The involvement of cryptocurrency in online crimes

Andrea Lisi
Department of Computer Science
Università di Pisa
andrea.lisi@phd.unipi.it

Abstract

A cryptocurrency is a virtual currency based on cryptographic operations. Cryptocurrency became very popular in the last years, especially for speculation. Given the absence of regulations, cryptocurrency are preferred by online criminals as payment of a service, of a ransom, and as revenue after a scam.

This report describes how cryptocurrency is involved and how it is gained from illegal actions, and how criminals can launder their coins to conceal their traces.

1 Introduction

Nowadays, cryptocurrency, such as Bitcoin or Monero, are very popular among people all over the world, and they are exchanged at high volume on a daily basis, especially through crypto exchanges, such as Coinbase or Binance. The popularity of cryptocurrency raised a lot in the past few years, especially on late 2017 due to Bitcoin reaching a price record (at that time) of about 20.000$ per bitcoin (BTC). Moreover, on the same period Decentralized Applications, applications whose ecosystem is based around cryptocurrency, became very popular especially thanks to Cryptokitties, a marketplace of unique digital cats. Currently, cryptocurrency and blockchain technology is studied and used for applications other than financial, for example supply chain management [33] and certification of digital objects through Non Fungible Tokens (NFT) [15].

Cryptocurrency allows Internet users to exchange digital coin all over the world without involving any central bank, for example with bank transfers or credit cards, allowing anyone also to pay another person living in a country where banks cannot transfer money because of restrictions. However, criminals do enjoy of this "freedom" as well. Indeed, currently illegal services on the Internet are mostly paid in cryptocurrency because they have no clear regulations. Cyber-attacks, such as ransomware attacks, also ask for ransoms in cryptocurrency, because it is safer than receiving money in a bank account. As a matter

of facts, companies hold a supply of cryptocurrency to pay for ransoms in case of an irreversible attack [25].

The data about the real usage of cryptocurrency is currently contradictory. A research from 2018 estimated that about half of the transactions in Bitcoin were payments and transfers involving illegal activities [17]. However, analyses performed by DEA in America says that cryptocurrency did have a high criminal usage, estimating in 2013 about 90% of Bitcoin transaction used to be behind illegal activities, but in 2018 the situation was reversed, i.e. estimating about 90% of Bitcoin transactions were involved in speculation and investments [30].

This report provides a view of some techniques and ways that criminals obtain cryptocurrency, and how they can spend them afterwards. The goal is to raise awareness that cryptocurrency are close to be used by the general public on a daily basis, and not only between a restricted group of specialized hackers, but also that criminals are trying to obtain them from the general public, for example through scams or ransoms.

2 Cryptocurrency, blockchain, and identity

According to Investopedia [22], there are three forms of electronic currencies: *digital currency*, a currency that is issued by banks in digital form, it is regulated by governments, and it allows users to perform long distance payments; *virtual currency*, an unregulated digital currency that is only available in digital form, and whose value, management, and usage rules are dictated by the organization, or group of developers, who issue that currency; *cryptocurrency*, a specific virtual currency whose operations are secured by cryptography.

The first implementation of a cryptocurrency is Bitcoin [28] whose paper was made public in 2009. Bitcoin is a peer to peer (P2P) protocol that allows peers to exchange a cryptocurrency, the bitcoin (BTC), without any third party authority that keeps and controls all the transactions of all its customers, such as a bank. Bitcoin solves the main problem of P2P virtual currencies: the *Sybil attack* [11]. A P2P system is vulnerable to a Sybil attack if a user can manipulate the system state by exploiting multiple peers, the Sybils, which all belong to the same user. A consequence of Sybil attack in a virtual currency ecosystem consists in the possibility to pay twice the same coin to two different recipients, also known as *double spending*.

In Bitcoin, the system state is the record of all the transactions made by the peers. Each peer stores the full record of transactions, the ledger, which is divided in blocks. Each block is uniquely identified by an hash value, and it is connected to the previous block by storing its hash. The result is a chain of blocks known as *blockchain*.

The peers cooperate to decide the next block, i.e. the next set of transactions and their order, to populate the ledger. In Bitcoin, the first peer who will solve a cryptographic puzzle, hard to find a solution but easy to verify the correctness of that solution, will be in charge to create and propose the next block. Once proposed, the other peers verify the correctness of the puzzle, the correctness

of the transactions reading their own copy of the ledger and, if everything is correct, they accept the new block, otherwise they refuse it. To incentivize peers to solve the puzzle, the peer who successfully propose a block receives a fixed amount of newly minted BTC as a reward. In Bitcoin, a block is produced on average every 15 minutes. This approach to upgrade the Bitcoin state is known as Proof-of-Work. Proof-of-Work prevents the Sybil attack because the chance a user has to upgrade the Bitcoin state does not scale with the number of peers controlled by the same user, and double spending is prevented because every peer knows the balance of every other peer. However, Bitcoin suffers from issues, such as the centralization of computational power on a few very powerful centers [2].

A peer does not "hold" BTC, but rather they can receive and send BTC through asymmetric cryptography operations. This is known as the *UTXO* (Unspent Transaction Output) model. A peer generates a private-public key pair through a *wallet*, a light-weight program that allows a peer to send transactions. A peer receives BTC, input, to their public key, and spends the BTC, output, by providing a valid digital signature for that public key. Therefore, a peer is *pseudonymous* in the Bitcoin system, meaning that a peer perform transactions behind an alias: the public key.

