CRYPTOCURRENCY: A TOOL AND TARGET FOR CYBERCRIME

Article · December 2018

CITATIONS
7

READS
6,005

2 authors:

Eveshnie Reddy
University of South Africa
8 PUBLICATIONS **16** CITATIONS
SEE PROFILE

Anthony Minnaar
University of Limpopo
52 PUBLICATIONS **252** CITATIONS
SEE PROFILE

CRYPTOCURRENCY: A TOOL AND TARGET FOR CYBERCRIME[1]

Eveshnie Reddy[2] and Anthony Minnaar[3]

ABSTRACT

Cryptocurrencies are prevalent in South Africa and gaining traction as an alternative online currency. Concomitantly, cryptocurrencies are also establishing themselves as an ideal currency for cybercriminals due to their unregulated and pseudo-anonymous nature. Cryptocurrencies can be used either as a tool or target in the facilitation of cybercrimes, including cyber money laundering, cyber extortion, phishing, hacking, cyber fraud and other financial crimes such as Ponzi and investment scams. Given the highly technical, decentralised and thus complex nature of cryptocurrencies, it is important for criminologists to have a basic understanding of the modus operandi used in 'cryptocurrency crime'. This article, therefore, illustrates the use of cryptocurrency in the facilitation of criminal activity through the review of existing literature. This article begins with a brief discussion on the history of cryptocurrencies. The technical underpinnings of a cryptocurrency are thereafter explained in order to contextualise their use in the facilitation of cybercrime. Lastly, an exposition of the crimes is presented in order to demonstrate how cryptocurrencies can be used as a tool and target in the facilitation of cybercrime.

Keywords: *Cryptocurrency; bitcoin; cybercrime; online; unregulated.*

INTRODUCTION

Broadly, in computer security technology the term 'cryptocurrency' technically refers to a cryptographic string of numbers and alphabetic symbols. However, the cryptocurrency known as Bitcoin (BTC), as the first of its kind to be developed in 2008, has become synonymous with the term cryptocurrency and the two are often used interchangeably. However, as other cryptocurrencies were launched in competition to Bitcoin the word 'token' has also been used to refer to cryptocurrency, but more as a "digital asset that exists on another [i.e. other than Bitcoin] cryptocurrency's blockchain" (see later explanation of this term). For example, on the Ethereum Blockchain there are different tokens that represent different values, whereas Bitcoin is valued in straight US dollar terms (Anon., [sa]: np).

Both in South Africa and globally, Bitcoin, as a cryptocurrency, has become the cryptocurrency of choice and has gained widespread use. In South Africa alone, over thirty thousand merchants are accepting bitcoin as payment (Mckane, 2017: np; Naidoo, 2017: np; Staff Writer, 2018a: np). However, there are no accurate statistics for gauging the number of people using cryptocurrencies in South Africa. This is due to the non-regulation of cryptocurrencies in South Africa and consequently, the lack of mandatory reporting and tracking standards such as 'Know-your-customer' (KYC) and due diligence. Moreover, according to the value of such transactions, it was reported in 2016 by the leading cryptocurrency exchange, Luno, that global estimates reveal that bitcoin, for example, accounts for 236 175 transactions per day (Alfreds, 2016a: np). Luno further indicated that in 2017 alone, bitcoins to the value of R128m were traded over a three-day period (Naidoo, 2017: np).

1. This is a reworked article adapted from the first author's unpublished dissertation: *Security measures for new payment mediums: A case study of fraudulent transactions using cryptocurrencies*. (MTech in Security Management, UNISA, 2017).
2. Lecturer. Department of Criminology & Security Science, School of Criminal Justice, College of Law, University of South Africa. Email: reddye@unisa.ac.za.
3. Research Professor of Criminal Justice Studies. Department of Criminology & Security Science, School of Criminal Justice, College of Law, University of South Africa. Email: aminnaar@unisa.ac.za / anthony.minnaar@gmail.com.

On a global level, Cambridge University researchers, Hileman and Rauch (2017: 3), estimate that there are over three million unique individuals who actively use cryptocurrency. Cryptocurrencies are created over the Internet (which itself is decentralised and unregulated), administered in a peer-to-peer (directly from one person to another) mode, using cryptography to protect the validity of the transactions. This eliminates the need for intermediaries such as banks, central authorities and payment-clearing houses. Cryptocurrencies are thus not sovereign to any particular jurisdiction, but rather an 'international online currency', which by design precludes the opportunity for central control by the government. Cryptocurrencies currently have no legal status or regulatory framework under South African law (South African Reserve Bank, 2014: 12; National Treasury, 2014: 3).

The innovative, unregulated nature of cryptocurrencies, and the level of anonymity such currencies offer, all serve as the main catalysts for the increased criminal activity associated with cryptocurrencies (Bray, 2016: 27). Cryptocurrencies have thus proven to be both a tool and target for a multitude of cybercrimes. According to the United Kingdom HM Treasury and Home Office, (2017: 40):

> "The threat posed by [cryptocurrencies] is higher, owing to their role in directly enabling cyber-dependent crime. This is evident in three areas: firstly, [cryptocurrencies] directly facilitate victim payments to cyber criminals. This includes malware attacks such as ransomware, and cybercrimes-as-an-extortion, in which victim ransom payments are predominantly requested to be paid in Bitcoin. Secondly, [cryptocurrencies] aid the growth of cybercrime-as-a-service. They constitute the primary method of payment for criminal-to-criminal payments and for the purchase of illicit tools or services sold online in the cyber-criminal marketplace. The ease with which such tools can be bought through digital currencies lowers the barrier to entry for low-sophistication cyber criminals, directly contributing to the growth of cyber-crime-as-a-service. Thirdly, [cryptocurrencies] play a vital role in laundering the proceeds of cyber dependent crime, directly facilitating cyber-criminal financial flows."

AN OVERVIEW OF CRYPTOCURRENCIES: HISTORY AND CONTEXT

The introduction of the concept of cryptocurrencies originated in an academic paper published by Satoshi Nakamoto in 2008 (Nakamoto, 2008: 1; Schatt, 2015: 20). Since the creation of Bitcoin, a plethora of cryptocurrencies has emerged. After Bitcoin, Ether, Litecoin and Ripple are the three most widely used cryptocurrencies. Coinmarket Cap estimates that there are 1 400 types of cryptocurrencies currently in circulation (Coinmarket Cap, 2018: np).

Cryptocurrencies, such as Bitcoin, were started as a means to provide an electronic payment system that was more secure and resistant to fraud than credit cards, eliminating the need for trusted intermediaries such as financial institutions. Since cryptocurrencies were not controlled by a central institution such as a government (or a State's Central Bank) or even a governing nonprofit, they were supposed to give the holder the reliability of gold, without the inconvenience of having to transfer a physical item to make a transaction (Hartshorn, 2018: np). Therefore, the rationale for the existence of cryptocurrencies is based on the contention that the creation, distribution and control of money does not have to be managed by the state and/or central banks. Cryptocurrencies thus challenge the traditional belief that central planning is necessary in order for money to work (Fioramonti, 2016: np). In conventional societies, the creation, distribution and control of money is regulated by the state and central banks, accompanied by a plethora of monetary policies and regulatory standards that users must oblige to. Such money is, in essence, sovereign currency, which is given legal tender status under government decree (such as the South African rand (ZAR)).

The European Central Bank (ECB) (2012: 6) took the lead in classifying cryptocurrencies. According to the ECB, cryptocurrencies are a sub-set of virtual currencies that comprise the following three categories:

1. Closed virtual schemes. In closed virtual currency ('in-game only') schemes, as the name implies, transactions (the currency earned from activities within this world can only be used to buy virtual goods and services within this (gaming) world) are confined to the virtual world and thus the scheme itself does not have any link to the real economy or any financial or banking systems. The entry requirement for these types of schemes is usually a subscription fee. Upon payment of the subscription fee, users have the option to earn virtual money based on their virtual activities performed within these worlds. An example of this currency is World of Warcraft (WoW) Gold. The direct purchase of this currency can be made using fiat (official) currency. However, once purchased, this currency cannot be exchanged or converted back into fiat currency.
2. Schemes with unidirectional flow enable both in-game purchases (virtual goods and services) and real-world purchases (the purchase of real goods and services). Facebook Credits (FB) and Nintendo Points are examples of the type of currencies unique to this scheme.
3. In virtual currency schemes with bidirectional flow, users are free to buy and sell virtual currency in accordance with fiat currency exchange and thus can be used the same way other convertible currencies are used in the real world. Both real and virtual goods and services can be purchased with this type of currency. Examples of currencies unique to this type of scheme include Linden Dollars (L$) (currency of the gaming world *Second Life*) and Bitcoin.

