominent coins as of June 2018 (22, 41).

How to spend cryptocurrency

One of the major concerns regarding cryptocurrency is finding ways to spend it. Conducting a search using a search engine was thought to be one of the best ways to look for ways, or merchants who accepts cryptocurrency. Gambling is also a way to spend cryptocurrency (43)

Spending cryptocurrency is not always possible, as some countries have banned trading of cryptocurrency. Some countries opted for a compromise in the form of regulations. Government regulations will be discussed in more detail below.

Government regulations

In response to several concerns such as environmental impacts of cryptocurrency mining and the risks of owning cryptocurrency, several governments had decided to take actions against cryptocurrency. Actions taken include total banning, and putting regulations in place.

China

As at February 2018, China had completely banned cryptocurrency trading within their country. The process actually began in September 2017, where it was announced that Chinese regulators declaring initial coin offerings illegal. This meant that cryptocurrency owners are not allowed to promote, much less sell, their cryptocurrency to anyone in the country. The regulatory action was said to be caused by growing fear from initial coin offerings, which caught investors' imagination that further led to phishing activities (6).

Ultimately, cryptocurrency was banned in total starting from February 2018. It was announced that the Chinese government's recent attempts to stamp out digital currency trading by shutting down domestic cryptocurrency exchanges were not successful in completely eradicating cryptocurrency trading, and that the government will strengthen measures to thoroughly remove any onshore or offshore trading platforms related to virtual currency trading (7).

South Korea

South Korea is another country that moved to regulate cryptocurrency. Initially, it was reported that South Korea planned to ban cryptocurrency trading, in light of cryptocurrency abuse. South Korea's justice minister at that time, Park Sung-Ki, mentioned there being great concerns regarding virtual currencies (19, 28). However, as at mid-January 2018, a ban had not been placed, but instead considered taxing cryptocurrency transactions, according to the South Korean finance minister at that time, Kim Dong-Yeon (18). Ultimately, the South Korean government officially banned anonymous cryptocurrency trading commencing at the end of January 2018 (17). This meant that cryptocurrency traders could only conduct cryptocurrency transactions from bank accounts set up under their real names.

Ukraine & Kazakhstan

Ukraine had started to intensify the search for methods to regulate cryptocurrencies, due to growing concerns in their capital, Kiev, that exploitation of the digital assets by criminals and geopolitical adversaries presented a growing national security risk (40). Ukraine's national security and defence council chief at that time, Oleksandr Turchynov, warned that the current legal vacuum posed a threat to the economy and security of the state. He also mentioned that given the rapid development of cryptocurrencies around the world, the issue could not be left out of attention, hence the plans to develop regulations. The soaring prices of cryptocurrency have made the market an increasingly lucrative target for cyber criminals. There was also a growing concern among regulators and governments that cryptocurrency could be used by organised crime-groups for money laundering (2, 35), and other criminal activities.

In a response to growing concerns of cryptocurrency being used, or simply being related to crimes, The Kazakhstan Association of Blockchain and Cryptocurrency submitted a proposal to the EAEU to create an advisory board on blockchain and cryptocurrency (10). The proposal was submitted during the Cryptoconference 2018 in Almaty, and had gathered some support for governments to adopt legislation to regulate the cryptocurrency market. The regulation was also aimed to prevent the use of cryptocurrency as a tool for illegal transactions, the legalisation of proceeds from crime, and the financing of terrorism.

Australia

As at April 2018, new laws for DCE providers operating in Australia were implemented by AUSTRAC (11). The new laws would cover regulation of service providers of cryptocurrency, such as cryptocurrency exchange marketplace.

The AUSTRAC CEO, Nicole Rose, announced that the new laws would strengthen the agency's compliance and intelligence capabilities to help DCEs implement systems and controls that can minimise the risk of criminals using them for purposes such as money laundering, terrorism financing, and cybercrime. With the new laws in place, DCEs with a business operation located in Australia must now register with AUSTRAC, and meet the government's AML/CTF compliance and reporting obligations.

How cryptocurrencies differ from flat currencies

As explained earlier, cryptocurrency differs from regular, flat currency. The difference lies in two major ways. Cryptocurrencies are only accepted as payment by other users – if no one accepts it, then it is considered worthless. Flat currency however, will always be accepted as payment by the government, at the very least. The second major difference is that cryptocurrency token supply is not managed by a central authority, whereas flat currency is managed by the government and can lead to either inflation, or deflation.