A peer can own multiple key-pairs, which is actually encouraged in order to protect the peer's privacy [38]. Despite that, all the transactions are linked together and visible on the blockchain, therefore as soon as the identity of a peer behind a transaction is disclosed, all the transactions concerning that identity can be tracked, no matter how many key-pairs that person uses [16]. This breaks the myth that users can exchange BTC anonymously.

2.1 Monero

Monero [27] is a cryptocurrency whose transactions are recorded on a blockchain and, like Bitcoin, the transactions follow the UTXO model and are validated by miners participating to a Proof-of-Work consensus with an average block time of 2 minutes. Monero is known as a privacy coin, which main goal is to protect the user's privacy through complete anonymity. Not only the sender and the recipient of a transaction are anonymous, but, unlike Bitcoin, the transactions from the same user cannot be linked together.

A Monero account is composed by the following data: a 95 characters long *public address*, which is used to receive payments; a private and public *view* key pair, which is used to display incoming transactions; a private and public *spend* key pair, which is used to send transactions.

The recipient privacy is protected with *stealth addresses*. A stealth address is a one-time public key that is part of a transaction, thus visible on the blockchain, and it is automatically and randomly generated for every transaction for every recipient a sender sends Monero (XMR) to. The stealth address is the address recorded on the blockchain, but an external observer cannot link that address neither to the sender nor to the recipient. The stealth address is computed as a function of the recipient's public view and spend keys, plus some random data to

generate a unique address. The transaction output is built so that the recipient is able to locate the transaction on the blockchain with their private view key, and to retrieve the amount on their wallet. Finally, the recipient can spend the XMR they received with their private spend key: they compute a one-time private key that corresponds to the one-time public key, which generated the stealth address, and they can spend the output with their private spend key.

The sender privacy is protected with *ring signatures*. A ring signature is a specific kind of digital signature that involves the actual signer and non-signer users, known as *decoy*, and which hides who the actual signer is. When a sender spends an output to a recipient, the sender chooses the size of the ring: this value is called *mixin*, and it represents the number of decoys. The sender randomly pulls from the blockchain a number of past transaction outputs equal to the mixin: all these outputs together, sender's and decoy's, form the inputs of the transaction signed by the sender private spend key. All the outputs together make the input of the transaction: an outside observer cannot tell which output belongs to the sender, and which outputs belong to the decoys. Since the actual signer is hidden, a double spending attempt from that private spend key is prevented with *key images*, a cryptographic key that is uniquely part of the output made up of each transaction in the ring signature: there exists a single key image for each output on the blockchain, which allows the block producers (miners) to verify that a new key image was never been used before, but it is not possible to detect which output in the ring created the key image.

The transaction amount is hidden with *ring confidential transactions* (ring CT). Before ring CT, a transaction had to be split because a ring signature could include only outputs of the same value, making the amount externally visible. With ring CT, Monero exploits cryptographic commitments, in particular *Pedersen commitments*, which allow a user to commit a value and keep that value hidden to others until the same user decides to reveal it: a commitment must not allow the user to modify the hidden value while it remains hidden. Let a be an output amount, x a random value, G a constant, and $H()$ a cryptographic hash function. The Pedersen commitment rCT stored on the blockchain is:

$$rCT = x \times G + a \times H(G) \tag{1}$$

Let T be a transaction with two inputs, I_1 and I_2, two outputs, O_1 and O_2, and a fee. The difference between the input commitments and the output commitment plus the fee must be zero to ensure that no Monero coins have been minted within that transaction T, i.e. $rCT_{I_1} + rCT_{I_2} = rCT_{O_1} + rCT_{O_2} + fee$. Since the commitments are public, this property can be easily verified by the miners. In particular, two Pedersen are created for the same transaction: one private and one dummy. The dummy one is the public one, and both are used to create an asymmetric key pair to generate the signature to place into the ring signature. More information can be found in [13, 29].

Finally, *range proofs* are used to prove that an output amount falls in the range $[0, 2^64)$. To reduce the size required to store N range proofs for N outputs of a same transaction, Monero utilizes *bulletproofs* [5].

All the above techniques combined provide complete anonymity and transaction untraceability to the Monero users.

Finally, like in Bitcoin, blocks are produced with a Proof-of-Work consensus called RandomX [18, 19], which is optimized for general purpose CPUs to prevent specialized hardware, less accessible than CPUs, to monopolize the block production. This is done by using two inputs: *data* and *code*. Specialized hardware can easily execute an operation with only *data* as input, but CPUs are more specialized in executing generic *code*. The RandomX algorithm follows these steps:

1. **Generate a random program:** the program is not generated with a high level syntax such as C, because the generation of instructions, abstract syntax trees, and compilation slows down the process. Instead, a program is represented as a buffer filled with random data without any syntax, so that any bytes data can represent a valid program;

2. **Translate the program into CPU machine code:** the program is translated in machine code finding a balance between hardware instructions, to improve speed, and CPU instructions, to support different architectures. However, since it is part of a Proof-of-Work, the code has to be inefficient enough to prevent code too easy to execute;

3. **Execute the program:** the execution of the program should exploit as many CPU components as possible. Examples are ALUs, FPUs, multi-level caching, and instruction level parallelism;

4. **Transform the output in a crypographically secure value:** using CPU efficient hash functions, like Blake2b or AES. The verification of the correctness of this value must done efficiently by miners.