Cryptocurrency is thus a sub-set of virtual currencies. However, it is important to note, irrespective of the above taxonomy, that cryptocurrencies were created for the "sole purpose of competing with legal tender" (Gans & Galburda, 2013: 1). In addition, the creation and technical underpinnings of a cryptocurrency is starkly different to that of virtual currency. For example: "A cryptocurrency is a math-based, decentralised convertible virtual currency that is protected by cryptography – it incorporates principles of cryptography to implement a distributed, decentralised, secure information economy" (Financial Action Task Force, 2014: 5). In contrast, virtual currencies have their roots in online gaming (virtual worlds). According to the ECB (2015: 25): "a virtual currency is a digital representation of value, not issued by a central bank, credit institution or e-money institution, which, in some circumstances, can be used as an alternative to money" (ECB, 2015: 25).

As clarified in Nakamoto's paper, "a purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution" (Nakamoto, 2008: 1). Thus, the primary purpose of cryptocurrencies is to serve as a medium of exchange (Franco, 2015: 12). However, it is beyond the scope of this article to provide a detailed discussion of the various financial applications and functions that cryptocurrencies can facilitate. For the purposes of this article, cryptocurrencies refer to a currency wherein the primary purpose is a medium of exchange or transfer of value.

The following elements of the cryptocurrency Bitcoin are presented in a systematic manner in order to provide a basic understanding of the cryptocurrency ecosystem. All altcoins (alternative cryptocurrencies other than Bitcoin) are based on the Bitcoin Protocol. These elements are essential in both the creation of the cryptocurrency and the functioning of the network.

1. Bitcoin uses open-source software. Open-source software has no restrictions in terms of who can access the software, leaving the network open for anyone to participate. This is similar to Facebook or Twitter and most Internet infrastructure. In order to be a part of the network (user) one must first download and install the software. The name of the Bitcoin software is 'Bitcoin core'.
2. Transactions take place on a peer-to-peer (P2P) network, which allows for direct communication from one user to another. This eliminates the need for intermediaries such as banks and payment clearing-houses, who serve to process or validate funds. When a credit or debit card purchase is made, for example, the transaction is only valid once a clearing-house has rendered it 'clear'.
3. While the use of intermediaries is eliminated, the transaction still needs to be 'cleared' or validated. To achieve this, the Bitcoin network uses a computational process known as '*mining'*. Mining, which serves to not only create cryptocurrencies, but also to validate transactions. Once a cryptocurrency is created, it employs cryptographic algorithms to protect the integrity of the transaction.
4. Public and private keys are used to transfer value from one person (or entity) to another and must be cryptographically signed each time transactions are made (keys are transferred) Proof of Work (PoW) or Stake of Work (SoW), depending on the type of cryptocurrency.
5. The key technological innovation behind the functioning of cryptocurrencies is the distributed ledger technology, referred to as the blockchain. It consists of several blocks that are generated each time a transaction is made and as such records the cryptocurrency addresses of the sender and recipient. The address identifies particular transactions and not bitcoins. All transactions are stored on a blockchain. The blockchain serves both as public leger (Schatt, 2015: 20-35; Franco, 2015: 60 - 95).
6. Accordingly, virtual 'wallets' and 'vaults' are used to store the bitcoin (represented by a string of numbers and alphabets)

The above elements work together to function as a secure, decentralised and distributed payment system and currency using 'intermediaries' that are 'outside' of the formal global financial and banking systems. In the world of cryptocurrency, there are two categories of intermediary institutions. The first category contains the exchanges where users buy, sell and store their virtual currency. The second category is made up of the people and companies who create and sell their own cryptocurrency, using what is called 'Initial Coin Offerings' (ICOs) (similarly to a company offering shares on the stock market in what is called an Initial Public Offering (IPO), which is basically a stock market launch) (Hartshorn, 2018: np).

THE USE OF CRYPTOCURRENCY AS A TOOL IN THE FACILITATION OF CYBERCRIME

The use of cryptocurrencies as payment for illegal goods and services on the Dark Web

The Dark Web and cryptocurrencies make up the ideal formula for quick, anonymous and relatively easy laundering of proceeds from illegal services and sales (Van Mieghem & Pouwelse, 2015: np). It is, therefore, not surprising that cryptocurrencies have become the payment of choice when it comes to electronic commerce on the Dark Web (Naik & Serumula, 2015: np). In 2018, the Centre of Sanctions and Illicit Finance in Canada and cybercrime investigation company Elliptic, conducted a joint study aimed at establishing cryptocurrency – money-laundering typologies. The study found that "darknet markets are a key source of illicit funds" (Fanusie & Robinson, 2018: 5). The Dark Web (also referred to as the 'darknet') is a corpus of websites that are visible to the public, but the Internet protocol (IP) addresses are

veiled with anonymity through software tools designed to anonymise the IP addresses. Therefore, no link to the servers of those addresses is available. The Onion Router (also known simply as TOR) and I2P (Second Order Intercept Point) are the most notable types of such software (Greenberg, 2014: np). TOR ranks as the highest used anonymous communication network with millions of daily active users (The TOR Project, 2017: np). According to data sourced from TOR, this is computer software that, once installed on a computer, manages all TOR connections. Once the TOR software is installed, it uses a chain of virtual channels, instead of a direct link, to connect users to a Dark website. The virtual channels enable the anonymous exchange of communication from individuals to organisations (or vice versa) over public networks through disguising or obscuring the Internet Protocol (IP) address. This makes it difficult to establish an IP address and consequently detect that particular Dark Website (Greenberg, 2014: np). The ease with which transactions can be facilitated on the Dark Web is set out below:

1. Finding a Dark Website (such as Agora, Alphabay, and so forth).
2. Installing the relevant tools.
3. When using your computer, your Internet protocol (IP) address shows. To eliminate this problem, Virtual Private Networks (VPN) are used with TOR to hide your location and identity. TOR and VPN can be downloaded on the Internet with full instructions.
4. Install encryption software for encrypting your communication. Pretty Good Privacy (PGP) software allows you to encrypt all communication you have chosen on the Dark Web. This can also be downloaded from the Internet.
5. Payment. Use PayPal or a credit card to purchase bitcoins from local Bitcoins.com Automatic Teller Machine (ATM); or exchange fiat cash for bitcoin. Storing the cryptocurrency in wallets. Download software such as Electrum or contact exchange companies that provide wallet services. The point is to evade identification on the web.
6. Create and set up your account. Choose your products, make your order.

Silk Road

In 2011, Ross William Ulbricht created a Dark Website known as Silk Road. Silk Road was a hidden website on the internet that served as an international online market place for the purposes of facilitating criminal activity. Primarily, Silk Road conducted and facilitated the online sale of narcotics, cybercrime exploit kits and credit card information, and even false passports. Secondly, Silk Road further enabled the anonymity of users by only accepting payment in bitcoin. Thirdly, in an effort to further anonymise transactions, Silk Road provided money-laundering services in the form of ‘mixers’ and ‘tumblers’ (see later section for an explanation of these two terms).

The United States government became aware of Silk Road in early 2011, and in order to ascertain the identity of the correct perpetrator, sought a Pen/trap order from the United States magistrates/judges in the Southern District of New York. The purpose of the Pen/trap order was to facilitate an undercover investigation that would ultimately provide evidence of the criminal activity facilitated on Silk Road, leading to the prosecution of the perpetrator(s). The investigation concluded in 2013 when the Federal Bureau of Investigation arrested Ulbricht. At the trial, Ulbricht admitted to creating the website, but denied that he administrated the website under the pseudonym, DEAD Pirate Roberts (DPR). Ulbricht was ultimately sentenced to life imprisonment without the possibility of parole (see Minnaar (2017) for more detail on the ‘takedown’ of Silk Road and the conviction of Ulbricht).

Darkode

An 18-month long joint global investigation, referred to as 'Operation Shrouded Horizon', led by the European Union's law enforcement agency, Europol, the US Federal Bureau of Investigations (FBI) and the United Kingdom National Crime Agency, involving the co-operation of 20 countries including Australia, Canada, Cyprus, Nigeria and the United Kingdom culminated in July 2015 with the arrest of more than 300 cybercriminals. These cybercriminals, using the TOR network, had created the 'Dark Web' Darkode. This served as an online forum for the electronic commerce and trading of (but not limited to) botnets, malware, stolen personal information, server credentials and credit card details – all obtained from hacking (FBI, 2015: np). However, following the shut-down of the Darkode Forum, the Darkode service was soon reactivated and updated; featuring blockchain proponents for the sole purpose of ensuring that users were not the police. The Darkode creation and its regeneration in a more sophisticated manner clearly shows that criminals will always find ways to counter online security controls and that is one of the key challenges that regulators, investigative authorities and cyber security experts continue to face in trying to get ahead of cybercriminals.

The use of cryptocurrency in the facilitation of money laundering

The Financial Crimes Enforcement Network (FinCen) provides for the following working definition of money laundering.

> "Making 'illegally-gained proceeds (i.e. 'dirty money') appear legal (i.e. 'clean'),' by 1) placing dirty money in the legitimate financial system, 2) layering it within additional transactions to obfuscate its origins, and 3) integrating it into the financial system with more transactions so the funds appear licit" (FinCen, 2017: np).