Popular cryptocurrencies (latest price)

There are thousands of cryptocurrency. It can be hard to determine which cryptocurrency is the best, or worst. There are several parameters that can be used to rank cryptocurrency: their price, market cap, supply rate, and existing volume in circulation. In terms of price, the four highest-ranked cryptocurrency as at June 2018 are Bitcoin, Bitcoin Cash, Mixin, and Ethereum (22).

Crime types in Australia

The types of crimes in Australia will be listed, and matched with some of the cases related to cryptocurrency discussed below. The types of crime happened in Australia according to Australian Criminal Intelligence Commission (ACIC) are illicit drugs, fraud, financial crimes, illicit firearms, money laundering, cybercrime, identity crime, exploitation of business structures, public sector corruption, and violence (8).

Some of the most recent crimes in relation to cryptocurrency

To understand more as to how cryptocurrency can be related to crimes, various case involving cryptocurrency in general, or a particular cryptocurrency such as bitcoin, various case that occurred in the last decade will be discussed below. Swoop for cases that occurred in the last decade was decided, as cryptocurrency, or at least the proof-of-concept, was published in 2009 by Satoshi Nakamoto (39).

6 December 2017 – Hacking of NiceHash

One of the case examples to be explained is the cyber-attack against Nicehash. The crime happened on the 6th of December 2017, where NiceHash, a crypto-mining company based in Slovenia, reported that their system was breached in a cyber-attack(4).

In terms of bitcoin-theft, the case was not the first reported case in the field. In February 2014, Mt. Gox, a bitcoin exchange based in Japan, reported a theft of 850,000 coins (12). Those bitcoins were worth nearly $500 million at that time. Mt. Gox were shut down not long after the case (13), and filed for bankruptcy protection in Japan, later that year (3). A study of this case found that a meteoric rise in price and rapid growth were associated with cryptocurrency, particularly bitcoin – this also attracted thieves/hackers (25).

Blockchain-related – Child pornography

In a report published in March 2018, German researchers found about 1,600 files of non-financial data, some linking to, or actually containing child pornography, and other objectionable materials, on the blockchain system that stores bitcoin transactions (44). It was explained that users of blockchain are able to add non-financial data for purposes such as describing a transaction's purpose, and insert benign messages or record information for other financial services. The objectionable contents were found to be imbedded in such data, and given that blockchain are viewable by practically all users, the data would be downloaded and persistently stored by them.

This discovery would place certain users of the bitcoin network in legal difficulties. The researchers also mentioned that this discovery could pose an obstacle for greater adoption and mainstream acceptance of bitcoin and other cryptocurrencies. Upon further analysis, the researchers found that most of the files were harmless, but some of the files contained copyright violations and the disclosure of the people's identifiable information, and at least eight files were said to containing sexual content (27). Amongst the child pornography materials, two files were found to contain 274 links to child pornography websites, and a file depicting a nude image of a minor.

Experts said that the files were likely to be downloaded as a part of notes to transactions, or inserted as the transactions themselves. Users of blockchain are able to add non-financial data for purposes such as describing a transaction's purpose insert benign messages, or record information for other financial services – anyone with access to bitcoin software such as miners, exchanges, and traders, have the ability to upload any content into the blockchain.

Arbitrary data insertion methods for bitcoin's blockchain

As explained before, aside from recording financial transactions, Bitcoin's blockchain are also able to be filled with non-financial data. Non-financial data can take a form of short messages via special transaction types, or even complete files. To add complete files into a blockchain, arbitrary data has to be encoded as standard transactions. There are two insertion methods for non-financial data: low-level insertion methods, and content insertion services.

Benefits and risks of arbitrary blockchain content

Bitcoin's blockchain design included several ways to insert arbitrary, non-financial data into its blockchain, both intentionally, and unintentionally. Potential benefits of engraving arbitrary data into the bitcoin's blockchain and the risks associated with them will be discussed further below.

Benefits

Bitcoin offered Coinbase, a digital currency exchange headquarters, and OP_RETURN, a special transaction template that allows one small data chunk as an attachment onto a transaction, as explicit channels to insert small chunks of non-financial data into their blockchain. The benefit of using OP_RETURN is that different services use OP_RETURN to link non-financial assets such as vouchers, to bitcoin's blockchain.

Risks

There are several risks associated with adding data into blockchain content, including copyright violations, malware, privacy violations, politically sensitive content, and illegal & condemned content.

In short, there are ways for someone to add an objectionable content into a blockchain, and cause harm if possessed or accessed by other users. Unlike systems such as social media platforms, file-sharing networks, and online storage systems, contents that are stored in a blockchain can be do so while remaining anonymous, making it hard to trace the culprit.