3 Obtaining cryptocurrency through online crime

Illegal actions, such as scams and threats, always existed. Nowadays, thanks to the large deployment of Internet, illegal activities found a new profitable market, and malicious users developed an entire new set of skills to exploit that market. Due to the increasing regulations that governments introduced to fight illegal movements of large amount of money through banks, criminals moved their interest in cryptocurrency, which are currently not regulated.

This section provides a small survey on crimes and attacks that criminals do to obtain cryptocurrency.

3.1 Scams

A *scam* is a stratagem to defraud a person after gaining their trust. Popular online scams are the fake virus popups and the refund scams. Both types of scams involve *social engineering* [24] techniques to let the scammer to gain the trust of the victim, to pressure, or even to threat the victim. The first step

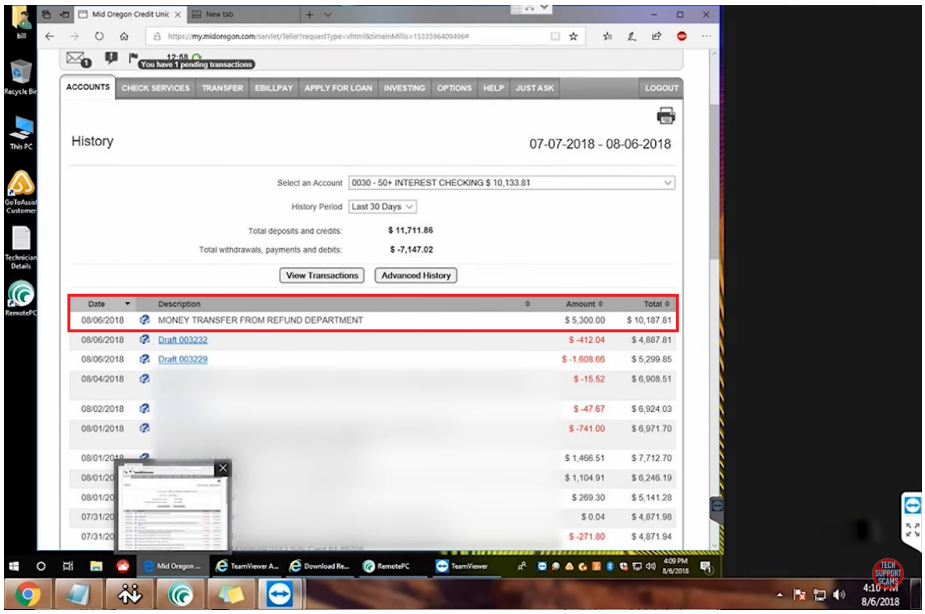

Figure 1: Refund scam: a screenshot of a victim's computer. The scammer moved 5300$ between two savings deposits of the victim's bank account, and he changed the HTML "Description" to look like a "genuine" money transfer to that deposit. The refund was promised to be 300$ [4]. Notice the Teamviewer software.

common to most of online scams is the installation of a remote access control software, such as Teamviewer, on the victims computer, and convince the victim to give them access to their computer.

The *fake virus popup scam* is very simple. An internet user goes, by mistake, to a predatory web page that pops up a fake alarm stating the computer is compromised, together with a banner showing a telephone number, belonging to a scammer, to call to receive technical support. The scammer will push the user to buy a fake antivirus software, or will execute fake or useless programs on the victim's computer to convince the victim the problem has been fixed, so that the scammer can charge the victim for the service.

A *refund scam* is more articulated and requires extra steps, but if effective the reward pays off. A victim gets contacted by a scammer who impersonates an employee of a big known company, such as Microsoft, and announces the victim that they have the right of a refund because of some miscalculation, or even because the company is going bankrupt. Typically, scammers convince the victim about the refund amount, e.g. 500 dollars, and in order to receive it the victim must give the scammer access to their computer with a remote access software, and then log in their home banking website. However, the scammer cannot simply make a money transfer from the victim account to

theirs, because often online banking requires a few extra steps, such as One Time Passwords (OTP) or two-phase confirmation with a smartphone. However, a transfer between different deposits belonging to the same bank account does not typically require any confirmation or password. Therefore, the scammer will fake a bank operation thanks to the access they previously got to the victim's computer.

To do that, the scammer exploits standard features of remote access software: with an excuse of "the computer is processing the refund", the scammer blocks the victim's input and blacks out their screen, therefore they make an internal transaction between two deposits in the same bank account, moving an amount larger than the refund, e.g. 5000 dollars. Before giving the victim the access to their computer back, the scammer modifies the HTML page on the browser to make the internal transfer to look like an external transaction (e.g. modify the transaction description to "REFUND FROM MICROSOFT", see Figure 1).

Next, two example tactics can be: 1) the scammer shows the victim that they have received too much, and they beg the victim to refund the scammer the difference (e.g. 5000 - 500 = 4500$) otherwise the scammer will lose their job; 2) the scammer asks the victim to type useless commands on the command prompt, e.g. "`Execute transaction from Microsoft = 500$`" while inserting an additional `0` to the amount right at the end[1] so that the victims reads a larger number. The scammer shows on the bank page (previously manipulated) that the victim received too much, blames the victim for their mistake, and threats them to send the difference back to the scammer.

