International Journal of Cyber-Security and Digital Forensics (IJCSDF) 7(4): 420-435
The Society of Digital Information and Wireless Communications (SDIWC), 2018 ISSN: 2305-001

Cryptocurrency and the Blockchain: A Discussion of Forensic Needs

Douglas A. Orr Ph.D.
University of North Georgia
82 College Circle
Dahlonega, GA 30597
douglas.orr@ung.edu

Drew M. Lancaster
Division of Information Technology & Sciences of Champlain College
163 S Willard St, Burlington, VT 05401
drew.lancaster@mymail.champlain.edu

ABSTRACT

The authors discuss matters concerning Cryptocurrencies in a global context. We also describe what a cryptocurrency is and provide a history of the currencies and their differences with government regulated moneys. Discussion follows with why these digital currencies are important not only to criminals, but also corporations and governments, and outlines the process for which transactions are held legitimate and how the data within the coins are stored. Although criminal activity has profited with cryptocurrencies, these currencies have become more mainstream. The authors identify key forensic artifacts that may be found on digital devices to track transactions and aid in connecting criminals to their malicious actions.

KEYWORDS

Blockchain, cryptocurrency, altcoin, anonymity, mining, currency, Bitcoin, organized crime, digital forensics.

1 INTRODUCTION OF CRYPTOCURRENCY

Cryptocurrencies are becoming better known and more widespread by the mainstream consumer each day. This is in part to the illegal and malicious activity by threat actors around the world using the currency as a form of payment for their actions. Although illegal activity has been connected to cryptocurrency, it is in truth a ledger of all transactions that retains the identity of those threat actors in perpetuum. Any consumer or investor may take advantage of digital currencies all over the world as there are no borders or boundaries for such coinage. Jan Lansky [1], a cryptocurrency researcher, has defined six requirements:

1) The system does not require a central authority, distributed achieve consensus on its state.
2) The system keeps an overview of cryptocurrency units and their ownership.
3) The system also defines whether new cryptocurrency units can be created. If new cryptocurrency units can be created, the system defines the circumstances of their origin and how to determine the ownership of these new units.
4) Ownership of cryptocurrency units can be proved exclusively cryptographically.
5) The system allows transactions to be performed in which ownership of the cryptographic units is changed. A transaction statement can only be issued by an entity proving the current ownership of these units.
6) If two different instructions for changing the ownership of the same cryptographic units are simultaneously entered, the system performs at most one of them.

Cryptocurrencies are simply 1s and 0s representing the owners as well as their transactions on a network of computers placed in a database that retain identity and ownership of the coins.

1.1 How Does It Work?

Cryptocurrency utilizes a peer-to-peer digital cash system that stores the transactions within a

database called a Blockchain. The Blockchain is a public ledger that keeps track of every transaction each coin has been transacted. The Blockchain is available to anyone within the network and allows each coin's ledger as well as each person's account to be open to the public. Each transaction is determined legitimate or not by a network of peers who confirm the transactions through *mining*. Mining will find the transactions, verify the ledgers involved, and then alert all other nodes within the network that the transaction was legitimate and to update such nodes ledgers as well. Thus, the peer-to-peer network monitors its own transactions and confirms that each digital ledger or Blockchain is up to date and verified by the network.

1.2 Legal Transactions

Digital coins can be used in everyday transactions for any number of purchases if both parties agree on the currency used. Online shopping can utilize cryptocurrencies if that web store accepts cryptocurrency as a form of payment. Digital currencies can be used for any activity normally using cash such as restaurants, hotels, and physical stores. Another useful idea for investing into cryptocurrencies is to pay for continuing education like specific training and college tuition. Investing into cryptocurrencies is much like investing in any stock or bond controlled by big business or various governments around the world. Essentially, cryptocurrencies can be used for anything as is cash currency.

1.3 Illegal Activity

Threat actors have managed, to their advantage, these cryptocurrencies even though all the transaction's data are stored and visible to anyone on a network. Cryptocurrencies are only anonymous if the owner of the coin is determined by a random series of letters and numbers with no identifiable attributes of the threat actor. With the use of an anonymous browser like Tor and a Virtual Private Network (VPN), a person can remain private while using cryptocurrencies. This anonymity has allowed criminals to remain hidden while performing many different criminal acts.

These illegal actions, just like their counter-part legal transactions, can replace cash currency for all criminal transactions. These crimes include sex trafficking, drugs, guns, fake identifications, assassinations, and even financing terrorism. White collar crimes can include tax evasion, identity theft, and money laundering. Then, there are computer generated crimes that include malware and child pornography. The most common malware used by cyber criminals is Ransomware. "Smaller ransomware families brought in another $150 million, and the FBI has reported $209 million in ransomware payments during the first three months of 2016" [2]. Using cryptocurrencies to facilitate digital crimes can become very profitable to anyone with a digital device. Pursuing illegal actions with the use of cryptocurrencies has created new complexities for law enforcement as digital coins can be used for anything.

2 HISTORY OF CRYPTOCURRENCY

Technology and money have gone hand in hand for centuries beginning with the first abacus. Then came cash registers supported with electricity emerging as the first point of sale machines. During the 1950s, the credit card came to be the efficient way of making transactions without the use of cash or paper promissory notes. The household personal computer gave rise to the likely creation of digital currency. It was not until recently, however, that Bitcoin became successful enough to change how we look at currency.

2.1 Before Bitcoin

The concept of Bitcoin, the first cryptocurrency, grew from several other proposed ideas over three decades. In 1989, DigiCash was created by David Chaum and used public and private key cryptography to enhance electronic payments. Consequently, the advancement in cryptography keys was significant. Adam Back's Hashcash brought about a proof-of-work concept in 1997 that is essential to cryptocurrency transaction verification. "The Hashcash cost-function is publicly auditable, because anyone can efficiently verify any published tokens" [3]. That became the basis for verifying transactions. Each

of these earlier attempts at digital currency lays the foundation for Bitcoin. The next step was the concept of storing transactions within a decentralized system. In 1998, Nick Szabo and Wei Dai proposed distributed digital money schemes. "The main idea behind these proposals was that balances were stored in a distributed database" [4]. The following year, Tomas Sander and Amnon Ta-Shma proposed digital coins that did not carry personal data but a hash of its serial number. To further the concept of proof-of-work, in 2004, Hal Finney introduced a Reusable Proof-Of-Work (RPOW) concept that had no need of being connected to an email address. This allowed the RPOW to be used freely without restriction. These concepts laid the foundations that would soon become the first cryptocurrency called Bitcoin.