The design and technical underpinnings of cryptocurrencies do not require all the above-mentioned steps associated with the laundering of money. Placing (step one) for example, does not apply to cryptocurrencies because they are already an encrypted form of unregulated currency, which can only enter a regulated financial system if that system allows such. Cryptocurrencies, therefore, do not have to be 'placed' in a financial system to become 'clean' because various conversion services already exist for the purpose of 'cleaning' 'dirty' cryptocurrencies. Fanusie and Robinson (2018: 5) identified the following conversion services through which cryptocurrencies can be laundered:

- Bitcoin ATM operator;
- Bitcoin exchange;
- Crypto-exchange;
- Gambling services;
- Mixers; and
- Multi-service.

Exchange companies offer a formal platform for the direct buying and selling (or trading, depending on the exchange and type of cryptocurrency) of cryptocurrencies. However, because these exchanges are not subject to the standard regulatory requirements (proper and extensive due diligence and 'Know-Your-Customer' (KYC) processes) to which regulated and registered exchanges are subjected (such as the Johannesburg Stock Exchange or the New York Stock Exchange). As a result, these exchanges can be exploited for the facilitation of money laundering. In addition, cryptocurrency exchanges offer consumers the option to cash-out purchased cryptocurrency via pre-paid, virtual credit cards and money business services (MBSs) (commonly referred to as 'money exchangers'; MoneyGram is an example of a MSB as the middleman). These MBSs (similarly to cryptocurrency exchanges, may not always

implement proper KYC and due diligence processes thus further facilitating money laundering activities. Of particular concern, is the use of legitimate MBSs that intentionally provide money-laundering services (Europol, 2014: 42).

Liberty Reserve

In *Kats et al v United States of America, Southern District of New York, 2016 (13) U.S 368*, the co-accused was sentenced to twenty years in prison for facilitating money-laundering activities via Costa Rican online payment processor company, Liberty Reserve. In 2013, Costa Rican online payment processor company, Liberty Reserve, was ended due to its role in the facilitation of money laundering, seven years after its inception in 2006. According to the United States (US) Justice Department (2016: np), Liberty Reserve processed a total of 78 million transactions to the value of eight billion dollars. These transactions comprised of the proceeds from crimes such as credit card fraud, hack attacks, identity theft, Ponzi scams and investment scams.

Users were required to provide basic information such as a name, date of birth and an e-mail address. This user information was not verified because Liberty Reserve did not implement the standard compliance functions such as Know Your Customer or due diligence. Users were thus free to provide pseudonyms and false particulars without any risk of their true identities having been established. The *modus operandi* used to launder the money was strategically planned; the users arranged for a traditional bank to wire money to an unlicensed third-party exchanger, meaning there was little oversight or regulatory standards applied. The money was then converted into a virtual or cryptocurrency thereby rendering it untraceable to its original source. The digital currency was then deposited into a Liberty Reserve account without any limits on the transaction value. Charging only a one percent service fee on each transfer, Liberty Reserve even offered its clients shopping cart functionality. All the transactions were irrevocable.

The money laundering activities of Liberty Reserve escaped detection due to the *modus operandi* it used. Deposits were never received by Liberty Reserve; instead, Liberty Reserve used various MBSs. These MBSs purchased the currency in bulk from Liberty Reserve and, thereafter, sold the currency in smaller fractions to people who wanted to exchange their fiat currency into digital currency (BBC News, 2016: np; Pereira & Alba, 2014: 3-4).

Add-on services on the Dark Web: 'Mixers' and 'tumblers'

In addition to the commerce of illegal goods, the Dark Web is also a host to a relatively new phenomenon, 'cyber-money laundering'. In particular, specific cryptocurrency laundering services exist on the Dark Web, most notably bitcoin laundering services known as 'tumblers' or 'mixers'. These services allow users to transfer their cryptocurrencies into a pool of existing cryptocurrencies. In effect, the transfer 'mixing' or 'tumbling' the funds and disarranging the transaction addresses of sender and receiver. As a result, users ended up with newly generated cryptocurrency addresses, thereby further hiding the financial trail. This makes it easier to move money throughout the processes of the Bitcoin system. However, it does not stop here; additional money laundering services are available to those who wish to eventually exchange their bitcoins for cash. These services are anonymous and allow users to exchange their bitcoins for fiat currency via Paypal and Western Union (Ciancaglini, Balduzzi, McArdle & Rosler 2015: 8-9; Europol, 2014: 42).

Concerns about cryptocurrency exchanges utilisation for money laundering purposes were of concern, not only to organisations such as the Financial Action Task Force (FATF), Interpol, Europol and the FBI, but also to Central Banks and various countries' Financial Services Regulators as well. For instance, in June 2018 Japan's Financial Service Agency (FSA) announced that as cryptocurrency exchanges grew their holdings of customer

cryptocurrency funds the FSA would ensure that they were in full compliance with all current international Anti-Money Laundering (AML) rules. Those licensed exchanges found in the FSA April 2018 inspections to have insufficient AML measures in place for spotting suspicious transactions would receive so-called "Business Improvement Orders" to comply with the AML rules, inter alia recruiting enough staff to cope with the growing volume of transactions on their platforms, improving their ID-verification processes and instituting stronger cybersecurity measures on their trading platforms to deflect any hacking attempts. In June 2018 the Japanese FSA had also issued its first-ever license rejection to a cryptocurrency exchange (FSHO) after this exchange had failed to properly implement security and AML improvements. In addition, to further comply with the AML regulations the Japanese self-regulatory group of cryptocurrency exchanges (Japanese Virtual Currency Exchange Association) directed all their members to strengthen their AML measures by prohibiting member platforms from listing the anonymous cryptocurrencies such as Monero and Dash (Zhao, 2018: np).

CRYPTOCURRENCIES: A TARGET FOR CYBERCRIME

Cryptocurrency exchanges, wallet providers and payment processors can be attacked by cybercrime. Cryptocurrency exchanges and payment processors are not immune to traditional forms of cybercrime. Many exchanges and payment processor companies have reported hacking and phishing attacks, which resulted in the loss of the cryptocurrency Bitcoin, and in some case, insolvency and the closing of the attacked exchanges (Amir, 2015: np; Pauli, 2015: np; Van Zyl, 2014: np).

Hacking

Hacking is regarded as one of the most "long-standing and highly publicised categories of cybercrime" (Furnell, 2010: 173). Hacking originated as a covert technical ability designed to gain access to computer or networked systems for the purposes of risk and threat assessment testing. The term 'white hat' is used to describe hacking activities that are non-criminal in nature while the term 'black hat' refers to any criminal related hacking activity (or attempt thereof). However, currently, the term hacking refers to any activity that includes the gaining or attempted gaining of unauthorised access to information technology (IT) systems (Furnell, 2010: 174) to either steal information, alter information, or make changes to the software or hardware of a device (Sushmita, Venkatasubramanian & Sundar, 2014: 183; Clarke, Clawson & Cordell, 2003: 2).

Within the context of cryptocurrencies, the purpose of hacking serves to either gain access to the private key, which is the password to a virtual wallet in which the cryptocurrencies are stored. The keys are the used to 'open' the wallet and steal the cryptocurrency. Alternatively, the hacker could take control of the cryptocurrency mining pool and redirect all of its computing power to 'mine' (i.e. 'dig for' and find somewhere on the web) a cryptocurrency for themselves. In addition, the hacker could also use a malicious code to infect a specific miner or the system of a company that offers mining software. The malicious code would be designed to look for the private keys stored on their system. Alternatively, they hack into their mining pool account and change the pay-out addresses to the hacker or cyber-attacker's, so that the cryptocurrency can be paid out to them (Hacker9, 2016: np).

In 2014, the then largest bitcoin exchange company in the world, Japanese-based Mt Gox filed for bankruptcy following a hacking attack in which 850 000 bitcoins at a then estimated US$473 million was stolen from its digital vaults (Agence France Presse (AFP), 2016: np). Since the Mt Gox attack, there have been numerous hacking, phishing and malware attacks on crypto-exchanges all over the world resulting in the loss of cryptocurrency, and in some cases, the closure of exchanges. Since then the following cryptocurrency exchanges were subject to major hacking attacks.

1. In 2014 it was reported that a Canadian wallet company, Flexcoin, had been subject to a cyber-attack in which more than US$500 000 worth of bitcoins were stolen (Rizzo, 2014: np).

2. In 2015 Kenyan Bank NIC experienced a ransom-type scam. It is alleged that two computer experts hacked into the bank's customer database and ordered a ransom of 200 bitcoins – the equivalent of KSh 6.2 million at the exchange rate at the time. It is alleged that the bank was threatened by the hackers who claimed they would circulate confidential customer information if the ransom was not paid (Commonwealth Working Group, 2015: 13).

3. In January 2015, bitcoin exchange Bitstamp suffered a hack in which 19 000 bitcoins were stolen. The estimated worth of the bitcoins was US$5 million. Despite the hack, Bitstamp is currently at the forefront of cryptocurrency exchanges, taking first place to its predecessor, Mt Gox.

4. In 2016, Hong Kong-based bitcoin exchange Bitfinex, lost an estimated 120 000 bitcoins to the value of US$72 million. The hack negatively impacted the cryptocurrency and caused the cryptocurrency price to drop in two days from US$603 per one bitcoin to US$ (Bovaird, 2016: np).