Since governments introduced regulations on money transferred through banks, scammers often ask for money through pre-paid gift cards that can be bought from many shops [8], and that cannot be linked to a specific person like bank transfers. A scammer asks the victim to buy a certain amount of gift cards to a nearby shop, and to tell them the code of each card. However, since shoppers get suspicious when a customers wants to buy 5000$ worth of Apple gift cards[2], often they ask for clarifications or simply refuse to give the gift cards to the customers, waiting for instructions. If a victim realizes of being scammed, if they act quickly they can call the customer service of the company issuing the gift cards to block them.

Due to the absence of regulations and the impossibility for a central governance to undo a transaction, scammers nowadays ask also for payments in cryptocurrency [9].

3.1.1 Cryptocurrency centered scams

Due to the current high popularity of Bitcoin and the raise of its price, which is nowadays about 50K$, cryptocurrency have become a new form of investment. Bogus investments promising high rewards in a short period became very popular around years 2017-2018. Many of the scams exploited a new form of

[1] Recall the scammer has remote access to the victim's computer.

[2] It happens that scammers who plays as a Microsoft employees do ask to be refunded with Apple gift cards.

fundraising known as Initial Coin Offering (ICO). An ICO [23] is a fundraising technique that pre-sells cryptocurrency tokens to fund a new cryptocurrency-based project. A person, during the ICO, funds the project by buying coins that can be used on the project once it is in production. The most successful ICO, 4 billions of USD, was raised by block.one, the start-up behind the development of the EOS.IO framework [6].

A research of 2018 done by Satis Group [12] classified about 78% of all ICOs as scams, but which collected in total "only" about 11% of the total investments on ICOs: about 1.3 billions of USD out of 12 billions. In another study, Sapkota et al. [34] conducted a research, mixing automatic and manual search, to detect the patterns behind scams related to ICOs. The authors classified 576 malicious ICOs in the following categories:

- **Dead or fake:** Convince to invest on a dead or fake project;
- **Exit:** Promoters disappear after collecting investments, or fail to pay back the investors;
- **Exploding airdrops:** Scammers manage to steal investors private keys;
- **Whitepaper plagiarism:** Propose a project copying the whitepaper of a popular one;
- **Pump and dump:** Convince others to invest in a cryptocurrency previously bought and, as soon the price raises, immediately sell everything;
- **Ponzi scheme:** Promise a victim large returns after an initial investment, and ask them to convince others;
- **Website:** Drive investors to use a malicious version of a popular website;
- **Pre-mine:** Instead of burning unsold tokens, divide them among the promoters, so each sold token has a lower price.

However, the categories proposed by Sapkota et al. can be generalized to cryptocurrency in general, and not only to ICOs. For example, pump and dump strategies can be applied to any cryptocurrency investment to alter their value with a massive organized acquisition in a short time frame, and then sell everything right after, which is organized thanks to online dedicated groups [26].

Finally, as last example of cryptocurrency related scam involves the social media. It is possible for users, especially famous ones, to have their account hacked and exploited by attackers. Therefore, the hacker can use the account of a famous, and potentially trusted, user to publish a post promising a big return in cryptocurrency if they receive a small amount first. A similar attack was performed on Twitter on 2020 (see Figure 2) and, according to BBC [1], during the short time it was online the Bitcoin addresses displayed in the tweets of targeted accounts received hundreds of contributions for a total amount higher than 100.000$.

Figure 2: A screenshot of the Twitter hacked account belonging to Elon Musk (notice the "verified" flag) asking for BTC.

3.2 Ransomware

A *ransomware* is a type of computer malware that attacks a victim's computer with the goal of asking for a ransom to the victim. As other malware, a ransomware can be included as a part of a file, typically hidden inside Microsoft Word document's macros[3], or can be downloaded by the victim themselves after clicking on a malicious link. Typically, a ransomware prevents the victim to access to their computer or their files, for example encrypting them all, but alternative attacks include also stealing private information and threatening the victim to publish them, or displaying fake police websites asking to pay for a fine for some illegal activity. Ransom payments have been carried out via bank transfers, premium SMS[4], gift-cards, and, recently, cryptocurrency.

A common implementation of a ransomware follows the Young et al. approach known as *Information extortion attack* [40] that uses hybrid encryption, i.e. both symmetric and asymmetric cryptography: a malware embeds, in its code, the public key of an asymmetric key pair and a random key generator; a malware infecting a device generates a random key that uses to encrypt all the files; the malware encrypts the encryption key with its public key, it deletes both the encryption key and all the files, and it displays a message to the victim asking for a ransom; the user is instructed on how to pay the ransom; if the user pays for the ransom and sends to the attacker the encrypted encryption key, the attacker, after checking the payment, decrypts the encryption key with their private key and sends the key back to the victim, who can get back access to their files. Figure 3 illustrates the attack.

Like online scams, it is difficult for an attacker to receive a remote payment through a bank transfer, because of regulations that ask banks to communicate suspicious payments. It has been observed that in the previous decade, that corresponds to the development of Bitcoin and other cryptocurrency, the number of ransomware attacks raised by a lot, and that many of the victims are willing

[3] A macro in Word is a command to automate frequent activities.
[4] A SMS that enables a paid service.