2.2 Bitcoin

In 2008, Satoshi Nakamoto (2009) released a whitepaper discussing a concept that would eliminate the third party needed required of financial institutions to manage, mediate, and process transactions. This concept would be based on cryptography between two parties leaving no need for an intermediary. To prevent double-spending, Nakamoto proposed the proof-of-work concept for a record of the transaction within the database provided throughout the network. Nakamoto (2009) did state that some fraud would occur. But through the network of nodes controlled by mostly trustworthy parties, this could be avoided. "They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them" [5]. The larger the ledgers would become; the more computer power would be required. Accordingly, the longest ledgers would become the most reliable verification as it would require a significant pool of computer power. A consensus would be created with this computer power to legitimize the transactions with the network. Now, this context provides a foundation for legitimizing Satoshi Nakamoto's Bitcoin.

3 OVER 1500 DIGITAL CURRENCIES AND CLIMBING

The amount of digital currencies within the world market grows with each year. According to CoinMarketCap [6], as of April 1, 2018, there were 1,596 different cryptocurrencies in circulation. The legitimacy of these currencies could be debated if compared to Jan Lansky's requirements previously discussed. Generally, however, any digital currency created after and following the basic concepts of Bitcoin are indeed a cryptocurrency. At the time of this writing, the prices ranged from $6,553.16 for Bitcoin down to fractions of a penny. Some are tokens that represent an asset that can still be exchanged such as Etherium. There are 9,914 markets available to trade the currencies as well. Digital currencies have become a booming industry despite the criminal attention within certain media outlets and the volatility of its respective markets.

3.1 Altcoin Boom

The term *altcoin* essentially describes alternatives to Bitcoin and the first altcoin was released in April of 2011 called Namecoin. From 2013 to 2014 the landscape of cryptocurrencies saw a boom in the amount the market value of cryptocurrencies. "From the beginning of the boom until the end of the bust a year later the altcoin space actually grew 5X from $100M to $500M" [7].

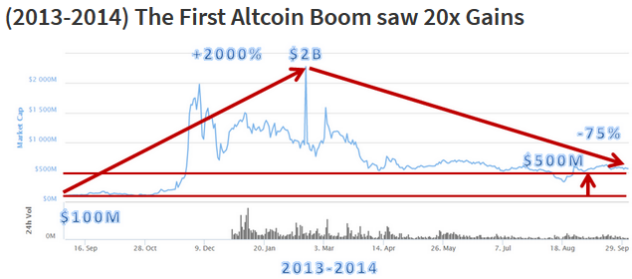

Figure 1. Depicts growth and loss of Altcoin Boom.

Since 2009, Bitcoin has dominated the landscape of cryptocurrencies. In recent years, however, this reign has been diminishing. Currently Bitcoin only holds only 37.7 percent of the cryptocurrency landscape [8].

4 WHY CRYPTOCURRENCIES MATTER

Cryptocurrency has changed the landscape of money around the world by removing financial institutional control. Cryptocurrencies are more

suited to how business is done every day by people. The purchases on Amazon, paying of bills every month, and normal every-day banking are done online and are but a few examples. For governments, this can be concerning and some jurisdictions have even made cryptocurrencies illegal within their borders. Some of these nations include Algeria, Bolivia, China, Ecuador while Vietnam allows for the holding and trading of currencies but not the use for payment. The theme among most of these restrictive nations is that there is simply an already legitimate financial institution in control of the government's money and that the intrusion of another currency and loss of revenue through transactional fees is not welcome. Although China banned the trading of cryptocurrencies in September 2017, little has slowed the currency's progress there.

Officials all over the world should be nervous as other such currencies have become appealing to their citizens giving their governments less control of what occurs within their borders. Cryptocurrencies are controlled by the people within the network above and beyond a certain political agenda. These new currencies could be used to avoid paying taxes which would result in the government losing revenue. Governments control cash flow to help regulate the economy. When there are hard times, they can print or withhold money thereby manipulating the economy to help maintain a balanced and stimulated economy. As these currencies are controlled by the majority within the network of nodes, the currency itself could unsettle the government's posture toward free-market commerce.

Some benefits of cryptocurrencies allow users in smaller less developed countries to invest and purchase items over their mobile phones and other digital devices. It protects the identity of the individual from criminal actors in the region attempting to destabilize the environment and control the local economy. It allows freedom fighters in war torn areas to remain hidden. Yet, it allows their warlords counterparts to also remain hidden thus creating two sides, each in need of being monitored forensically should a criminal venture be discovered. Ultimately, such forensic investigations aid in protecting the innocent. Cryptocurrency donations may be used to support terrorist organizations through the purchase of weapons and propaganda. But, digital currency can also be used to help protect those in direct conflict of terrorist groups in poorer countries around the world. Whether digital forensics is used to protect the innocent or investigate the crimes around the world, the digital currency landscape is constantly changing and creating new perspectives to an emerging problem making our interest in cryptocurrencies keener by the day.

4.1 Government Regulation

Each nation is dealing with cryptocurrencies differently through creating regulation, prohibiting it, or a reluctance to more forward approach. This last approach seems to be what the United States has adopted as there is no coherent approach to cryptocurrencies given there are warnings that investing in these currencies can be volatile and dangerous as compared to gambling. In the United States, there are other hurdles to as well as each individual state can treat cryptocurrencies differently especially when it comes to licensing and commerce in general. "In addition to the federal securities laws, every state has its own set of securities laws—commonly referred to as "Blue Sky Laws"—that are designed to protect investors against fraudulent sales practices and activities" [9]. Legislation has been introduced to combat illegal activities including terrorism, money laundering, Internal Revenue Tax laws, and acts to protect financial transactions. The complications that come from cryptocurrencies have made governments not only notice but also struggle to regulate these currencies as the landscape changes.

In contrast to the United States, China has taken a more draconian approach to regulate cryptocurrencies. "Starting off by banning ICOs, China ordered a bank account freeze associated with exchanges, kicked out bitcoin miners, and instituted a nationwide ban on internet and mobile access to all things related to cryptocurrency trading" [10]. This is in part to end corruption and manage wealth within its own borders. At first, South Korea was very liberal with regulations but now threatens to shut down exchanges as well. This made for a very hostile environment concerning cryptocurrencies within its borders. Each country has taken a

different approach on how to handle these concerns adding to the volatility of cryptocurrency markets around the world.

