DOI: https://doi.org/10.30525/2256-0742/2021-7-5-67-72

CRYPTOCURRENCY AS AN INSTRUMENT OF TERRORIST FINANCING

Valeriia Dyntu[1], Oleg Dykyj[2]

Abstract. *The purpose of the article* is to explain the use of cryptocurrency as a terrorist financing tool. This article has emphasized the ways, which terrorists appraise for being a reliable fundraising means and their adoption. *Methodology*. For the purposes of the study, the methods of scientific abstraction, synthesis, observation, generalization, as well as the method of induction of literature and legal documents were used to determine the features of bitcoin, promoting and preventing its use for terrorism financing. *Results*. The development of the Internet and electronic devices has radically changed all spheres of human life, including criminal activity. Digitalization has led to the improvement of ordinary crimes and the emergence of new types of crime, which, in principle, cannot exist without special digital electronic devices. Among the first implementers of new technologies were terrorists, who took advantage of digitalization to increase profitability. Thus, terrorists have now significantly increased their attention to cryptocurrency as a digital means of payment, namely Bitcoin. Bitcoin has a number of features that have attracted the attention of criminals as a way to evade responsibility for a crime. In particular, decentralization avoids the need for confirmation by a central authority, and pseudo-anonymity provides a certain level of anonymity. In addition, terrorists are aware that Bitcoin's confidentiality is extremely fragile and needs to be enhanced. The paper analyzes several ways to enhance anonymity, such as software that anonymizes traffic and prevents IP identification, peer-to-peer mixers, centralized mixing services (tumbler), and other approaches. It is worth emphasizing that for the fight against crime, the main issue is the de-anonymization of the Bitcoin owner/user, which allows the identification of the criminal. Currently, law enforcement agencies use direct and indirect de-anonymization, proliferation analysis, quantitative analysis, time analysis, and transactional network analysis, among others, to achieve the above goal, which are discussed in detail in this article. In addition, agencies around the world investigated and uncovered terrorist groups and their financial facilitators. Specifically, on August 13, 2020, the U.S. Department of Justice's Office of Public Affairs announced "the largest cryptocurrency seizure in the context of terrorism in history." To investigate the agenda, the legal documents of those investigations that contain information about the terrorist fund-raising mechanism were examined and analyzed. The legal documents revealed that these investigations used the aforementioned de-anonymization approaches.

Key words: cryptocurrency, Bitcoin, terrorism-financing, criminal investigation, de-anonymization.

JEL Classification: K14, K24, L86, O17, O33

1. Introduction

Technological advances and transformative scientific achievements have changed the familiar way of life and, consequently, criminal behavior as part of human activity. The transition to the digital economy, in addition to positive improvements such as the high speed of transactions, unification of the global payment system, etc., has created new challenges that modern society has to face. More precisely, because of digitalization, the methods and ways of committing some crimes have changed.

In particular, digitalization has led to the improvement and development of traditional types of crime that have been known for a long time. Ordinary criminal activity has shifted to the online space, which has made it more productive and efficient thereby

Corresponding author:
[1] National University "Odessa Law Academy", Ukraine.
E-mail: dyntuvaleriia@gmail.com
ORCID: https://orsid.org/0000-0002-8948-1845
ResearcherID: AAO-3927-2020
[2] National University "Odessa Law Academy", Ukraine.
E-mail: olegdykyj@gmail.com
ORCID: https://orsid.org/0000-0001-9659-9350
ResearcherID: G-4515-2017

modernizing its characteristics such as speed, anonymity, limitlessness, etc. For example, the Internet and Darknet are used as a platform for the illegal sale of drugs (Silk Road, Evolution, Agora, etc.), and digital payment systems are used for money laundering (Liberty Reserve case, etc.). In addition, cryptocurrency is used for pump-and-dump schemes that used to apply to stocks. In the schemes mentioned in recent years, scammers use susceptible cryptocurrency markets to create artificial attention and demand based on far-fetched information and encourage unwitting investors to buy the currency. What's more, offenders can issue a new token and spread positive news about its use, as they did with SaveTheKids in 2021. Additionally, digitalization has led to the emergence of a new type of crime that did not exist before the invention of the computer and the Internet, namely cybercrime. Technically, the realization of these crimes is impossible without special digital electronic devices. For example, malicious software (malware), hacker attacks, ransomware attacks, etc.