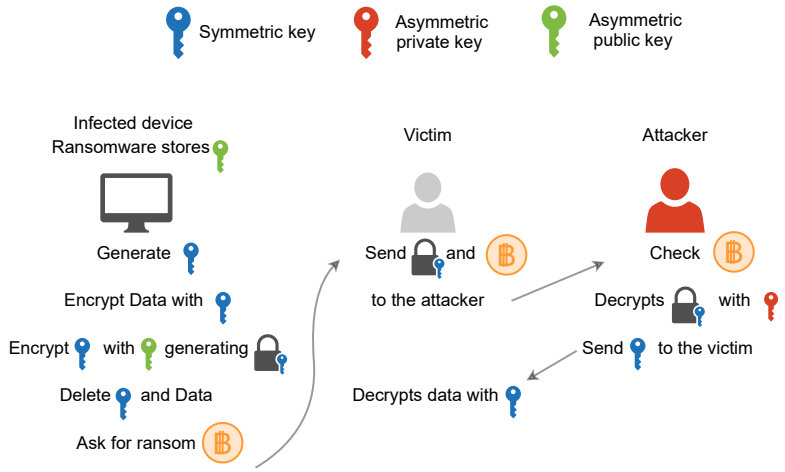

Figure 3: The scheme of an information extortion attack performed with a ransomware.

to pay a few hundreds of dollars to get their personal data back, despite of the suggestions to contact authorities first [7, 21].

A popular ransomware that encrypts the data and asked for a ransom in BTC was *WannaCry*. The attack was conducted in May 2017, and it is estimated it affected hundred of thousands of old Windows computers all over the world. After encrypting all the files, the ransomware locked the computer to display a single page (see Figure 4) warning the victim of the situation and giving them the instruction and the Bitcoin address to pay for the ransom that was 300$. It has been observed the attacker used three different Bitcoin addresses, and that the decryption after the ransom was performed manually [25]. However, regardless to the large scale of the attack, after a week only 50.000$ was paid, and only 143.000$ three months later. This relatively small amount can be a consequence of a combination of: *i)* a high complexity to pay for the ransom, for example the difficulty to collect BTC in time to pay for the ransom, either considering Bitcoin may be a completely new concept for many users, or due to the delays for the user to register and verify their identity on a crypto exchange; *ii)* a relatively low gravity of the consequences, because if a user is used to back up their data, WannaCry has low gravity. Despite the small gain for the attackers, the attack caused one of the highest financial losses whose estimations range from hundreds of millions up to four billions USD [10].

Finally, even if WannaCry did not have a financial success, other ransomware did: it was estimated that CryptoLocker, a ransomware for Windows, extorted about 28 million USD from its victims who paid with pre-paid vouchers or BTC, while the most profiterable example is CryptoWall, which extorted about 325 million USD in BTC [10].

Figure 4: A screenshot of a WannaCry ransomware on an infected computer.

3.3 Online black markets

A black market is a clandestine exchange of, eventually illegal, goods and money that do not follow any institutional regulation. In an online black market this exchange happens between two users remotely.

Most of the services that an average Internet user utilizes, such as social networks, email, shared platforms, and content platforms, are indexed by search engines, such as google, bing, and duckduck go: this set of indexed services belong to the so-called *surface web*. However, a machine can communicate to another machine that is not indexed by a search engine, for example a user may connect to a personal server, or a company may have an internal platform shared only among its remote branches. Such connection, typically secured with a password, can be established only if a user knows the precise URL, in case of a resource, or IP address, in case of a machine. This set of non-indexed contents and machines, that is estimated to be much larger than the size of the indexed services, is known as *deep web*. If a person hosts a black market on either an indexed or non-indexed location it can be easily detected, especially if indexed, tracked, and taken down by authorities. Therefore, these types of webs are not suitable to run a black market, even if it works behind the hoods of a genuine e-commerce service.

A *darknet* is a P2P overlay over the Internet that can be accessed only by means of specific software that provides anonymous connections, for example with the *onion routing*. The Tor project [36] is the most known browser that allows a user to navigate the Internet anonymously, and also to participate to a darknet. The set of darknets is known as the *dark web*.

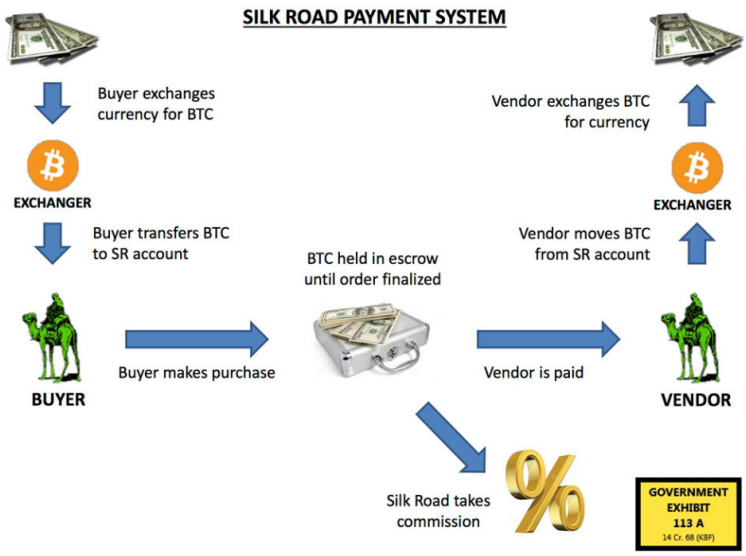

Figure 5: A flow chart of how Silk Road worked.