5 WHY BIG BUSINESS IS CURIOUS

Large corporations have kept a close eye on cryptocurrencies for their own use and remained concerned for its volatile nature. Bill Gates talked about Bitcoin in a positive nature citing easier uses other than its bulkier counterparts [11]:

"Bitcoin is exciting because it shows how cheap it can be. Bitcoin is better than currency in that you don't have to be physically in the same place and, of course, for large transactions, currency can get pretty inconvenient." – Bill Gates

Warren Buffet took a different approach in 2014 [12]:

"*Stay away from it. It's a mirage basically*." Warren Buffett

These varying degrees of perspective is another example of the uncertain landscape that it brings. Investment firms see cryptocurrencies as all locked together. When Bitcoin peaked at its highest market value and then tumbled 65% so did other cryptocurrencies. Until each currency can fluctuate independently of the others, investment firms will be very reluctant to acquire them.

The underlying technology of these cryptocurrencies, however, is what big companies are eyeing for the future. The blockchain can change how a company does its business in a couple different ways. A company's larger transactions can be smoother with the use of cryptocurrencies as Bill Gates has mentioned. These seamless transactions lead to less time spent that the money is legally acquired and exchanged properly. Regulators overseeing large transactions could also take advantage of the trusted blockchain ledger.

The technology within the blockchain is simply referred to as a database to store transactions. The use of this technology has now extended beyond cryptocurrencies and aided companies in managing their assets. British Airways has tested blockchain technology to manage flights with FlightChain. "FlightChain has demonstrated that blockchain is a viable technology choice for the use case of providing a single source of truth for data, specifically real-time flight information" [13]. FlightChain provides an opportunity for the use of blockchain technology in vital areas of real-world control, using the airline industry as an example.

The supply chain for such companies can utilize the technology to provide proof of acquisition. The fishing industry, for example, can determine whether fish were caught illegally with geo locations stored within the database ledger. Walmart has begun to monitor supply of certain fruits like mangos in the same way. Nestle and Dole are also looking at blockchains to address food safety issues and track their products from the field to shelf. Burger King in Russia began to use a blockchain ledger to provide their customers with a reward system for items on the menu. The same might be said for any service or commodity produced around the world, the location it was created, the geo locations the items have travelled, and proof that the items were not replaced or duplicated.

5.1 Problems for Big Business

The problems that lay ahead for big business adopting cryptocurrencies across the board are front end heavy. This means that it will require a great deal of upfront money to adjust to how their business might handle the currency. A decision will need to be made regarding which coin to use if not Bitcoin is not the primary choice. Perhaps the company would use Etherium, the leading token currency. Next comes the unstable market place providing high-risk money services that do not charge large fees to cover losses from currency fluctuations. Governments may or may not have regulations in place or might even be preparing to add regulation that the company requires to protect future assets. While cryptocurrencies are volatile, governments are uncertain regarding the level of regulation necessary and therefore big business is forced to operate in a high-risk environment. Patience will be key for big business before they adopt cryptocurrencies across the board.

Banks are beginning to care about the emerging cryptocurrencies because they directly affect their profit. Cryptocurrencies are used to avoid banking fees, transactional control, and credit bearing rules. Banks can offer the opinion that cryptocurrencies are unstable and risky with no

real future of persistence. But in the realm of globalization, cryptocurrencies are in fact aiding and quickening globalization at an alarming rate as banks and governments grapple to control currency. The essential function of a bank is to hold money, lend money, and be an intermediary for others involving assets and money. Cryptocurrency provides the means for normal people to control all those aspects themselves.

6 THE PRICE OF CURRENCY

Cryptocurrencies are decentralized and independent of any central bank. So there is no intrinsic value to a cryptocurrency other than what people or groups are willing to trade for it. Cryptocurrencies are not backed by any other commodity, such as gold for example. Each unit of cryptocurrency's amount is determined by the user and any transaction completed is performed and validated by a peer to peer network. Over 1902 different markets, there are 615 cryptocurrencies traded. This becomes a very large area for law enforcement to regulate criminal activity involving these currencies. Each network can control each unit of measure for the currency as well. This means that a coin can equal a U.S. Penny, 100 Yen, or a kilowatt of power, all determined by the Users within the network. The decentralized design and lack of government regulation leaves the programmers of a cryptocurrency to develop coding rules to better regulate the currency's market capitalization and volume. A combination of the currencies coding, market value, and outside influences determine the pricing of a cryptocurrency.

Cryptocurrencies are subject to price fluctuations like any other currency around the world. But currently, it is affected by items in a more hostile way due to its maturity and inherent volatility. Supply and demand plays an initial role within the price of a cryptocurrency as there are only a certain amount of coins created. Like governments printing more money, cryptocurrencies can do the same to stimulate its economy. Like stocks in the market, a cryptocurrency can split at a certain point depicted by the community and this consequently might increase or decrease the price. The market being diluted by more and more altcoins could drive prices down for lesser known currencies. Until digital coins stabilize, these markets will continue to be hostile to the average investor.

A couple of matters that might not be immediately recognizable but that might affect a price of a digital currency is the difficulty of mining the transactions and the energy used for them. The more difficult it is to mine a currency the more energy is required. This reflects the secure nature of the cryptography associated with the currency. Increased security creates a higher cost to manage the transactions due to the increase in computer power required for the proof-of-work of the transaction. This also adds to the energy required to run the computer power while mining the currency.

How the currency behaves plays a larger role in its price fluctuation. Bitcoin acts as a transactional currency and is used to exchange for goods and services like government money used for every day purposes. A platform currency, like Etherium, creates a stage for other currencies and applications. It utilizes smart contracts so applications can run without third-party needs, interruption, or censorship. Smart contracts contain rules and penalties for agreements within the transaction. Examples for platform currencies may include legal contracts, credit enforcement, crowdfunding, and driving licenses. For example, as soon as a traffic ticket is issued by the officer writing the ticket, the driver's license (which was purchases under a smart contract) will get added points or even suspended, dues process aside. The third type of currency is utility tokens that are used to store services. These can be purchased wholly or partially and redeemed for the service provided. Much like market stocks or paper currencies, *how* the utility token is purchased plays a significant role in its price.

Public perception of the cryptocurrency can directly affect the price much like corporation postures affect their stocks. The media and what they say about a currency can be detrimental or helpful to a currency. The media could report that a currency exchange has been hacked and the data sold to the highest bidder on a dark website. Or, it could be reported that a smart contract currency was used to help protect the fish used for sashimi around the world. These reports can significantly alter the price of the currency. It may also depend on what type of

media outlet is covering cryptocurrencies. For example, a CNN report would be more effective than a website article for a small firm. The volatility of the currency itself or the continued use of threat actors using ransomware with no repercussions could be harmful for public perception. Until cryptocurrencies become more stable, public perception will play a role in most of currencies.