It is noteworthy that despite its recent appearance, the development of cybercrime has reached impressive scale. According to a new report by the Center for Strategic and International Studies (CSIS) and McAfee, cybercrime now costs the world nearly $600 billion, or 0.8 percent of global GDP (Economics of Cybercrime, 2017). In 2017, for example, one of the most devastating cyber attacks occurred with the NotPetya malware, which caused an estimated $10 billion in damage. It should be noted that the development of cybercrime is in step with the times and responsive to change. For example, in 2020, the CovidLock malware became widespread due to the COVID-19 pandemic. It was claimed to give users access to statistical information about COVID-19. However, it was infected with ransomware. CovidLock had a screen lock feature that denied the victim access to their phones. The main purpose of ransomware is to extort money, which in this case was done in Bitcoin. CovidLock demanded $100 in Bitcoin in 48 hours. Otherwise, there was a threat of public leakage of personal data and erasure of phone memory. Thus, digitalization has created an environment that has fostered the development of existing crimes and the creation of new crimes that have a huge impact on the growth of crime. This process is constantly in flux.

2. Brief information about Bitcoin

It is worth emphasizing that terrorists are always among the first users of new technologies that can increase the profitability of their efforts and push them to achieve their malevolent goals. According to the Global Terrorism Index 2020 report, the global economic impact of terrorism in 2019 was $26.4 billion (Terrorism Index, 2020). It should come as no surprise that terrorists have adapted the function of the digital economy with all its advantages. Initially, terrorist organizations used fiat currency to transfer funds and raise money, the use of which caused many problems (money laundering controls, bank policies, etc.). Nowadays, despite its relatively short existence, terrorists have significantly increased their attention to cryptocurrency, particularly Bitcoin.

Bitcoin is a decentralized digital currency for storing and validating transaction data based on a peer-to-peer (P2P) distributed network (Nakamoto, 2009). Data is stored in a public ledger, the basis of which architecture is blockchain. Blockchain organizes its data into blocks that are connected in a chain. Each block contains a hash of the previous block and a Merkle tree of transactions. Any changes in the transaction information cause the Merkle root hash and, consequently, the hash of a particular block to change.

For a better understanding of the nature of Bitcoin, it is worth considering the Elliptic Curve Digital Signature Algorithm (ECDSA) as an essential part of it. ECDSA is the elliptic curve analog of the Digital Signature Algorithm (DSA). DSA can be considered as a variant of the ElGamal signature scheme. The possibility of using the discrete logarithm problem in public key cryptosystems was recognized in 1976, when Diffie & Hellman (1976) introduced public key cryptography. Koblitz (Koblitz, 1987) and Miller (Miller, 1986) independently introduced Elliptic-curve cryptography. Scott Vanstone proposed the ECDSA in 1992 in response to a request from the National Institute of Standards and Technology for public comment on their Digital Signature Standard (DSS) proposal. It can be seen as an effective variant of ElGamal's (ElGamal, 1985) digital signature scheme. It was adopted: in 1998 as an International Standards Organization standard (ISO 14888-3); in 1999 as an American National Standards Institute I standard (ANSI X9.62); in 2000 as an Institute of Electrical and Electronics Engineers standard (IEEE 1363-2000) and Federal Information Processing Standard (FIPS 186-3).

In continuation of the above, any user can create a fake address that includes the corresponding public/private key pairs stored in the user's wallet. The problem of forgery can be solved by signing the created transaction with the user's private key. The information about the transaction must then be sent out to the P2P network nodes. The payer's public key can be used to verify the correctness of the corresponding private key, which was used to sign the transaction. Accordingly, the characteristics of Bitcoin, such as decentralization, transparency, and irreversibility, increase its reliability. Since the use of blockchain eliminates the need for a central authority, each user can have access to any public address, transaction, and furthermore, transaction history cannot be changed.

3. Bitcoin anonymization and de-anonymization

Among other features that Bitcoin undoubtedly possesses is the fact that it is gradually sinking into disrepute because illicit use has given rise to the myth of complete anonymity as its additional feature. It takes careful consideration and a deep dive into the details to understand how Bitcoin's anonymity works and can be compromised. First of all, it should be emphasized that Bitcoin has several anonymous features:

1. The Bitcoin address is not linked to the user's personal information at the protocol level.

2. Transactions are also not linked to the identity of the user. If miners agree to include the transaction in the block, anyone can transfer bitcoins from one address to any other address, without having to disclose personal information.