5. In one audacious Bitcoin theft scheme, Michael Richo, a 35-year-old from Connecticut in the US, started out in 2016 with a scheme to steal bitcoin from people involved in illegal deals through dark web marketplaces. Richo's modus operandi was as follows:

   i) created fake login pages for various online marketplaces;
   ii) posted links to them on a number of dark web forums;
   iii) when individuals attempted to log in, they effectively handed their username and password to him.

Once he had 'hooked' a victim, he monitored these accounts and as soon as the victims deposited bitcoins with the real marketplace, he withdrew the bitcoins to his own bitcoin wallet before the individual could spend them. He then sold the stolen bitcoins to others in exchange for US currency, which was then deposited into bank accounts he controlled or was provided to him through Green Dot Cards, Western Union transfers, and MoneyGram transfers. This last step of the scheme is what led investigators to him. When he was arrested, they found over 10 000 stolen user credentials on his computer. It was estimated that he managed to steal over $365 000 through this scheme. He was eventually charged with access device fraud, computer fraud, wire fraud, identity theft and money laundering offences.

During 2017, cryptocurrency hacking escalated considerably with a number of exchanges and traders in various cryptocurrencies being attacked and losing large amounts of either bitcoins or other cryptocurrency tokens. Among the major cryptocurrency hacks during the year were the following:

6. In July 2017, Bithumb, one of the largest Bitcoin and Ether exchange platforms suffered a breach resulting in the theft of billions of South Korean Won (Waqas, 2017: np).
7. Also in July 2017, CoinDash (ISO), an Israeli cryptocurrency social trading start-up announced that its crowdfunding page was compromised during a Token Sale event and as a result, hackers stole Ethereum tokens worth US$7 million (Waqas, 2017: np).
8. Again in mid-July 2017, Veritaseum, another cryptocurrency platform announced that their Initial Coin Offering (ICO) suffered a data breach in which around US$8.4 million worth of Ethereum were stolen (Waqas, 2017: np).

9. On 20 July 2017, an unknown hacker stole US$32 Million in Ethereum from three Multisig wallets by exploiting a critical security flaw in its multi-signature wallet software (Waqas, 2017: np).

10. In August 2017 there occurred a breach of the Enigma Marketplace, which was a decentralised marketplace and cryptocurrency investment platform from which hackers stole US$500 000 in Ethereum tokens (Waqas, 2017: np).

11. Later in the year (November), Tether, a start-up firm offering dollar-backed cryptocurrency had their security wall breached with the hackers removing US$30 million worth of cryptocurrency tokens from the Tether Treasury wallet and sent to an unauthorised Bitcoin address. This forced Tether to suspend the Tether back-end wallet service and, as a result, also announced that they would not redeem any of the stolen tokens and would attempt to recover them or alternately block them from entering the broader cryptocurrency system. By blacklisting the stolen tokens, hackers would then not be able to convert them to US dollars. But, irrespective of such blacklisting, those tokens were lost to the cryptocurrency traders subscribed to Tether's wallet services (Waqas, 2017: np).

12. But these were not the last cryptocurrency hacks in 2017. In early December 2017 hackers carried out a heist on a leading digital currency platform, NiceHash, stealing more than 4 700 bitcoins worth more than US$70 million. NiceHash, which described itself as the largest marketplace for mining digital currencies, suspended its operations because of this security breach (Iyengar, 2017: np).

13. In late December 2017 the last of the major cryptocurrency hacks occurred when the Seoul, South Korea-based bitcoin exchange, Youbit, closed down and entered bankruptcy proceedings after a cyberattack claimed 17 percent of its bitcoin assets (Kong & Tweed, 2017: np).

These cyber heists of bitcoins and other cryptocurrency tokens are reminders about the inherent vulnerabilities of certain digital currency platforms.

Phishing

Phishing is a type of cybercrime that uses social engineering tactics, in particular, e-mail communication to deceive individuals or organisations into believing that they are communicating with legitimate established enterprises. In phishing attacks, e-mail communication is used as the *modus operandi* to carry out the attack. The aim of a phishing attack is to successfully deceive the victim into believing that the communication received is from a legitimate enterprise, such as a bank. Once this is achieved, the objective is to yet again deceive the victim into providing the 'phisher' with personal information. Such information usually comprises of bank account details, credit or debit card details, addresses and personal identification numbers (ID) (Maras, 2012: 352). In the case of cryptocurrencies, the information targeted is wallet addresses, which comprise of a string of numbers. A twist to the direct hacking and stealing from a cryptocurrency exchange is the 'spoofing' of a legitimate exchange website. The following are examples of payment-processor companies and cryptocurrency exchanges that suffered phishing attacks:

1. In 2015, Ukraine victims lost over US$50 million due to a phishing attack. Spoofed websites were created to represent legitimate Ukrainian online wallet service, Blockchain. Info. The perpetrators used the same wallet service name, but changed the spelling in subtle ways in order trick users. For example: 'block-clain.info' and 'blockchien.info' (Amir, 2015: np).
2. Atlanta-based bitcoin payment processor company, BitPay, was the victim of a phishing attack, which resulted in losses amounting to US$1.8 million dollars. The modus operandi to perpetrate this phishing attack took the form of a classic identify theft style, stealing the identity of the company's Chief Financial Officer (CFO). Using a fake e-mail address and under the stolen identity of BitPay's CFO, the perpetrator requested three separate transactions of 5 000 bitcoins to be transferred to SecondMarket. The perpetrator solicited details regarding BitPay's procedure of transactions from BitPay's customers. The perpetrator twice requested transactions to SecondMarket to the value of 1 000 bitcoins, using an identified wallet address, and then requested 3 000 bitcoins to be sent, using a different wallet address. The perpetrators gained access to the BitPay's wallet, which was provided by bitcoin exchange Bitstamp (Amir, 2015: np).
3. Canadian bitcoin exchange Cavirtex suffered a breach attack in 2015 that resulted in its closure. It is alleged that two factor authentication credentials were compromised through a phishing attack. The attack affected two factor secrets and hashed passwords stored in an older database and did not match log-in details to identification records. Users were advised to immediately change their passwords and erase Cavirtex browser cookies. Luckily, the attack did not result in the loss of customer funds (Pauli, 2015: np).
4. Digital currency exchange service, Shapeshift, head-quartered in Zug, Switzerland, had to go offline after a security incident. An unknown quantity of funds had been taken from the service's connected wallets. Customers with pending orders would receive their money within 24 hours; the company said Hardware digital asset wallet, KeepKey, has integrated with Shapeshift, as security concerns following the Bitfinex hack drive demand for cryptocurrency cold storage solutions. A statement said the number of KeepKey users had exploded since the Bitfinex attack (Allison, 2016: np).
5. In mid-2017, the US-based cryptocurrency exchange Bittrex, known for buying and selling cryptocurrencies and digital tokens became a target for hackers. But, the modus operandi of the hackers was to set up a fake website pretending to be the official site for the Bittrex exchange. But, in reality, it was a phishing domain, not only stealing login credentials of unsuspecting users, but also the money saved in the exchange. The original site address for the Bittrex exchange was Bittrex.com while the fake one was: Blttrex.com. The difference between both addresses was 'i' and 'I' or 'L' instead of an 'i', all of which was enough to target those unfamiliar with phishing webpages. In addition, the fake site was a replica copy of the login page of Bittrex, again something which assisted the cyber criminals to carry out their scam (Amir, 2017: np).

Malware (malicious code)

Malware is an umbrella term that refers to malicious software. This malicious software, as the name implies, is designed to cause damage to a computer or network. It has the objective of bypassing authentication or securing remote access to computers and related devices in order to carry out their main aim, which is usually the theft of information (Maras, 2012: 349; Vinay & Balakrishnan, 2014: 387-388). Historically, viruses, Trojan horse programs and worms were the main types of malware. In recent years, there has been a steady expansion of the