7 ILLEGAL ACTIVITY USING CRYPTOCURRENCY

Ransomware played a significant role in bringing cryptocurrency to the forefront. The ransomware's payload will encrypt a system, partially or in whole, and demand payment. This payment is usually made using the cryptocurrency of the actor's choice. When the payment is made, the encryption key is released and the data can be restored. This type of malware is used to compromise everything from personal computers to corporate networks seizing hospital records to larger government archives. Sensationalized by the media, such incidents bring malware to the forefront of national attention with the use of cryptocurrency as an added attraction.

7.1 Organized Crime

The tactic ransomware uses is well-suited for organized crime. In efforts to meet their own financial demands and the changing landscape of the world through technology, organized crime has claimed a foothold in ransomware. Using ransomware, thieves can make a significant amount of money using cryptocurrencies. Other organized criminal acts can include extortion, blackmail, and kidnapping demands, all of which utilize cryptocurrency as a form of payment. It is much easier to transact cybercurrency than with bag full money. Now, organized "crime figures, previously arrested for crimes such as extortion, drug trafficking and human smuggling are collaborating with other criminals to bring segments of the young hacker community under their control" [14]. As Criminal organizations change their own approach to make a profit, a better understanding of digital forensics is required to investigate these groups.

Criminal organizations rely upon anonymity to hide from law enforcement. When the blockchain within an illegal transaction is discovered, it allows law enforcement to identify patterns of criminal activity to prosecute these organized crime syndicates. Each transaction on the blockchain then becomes another piece of the puzzle for investigators to track, especially if the currency is used between or among other organized crime syndicates or used to purchase items by way of these criminal acts. Tracking the blockchains and transaction identities found within wallets and other artifacts on digital devices allows government agencies to fight these criminal enterprises.

7.2 Other Crimes

One of the most infamous illegal franchises involving cryptocurrency is the Silk Road. Activities the Silk Road included selling of guns, various criminal services, human trafficking, and internet crimes like ransomware. "In less than three years of inception, Silk Road had turned over $1.2 billion in revenue,using cryptocurrency as the medium and sophisticated encryption software, Tor, to conceal the identity of its users" [15]. The Silk Road was simply the first mainstream case to involve the darknet. Recently the Federal Bureau of Investigations along with law enforcement agencies around the world took down AlphaBay [16]. The transactions totaled more than $1 billion in digital currencies. The takedown of the site included the seizure of multiple locations of servers around the world. These types of sites will continue to pop up around the internet and the need for digital forensics to combat them has become higher.

The other example is Mt Gox, as it was the largest exchange in 2014 when it was hacked. Over many years, the company lost over $460 million dollars of investor's investments. For these examples, we should also mention the Tor Project. Originally Onion Router, the Tor Project was developed by the United States Navy to protect communications. With the Tor Project obscuring internet traffic relays as well as the limited anonymity cryptocurrencies hold for their users, these instances serve a fair argument *against* the use of cryptocurrencies.

7.3 Attacks on Cryptocurrencies

There exist a multitude of crimes involving cryptocurrencies themselves of which a user might be mindful. These crimes might begin with the theft of a *wallet*. The wallet contains all the information needed to access the cryptocurrency and can be captured through properly executed malware, a physical device such as a USB, or the digital device itself stolen for examination. During an Initial Coin Offering (ICO), a hacker can quickly alter a URL website with providing victims a fake ICO website where their information and currencies are compromised. Once more, regulation of the ICOs is dictated solely by the owners. Accordingly, a criminal actor could hack a payment gateway and intercept cash flows by tricking an internet provider into believing they are the domain owners. These examples are just a few examples where criminals are becoming more adaptive to their environment by attacking the currencies themselves.

7.4 Using Cryptocurrencies to Illegally Make Money

In May of 2018, the Federal Bureau of Investigations Indicted founders of three cryptocurrency companies for defrauding investors. Taking advantage of growing interest in currency investments [17]. These actors are accused of taking advantage of people's interest within digital currencies to make money. There is a rise in virtual currency schemes to cheat victims out of money while mistakenly thinking they are investing in a currency which doubled, according to the FBI from 2013 to 2014 [18]. This again proves the need for enhanced digital forensics oversight into cryptocurrencies.

Anyone can profit from the illegal gains of cryptocurrency exchanges. A chiropractor and his son from Shreveport, Louisianapleaded guilty to operating an illegal Bitcoin exchange [19]. Each of these cases provide the need for digital forensics to combat Illegal activity protecting the public from fraudulent threat actors.

8 ANONIMITY OR NOT

Cryptocurrencies are anonymous to a certain degree in that when a wallet or file holding the identifiers of a currency is found, it is then that these transactions within that file can be tracked. These tracked identifiers can lead to more traceable transactions and possibly the eventual identification of the owner. This is the result of a blockchain ledger becoming public to reveal cryptographed identifiers. Although a blockchain is a public ledger, an actor may take a few steps to remain anonymous keeping enforcement agencies at bay to avoid identification.

8.1 How to Stay Hidden

A criminal actor can take a few steps to remain hidden while using cryptocurrency. One might begin with Virtual Private Networks (VPN) and the Tor, or Onion Router Network. VPNs add security to a User's network using secure protocols. These protocols will encapsulate the User's activities on a system and allow them to appear in another location around the world and under a different identifier. Using VPN in tandem with the Tor router network substantially increases the chance of anonymity.

8.2 Mixers

One actor making the investigation of cryptocurrencies more difficult are called *mixers*. These mixers take coins from many different sources and redistribute them to hide the original owner of the coin and the transactions with whom they are involved. To make this even more difficult, the mixer may be able to break coins up into smaller bits before redistribution. This makes tracking a transaction using the currency's blockchain increasingly difficult.

8.3 Transaction Addresses

User-specific addresses of cryptocurrencies and their respective transactions can be obtained from wallets and other files stored on digital devices. Each of these addresses, if used more than once, can track and link transactions together. A User can have more than one address within their wallet or file containing the data. Accordingly, it is suggested that, each time a new transaction occurs, for a User to create a new address to further obfuscate the identity of

the owner. This indeed further hampers enforcement and the regulation of illegal transactions calling to attention the important for enforcement agencies to be patient in handling these cases as it can take years to identify the criminal actor. Incidentally, to enjoy increased privacy, some currencies create a stealth address inherently built into the system like Monero. A stealth address allows a User to create a one-time address for every transaction.

9 THE BLOCKCHAIN

A blockchain is simply a method for creating a record of transactions through a peer to peer ideology, a simple term for sharing and structuring data within a network. Blockchains are about more than cryptocurrencies. They cogently create permanent records of the transactions they manage. The first blockchains created were to aid in verifying transactions of certain assets. Consequently, these monies would be moved onto other transaction systems.