3. Bitcoin transaction information is transmitted by randomly selected nodes on the P2P network. Bitcoin nodes connect to each other via IP addresses. Thus, the nodes are not aware if the transaction was created by the node that transmitted the information or if it simply redirected the data.

However, bitcoin itself is not anonymous, as the official bitcoin website makes clear: "Bitcoin is not anonymous and cannot offer the same level of privacy as cash" (About Bitcoin, 2021). Furthermore, according to Reid and Harrigan (2011), anonymity was not the primary goal for Bitcoin as a crypto-currency, "however, Bitcoin is often referred to as anonymous. We conducted a passive analysis of anonymity in the Bitcoin system using publicly available data and network analysis tools. The results show that the actions of many users are far from anonymous" (Reid & Harrigan, 2011). All confirmed transactions are publicly announced on the blockchain (Meiklejohn et al., 2013), thereby all transactions are pseudonymous (Ober, Katzenbeisser & Hamacher, 2013). Moreover, according to the FBI's Intelligence Assessment, Bitcoin's anonymity depends on the user's actions (Federal Bureau of Investigation, 2012). Thus, user information can be de-anonymized, which basically means tying a public Bitcoin address to a user's identity or IP address.

As the aforementioned information suggests, Bitcoin's privacy is extremely fragile. Terrorists are aware of this and use several means to enhance Bitcoin's anonymity. Some of them will be considered below.

First, the user can use TOR/I2P software or any other similar tool that provides anonymization of traffic and prevents IP-identification. Users can then generate a new address for any transaction, making it difficult to tie it to a specific person. Hierarchical deterministic (HD) wallets do this automatically and deterministically. HD wallets contain keys in a tree-like structure, starting with an initial seed provided by some user, and in which parent keys can produce subsidiary keys, and so on to infinity.

In addition, Bitcoin can be bought and sold through exchange sites and other trading platforms. It should be noted that cryptocurrency exchanges can be centralized and decentralized. A centralized crypto-currency exchange is created and managed by a third party, which acts as an intermediary, monitors the course of trading, and ensures the stability of the process. A decentralized exchange assumes no third-party supervision and is based on a P2P network and an open protocol. In this case, users have more control, because the storage of assets is in the hands of the exchange. At the same time, cryptocurrency exchanges can be used as a kind of anonymizer. If the exchange site is big enough, the Bitcoins deposited into the account will effectively mix and turn into completely different Bitcoins when withdrawn later, and even without a service fee.

Another means of anonymization are centralized mixing services (tumbler). In general, the user sends an amount of bitcoins to the tumbler service, pays a fee, and receives the same amount of completely different bitcoins, or the tumbler service transfers the bitcoins to the address specified by the user. The level of anonymization depends on the total number of users and Bitcoins available for mixing. Mixing services may vary depending on the amount of commission, the authentication and registration process, and the time delay. This method has many disadvantages related to the reliability of the mixing service (reliability of data collection, storage and protection, security, confidentiality, etc.).

Another way is through Bitcoin peer-to-peer mixers. It is based on peer-to-peer groups of Bitcoin users who are willing to mix their Bitcoins and make exchanges without a third party. This allows users to exchange Bitcoins directly. The CoinSwap, CoinJoin protocols allow multiple users to collect one exchange transaction in several stages. When the transaction is fully collected, it sends users' Bitcoins to each other according to the destination. Any participant does not know the interconnection between the initial and final coin addresses. To further confuse blockchain traffic analysis, the aforementioned procedure can be performed in multiple rounds with multiple recipients. It should be emphasized that the development and improvement of mixing tools is a continuous process. New mixer services are appearing every day, offering updated anonymization solutions.

However, despite attempts to increase Bitcoin's anonymity, it can be de-anonymized. Consider several ways to de-anonymize it.

Firstly, de-anonymization can be **direct** or **indirect**, depending on the way in which the user cooperates. **Direct de-anonymization** involves making personal

contact with the user (e.g., for sales or payment purposes). When communicating, information about the public address is extracted. For **indirect de-anonymization**, user data is collected from publicly available sources. Digital user names can be found on various websites, social networks, laundry services, etc. A Bitcoin address can be linked to a specific person if his/her personal information was somehow connected to such a Bitcoin address. These can be addresses used to deposit or withdraw funds from a regulated exchange or wallet, public donation addresses, or addresses used to send Bitcoin using personal information (for example, when paying in an online store). A telling illustration of the use of both methods is the Silk Road investigation, in which they were used to identify the person and whereabouts of the chief administrator of the darknet market website Ross William Ulbricht, known as Dread Pirate Roberts. Specifically, law enforcement linked Ross Ulbricht's Google and LinkedIn profiles, which contained his photos, to provide a visual link between the two computer profiles online.