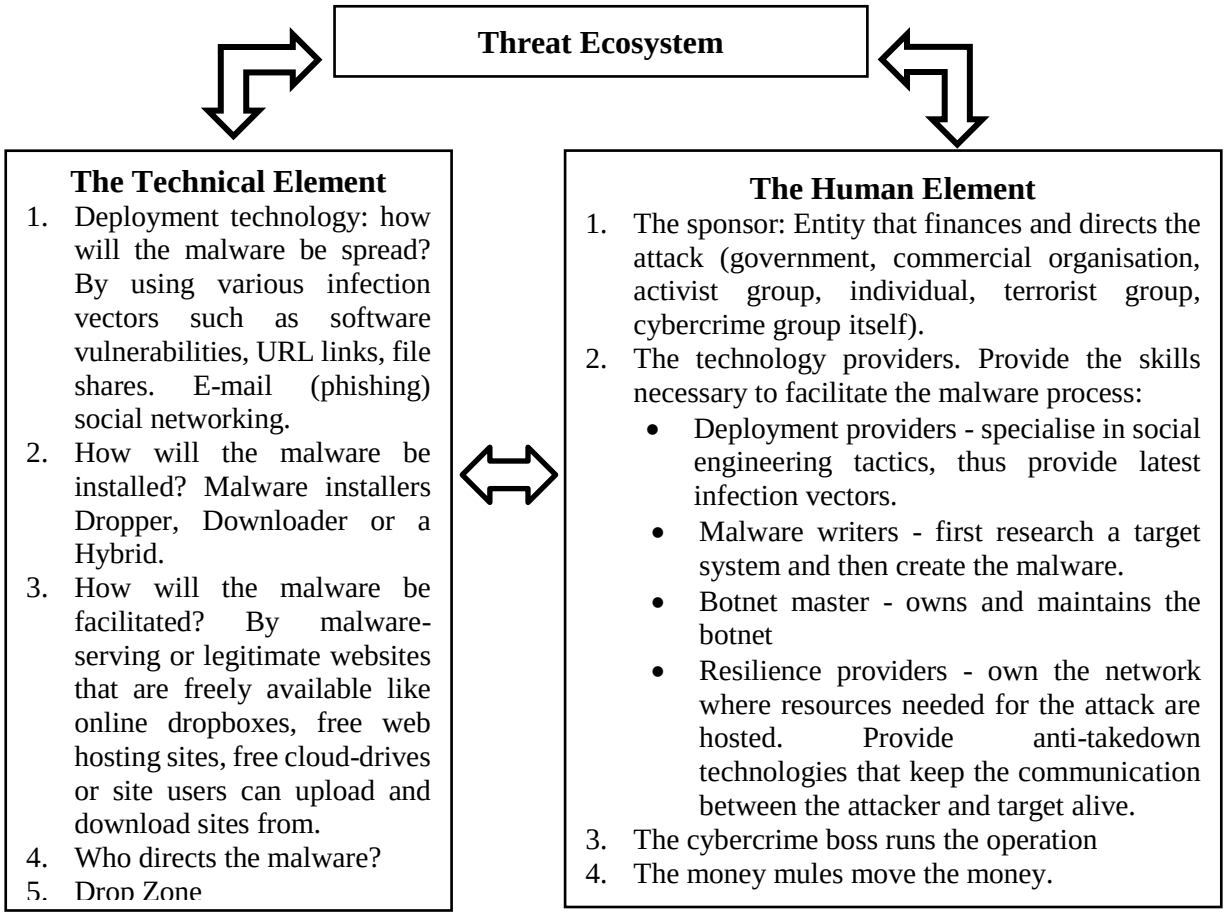
sophistication in the design as well the ability of malware to cause massive damage to large-scale systems (Elisan, 2013: 16-56; Vinay & Balakrishnan, 2014: 387).

Currently, the term is wider and includes other types of legitimate automated programmes that can be used for malicious activity. Such terms include bots (also referred to as botnets, bot army, bot herd, zombie horde and zombie network) and riskware (which comprises spyware, adware, hacker tools and joke) (Elisan, 2013: 57). Malware is, therefore, considered a priority crime in most jurisdictions. This has been illustrated in South Africa through the promulgation of the South African Cybercrimes and Cybersecurity Amendment Bill of 2015. In particular, chapter 2, section 9 of the Bill makes specific provision for the detection and investigation of malware-related crimes (Cybercrimes and Cybersecurity Bill of 2015, 2015: 18-19).

Network security experts, James and Sherin (2014: 361) contend that managing vulnerabilities in software is challenging, largely due to the complexity, extensibility and connectivity of networked systems. The decentralised structure of the system and its open-source software allow for design and improvement of the protocol, and the system can become more vulnerable to certain types cybercrime. An example of such vulnerabilities is the 'fixed open space' on the blockchain ledger (on certain cryptocurrency protocols) was discovered by a team of researchers from Interpol. According to the research findings, this 'open space' in the blockchain can be used to embed malicious code and other illegal information such as child abuse images and so on (Interpol, 2015: np; Reutzel, 2016: np).

Malware threat ecosystem

Figure 1: The Malware threat ecosystem



(Source: Authors' own elaboration as adapted from Elisan, 2013: 86-100).

The above figure illustrates the technical and human elements involved in a cybercrime pursuit. The variants used in the technical elements are not explained in further detail, because that would be beyond the scope of this article. Evident from the figure, both the technical and human elements are interdependent on each. Both create the malware and carry out the planned goal of stealing data. Now that the threat ecosystem of malware have been set out, the following section presents the different types of malware and their *modus operandi*.

Types and purpose of cryptocurrency malware

The following table represents the malicious codes that targeted the cryptocurrency Bitcoin. Specific mining and wallet-stealing malware was detected in 2014. Since then, these types of malware have evolved to more advanced types or changed completely to more sophisticated types (Trend Labs, 2014: np).

Table 1: Types of cryptocurrency malware

Detection name	Modus operandi	Detection date
BKDR_BTMINE	*Mines* bitcoins by downloading *miners*	2011
KELIHOS	Looks for and steals *wallet.dat* files	2013
SHIZ	Monitors bitcoin-related processes for stealing purposes	2013
COINMINE (DevilRobber)	Copies all of the contents of *wallet.dat* and sends them to File Transfer Protocol (FTP) servers	2013
FAREIT/TEPFER (Pony)	Looks for and steals *wallet.dat.wallet,* and *electrum.dat* files	2014
KAGECOIN	*Mines* for bitcoins on Android devices	2014
PONYBOTNET	Steal personal information	2014
TROJAN.COINBITCLIP	Transports an extensive list of bitcoin addresses and then switches it with the closest match. This tricks the user into sending cryptocurrency to the perpetrator.	2014
BITCOINWISDOM	Uses malicious code to redirects payments to the bitcoin addresses.	2015
CRYPTOWALL	Ransomware encrypts files demands ransom in bitcoin	2015
CRYPTOLOCKER	Ransomware encrypts files demands ransom in bitcoin	2015
CRYPTOJACKER	*Mines* cryptocurrency on infected computers and funnel earnings back to its criminal controllers	2018

(Source: Authors' own elaboration as adapted from, TrendLabs, 2014; Brave New Coin, 2014; Ward, 2014; Stoyanov, 2014; Cyprus Mail, 2014).

Cyber extortion and Ransomware

Research conducted in 2014 by the European Police Office (Europol) revealed that the cryptocurrency Bitcoin was used as ransom in an estimated one third of reported cyber-extortion cases in Europe. Of these reported cases, Europol noted that Bitcoin also featured as a ransom option in real-life kidnapping cases. From all the cryptocurrencies in circulation, Bitcoin is thus the single most common decentralised cryptocurrency used in extortion cases (Europol, 2014: 3). The following examples illustrate how the malicious code, *cryptolocker*, attacked certain computer networks by encrypting files on those specific computers and demanding bitcoins to be paid as the ransom.

Cryptolocker

Both in South Africa and internationally, there has been a rapid rise in both organisations and individuals becoming victims of the ransomware virus, Cryptolocker (ITWeb, 2016: np). In South Africa, the statistics are unclear. News and media reports have highlighted incidents of the Cryptolocker virus, but the extent in terms of victims and monetary loss remain unknown. For example, media coverage by the investigative television show, Carte Blanche, revealed that Cryptolocker targeted a few small companies in 2015. SA and local companies are not reporting incidents for fear of reputational damage. The impact of ransomware is difficult to calculate, since many organisations opt to simply pay to have their files unlocked. A report on the Cryptowall v3 ransomware campaign, issued in October of 2015 by the Cyber Threat Alliance, estimated that the cost of that single attack was US$325m (Alfreds, 2016b: np).

On the international front, countries such as Australia and the United Kingdom have suffered ransom attacks, which targeted 500 000 victims with a profit of US$3 million dollars (Ward, 2014: np). These viruses encrypt computer files and demand a ransom to decrypt the files; the ransom of choice being the cryptocurrency Bitcoin. Perpetrators use traditional cybercrime methods, such as phishing (e-mail), spam, fake software updates and drive-by-download attack on a bogus or spoofed website. The intent is to lure a victim into clicking or opening the link or attachment. Once the attachment is opened, the malware is released and is directed straight to the hard drive of the computer, which is then encrypted by the malware. The victim's computer screen will then read 'ransomware alert', which cannot be minimised. It is then at this point that the perpetrator will 'offer' to decrypt (unlock) the files or hard-drive upon payment of bitcoins (Blackwood, 2015: np). The deployment methods used to spread the Cryptolocker virus, to date, have been via phishing attacks, spoofed websites and bogus software updates.

In order to pay the ransom in bitcoin, the victim(s) first have to acquire bitcoins. In some instances, the alert comes with a message that advises the victim how to go about acquiring these bitcoins. Bitcoins can be acquired in one of three ways. The first, and easiest way, is to purchase bitcoin from a local exchange company.