9.1 Like a Ledger as a Distributed Database

Each transaction within a blockchain is stacked on top of the previous one. Each transaction is considered a block and has a reference to the previous block within the chain. All blocks are recorded form the beginning of the chain's creation to the last transaction thus creating the database within the blockchain. A rule of coding is implemented to ensure there are no duplicate transactions using cryptographic hashes. A mathematical equation is executed until there is a match and/or below a certain threshold, thereby forcing the creation of a new transaction. This can be a simple hash of a random phrase or random characters itself. Each blockchain creates its own rules for this mathematical question.

A private key is used to sign transactions by the User. As an example, Bitcoin uses a hash as an identifier of the coin owner that resembles the string below:

ntdqah0sr3r7x4kvg5l6d3lgdn39ret9gtzz3f5msr

It is shown as the hash of the identifying algorithm instead of any identifying information of the User. This makes identifying the actors within an illegal transaction much more difficult to match them with the identifying address of all the coins involved with the transaction. The first block created within Bitcoin is presented below:

hash":"000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f",
"ver":1,
"prev_block":"0000000000000000000000000000000000000000000000000000000000000000
00000",
"mrkl_root":"4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b",
"time":1231006505,
"bits":486604799,
"fee":0,
"nonce":2083236893,

Figure 2. Shows the first block of Bitcoin [20].

A system that uses hashes as identifiers is a system that is transparent and incorruptible. The addresses added to the chain cannot be changed or the hashes would be different and by simply comparing one block to the same block on another node provides proof of change. An alert is then issued.

9.2 Network of Nodes

The network of nodes consists of all digital devices connected to the currency or blockchain network thereby creating a decentralized aspect of blockchains. This creates no central point of failure or point of attack for malicious actors. Each node is owned and maintained by an entity consisting of a person or group of people that maintain the digital devices for that node. When the whole of a blockchain is located within a single node it is called a *full node*. A full node, in most networks, can cast its vote when a decision is to be made about the current or future of the network currency or blockchain. During a consensus-based decision for the network, it is important to take into consideration nodes that are not functioning at the time of consensus which may directly affect the rules of the consensus. But it is also this network of nodes that allow a blockchain to remain a part of the community and not under the control of a single group.

9.3 Transparent and Incorruptible

Blockchains are transparent and incorruptible. It is their built-in function, as it were, to monitor the network. Because the data of the blockchain are held over several nodes within the network, it

is extremely difficult to attack the blockchain or manipulate it in any way. This redundancy helps to prevent any manipulation of the chain and will signal alerts to the nodes resulting in the nodes acting upon that intrusion. It is possible to alter the data within the chain. But to do so would take a great deal of computing power and money which would result in a loss of profit for the criminal actor thereby protecting the network and blockchain.

9.4 Types of Blockchains

There are three different types of blockchains currently in use. The first is Public Blockchains that are used within cryptocurrencies. These use an open-source platform allowing for the maintaining of the blockchain to be performed by the open-source community. Any changes to the code within the blockchain are taken to a vote by the community, making it very difficult to impose arbitrary changes. The second blockchain is Permissioned which controls what roles people play within the system. The code is either open source or private depending on the ownership. The third is a Private blockchain that is usually small in size and used to trade confidential information between trusted parties. These blockchains all have essentially the same underlying code that creates a permanent record of the transactions that are traceable and verifiable.

9.5 A Transaction

The order of a transaction within a blockchain can be simplified to a few steps. The first is a User requests a transaction to take place which broadcasts the request over the peer-to-peer network. The network of nodes then validates the User status and the transaction request. Once the transaction is verified by the network, the request is added to other transactions using the currencies previous addresses as a reference creating a new block of data. The new block is then added to the existing blockchain and the transaction is complete.

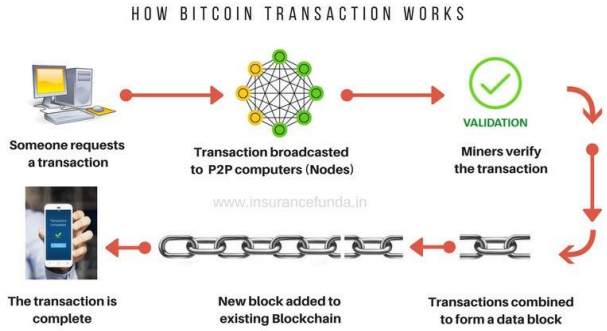

Figure 3. Shows example of a transaction [21].

9.6 Smart Contracts

Etherium consists of a blockchain but differs from cryptocurrencies in that it utilizes smart contracts. A smart contract is code for when a condition is met the execution of the program may commence. This can be a simple membership in an organization during contract renewal when the membership is expired or the User is prompted to pay more currency. A smart contract can be created for any type of real world service. Once the service meets the criteria of the smart contract, the payment is sent.

10 HOW CRYPTOCURRENCIES STAY LEGITIMATE THROUGH MINING

Legitimate cryptocurrency transactions can be broken down into a couple steps. The owner of a coin must be able to provide a public key for that coin so that it can be verified by nodes within the network obtained from a reliable source deemed by the network. Each coin is then considered expended when a transaction takes place and is not subject to being used again within the same transaction. Finally, the transaction is logged within the coin's blockchain and updated across the network of nodes. The transactions are then verified through mining.

10.1 Mining Transactions

Each transaction within a cryptocurrency blockchain is verified by the mathematical computation and added to the chain by miners. A miner is a person or entity a part of the community that verifies and adds the transactions to the currencies chain. Mining requires significant computer power and special applications to solve the mathematical problems.

An issue that has risen due to the need of computer power to mine transactions is the infection of other computer systems by miners who perform this task. Malware is injected into a system of computers using various sources and the computer's power is then converted to mine for the criminal actors. Because the computer system is only used for its power, a lot of the times it goes unmonitored as it only affects the power of the system and is hardly noticed. Acquiring other computers through malware has become quite the rage for criminal actors. It is a cheaper form of work than purchasing the computer power themselves.

10.2 Proof-of-Work or Proof-of-Stake

A miner gets paid by proving a transaction has taken place through providing a Proof-of-Work (POW) or Proof-of-Stake (POS). The POW concept is broken down to simply the first miner that solves the mathematical problem within the transaction gets the pay determined by the network for that transaction. A POS option for transactions is the miner, or in this case the forger, is selected in a deterministic way thus removing the competition involved in mining. A pool of forgers is created and the forger creates the new block for the transaction and gains a monetary fee for creating the block, thus verifying the transaction.

The POS has benefits over a POW system but also has its concerns as well. The benefits are that it takes far less energy for the transactions which require non-cryptocurrency monetary needs to pay for such power. This keeps the pricing for the currency more consistent. This also allows for lower income Users to compete with larger groups. But the difficulty of a POS system is the security of the underlying algorithm which must be as secure as possible to protect against criminal actors. Within the POW system, it would take a vast amount of money to attack the whole network of miners attempting to validate the transactions versus one entity in the POS system.