It should also be noted that Lerner (Lerner, 2013) and Koshy (Koshy, Koshy & McDaniel, 2014) et al. were the first to suggest the possibility of Bitcoin wallet being linked to the IP address of its owner. Besides, Reid and Harrigan (Reid & Harrigan, 2011) argue that limited anonymity depends on blockchain technology itself. As mentioned, there is a public ledger of all verified transactions to prevent double spending. In this regard, de-anonymization can be provided by **transactional network analysis**. Its main idea is to define multiple inputs combined into a single transaction. All addresses that are used as input for a transaction can be grouped in the user's network, and presumably they can belong to the same person. In principle, all of these inputs could have been generated by other addresses, but the fact that they are linked in a single transaction suggests that all of these inputs, and therefore all of the linked addresses, are controlled by a single user.

Moreover, this strategy can be used in conjunction with the "shadow" address mechanism. Essentially, transactions can rarely have one input and one output, since the number of Bitcoins sent (output) must equal the number previously received (input). Often a transaction consists of many small inputs. This happens because the entire amount of the previous transaction is forcibly expended; thus, the user is unable to use the input part. For the same reason, a transaction consists of several outputs. For the purpose of returning "change," Bitcoin uses a so-called change address, which is called a "shadow address". These addresses allowed users to create a transaction that returned surplus Bitcoins from the input to the sender. In this way, the transaction would return the money to the user making the input and could be matched with the user.

In addition, several analyses can be used for **de-anonymization**. One of them is **dissemination analysis**, the main idea of which is to calculate the share of Bitcoins in a certain address that have been transferred from a certain address. Then it should be determined whether these addresses are connected by a single direct transaction or a chain of transactions. Others are **quantitative analysis**, which does not look at specific transactions but examines specific amounts, and **time analysis**, which tracks specific time intervals.

4. Examples of terrorist fundraising schemes

In recent years, it can be noted the constant acceleration of the use of cryptocurrency to finance terrorism. In 2020, investigations into cryptocurrency terrorist financing schemes were more unveiled than ever before. Agencies around the world (France, Great Britain, the U.S., India, etc.) have investigated, uncovered terrorist groups and their financial facilitators. Notably, on August 13, 2020, the U.S. Department of Justice Office of Public Affairs announced "the largest cryptocurrency seizure in the context of terrorism in history". Three Foreign Terrorist Organization (FTO) groups have allegedly used cryptocurrency and social media to attract attention and raise funds for their terrorist campaigns. U.S. authorities seized millions of dollars, more than 300 cryptocurrency accounts, four websites and four Facebook pages associated with the criminal enterprise (Global Disruption, 2020).

Consider several schemes that have been uncovered in the above-mentioned investigations.

Terrorist fundraising scheme example 1.

Fundraising was done partly through social media and the three official FTO websites. The organization and their fronts launched a Bitcoin fundraising campaign in early 2019 and it was conducted in three phases.

In the first phase, the FTO encouraged adherents to donate and required them to send Bitcoins to a single Bitcoin address hosted on a U.S. Bitcoin exchange.

Approximately May 11, 2017 and January 31, 2019, an FTO members opened Virtual Currency Exchange (VCA) 3 and VCA 1 accounts, respectively, on Virtual Currency Exchange (VCE) 1. In order to register the account, they provided an email address to VCE 1.

On January 31, 2019, a test transaction was conducted from VCA 3 to VCA 1, designed to confirm that VCA 1 is open and usable.

In addition, around January 31, 2019, the FTO launched a public fundraising campaign on its Twitter account asking for Bitcoin donations. The Twitter message included the aforementioned Bitcoin deposit address where donors could send their donations.

On the same day, January 31, 2019, VCA 2 was created for VCE 1. The IP address used to set up VSA 2 resolved to the same IP address that was used to log into VSA 1 on the same date. VSA 2 turned out to be a burner account because it did not conduct any transactions.

In the second phase, the FTO decided to use a Bitcoin exchange within the FTO-controlled infrastructure and directed donors to donate to a single Bitcoin address based within the FTO rather than on a third-party Bitcoin exchange.

The FTO registered an additional VCA 4 using the same email account used for VCA 1. Then, approximately Feb. 1, 2019, the FTO called for donors to send donations to the new VCA 4 bitcoin deposit address.