The onion routing [31] is used to send and receive messages to and from nodes participating to an onion network. A message is wrapped within as many layers, like an onion, of encryption as the number of hops the packet should do from the sender to the recipient. Through an onion proxy, the sender selects a set of nodes that forms the path of message, and it encrypts each i_{th} layer of the onion with the public key of the i_{th} node in the path. This protects, at each intermediate hop, the privacy of the sender, of the recipient, of the message, and of all the other nodes within the route: an intermediate node will know only its predecessor and its successor.

With onion routing, it is more difficult to perform traffic analysis, and to trace the origin and the destination of Internet messages. While this protocol protects people doing possibly dangerous jobs, such as journalists, it protects criminals as well. In their work Faizan et al. [14] analyzed more than 4.000 dark web services, and found that more than half of them involve activities considered illegal under the United States laws (although some could be legal under other jurisdictions). The authors found that almost 500 services are about Bitcoin, including mixer services. Mixer services pool together Bitcoin transactions in random combinations to make the tracing on the blockchain more difficult.

A popular drug black market working on the dark web between 2011 and 2013 was Silk Road [39]. Silk Road was an intermediary between customers and sellers, like Ebay, and allowed the customers to pay the sellers in BTC while keeping a commission for the service. As shown in Figure 5, during the purchase the BTC were held in an escrow account until the product was successfully sent to the customer. During its lifetime, Silk Road generated about 9 billions of

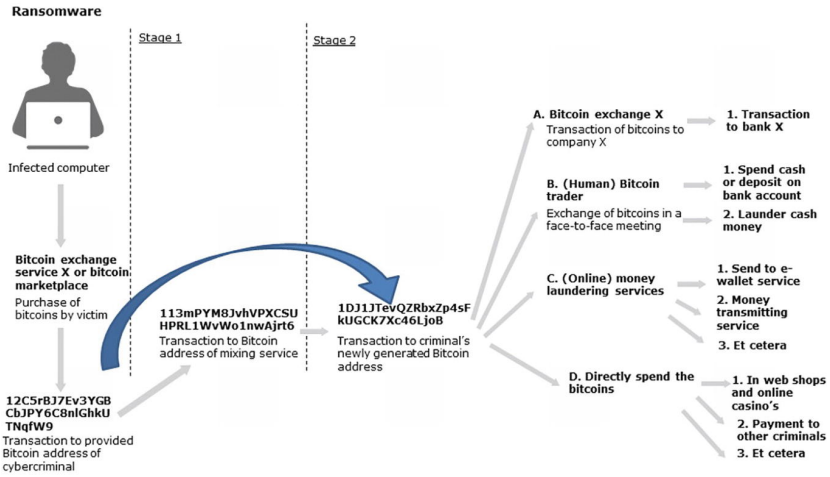

Figure 6: The process to launder BTC gained as a ransom [10].

BTC of revenue for the sellers, and it earned about 600.000 BTC from the commissions [37]. Right after its seizure in 2013, the Bitcoin price dropped in a day from 145 to 109 USD [20], which was a significant price drop at that time.

4 Cryptocurrency laundering

In pseudonymous transparent cryptocurrency, such as Bitcoin, the activity is not as anonymous and protected as initially conceived. Exploring the blockchain it is possible to trace the movements of the coins back to their origin, and to analyze the transactions to clusterize multiple addresses to a single address [32]. Moreover, it is possible to prevent Bitcoin clients to deny accesses from clients behind anonymity software, such as Tor, in order to expose their IP address and to associate the IP address to the pseudonym [3]. Therefore, it is important to launder the cryptocurrency earned via illegal activities before spending them [25, 10].

Figure 6 shows a sample process to launder BTC obtained from a successfull ransomware attack [10].

At **Stage 1**, which may be skipped according to the authors, the attacker sends the revenue to a mixing, or mixer, service specialized to aggregate transactions. Such services are also known as *crypto mixers* or *tumblers*.

A tumbler is a centralized service, typically running on the dark web, which receives BTC from several sources, it creates a complex web of transactions mixing all the received BTC with a similar value, and it finally sends the requested amounts to the specific addresses. A tumbler keeps a fee that is between 1-3% of the mixed amount. In this way, it becomes much more difficult to track the path of a sequence of transactions. Tumblers are not illegal services, but they

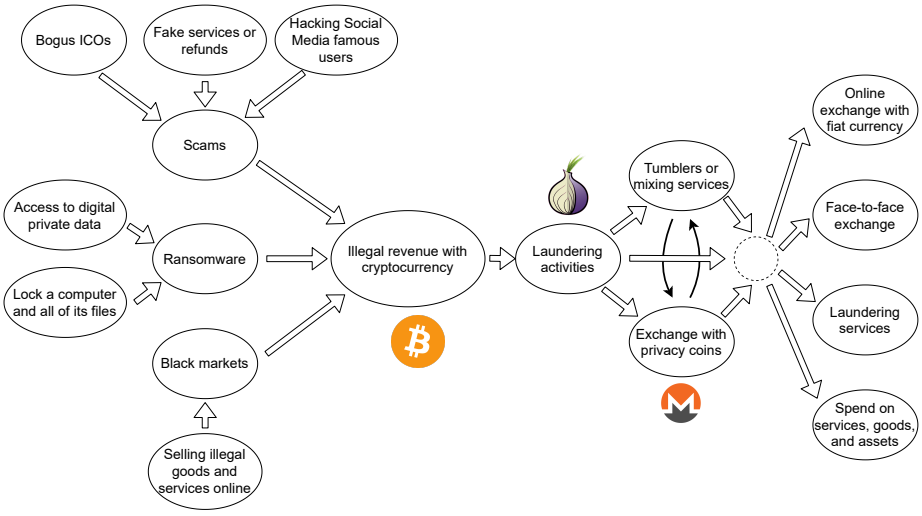

Figure 7: A summary of illegal activities to gain cryptocurrency, and a few examples of its laundering.

can be charged of money laundering offense if they do launder BTC proven to come from illegal sources. Finally, P2P tumblers exist as well: users cooperate together in a group to build the web of transactions without a central party, therefore minimizing the risk of theft and saving the commissions.