11 FINDING THE EVIDENCE

The globalization of currency will have a significant effect on how we conduct criminal investigations. Investigators will require special legislative permission or otherwise to conduct inquiries within another nation states as cryptocurrency has no borders. However, the blockchains within the cryptocurrency do allow investigators to obtain owner managed data on transactions without special permissions from financial institutions. Thus, finding evidence on a seized digital device is essential in criminal investigations involving cryptocurrencies.

Applications exist to assist Users with managing cryptocurrency adding to the difficulty of finding artifacts needed for a forensic investigation. Knowledge of these applications and where they store the data is important, especially if the application encrypts or attempts to hide the data requiring a passcode. An application can simply encrypt data, monitor transactions and not store the data as identifiable. As each application may handle data differently, it is important for an investigator to understand what each application does and how it manipulates and stores the data.

11.1 Random Access Memory (RAM)

Acquisition of data on devices acts like any other digital investigation: Acquire the Random-Access Memory (RAM), image the drive, and detail a network map of connected devices. When a device is encountered, an investigator must determine how to handle the device to maintain the integrity of the data. This is important to understand when acquiring the RAM. While the system is live and RAM acquisition is negotiated, the device will indeed be changed in some minor way. These minor changes must be noted within the report to account for any differences. A good tool to use for acquiring RAM is Volatility which is a collection of open source tools for RAM collection. Using a familiar tool aids in determining what changes may be made while doing the acquisition.

The data on RAM acquired from a device can be minimal. It could, however, contain all the processes currently running on the device. This helps to determine if the data is encrypted, what programs are running in case some of them may harm the acquisition of the evidence, and applications that may contain the artifacts in question. Volatility will detect any connected device that might not be seen through a wired connection. The device could be controlled

remotely by miners saving a dollar on their own equipment or a hidden on a hard drive located somewhere within the domicile. Previously extracted files on the system can be found within the RAM as it is memory that is overwritten as more data is used by the RAM.

11.2 Wallet

Artifacts of Bitcoins on digital devices are stored in wallets. These wallets contain several bits of knowledge needed for an investigator. The location of the wallet files can be different with each application. The wallets can contain transactional data with timestamps. Although the names within the wallet are the specific created address, they can be tracked and used to identify people or groups. Just like any other banking statement, this can be disclosed and used in a court of law. In some instances, these wallets are lost or stolen without the existence of a backup. The cryptocurrency is then lost to the user.

Cryptocurrencies can store data under different names and in different locations, so it is important to understand where they reside on the device. Bitcoin files can be labeled *wallet.dat* while files for other currencies and applications could be labeled something different like *file.wallet*. The basics of a wallet, however, contain the transactional data needed within a table. Addresses used for the various transactions encountered and timestamps of those transactions can be in the table. These addresses can then be compared to other known acquired devices for connections of activity or proof of transactions for legal purposes. If the identity of an owner of a hash is found, that hash can be tracked along the blockchain to determine that said transactions have taken place. The hashes encountered can also relate to other known identities.

China has recently been allowed to use the blockchain to authenticate evidence in a court case [22]. This particular case introduced the idea of using the blockchain hashes to authenticate evidence used in the court case. As law enforcement and governments around the world begin to create legal uses of the blockchain the need for digital forensics within this scope will increase.

11.3 Artifacts on the Drive

Each system stores data differently according to its folder structure. A program might store backups of the wallet in different locations. The entire blockchain could be located within the disk as well as a file containing addresses of previous interactions to make connections faster in the future. Just where these artifacts are located on a device will depend on what medium is storing the data and the folder structure of the device. The following is an example of data found on a drive within the AppData folder:

Evidentiary Artifact	Location
Bitcoin-Qt program	C:\Users\XXXX \AppData\Roaming\Bitcoin
"blocks" subfolder	C:\Users\XXXX \AppData\Roaming\Bitcoin
"chainstate" subfolder	C:\Users\XXXX \AppData\Roaming\Bitcoin
"index" subfolder	C:\Users\XXXX\AppData\Roaming\Bitcoin\blocks
wallet.dat	C:\Users\XXXX \AppData\Roaming\Bitcoin
debug.log	C:\Users\XXXX \AppData\Roaming\Bitcoin

Figure 4. Shows an example of data on a drive [23].

What a device contains will depend its purpose or role in the currency exchange. A computer unknowingly used for mining will contain the application used to mine data hidden on the drive. This can be found by isolating the power on the system and determining its specific use. Alternatively, a system could be encrypted to hide transactions that deal with a pedophile or a phone could hold the transactions used to fund a terrorist group. Whatever the device, it is important to understand that technology is always changing as well as its intended use.

By using tools like Magnet IEF, an investigator can find logs including queries of sites using the digital funds. But finding this evidence on a threat actors digital device can aid in solving not only the crimes of that threat actor, but also identifying others involved within their network.

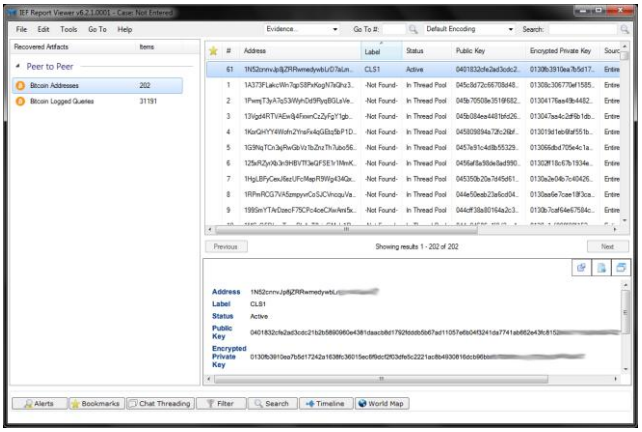

Figure 5. Shows Magnet IEF report [24].

Currency addresses, queries, and individual records can be found using tools like Magnet IEF. This data can then be analyzed to determine the owner and their actions.

The recent Department of Justice (DOJ) indictments of Russian threat actors revealed the use of the analysis of artifacts within the Bitcoin blockchains to connect the online personas back to the actors involved with the hacks [25]. The same Bitcoins used to purchase domain names to spear-phish information for the hacking was also used to register the dcleaks.com domain which provided the leaks. In another instance the same currency was used to log into a Twitter account as was to purchase the VPN used.

11.4 Network Artifacts

With the aid of tools like Wireshark, an acquisition of network traffic occurring during transactions may be captured. Within the acquired messages are specially coded transactional data.