Using clustering methods, law enforcement determined that VCA 4 was combined with nine other bitcoin addresses. Clustering of bitcoin addresses showed the presence of a common owner/controller.

To summarize: the first two stages used one specific account number (static Bitcoin addresses) where anyone could send donations. In such a situation, VCE can examine individual Bitcoin addresses, identify a terrorist trail, and take legal action, such as freezing the transactions in question. In the second phase, about 1,16938125 bitcoins were collected through 65 transactions.

In the third phase, the FTO used a dynamic Bitcoin system. On their official site, any donor could obtain new Bitcoin addresses. In addition, the FTO launched two additional official sites, which domain is in the same area, to collect Bitcoins for the campaign. Presumably, all three sites are registered and operated by the same person. Two of the sites contained identical information regarding donation schemes. The content of the third of these had similarities in the use of photo and the donation process. About 2.39361558 bitcoins were collected through 124 transactions using the aforementioned algorithm.

Along with this, direct de-anonymization was used during the investigation. In particular, the FTO website included an e-mail address for contact. Consequently, the law enforcement agent began an e-mail correspondence in which the agent requested the purpose for which the money would be used and expressed the intention to donate $1,100. On the same day, several responses were received explaining the use of the money, as well as a request for an estimated donation amount for a money transfer easement. In addition, it was indicated that donations could be sent via MoneyGram or Western Union.

Throughout all three phases of the FTO fundraising campaign, the terrorist organization received donations from cryptocurrency accounts located on various virtual currency exchanges.

Once the FTO collected BTC from donor accounts as part of this fundraising campaign, the organization typically converted the virtual currency into traditional fiat currency or exchanged it for something of value to spend the BTC. Law enforcement tracked at least one cash-out transaction during an investigation using blockchain analysis (Civil Action, 2020).

The FTO and its affiliated terrorist groups use multi-level transactions to take over the BTC movement.

Terrorist fundraising scheme example 2.

It is worth noting that the FTO has supervised a BTC money laundering network, using Telegram and other social media channels to collect BTC donations for its illegal purposes. The FTO uses social media and Telegram channels to act as charities, but they raise funds for illegal activities.

In April 2019, the administrator of the now-defunct Telegram group FTO provided a bitcoin address as a repository for donations to FTO. Messages in the Telegram group during the same time period advertised fundraising campaigns for soldiers. The group's media content included watermarked images and additional information about the FTO.

Approximately May 5, 2019, virtual currency accounts (VCAs) AQ1 sent their entire BTC balance, approximately 0.14610741 BTC, to the BTC address cluster containing the root address (VCA AQ2).

VCA AQ2 can be seen as a central hub for the collection of funds and their further redistribution through the money laundering network. Approximately from February 25, 2019 to February 5, 2020, VCA AQ2 received around 15.27050803 BTC through 187 transactions. Between February 25 and July 29, 2019, VCA AQ2 sent approximately 9.10918723 BTC through 38 transactions to a virtual currency exchange account (VCA AQ1) (Preliminary Assessment, 2021).

The FTO subsequently used a common money-laundering technique by which the proceeds were funneled to various online gift card exchanges where users could exchange cryptocurrency for various gift cards.

In both cases, law enforcement used blockchain analysis, specifically involving large databases that grouped BTC transactions into "clusters" by analyzing the data underlying the BTC transactions.

5. Conclusions

To summarize, digitalization has changed all areas of human activity, including criminal ones. This contributed to the improvement of conventional crimes, the development and creation of new types, which, accordingly, could not be created without special digital electronic devices. The gradual increase in the number of cybercrimes demonstrates the applicability of new technologies in criminal activity. The main characteristics that attract criminals to cybercrime are the high speed of action, accessibility, limitlessness, uncertain jurisdiction of states, and difficulty for legal investigation.

It is worth emphasizing that one of the clear results of digitalization is the creation of cryptocurrency. Bitcoin and other cryptocurrencies have changed not only the financial system, but also the ways and means of criminal activity. The global nature of blockchain has pushed crime beyond national borders. Peer-to-peer networks, mixers and other means of increasing anonymity have made it possible to hide financial transactions. Digital infrastructure has created a favorable environment for money laundering, other financial crimes, and international funding of terrorist organizations.

Terrorist organizations are now using an integrated approach, combining social media, messengers and cryptocurrencies for international fundraising. The terrorist organization attracts many donors around the world by posting detailed instructions on the cryptocurrency transaction process on social networks and messenger channels, following which potential donors can discreetly invest in terrorist ideology.