At **Stage 2** the criminal finally receives their revenue to one or more addresses of their possession and they wish to use them. The BTC can be exchanged in fiat currency, such as dollars or euros, for example through a cryptocurrency exchange, face-to-face with another person, or through online laundering services on the dark web, services that receive cryptocurrency in exchange for fiat. In addition to mixing services, a launderer may conceal their tracks exchanging BTC for privacy coin such as Monero (XMR), and then to BTC again due to their higher popularity and acceptance: however, doing this only through exchanges does not effectively protect the spender anonymity even though Monero is involved, because crypto exchanges associate payment IDs to transactions [35], which can be used to track the spender; therefore, the spender should execute their transactions through official Monero wallets, and more the transactions performed higher the concealment. Finally, a criminal can directly spend the BTC for services, goods, or assets.

5 Conclusion

This report collected and described some of the illegal techniques used by criminals to obtain, launder, and spend cryptocurrency, which are summarized in Figure 7. All the techniques are derived from traditional techniques to ille-

gally get money from victims, such as through scams, ransoms, or through a black market, but they modernized exploiting cryptocurrency, digital money that, unlike electronic transfer of fiat currency, are managed by a P2P network and currently difficult to regulate and to govern. Bitcoin is the most popular cryptocurrency, therefore it is easy to buy and it is accepted in many places, especially on the dark web, legally or illegally. However, Bitcoin transactions can be tracked, and its users only have pseudonymous privacy, and no privacy for what concerns the amount spent in a transaction. For this reason, privacy coins such as Monero are getting more attention, especially thanks to the total level of privacy and concealment that they offer, but they are less popular and harder to obtain and to spend.

After cryptocurrency has been obtained through illegal activities, it is important to launder the revenue because, as said, the most popular cryptocurrency are easier to get but easier to track. Therefore, before spending cryptocurrency it is important to conceal the transactions and un-link them to the known addresses used in scams or ransomware , for example through mixing services and/or pass through several privacy coin transactions to conceal the path.

References

[1] BBC. *Major US Twitter accounts hacked in Bitcoin scam*. URL: https://www.bbc.com/news/technology-53425822. [Online].

[2] A. Beikverdi and J. Song. "Trend of centralization in Bitcoin's distributed network". In: *2015 IEEE/ACIS 16th International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*. 2015, pp. 1–6. DOI: 10.1109/SNPD.2015.7176229.

[3] Alex Biryukov, Dmitry Khovratovich, and Ivan Pustogarov. "Deanonymisation of Clients in Bitcoin P2P Network". In: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. CCS '14. Scottsdale, Arizona, USA: Association for Computing Machinery, 2014, pp. 15–29. ISBN: 9781450329576. DOI: 10.1145/2660267.2660379. URL: https://doi.org/10.1145/2660267.2660379.

[4] Jim Browning. *The Refund Scam*. URL: https://youtu.be/X4PllvUowaQ. [Online].

[5] Benedikt Bünz et al. "Bulletproofs: Short proofs for confidential transactions and more". In: *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE. 2018, pp. 315–334.

[6] CNBC. *A blockchain start-up just raised $4 billion without a live product*. URL: https://www.cnbc.com/2018/05/31/a-blockchain-start-up-just-raised-4-billion-without-a-live-product.html. [Online].

[7] CNBC. *Ransomware spiked 6,000% in 2016 and most victims paid the hackers, IBM finds.* URL: https://www.cnbc.com/2016/12/13/ransomware-spiked-6000-in-2016-and-most-victims-paid-the-hackers-ibm-finds.html. [Online].

[8] Federal Trade Commission. *Paying Scammers with Gift Cards.* URL: https://www.consumer.ftc.gov/articles/paying-scammers-gift-cards. [Online].

[9] Federal Trade Commission. *Scams telling you to pay with Bitcoin on the rise.* URL: https://www.consumer.ftc.gov/blog/2019/11/scams-telling-you-pay-bitcoin-rise. [Online].

[10] Bart Custers, Jan-Jaap Oerlemans, and Ronald Pool. "Laundering the Profits of Ransomware: Money Laundering Methods for Vouchers and Cryptocurrencies". In: *European Journal of Crime, Criminal Law and Criminal Justice* 28.2 (9Jul. 2020), pp. 121–152. DOI: https://doi.org/10.1163/15718174-02802002. URL: https://brill.com/view/journals/eccl/28/2/article-p121_121.xml.

[11] John R Douceur. "The sybil attack". In: *International workshop on peer-to-peer systems.* Springer. 2002, pp. 251–260.