The second option is to purchase bitcoin directly from another person. The third and perhaps most difficult way to obtain bitcoins is through mining as a user on the bitcoin network. Once a victim purchases bitcoin from this exchange company and pays the ransom to the perpetrator, the perpetrator can then easily exchange that bitcoin for the legal tender of that jurisdiction – like bitcoins for the South African rand or bitcoin for US dollars. Since most exchanges are not subject to any regulatory laws or due diligence processes, the source of the funds being exchanged is not probed, giving perpetrators the freedom to commit this crime with much ease and little fear of conviction (for more detailed information on how ransomware works see Minnaar, 2016).

In October 2015, UK telecoms company, TalkTalk, experienced a cyber-attack that stole subscriber details. Upon receipt of the stolen details, a ransom demand of bitcoin was made. The extortionists behind this ransom demanded the number of bitcoins to be equivalent in value

to £80 000 in fiat currency. The proceeds of this crime were estimated at US$3million (Ahmed, 2015: np).

Computer security firm Trend Micro warns that ransomware will continue to flourish as threats evolves and new ransomware techniques are developed. In addition, the target market is wider as ransomware reaps profits from larger organisations, such as educational and healthcare institutions, government agencies and other big businesses or service providers (Trend Micro, 2018: np).

Scams and Ponzi Schemes

In January 2015, researchers Marie Vasek and Tyler Moore examined a number of fraudulent websites in order to gauge the number of cryptocurrency scams between 2011 and 2014. The findings of the study indicated that forty-one scams were in operation for the period 2011-2013. The scams targeted 13 000 victims in total with an estimated monetary loss of US$11 million. These researchers define a scam as "operations established with fraudulent intent" (Vasek & Moore, 2015: 15).

A Ponzi scheme is a type of scam that uses an investment business front to deceive people into investing money. The perpetrators behind Ponzi schemes usually lure people (or entities) into investing their money by promising the investors high profits at little or no risks. Using a cyclic technique, existing investors are paid with the money provided by the new investors and thus the money in reality is not invested anywhere at all. This type of scam is dependent on a constant cash flow in order to carry on (Maras, 2012: 353). The following cases represent Ponzi schemes using the cryptocurrency Bitcoin.

1. The Security and Exchange Commission v. Shavers (No. 4:13-CV-416)

In 2013, the first federal securities fraud case involving a bitcoin Ponzi scheme was opened. The mastermind behind this scheme, Trendon Shavers, ran a Ponzi scheme named Bitcoin Savings and Trust (BCS&T) in which he defrauded investors. Using the traditional modus operandi technique unique to Ponzi schemes, Shavers lured investors into investing bitcoins with the guarantee of high returns. In reality, the invested bitcoins were never invested anywhere, but rather used to pay new investors. After a three-year investigation (2013-2016) Shavers was found guilty of wire fraud and securities fraud and was sentenced to 18 months imprisonment with a fine. It was reported that Shavers fraudulently gained an estimated 146 000 worth of bitcoins from this scheme, a figure worth US$807,380 based on the average price of bitcoin during the time the scheme was active. Currently, 146,000 worth of bitcoins average to US$97 million dollars. This is the amount Shavers would have fraudulently gained had the scheme gone undetected (United States Department of Justice, 2016: np).

2. Community X

In December 2013, a Dark Web site called Community-X was created. This website was dedicated to the manufacturing, selling, buying, distribution and passing of counterfeit Ugandan Federal Reserve Notes (FRNs), which were claimed to have been manufactured by the creator of the Community X. An online forum was used to advertise the sale of the Federal Reserve Notes and also served as an information sharing medium on how to best distribute the notes. Once the notes were sold, they were disseminated via out of sight stores in Uganda and the Unites States of America (USA) in exchange for bitcoins. Expert teams within the FBI tracked down the website in 2015 (FBI, 2015: np).

3. Cyprus

A warrant of arrest based on fraudulent activity was issued for the founder of Cyprian company, Neo & Bee. Neo & Bee practised as an organisation that allowed concomitant deposits of bitcoin and Euros. However, customers claimed that they did not receive their purchased bitcoins. The organisation was operational in two areas of Cyprus, however, no reported

incidents of fraudulent activity in Nicosia were noted (Commonwealth Working Group, 2015: 12).

4. BTC Global

In 2018, an estimated 27 500 people, including, Americans, South Africans and Australians were scammed into investing between R16 000 and R1.4-million with commodities and forex trading company, BTC Global. The current estimated monetary loss stands at US$50 million and could increase if more victims come forward. The investigation is being spearheaded by the Hawks and it remains unknown whether the scam was a Ponzi scheme. In addition, the identity and nationality of the perpetrators has not yet been established. One of the charges against BTC Global includes the contravention of the Financial Advisory and Intermediary Services Act. It remains to be seen if this charge will stand. If BTC Global is successfully charged with the said contravention, it may set a precedent for other legislative developments pertaining to the use of cryptocurrencies in South Africa (Staff Writer, 2018b: np).

CONCLUSION AND RECOMMENDATIONS

This article has tried to broadly illustrate the use of cryptocurrency in the facilitation of a variety of cybercrimes utilising cryptocurrency exchange blockchain technology (anonymity of transactions) and other cyber-vulnerabilities in the process. As is evident from some of the above-mentioned cases, cryptocurrencies are an international online currency that can be used in many ways to facilitate cybercrime. Strategic and collaborative efforts by investigative authorities on a global level are thus crucial in the successful prosecution of such cybercrime. Further research should be carried out in order to:

a) identify the key challenges that cryptocurrencies present to the South African criminal justice system in terms of investigation and prosecution;

b) determine the effectiveness of current criminal and procedural laws in effectively investigating and successfully prosecuting cryptocurrency-related crime;

c) improve international policing co-operation against cybercriminals; and

d) enhance co-operation between law enforcement agencies and utilise cybersecurity expertise from the private sector and adopt the latest/updated preventative and investigative software to combat the use of cryptocurrencies by cybercriminals on the Dark Web.

With reference to the last recommendation, law enforcement agencies around the world have also begun targeting in particular Bitcoin use in the facilitation of criminal activities on the Dark Web. But, as law enforcement agencies started adopting software tools developed by cybersecurity companies to monitor people using Bitcoin, and as per usual response by criminals, cybercriminals began switching to other cryptocurrency tokens. In November 2017 Europol had raised the alarm and identified Monero, (designed to avoid tracking) Ethereum and Zcash as becoming more popular for use on the digital underground. Europol had found that online extortionists/blackmailers, using ransomware to lock their victims' computers until they made a payment in cryptocurrencies, had switched to demanding their ransom in these cryptocurrencies (Monero being the most popular) instead of Bitcoin (Kharif, 2018: np).

But, as the fight against the use of cryptocurrencies continues with technical advances, so too does the development of more 'private' and untraceable cryptocurrencies. They go, so to speak, hand-in-hand. In Monero's case, criminals began using it as law enforcement instituted better tracking software, Bitcoin's underlying technology began to work against its use. Bitcoin's blockchain, the digital ledger that meticulously records which addresses send and receive transactions, including the exact time and amount – all of which is very useful data to use as evidence in prosecuting cybercriminals. So, with Bitcoin, law enforcement agencies

only need to match an address to a crime and then monitor the Bitcoin internet sphere carefully enabling the cyber-police to track the funds disappearing and reappearing in other locations. Cyber investigators have developed databases and techniques for analysing that information to identify a physical location of cyber activity and eventually be able to make a physical arrest of the cybercriminals (Kharif, 2018: np). For example, a certain internet café known to have a certain Bitcoin address, and a wallet used by an extortionist transfers the same amount there every morning at nine o'clock. Investigators can, therefore, stop at this location and make a physical arrest. In this way the cyberpolice are slowly breaking down the anonymity provided to cybercriminals by the use of cryptocurrencies for the perpetration of a range of cybercrimes. Anonymity and the 'hiding' of transactions on the Dark Web being one of the major advantages of the use of cryptocurrencies for cybercrime activities on the Dark Web.

But, Monero's attraction was that it encrypts the recipient's address on its blockchain and generates fake addresses to obscure the real sender. It also obscures the amount of the transaction. The Monero system is so effective that current tracking software, designed to red flag tokens (coins) suspected of being obtained through crime now tags almost everything converted into or out of Monero as 'high risk' – code for suspected illicit criminal activity (Kharif, 2018: np). This 'flagging' complicates the problem for law enforcement agencies in combating any flows of cryptocurrencies for illicit purposes (analysis of Bitcoin was able to pinpoint illicit flows within legitimate use of cryptocurrencies to a greater degree of accuracy).