Thus, in this context, law enforcement agencies must continually raise their awareness of rapidly evolving cryptocurrencies and the ways in which they can be abused in order to counter their threats.

References:

"This is Our House!" A Preliminary Assessment of the Capitol Hill Siege Participants (2021, March). The official website of GW Program on Extremism. Available at: https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Criminal%20Complaint_Al-Ikhwa%20Accounts.pdf (accessed 08 December 2021).

Case 1:20-cv-02227 Document 1 Filed 08/13/20 Page 1 of 52 Civil Action No. 20-cv-2227 (2020). The official website of GW Program on Extremism. Available at: https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Criminal%20Complaint_Al-Qassam%20Brigade%20Accounts.pdf (accessed 08 December 2021).

Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE transactions on Information Theory*, vol. 22, no. 6, pp. 644–654.

Elgamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469–472. CiteSeer^x. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.476.4791&rep=rep1&type=pdf (accessed 08 December 2021).

FBI (Federal Bureau of Investigation) (2012). Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity. 24 April. WIRED. Available at: http://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf (accessed 08 December 2021).

Frequently Asked Questions. Find answers to recurring questions and myths about Bitcoin (2021). Bitcoin.org. Available at: http://bitcoin.org/about.html (accessed 08 December 2021).

Global Disruption of Three Terror Finance Cyber-Enabled Campaigns: Largest Ever Seizure of Terrorist Organizations' Cryptocurrency Accounts (2020, August 13). The official website of U.S. Department of Justice. Available at: https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns (accessed 08 December 2021).

Global Terrorism Index 2020: Measuring the Impact of Terrorism, Sydney, November 2020 (2020). The official website of Institute for Economics & Peace. Available at: https://visionofhumanity.org/wp-content/uploads/2020/11/GTI-2020-web-1.pdf (accessed 08 December 2021).

Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of computation,* vol. 48, no. 177, pp. 203–209.

Koshy, P., Koshy, D., & McDaniel, P. (2014). An Analysis of Anonymity in Bitcoin Using P2P Network Traffic. 18th International Conference on Financial Cryptography and Data Security, FC 2014 (Barbados, 3-7 Mar 2014) Springer, Berlin, Heidelberg, pp. 469–485. Available at: https://link.springer.com/chapter/10.1007%2F978-3-662-45472-5_30 (accessed 08 December 2021).

Lerner, S. (2013, January 11). New vulnerability: know your peer public addresses in 14 minutes. Bitcoin Forum. Available at: https://bitcointalk.org/?topic=135856,2014 (accessed 08 December 2021).

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2013). A fistful of bitcoins: Characterizing payments among men with no names. In Proceedings of the 2013 Conference on Internet measurement conference, 2013, ACM, New York, pp. 127–139. DOI: https://doi.org/10.1145/2504730.2504747

Miller, V. S. (1986). Use of Elliptic Curves in Cryptography. In: Williams H.C. (eds) Advances in Cryptology – CRYPTO '85 Proceedings. CRYPTO 1985, pp. 417–426. Lecture Notes in Computer Science, vol. 218. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/3-540-39799-X_31

Nakamoto, S. (2009). Bitcoin: A peer-to-peer electronic cash system (2009). Bitcoin.org. Available at: https://bitcoin.org/bitcoin.pdf (accessed 1 December 2021).

Ober, M., Katzenbeisser, S., & Hamacher, K. (2013). Structure and Anonymity of the Bitcoin Transaction Graph. *Future Internet,* vol. 5, no. 2, pp. 237–250. MDPI AG. DOI: http://dx.doi.org/10.3390/fi5020237

Reid, F., & Harrigan, M. (2011). An Analysis of Anonymity in the Bitcoin System. *2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing,* 2011, pp. 1318–132. DOI: https://doi.org/10.1109/PASSAT/SocialCom.2011.79

Reid, F., & Harrigan, M. (2011, Sept. 30). Bitcoin is not anonymous. Fergal Reid's blog. Available at: http://anonymity-in-bitcoin.blogspot.com.br/2011/07/bitcoin-is-not-anonymous.html (accessed 08 December 2021).

There's Nowhere to Hide from the Economics of Cybercrime (2017). The official website of McAfee Enterprise. Available at: https://www.mcafee.com/enterprise/en-us/solutions/lp/economics-cybercrime.html (accessed 08 December 2021).