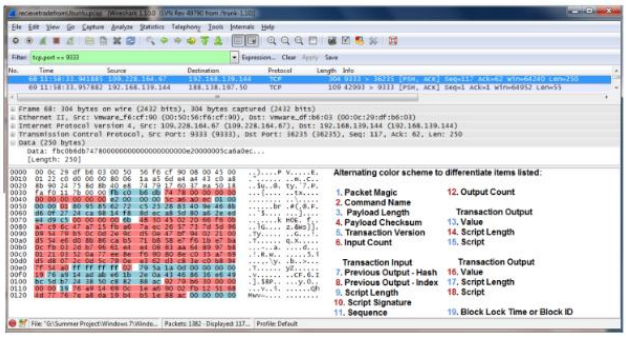

Figure 5. Shows a Wireshark acquisition [26].

Addresses can be acquired from a network and real-time transactions can be applied to criminal actors. IP addresses of participants in conversations and all searches may be found using a tool like Wireshark. Such acquisitions may identify where the actors shop online for their illegal actions, with whom they contact, and when transactions take place. These artifacts can be especially detrimental for a defense team in court.

12 CURRENCY MONITORING TOOLS

Tools like Elliptic have begun to aid in identifying illegal activity using digital currencies. These tools use public blockchain data with known addresses of threat actors to track the usages of the currency. This data is analyzed to determine transactions and usage of currency exchanges and mixers to aid in laundering the money. Elliptic has tracked data between 2013 and 2016 to determine the largest sources of illicit use of exchanges and mixers.

ORIGIN OF ILLICIT BITCOINS ENTERING CONVERSIONS SERVICES: LARGEST SOURCES					
Name	2013	2014	2015	2016	All Years
Abraxas	-	0.00%	8.99%	-	3.00%
Agora	0.02%	42.43%	47.89%	0.05%	26.30%
AlphaBay	-	0.00%	9.38%	46.65%	6.26%
Evolution	-	8.35%	10.09%	-	5.40%
Middle Earth Marketplace	-	0.05%	5.59%	-	1.88%
Nucleus Market	-	0.01%	13.6%	31.21%	6.63%
Sheep Marketplace	8.42%	-	-	-	3.00%
Silk Road	89.89%	-	-	-	32.03%
Silk Road 2.0	1.03%	40.50%	-	-	10.21%
Total	99.37%	91.35%	95.54%	77.92%	94.70%

Figure 5. Shows moneys entering exchanges. [27]

The importance of these tools in monitoring and tracking threat actors around the world is becoming paramount for law enforcement. These tools accompanying forensics of digital currencies will aid in combating these illegal activities.

13 BLOCKCHAIN CAN DO GOOD

The technology within blockchains can be used for other purposes across different industries. One advantage of a blockchain is the elimination of a third-party, such as banks, required for such transactions. For a long time, a third-party has been used to handle a transaction because they are a trusted source. But when that trusted source does something accidental or malicious with those transactions, there can be detrimental consequences. Third-parties have been in place for a long time throughout currency history and it is embedded in the minds of many to trust these entities. So, it is difficult for a layperson to accept that there may be no need for a third-party. The elimination of a third-party within transactions creates a less than likely chance of corruption of said transaction and eliminates any fees for the third-party's involvement.

Voting blockchains provide immediate verifiable results and help to eliminate voter fraud. On March 7, 2018, the Swiss-based company used a blockchain with the approval of the National Electoral Commission Sierra Leone as an international observer to collect voting data.

Leonardo Gammar, the Chief Executive Officer of Agora stated, "We're really interested in helping new democracies protect their democracy," said Gammar, who is half Tunisian and spoke of his experience while watching the North African country develop independently following the Arab Spring uprising [26]. A voting blockchain could assist developing nations with new democracies to protect the votes against corruption from local warlords or other malicious entities.

Other uses of the blockchain can include healthcare and industries that need to deal with nefarious production practices. Healthcare providers can have access to information from multiple sources about their patients that is updated immediately to address an emergency without waiting for background information stored on another healthcare provider's database. This could also include family history to help provide a larger picture to determine the best approach for the patient. Again, there remains a trust issue with such technology when a decentralized database in place. It allows for more access points of the data and security of the database would be the most essential need for this type of blockchain. Industries such as clothing can use blockchains to track where a piece of clothing is produced to better combat underage and slave labor practices. These technologies are in production and are being tested as options to other mainstream technology solely owned and managed by one person or a small group. Blockchains can be used to eliminate third party involvement and control of data by a select few to combat corruption in any media form making things more trackable for forensic investigators.

14 CONSLUSION: WILD WEST WITHOUT FORENSICS

Forensic monitoring of the cryptocurrency landscape will become essential to protect layman persons from a wild west of digital currency. Digital forensics is used every day to combat criminal actions all over the world and this has evolved into the digital currencies used. Criminals are beginning to attack markets, personal wallets, and using a currency's own code to project illegal items or actions onto individual systems. Developing applications like Elliptic can aid in digital forensic monitoring and investigations of illegal activities using cryptocurrencies. Elliptic monitors Bitcoin activity looking for suspicious patterns within the public Bitcoin ledger. Criminal activity is evolving, and enforcement agencies need to immediately address these issues.

Already there have been actions of one currency or blockchain attacking another entity for creating a technology that limits low end consumers from mining efficiently. Blockchain technology should be created to avoid narrowing the field of miners to include only specific groups like high end mining groups with the server capability to control most of the mining done. Regulations of cryptocurrency actions are limited to the network of nodes or the company that controls the currency. Forensics can be used to combat these situations and might help to keep cryptocurrencies legitimate.

Hacking of cryptocurrency markets have increased recently resulting in millions of losses. These attacks are initiated through phishing scams, social engineering of company employees, attacks on individual wallets, and distributed denial of service attacks on the markets. Currencies themselves could use these actions to attack another currency to decrease the market value thus resulting in an increase of its own monetary value. Criminals find that attacking the markets are a quick way to make money and they do their best to hide their actions just like any other digital crime. The difference here is that these instances have international monetary ramifications.

In sum, it will be necessary for government enforcement agencies, instructional institutions, and the open source community to further develop digital forensic applications and procedures to combat new arising scenarios within the cryptocurrency and blockchain landscape. These scenarios include individual activity, groups of criminals, and governments all over the world, thus creating a need for a global community or organization to aid in monitoring and investigating the actions surrounding digital currencies. These newly formed or forming groups should collaborate with educational institutions to create and endorse programs that educate others in forensic techniques of blockchains and cryptocurrencies. Without continued and quick growth of the

forensic community to combat illegal and immoral actions there will soon become a Wild West of activity involving cryptocurrencies and blockchains.