Examining the data (non-financial data)

There are three methods to examine non-financial data in a blockchain: low-level insertion methods detectors, and service detectors, and suspicious transaction detectors.

Low-level insertion method detectors

The low-level insertion method detectors were designed to match individual transactions that are likely to contain non-financial data. They detect manipulated financial transactions, as well as OP_RETURN, non-standard, and Coinbase transactions.

Service detectors

The service detectors enabled the detection and extraction of files based on the service' protocols, and also tracking of data used in service-created transactions.

Suspicious transaction detectors

The suspicious transaction detectors examine standard transactions that are likely to carry non-financial data, but were not detected. For a transaction to be examined by this method, it has to have at least 50 suspicious outputs.

Illegal drugs

There was a reported case in India about a drug trade related to cryptocurrency (9). An arrest was made by the police against two university students that were caught purchasing drugs using cryptocurrencies. The duo would purchase an amount of drug, and then have it transported into a particular place where it'll be picked up.

It was not the first case where cryptocurrency was used to purchase drugs. There was a case in 2011, where a university student sold/auction drugs via an online drug marketplace called 'Silk Road'. The student had created a fake profile and auctioned drugs online, where customers would buy, and have it delivered to an address of their choice. The method of payment was cryptocurrency, with different drugs cost different amount of coins. The case was ultimately solved when police made an arrest of the student in a public library, where he logged in into his Silk Road profile (33).

9 March 2018

In a newspaper article published on March 2018, it was announced that Pavel Lerner, a cryptocurrency businessman, was kidnapped in Ukraine by armed assailants, and was forced to pay $1 million ransom in the form of bitcoins from his digital wallet (38).

Base on the case examples mentioned, in terms of type of crimes in Australia by ACIC, cryptocurrency had been used in two categories of crimes: illicit drugs (Silk Road), cybercrime (hacking of NiceHash).

Cryptocurrency's forensic significance

As it was evident that cryptocurrency were used in various crimes, the need to understand how to forensically examine the items involved in a crime arose. It was explained earlier that to conduct a cryptocurrency transaction, a person would require a device (cryptocurrency wallet) and an account (of a particular cryptocurrency) (22, 41). As such, forensic examination would be conducted surrounding those components, both digital and hardware, that make up cryptocurrency transaction (26).

A study was done in 2015 by Michael Doran on forensically examine Bitcoin artefacts/exhibits. Details on various aspects of forensic examinations explained in that study will be included in discussions below.

Investigation process of digital evidence

According to DFRWS 2001, a successful Investigation Process in Digital Forensic science would contain 6 phases: 1) Identification, 2) Preparation, 3) Collection, 4) Examination, 5) Analysis, and 6) Presentation (26, 32). Processing a case surrounding cryptocurrency can be difficult due to the principles that Nakamoto implemented to keep cryptocurrency transactions anonymous. Due to anonymity, some evidence are more difficult to obtain and interpret (29).

Despite the difficulties, a successful investigation can be done by escalating though the process of the Investigation Process for Digital Forensic Science. It was mentioned that in the Collection phase, the forensic investigator needs to search for, document, and collect any object or data that could potentially contain digital evidence (23). These objects include cell phones, PDAs, laptops, tablets, desktop computers, or iPods. Various types of evidence may be available in the memory compartment relating to cryptocurrency, including running cryptocurrency processes and services, system information, information about logged-in users, registry information, chats history, recent cryptocurrency web-browsing activities, and running cryptocurrency malware. As evidence are collected, either physically or via data extraction or imaging, the forensic investigator can begin examining data and assigning the level of importance of each evidence (26).

Investigation methods of digital evidence

As explained above, evidence such as laptop and desktop computer can be collected and examined in regards to digital forensic investigation. To examine such evidence, both traditional and digital approach should be taken.

Traditional forensic

In this approach, a forensic examiner would examine the device itself, rather than the content. Aspects to consider include fingerprints, and DNA evidence from a sample that may be present on the exhibit. In dusting for fingerprints, the investigator would dust areas that are prominent with samples, such as keyboard on a laptop, and display touch-screen on a modern cell phone (46).

Digital forensic

The digital approach would examine the “content” of an exhibit such as laptop, rather than the surface. In the study by Doran in 2015, several tools were mentioned and used, including Tableau Imager 3.1.2, EnCase 6.19.7, Internet Evidence Finder 6.2.3, and Winen.exe (26). Tableau Imager 3.1.2 is a forensic imaging tool that is used to acquire a bit-for-bit copy of a piece of media. Encase 6.19.7 is a forensic program designed for forensic examiners and trained investigators who conducts full forensic examinations on any type of digital media. Encase allows the forensic examiner to acquire data rapidly from various types of device, and perform an in-depth forensic analysis of the media.