A recent example of the innovative nature ('staying-one-step-ahead') of cybercriminals in their exploitation of cryptocurrency to further their criminal exploits was their use of a new recently detected crytpocurrency hacking campaign (the so-called *DarkGate* Campaign), which made use of malware capable of bypassing (avoiding detection) traditional antivirus software. DarkGate targeted Microsoft Windows PCs by way of Torrent files. Such Torrent files are most commonly associated with pirated content, but the technology itself is not illegal and can be used by consumers and businesses alike to share files of large sizes. In this case, however, the infected .torrent files pretend to be pirated versions of popular television shows and films. The DarkGate malware uses a variety of so-called 'smokescreen' techniques to evade any standard antivirus software. It then enables the hackers to send commands remotely and for the malware to transfer stolen data, from DNS[1] records from legitimate services DNS records. By hiding within reputable DNS services allows the hack attack to pass a reputation check when it comes to suspicious or suspect services or shields hosting platforms, which have become associated with malware and criminal campaigns. As the DarkGate malware penetrates a system it does its own scan to detect any common antivirus software that might be lying in wait for it. The malware also makes use of recovery tools to prevent files critical to its operation from being deleted by the antivirus solution. When executed, DarkGate installs 'User Account Control' (UAC) bypass so as to gain system privileges, then downloads and executes more malware. These then allow DarkGate users to steal credentials associated with a victim's cryptocurrency wallets, execute ransomware payloads, create a remote access tunnel for operators to hijack the system, and also implement covert cryptocurrency mining operations. All criminal activity enabled by the initial circumvention of any antivirus, which allowed these hackers to proceed to empty cryptocurrency wallets (Osborne, 2018: np).

As law enforcement improve their cryptocurrency cyber-investigation capabilities and expertise, in co-operation with private sector cybersecurity specialists, the cybercriminals will, no doubt, continue to exploit any cryptocurrency vulnerabilities to expand their cybercrime activities. But, many governments are leaning towards some sort of formal regulation of the use of cryptocurrencies, not only so that cryptocurrency transactions as a financial service, but also profits in trading in them, can be taxed. This will immeasurably assist law enforcement in the overall fight to contain global cybercrime.

ENDNOTES

1. DNS (Domain Name System) is one of the internet's most important protocols that allows DNS servers to translate web addresses into their IP addresses and thereby connecting web browsers with websites.

LIST OF REFERENCES

Agence France Presse (AFP). 2016. 10 held for Bitcoin money laundering. Fin24, 21 January. Available at: http://www.fin24.com/Tech/News/10-held-for-bitcoin-money-laundering-20160121 (accessed on: 25 January 2016).

Ahmed, K. 2015. TalkTalk: Could this be an extortion attack? *BBC News*. 23 October. Available at: http://www.bbc.co.uk/news/business-34613137 (accessed on: 9 December 2015).

Akhgar, B., Chora, M., Brewster, B., Bosco, F., Vermeersch, E., Luda, V., Puchalski, D. & Wells, D. 2016. A consolidated taxonomy and research roadmap for cybercrime and cyberterrorism. (Pp. 295-322). In B. Akhgar & B. Brewster (Eds). *Combatting cybercrime and cyberterrorism: Challenges, trends and priorities*. Cham, Switzerland: Springer Nature.

Alfreds, D. 2016a. Bitcoin set for local growth, despite challenges. *Fintech24*, 4 March 2016.

Alfreds, D. 2016b. Here's how ransomware hits SA. *Fin24tech*, 14 April 2016. Available at: https://www.fin24.com/Tech/Cyber-Security/heres-how-ransomware-hits-sa-20160414 (accessed on: 12 May 2016).

Amir, U. 2015. Phishing attack causes Bitcoin payment processor BitPay to lose $1.8m. *HackRead*, 19 September. Available at: https://www.hackread.com/phishing-attack-on-bitcoin-payment-processor/ (accessed on: 23 September 2015).

Amir, U. 2017. Fake Bittrex cryptocurrency site stealing user funds. *HackRead*, 19 August. Available at: https://hackread.com/fake-bittrex-cryptocurrency-site-stealing-user-funds (accessed on: 22 August 2017).

Anon. [sa]. What is a cryptocurrency token? *CryptocurrencyFacts.com*. Available at: https://cryptocurrencyfacts.com/what-is-a-cryptocurrency-token/ (accessed on: 15 April 2018).

Blackwood, F. 2015. Cryptolocker virus: Australians forced to pay as latest encryption virus is "unbreakable", security expert says. *Abc.net*, 10 August 2015. Available at: http://www.abc.net.au/news/2015-08-09/australians-paying-thousands-after-ransomware-virus-infection/6683618 (accessed on: 23 December 2015).

Bray, J.D. 2016. Anonymity, cybercrime, and the connection to cryptocurrency. *Online Theses and Dissertations*. Available at: http://encompass.eku.edu/etd/344 (accessed on: 7 January 2018).

Chainalysis. 2017. The rise of cybercrime on Ethereum. *Chainalysis*, 7 August. Available at: https://blog.chainalysis.com/the-rise-of-cybercrime-on-ethereum/ (accessed on: 12 January 2018).

Ciancaglini, V., Balduzzi, M., McArdle, R. & Rosler, M. 2015. Exploring the Deep Web. *Trend Micro*, 2015. Available at: https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_below_the_surface.pdf (accessed on: 15 December 2015).

Clough, J. 2015. *Principles of cybercrime.* (2nd edition). Thousand Oaks, CA: SAGE.

Elisan, C.C. 2012. *Malware, rootkits and botnets: A beginner's guide*. New York: McGraw Hill.

European Central Bank. 2012. Virtual Currency Schemes: 2012. Available at: *www.ecb.europa.eu:virtualcurrencyschemes2012en.pdf* (accessed on: 12 August 2013).

European Central Bank. 2015. *Virtual currency schemes: A further analysis*. Available at: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf (accessed on: 15 December 2015).

European Police Office (Europol). 2014. *Internet organized crime threat assessment: 2014*. Available at: https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015 (accessed on: 20 June 2016).

European Police Office (Europol). 2015. *The Internet organised crime threat assessment: 2015*. (IOCTA). Available at: https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015 (accessed on: 12 January 2016).

Fanusie, Y, J & Robinson, T. (2018. Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services. *Foundation for Defense of Democracies Centre on Sanctions and Illicit Finance (CSIF),* 12 January 2018. Available at: http://www.defenddemocracy.org/media-hit/yaya-j-fanusie-bitcoin-laundering/ (accessed on: 20 January 2018).

Federal Bureau of Investigations (FBI). 2015a. *Cybercriminal forum taken down*. Washington DC: Federal Bureau of Investigations. Available at: https://www.fbi.gov/news/stories/2015/july/cyber-criminal-forum-taken-down/cyber-criminal-forum-taken-down (accessed on: 9 December 2015).

Federal Bureau of Investigations (FBI). 2015b. *Four charged in international Uganda-based cyber counterfeiting scheme.* 2 April. Washington DC: Federal Bureau of Investigations. Available at: https://www.fbi.gov/contact-us/field-offices/pittsburgh/news/press-releases/four-charged-in-international-uganda-based-cyber-counterfeiting-scheme (accessed on: 20 July 2016).

Financial Action Task Force (FATF). 2014. *Virtual currencies: Key definitions and potential AML/CFT risks.* [Sl]: Financial Action Task Force. Available at: http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf (accessed on: 15 December 2015).

Fioramonti, L. 2017. Alternative currencies are the future: Why it matters for development. *The Conversation,* 2 July. Available at: https://theconversation.com/alternative-currencies-are-the-future-why-it-matters-for-development-80036 (accessed on: 12 October 2017).

Franco, P. 2015. *Understanding Bitcoin: Cryptography, engineering, and economics.* London: John Wiley & Sons.

Gans, J.S. & Halaburda, H. 2013. *Some economics of private digital currency*. Bank of Canada, Working Paper, November. Toronto: Bank of Canada. Available at: http://www.bankofcanada.ca/wp-content/uploads/2013/11/wp2013-38.pdf (accessed on: 12 August 2015).

Greenberg, A. 2014. Hacker lexicon: What is the Dark Web? *Wired*, 19, November 2014. Available at: http://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/ (accessed on: 12 January 2015).

Hartshorn, R. 2018. The trouble with cryptocurrency's viral growth. *The New York Times*, 25 September. Available at: https://www.nytimes.com/2018/09/25/opinion/cryptocurrency-bitcoin-viral-growth.htm (accessed on: 27 September 2018).

Higgins, S. 2018. Cisco: Bitcoin phishing scam bagged $50 million over three years. *Coindesk,* 15 February 2018. Available at: https://www.coindesk.com/cisco-50-million-bitcoin-phishing-scam-mimicked-blockchain-web-wallet/ (accessed on 26 February 2018).

Hileman, G. & Rauch, M. 2017. 2017 Global Cryptocurrency Benchmarking Study. 6 April. Cambridge, UK: Cambridge University. Available at: https://www.jbs.cam.ac.uk/.../2017-global-cryptocurrency-benchmarking-study.pdf (accessed on: 5 May 2017).

Iyengar, R. 2017. More than $70 million stolen in bitcoin hack. *CNN Tech,* 8 December. Available at: http://money.cnn.com/2017/12/07/technology/nicehash-bitcoin-theft-hacking/index.html (accessed on: 10 January 2018).

James, A. & Sherin, S. 2014. Trust issues in modern embedded computing. (Pp. 361-369). In S.M. Thampi, B. Bhargava & P.K. Atrey (Eds). *Managing trust in cyberspace*. New York: CRC Press, Taylor & Francis Group.