15 REFERENCES

1. Lansky, Jan. (2018). Possible State Approaches to Cryptocurrencies.*Journal of Systems Integration.*(p. 19).
2. Korolov, M. (2018). *Ransomware took in $1 billion in 2016--improved defenses may not be enough to stem the tide*. *CSO Online*. 4. Retrieved 1 April 2018, from https://www.csoonline.com/article/3154714/security/ransomware-took-in-1-billion-in-2016-improved-defenses-may-not-be-enough-to-stem-the-tide.html
3. Back, A. (2002*). Hashcash - Amortizable Publicly Auditable Cost-Functions* (p. 4).
4. Franco, P. (2015). *Understanding Bitcoin* (p. 164). Church Way, Oxford, UK: Sparks.
5. Nakamoto, Satoshi (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. (p. 8).
6. All Cryptocurrencies | CoinMarketCap. (2018). *Coinmarketcap.com*. Retrieved 1 April 2018, from https://coinmarketcap.com/all/views/all/
7. gamerveda. (2018). *History Lesson: Putting the Rise and Fall of Altcoins into Perspective*. *Steemit*. Retrieved 1 April 2018, from https://steemit.com/cryptocurrency/@gamerveda/history-lesson-putting-the-rise-and-fall-of-altcoins-into-perspective
8. *Rise of Altcoins: Bitcoin Dominance Index Drops to All-Time Low at 37.7%*. (2018). *CCN*. Retrieved 1 April 2018, from https://www.ccn.com/bitcoin-dominance-index-drops-to-all-time-low-at-37-7-rise-of-altcoins/
9. *SEC.gov | Blue Sky Laws*. (2018). *Sec.gov*. Retrieved 1 April 2018, from https://www.sec.gov/fast-answers/answers-blueskyhtm.html
10. Nelson, A. (2018). *Cryptocurrency Regulation in 2018: Where the World Stands Right Now*. *Bitcoin Magazine*. Retrieved 1 April 2018, from https://bitcoinmagazine.com/articles/cryptocurrency-regulation-2018-where-world-stands-right-now/
11. *Bill Gates: Bitcoin Is Exciting Because It's Cheap*. (2018). *Bloomberg.com*. Retrieved 1 April 2018, from https://www.bloomberg.com/news/videos/2014-10-02/bill-gates-bitcoin-is-exciting-because-its-cheap
12. Kim, T. (2017). *Bitcoin up sevenfold since Warren Buffett warned digital currency was a 'mirage'*. *CNBC*. Retrieved 1 April 2018, from https://www.cnbc.com/2017/09/07/bitcoin-up-sevenfold-since-warren-buffett-warned-digital-currency-was-a-mirage.html
13. *Research into the usability and practicalities of blockchain technology for the air transport industry.* (2018). (p. 13). FlightChain.
14. DiMarino, F., & Roberson, C. (2013). *Introduction to Corporate and White-Collar Crime* (p. 83). Boca Raton, Fl. CRC Press.
15. Grobman, S., & Cerra, A. (2016). *The Second Economy: The Race for Trust, Treasure and Time in the Cybersecurity War* (p. 7). New York, NY. Intel Corp.
16. AlphaBay Takedown. (2018). Federal Bureau of Investigation. Retrieved 3 September 2018, from https://www.fbi.gov/news/stories/alphabay-takedown
17. Founders of Cryptocurrency Company Indicted in Manhattan Federal Court with Scheme to Defraud Investors. (2018). Justice.gov. Retrieved 3 September 2018, from https://www.justice.gov/usao-sdny/pr/founders-cryptocurrency-company-indicted-manhattan-federal-court-scheme-defraud#_ftn1
18. Virtual Currency Schemes. (2015). Federal Bureau of Investigation. Retrieved 1 September 2018, from https://www.fbi.gov/audio-repository/news-podcasts-thisweek-virtual-currency-schemes.mp3/view
19. Former Shreveport chiropractor, son plead guilty to operating illegal bitcoin exchange business. (2016). Justice.gov. Retrieved 24 August 2018, from https://www.justice.gov/usao-wdla/pr/former-shreveport-chiropractor-son-plead-guilty-operating-illegal-bitcoin-exchange
20. defraud#_ftn1Sammons, J. (2015). *Digital forensics* (p. 7). Waltham, MA.Elsevier.
21. Anish, L. (2017). *Bitcoin and other cryptocurrencies - all you need to know - Insurance Funda. Insurance Funda. Retrieved 23 April 2018, from* http://insurancefunda.in/bitcoin-cryptocurrency/
22. Zhao, Wolfie (2018). *Blockchain Can Legally Authenticate Evidence, Chinese Judge Rules - CoinDesk. (2018). CoinDesk. Retrieved 8 September 2018, from https://www.coindesk.com/blockchain-can-legally-authenticate-evidence-chinese-judge-rules/*
23. Carbone, R. (2015). *A Forensic Look at Bitcoin Cryptocurrency*. (p. 27). SANS Institute InfoSec Reading Room.
24. Bitcoin Forensics – A Journey into the Dark Web - Magnet Forensics Inc. (2013). Magnet Forensics Inc. Retrieved 9 September 2018, from https://www.magnetforensics.com/computer-forensics/bitcoin-forensics-a-journey-into-the-dark-web/
25. Robinson, D. (2018). Bitcoin Blockchain Analysis & DOJ Indictment of Russian Hackers. Elliptic.co. Retrieved 9 September 2018, from https://www.elliptic.co/our-thinking/doj-indictment-russian-hackers-blockchain-analysis
26. Miller, P., Nudd, L., Vance, C., & Fenger, T. (2014). *Cryptocurrency Artifact Analysis*. *Marshall.edu*. Retrieved 23 April 2018, from http://www.marshall.edu/forensics/files/MIller-Poster.pdf
27. Fanusie, Y., & Robinson T. (2018). *Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services*. Elliptic. (p. 6).
28. Finnan, D. (2018). *Sierra Leone tests blockchain technology for tallying election results*. *RFI*. Retrieved 22 April 2018, from http://en.rfi.fr/africa/20180315-sierra-leone-tests-blockchain-technology-tallying-election-results

29. Lomas, N. (2018). *Elliptic takes in $5M for its blockchain forensics tool*. *TechCrunch*. Retrieved 8 March 2018, from https://techcrunch.com/2016/03/21/elliptic-takes-in-5m-for-its-blockchain-forensics-tool/ (Links to an external site.)
30. Johnson, B. (2018). Monero's War Against Big Businesses and High-Speed Hardware – Cryptocurrency Market. Currencymarket24.com. Retrieved 22 April 2018, from http://currencymarket24.com/moneros-war-against-big-businesses-and-high-speed-hardware/