Internet Evidence Finder 6.2.3 is a forensic program that allows forensic investigators to recover data from social networking sites, instant messenger chats, file-sharing apps, mobile backups, web-browser history, and pictures & videos. In the study by Doran in 2015, the Internet Evidence Finder produced information such as the Public Key and the Public Key hash of addresses, and transaction history that was conducted in the test environment. By revealing the presence and identity of a Public Key in a particular device, it can be concluded that the owner or the user of the Key was indeed involved in a particular transaction - this could help in solving investigating illegal transactions such as drug payments, terrorist funding.

Lastly, Winen.exe is a RAM acquisition tool that collects information from a RAM and places the collected information into a file that can be stored on an external device (26). In the study by Doran in 2015, the analysis of a RAM under test environment provides results that matched the Bitcoin wallet addresses, transactions, and Bitcoin applications on the test system.

Conclusion

In conclusion, cryptocurrency indeed have a relation to crimes. There have been cases where cryptocurrency was used to commit a crime such as purchasing a drug, kidnapping a person and demand ransom in the form of cryptocurrency, and hacking into a cryptocurrency marketplace to steal cryptocurrency. Based on the crime types listed by ACIC, two crime categories have been proved to be related to cryptocurrency: cybercrime, and illicit drugs. As cryptocurrency are able to continue to rise, so too are the number of people that accept them as payments – this can be a cause for a crime. It was proven in a study conducted in 2015 by Michael Doran that tools such as Tableau Imager 3.1.2, EnCase 6.19.7, Internet Evidence Finder 6.2.3, and Winen.exe could be used to forensically examine the content of an exhibit related to digital crime. Information that can be acquired through such investigation includes identity of the owner or user of an account or device that was used in a crime, and matching address of a particular account to a transaction, including "criminal" transaction. One of the flaws of the study by Doran in 2015 was that the study was centred on Bitcoin and not cryptocurrency in general. Future study could try replicating or conducting similar study using similar tools used, on other cryptocurrencies such as Ethereum, Bitcoin Cash, and Mixin.

References

1. 25 Percent of New Worms in 2010 Are Designed to Spread Through USB Devices, According to PandaLabs. NewsRX LLC; 2010. p. 22.

2. Benzinga: Today In Cryptocurrency: Japan Money Laundering Crackdown, Market Flooded With ICOs. Chatham: Newstex; 2018.

3. Bitcoin fallout: Mt Gox files for US bankruptcy protection. Money Life. 2014 2014/03/11/.

4. Bitcoin marketplace NiceHash hacked, over $60 mn lost. The Day After 2017.

5. BitUN Release World's First Cryptocurrency Cold Wallet for Institutions. PR Newswire Asia U6 - ctx_ver=Z3988-2004&ctx_enc=info%3Aofi%2Fenc%3AUTF-8&rfr_id=info%3Asid%2Fsummonserialssolutionscom&rft_val_fmt=info%3Aofi%2Ffmt%3Akev%3Amtx%3Ajournal&rftgenre=article&rftatitle=BitUN+Release+World%27s+First+Cryptocurrency+Cold+Wallet+for+Institutions&rftjtitle=PR+Newswire+Asia&rftdate=2018-05-25&rftpub=PR+Newswire+Association+LLC&paramdict=en-US U7 - Newspaper Article. 2018.

6. China bans cryptocurrency "initial coin offerings". China Economic Review - Daily Briefings 2017.

7. China to completely ban cryptocurrency trading, SCMP says. The Fly 2018:0.

8. Crime types: Australian Criminal Intelligence Commission 2018 [Available from: https://www.acic.gov.au/about-crime/crime-types.

9. Cryptocurrency drug trade, 2 held. The Times of India. 2018.

10. Kazakhstan Blockchain Association calls for cryptocurrency regulation in EAEU. Interfax : Central Asia General Newswire 2018.

11. Media Release: New Australian laws to regulate cryptocurrency pr. MediaNet Press Release Wire 2018.

12. Mt. Gox finds 200,000 missing bitcoins. Management Compass. 2014 19 May 2014.

13. . United States, Chatham: Newstex. 2015-04-21. [cited 2018]. Available from: http://libproxy.murdoch.edu.au/login?url=https://search-proquest-com.libproxy.murdoch.edu.au/docview/1674518473?accountid=12629.

14. Private Key: Investopedia; 2018 [DEFINITION of 'Private Key']. Available from: https://www.investopedia.com/terms/p/private-key.asp.