Kharif, O. 2018. Criminal underworld is dropping Bitcoin for another currency. Fin24, 2 January. Available at: https://www.fin24.com/Tech/News/criminal-underworld-is-dropping-bitcoin-for-another-currency-20180102 (accessed on: 10 January 2018).

Kong, K. & Tweed, D. 2017. North Korea is suspect in hack of Seoul Bitcoin Exchange. Bloomberg, 21 December. Available at: https://www.bloomberg.com/news/articles/2017-12-21/north-korea-said-to-be-suspect-in-hack-of-seoul-bitcoin-exchange (accessed on: 10 January 2018).

Kyodo, J. 2017. 170 money-laundering cases in Japan involved cryptocurrency in six months since April. *The Japan Times*, 30 November 2017. Available at: https://www.japantimes.co.jp/news/2017/11/30/national/crime-legal/police-say-170-cryptocurrency-laundering-cases-suspected-six-months-april/#.Wp7PyE1Dupo (accessed on: 3 January 2018).

Maras, M.H. 2012. *Computer forensics: Cybercriminals, laws and evidence*. Canada: Jones and Bartlett Learning.

Mathews, L. 2018. Hackers abuse Google ad network to spread malware that mines cryptocurrency. *Forbes*, 26 January 2018. Available at: https://www.forbes.com/sites/leemathews/2018/01/26/hackers-abuse-google-ad-network-to-spread-malware-that-mines-cryptocurrency/#5f3b4d817866 (accessed on: 26 January 2018.

Mckane, J. 2017. Bitcoin and cryptocurrency on the rise in South Africa. *MyBroadband*, 14 April 2017. Available at: https://mybroadband.co.za/news/banking/206590-bitcoin-and-cryptocurrency-on-the-rise-in-south-africa.html (accessed on: 5 May 2017).

Meiklejohn, S., Pamorole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M & Savage, S. 2013. A fistful of bitcoins: Characterizing payments among men with no names. Proceedings of the 13th ACM Internet Measurement Conference. *Communications of the ACM*, 59*(*4), 86-93. Available at: https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf (accessed on: 12 June 2015).

Minnaar, A. 2016. Organised crime and the 'new more sophisticated' criminals within the cybercrime environment: How 'organised' are they in the traditional sense? *Acta Criminologica: Southern African Journal of Criminology,* 29(2): 123-141.

Minnaar, A. 2017. Online 'underground' marketplaces for illicit drugs: The prototype case of the Dark Web website '*Silk Road*'. *Acta Criminologica: Southern African Journal of Criminology. Special Edition: Illicit drugs: Local and International realities.* 30(1): 23-47.

Naidoo, P. 2017. South Africans trading big volumes in bitcoin. *Tech Central*, 15 August. Available at: https://techcentral.co.za/south-africans-trading-big-volumes-bitcoin/76329/ (accessed on: 20 December 2017.)

Naik, S. & Serumula, R. 2015. Dark Web thriving in SA. *Saturday Star,* 17 October 2015. Available at: http://www.iol.co.za/news/south-africa/dark-web-thriving-in-sa-1931641 (accessed on: 20 January 2016).

Nair, N. 2018. $50-million cryptocurrency scam cripples South African investors. *Herald Live,* 1 March 2018. Available at: http://www.heraldlive.co.za/news/2018/03/01/50-million-crytocurrency-scam-cripples-south-african-investors/ (accessed on: 2 March 2018).

Nakamoto, S. 2008. Bitcoin: A peer-to-peer electronic cash system. Available at: https://bitcoin.org/bitcoin.pdf (accessed on: 20 March 2015).

New York Department of Financial Services. 2018. BitLicense Regulatory Framework. Available at: http://www.dfs.ny.gov/legal/regulations/bitlicense_reg_framework.htm (accessed on: 2 April 2016).

Osborne, C. 2018. Most antivirus programs fail to detect this cryptocurrency-stealing malware. *Zero Day*, 16 November. Available at: https://www.zdnet.com/article/this-stealthy-malware-circumvents-antivirus-software-to-steal-your-cryptocurrency/ (accessed on 17 November 2018).

Samani, R., Paget, F. & Hart, M. 2013. Digital laundry: An analysis of online currencies, and their use in cybercrime. Santa Clara, CA: McAfee Labs Incorporated. Available at: http://www.mcafee.com/us/resources/white-papers/wp-digital-laundry.pdf (accessed on: 20 December 2014).

South African National Treasury. 2014. User alert: Monitoring of virtual currencies. Available at: http://www.treasury.gov.za/comm_media/press/2014/2014091801---User-Alert-Virtual-currencies.pdf (accessed on: 16 August 2015).

South African Reserve Bank. 2014. Position paper on virtual currencies. Available at: https://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Documents/Position-Paper/Virtual-Currencies-Position-Paper--Final_02of2014.pdf (accessed on: 18 May 2015).

Staff Writer. 2018a. What to expect from Bitcoin in 2018. *Business Tech*, 17 January. Available at: https://businesstech.co.za/news/banking/219667/what-to-expect-from-bitcoin-in-2018/ (accessed on: 12 February 2018).

Staff Writer. 2018b. South Africans hit by massive Bitcoin scam. *MyBroadBand*. 1 March. Available at: https://mybroadband.co.za/news/cryptocurrency/250893-south-africans-hit-by-massive-bitcoin-scam.html (accessed on: 20 February 2018).

Stoyanov, D. 2014. Malicious chrome extension steals users' Bitcoins. *Virus Guides*, 14 March. Available at: http://virusguides.com/malicious-chrome-extension-steals-users-bitcoins/ (accessed on: 9 March 2016).

The Commonwealth Working Group. 2015. Commonwealth Working Group on virtual currencies. Available at: http://thecommonwealth.org/sites/default/files/pressrelease/documents/P14195_ROL_Virtual_Currencies_D_Tait_V5_LoRes.pdf (accessed on: 20 March 2016).

The Commonwealth Working Group. 2015. *Working group report: Commonwealth Working Group on virtual currencies*. Canberra: The Commonwealth Working Group. October. Available at: http://thecommonwealth.org/sites/default/files/pressrelease/documents/P14195_ROL_Virtual_Currencies_D_Tait_V5_LoRes.pdf (retrieved on: 20 March 2016).

Trend Micro. 2018. 3 reasons the ransomware threat will continue in 2018. *Trend Micro,* 24 January. Available at: https://blog.trendmicro.com/3-reasons-the-ransomware-threat-will-continue-in-2018/ (accessed on: 20 January 2018).

US Department of Justice. 2016. Liberty Reserve founder sentenced to 20 years for laundering hundreds of millions of dollars. Washington DC: U.S. Department of Justice. Available at: https://www.justice.gov/opa/pr/liberty-reserve-founder-sentenced-20-years-laundering-hundreds-millions-dollars (accessed on: 7 November 2016).

US Department of the Treasury. 2017. History of Anti-Money Laundering Laws. Washington DC: U.S. Department of the Treasury, Financial Crimes Enforcement Network. Available at: https://www.fincen.gov/history-anti-money-laundering-laws (accessed on: 16 January 2018).

United Kingdom Government. 2017. *National risk assessment of money laundering and terrorist financing 2017*. Available at: https://www.gov.uk/government/publications/national-risk-assessment-of-money-laundering-and-terrorist-financing-2017 (accessed on: 20 January 2018).

Van Mieghem, V. & Pouwelse, J. 2015. Anonymous online purchase with exhaustive operational security. 27 May. *ArXiv*: 1-7. Available at: https://arxiv.org/pdf/1505.07370.pdf (accessed on: 20 November 2017).

Vasek, M. & Moore, T. 2015. There's no free lunch, even using bitcoin: Tracking the popularity and profits of virtual currency scams. Available at: www.cs.unm.edu/~vasek/papers/vasekfc15pres (accessed on: 2 April 2016).

Vinay, M.S. & Balakrishnan, M. 2014. A comparison of three sophisticated cyber weapons, (Pp. 387-404). In S.M. Thampi, B. Bhargava & P.K. Atrey (Eds). *Managing trust in cyberspace*. New York: CRC Press, Taylor & Francis Group.

Ward, M. 2014. Cryptolocker victims to get files back for free. *BBC News*, 6 August. Available at: http://www.bbc.com/news/technology-28661463 (accessed on: 20 July 2015).

Waqas. 2017. Hackers stealing $30 million worth of cryptocurrency in Tether hack. *HackRead*, 21 November. Available at: https://www.hackread.com/hackers-steal-30-million-worth-cryptocurrency-tether-hack (accessed on: 25 November 2017).

Zhao, W, 2018. Major crypto exchanges face action over money-laundering fears. *CoinDesk*, 19 June. Available at: https://www.coindesk.com/major-crypto-exchanges-face-action-over-money-laundering-fears/ (accessed on: 25 June 2018).

Zorz, Z. 2017. Man stole bitcoin by phishing individuals on the dark web. *HelpNet Security*, 10 July. Available at: https://www.helpnetsecurity.com/2017/07/10/dark-web-phishing/ (accessed on: 13 July 2017).

Case Law

Kats et al v United States of America, Southern District of New York, 2016 (13) U.S 36.