[12] Sherwin Dowlat and Michael Hodapp. "Crypto Asset Market Coverage Initiation: Network Creation". In: *Satis Group (Satis Group)* (2018).

[13] Monero Stack Exchange. *Can someone walk me through a simple example to explain how RingCT works?* URL: https://monero.stackexchange.com/questions/3683/can-someone-walk-me-through-a-simple-example-to-explain-how-ringct-works?rq=1. [Online].

[14] Mohd Faizan and Raees Ahmad Khan. "Exploring and analyzing the dark Web: A new alchemy". In: *First Monday* (2019).

[15] Francesca Fallucchi et al. "Blockchain Framework in Digital Government for the Certification of Authenticity, Timestamping and Data Property". In: *Proceedings of the 54th Hawaii International Conference on System Sciences.* 2021, p. 2307.

[16] Giulia Fanti and Pramod Viswanath. "Deanonymization in the bitcoin P2P network". In: *Proceedings of the 31st International Conference on Neural Information Processing Systems.* 2017, pp. 1364–1373.

[17] Sean Foley, Jonathan R Karlsen, and Tālis J Putniņš. "Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?" In: *The Review of Financial Studies* 32.5 (2019), pp. 1798–1853.

[18] Github. *RandomX.* URL: https://github.com/tevador/randomx. [Online].

[19] Github. *RandomX Design.* URL: https://github.com/tevador/RandomX/blob/master/doc/design.md. [Online].

[20] Guardian. *Bitcoin price plummets after Silk Road closure*. URL: https://www.theguardian.com/technology/2013/oct/03/bitcoin-price-silk-road-ulbricht-value. [Online].

[21] HelpNetSecurity. *Ransomware back in big way, 181.5 million attacks since January*. URL: https://www.helpnetsecurity.com/2018/07/11/2018-sonicwall-cyber-threat-report/. [Online].

[22] Investopedia. *Digital currency*. URL: https://www.investopedia.com/terms/d/digital-currency.asp. [Online].

[23] Investopedia. *Initial Coin Offering*. URL: https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp. [Online].

[24] Katharina Krombholz et al. "Advanced social engineering attacks". In: *Journal of Information Security and Applications* 22 (2015). Special Issue on Security of Information and Networks, pp. 113–122. ISSN: 2214-2126. DOI: https://doi.org/10.1016/j.jisa.2014.09.005. URL: https://www.sciencedirect.com/science/article/pii/S2214212614001343.

[25] Nir Kshetri and Jeffrey Voas. "Do crypto-currencies fuel ransomware?" In: *IT professional* 19.5 (2017), pp. 11–15.

[26] Massimo La Morgia et al. "Pump and Dumps in the Bitcoin Era: Real Time Detection of Cryptocurrency Market Manipulations". In: *2020 29th International Conference on Computer Communications and Networks (ICCCN)*. IEEE. 2020, pp. 1–9.

[27] Monero. *Monero*. URL: https://www.getmonero.org/. [Online].

[28] Satoshi Nakamoto. *Bitcoin: A peer-to-peer electronic cash system*. Tech. rep. Manubot, 2019.

[29] Shen Noether. *Ring Signature Confidential Transactions for Monero*. Cryptology ePrint Archive, Report 2015/1098. https://eprint.iacr.org/2015/1098. 2015.

[30] Bloomberg Quint. *Bitcoin Speculators, Not Drug Dealers, Dominate Crypto Use Now*. URL: https://www.bloombergquint.com/markets/bitcoin-speculators-not-drug-dealers-dominate-crypto-use-now. [Online].

[31] Michael G Reed, Paul F Syverson, and David M Goldschlag. "Anonymous connections and onion routing". In: *IEEE Journal on Selected areas in Communications* 16.4 (1998), pp. 482–494.

[32] Dorit Ron and Adi Shamir. "Quantitative analysis of the full bitcoin transaction graph". In: *International Conference on Financial Cryptography and Data Security*. Springer. 2013, pp. 6–24.

[33] Sara Saberi et al. "Blockchain technology and its relationships to sustainable supply chain management". In: *International Journal of Production Research* 57.7 (2019), pp. 2117–2135.

[34] Niranjan Sapkota, Klaus Grobys, and Josephine Dufitinema. "How much are we willing to lose in cyberspace? On the tail risk of scam in the market for Initial Coin Offerings". In: *On the Tail Risk of Scam in the Market for Initial Coin Offerings (November 18, 2020)* (2020).

[35] Steemit. *Tutorial on Bitcoin laundering with the help of Monero*. URL: https://steemit.com/monero/@vhcexexchange/tutorial-on-bitcoin-laundering-with-the-help-of-monero. [Online].

[36] Tor. *Tor project*. URL: https://www.torproject.org/. [Online].

[37] *Ulbricht Criminal Complaint*. URL: https://web.archive.org/web/20140220003018/https://www.cs.columbia.edu/~smb/UlbrichtCriminalComplaint.pdf. [Online].

[38] Bitcoin wiki. *Address reuse*. URL: https://en.bitcoin.it/wiki/Address_reuse. [Online].

[39] Wired. *How the Feds Took Down the Silk Road Drug Wonderland*. URL: https://www.wired.com/2013/11/silk-road/. [Online].

[40] Adam Young and Moti Yung. "Cryptovirology: Extortion-based security threats and countermeasures". In: *Proceedings 1996 IEEE Symposium on Security and Privacy*. IEEE. 1996, pp. 129–140.