15. Public Key: Investopedia; 2018 [DEFINITION of 'Public Key']. Available from: https://www.investopedia.com/terms/p/public-key.asp.

16. ShadowPad: How Attackers Hide Backdoor in Software Used by Hundreds of Large Companies Globally. Business World 2017.

17. South Korea bans anonymous cryptocurrency trading. Al Jazeera America 2018.

18. South Korea Considers Taxing Cryptocurrency Transactions – Finance Minister. Sputnik 2018.

19. South Korea Plans to Ban Cryptocurrency Trading. Business World 2018.

20. A voracious appetite; Mining cryptocurrencies. The Economist. 2018;428(9107):8.

21. Bouveret A, Haksar V. What Are Cryptocurrencies? Finance and Development. 2018;55(2):26-7.

22. Brauneis A, Mestel R. Price discovery of cryptocurrencies: Bitcoin and beyond. Economics Letters. 2018;165:58-61.

23. Carrier BD. A hypothesis-based approach to digital forensic investigations: ProQuest Dissertations Publishing; 2006.

24. Castiglione C. One Month: One Month

2017. [cited 2018]. Available from: https://learn.onemonth.com/hot-wallet-vs-cold-storage/

25. Cheung A, Roca E, Su J-J. Crypto-currency bubbles: an application of the Phillips–Shi–Yu (2013) methodology on Mt. Gox bitcoin prices. Applied Economics. 2015;47(23):2348-58.

26. Doran MD. A forensic look at Bitcoin cryptocurrency: ProQuest Dissertations Publishing; 2014.

27. English C. Bitcoin kiddie porn: rpt. New York Post (New York, NY). 2018.

28. Gambe RL. South Korea planning ban on cryptocurrency trading. SNL Asia-Pacific Financials Daily 2018.

29. Greenberg A. Follow the Bitcoins: how we got busted buying drugs on Silk Road's black market. Forbes Retrieved from http://www forbes com/sites/andygreenberg/2013/09/05/follow-thebitcoins-how-we-got-busted-buyingdrugs-on-silk-roads-black-market. 2013.

30. Guri M. BeatCoin: Leaking Private Keys from Air-Gapped Cryptocurrency Wallets. 2018.

31. Guri M, Elovici Y. Bridgeware: the air-gap malware. Association for Computing Machinery, Inc; 2018. p. 74-82.

32. Harrell C. Overall DF investigation process. Retrieved February: Journey Into Incident Response; 2010. p. 2014.

33. Hout MCV, Bingham T. 'Silk Road', the virtual drug marketplace: A single case study of user experiences. International Journal of Drug Policy. 2013;24(5):385-91.

34. Hoy MB. An Introduction to the Blockchain and Its Implications for Libraries and Medicine. Medical Reference Services Quarterly. 2017;36(3):273-9.

35. Jacquez T. Cryptocurrency the new money laundering problem for banking, law enforcement, and the legal system: ProQuest Dissertations Publishing; 2016.

36. Koblitz N, Menezes AJ. Cryptocash, cryptocurrencies, and cryptocontracts. Designs, Codes and Cryptography. 2016;78(1):87-102.

37. Langner R. Stuxnet: Dissecting a Cyberwarfare Weapon. IEEE Security & Privacy. 2011;9(3):49-51.

38. Mowat L. Cryptocurrency shock as blockchain crime 'used to finance terrorism' in Ukraine. Express (Online). 2018.

39. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System2009.

40. Olearchyk R, Murphy H. Ukraine steps up effort to regulate cryptocurrencies. FTcom 2018.

41. Phillips RC, Gorse D. Cryptocurrency price drivers: Wavelet coherence analysis revisited. PloS one. 2018;13(4):e0195200.

42. Pichel A. TrendLab Security Intelligence Blog [Internet]: Trend Micro. 2013 25-12-2013. [cited 2018]. Available from: https://blog.trendmicro.com/trendlabs-security-intelligence/new-cryptolocker-spreads-via-removable-drives/.

43. Roose K. Kodak's Dubious Cryptocurrency Gamble. The New York Times. 2018.

44. Shaban H. People are using bitcoin's system to share child pornography, researchers say: Bitcoin's blockchain offers a permanent tamper-proof record of financial transactions, but researchers say illegal content stored there can also pose a risk to users. Washington: WP Company LLC d/b/a The Washington Post; 2018.

45. Smith M. Attackers hack Linux Mint website to add ISO with backdoor. Network World (Online) 2016.

46. Sodhi GS, Kaur J. Powder method for detecting latent fingerprints: a review. Forensic Science International. 2001;120(3):172-6.