CRYPTOCURRENCY IN THE SYSTEM OF MONEY LAUNDERING

Valeriia Dyntu\(^1\), Oleh Dykyi\(^2\)

Abstract. The target of the article is to study the place of the cryptocurrency in the process of money laundering. The subject of the article is to investigate the ways and means of usage cryptocurrency for money laundering, the possibilities, and limits. Problem's setting. The authors of the paper have emphasized that despite the broad usage of cryptocurrency all over the world for different kinds of purchasing and transactions, there is no unified position regarding the definition of cryptocurrency, as well as its legal status. Moreover, the aforementioned circumstances trigger the difficulties during the criminal investigation of money laundering by using cryptocurrency. Thus, law informant agencies are facing challenges with the identification of criminals' personality and the fact of crime commitment. In addition, in the article, the authors articulate the main concept of cryptocurrency: anonymity and decentralization, which engender the main aggro while crime investigation. Methodology. The research is based on an analysis of historical stages of cryptocurrency creation: from Friedrich August von Hayek's idea of "currency independent from banking and governmental" to the establishment of decentralized currency. Moreover, there were analysed the cases of money laundering where criminals who used cryptocurrency have been identified and press charged. In addition, the comparative methods were used to collate different positions regarding cryptocurrency all over the world and inside Ukraine. The position of the main authorities and organizations regarding the legal status of cryptocurrency was investigated as well. The results of the study revealed that a cryptocurrency is a convenient tool for money laundering because it gives relative anonymity for the owner of the currency, as far as it does not require any personal information about the user and his location. Aforementioned feature minimizes the opportunity for law enforcement agencies to track back the criminal activity and to identify the criminal personality. Furthermore, cryptocurrency transactions are out of the government control because for conducting any transactions by using cryptocurrency, there is no need for their verification by third parties like a bank, governmental authority or nongovernmental organizations. In addition, the user can have more than one account and conduct transactions from different places at the same time.

Key words: cryptocurrency, money laundering, criminal investigation.

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

1. Introduction

XXI century became the era of skyrocket and rapid development of science and technology, which is unthinkable without the World Wide Web. However, the creation of the aforementioned indispensable tool counts less than 50 years.

In 1969, Charley Kline made first but an unsuccessful attempt of remote login the computer of Stanford Research Institute. This date can be considered as a day of creation of a new way of interaction between people all over the world. Then in 1989, Tim Berners-Lee offered CERN the concept of the new distributed information system, which he named the World Wide Web. Since that time all spheres of life step by step have shifted their main activities into the augmented reality of the World Wide Web. The same fate befell the economy, which during the last 15 years has digitalized almost all main processes. The latest breakthrough in the digital economy was done by the creation of new means of payment – cryptocurrencies, which emission and accounting are based on asymmetric encryption by utilizing cryptographic methods of protection.

Currently, the attitude to the cryptocurrency has different avenues, from complete abnegation of its potential and benefits to all-consuming adoration as a future way for liberation out of financial government control. We do not support any of the radical viewpoints regarding cryptocurrencies considering it as a tool, which has advantages and disadvantages.

However, law enforcement agencies all over the world identify the use of cryptocurrencies for commitment to different types of crime, mostly correlated with
economic and financial spheres, in particular, money laundering. Aforementioned anxiety triggers the necessity for deep research of ways and means of using cryptocurrencies in the process of money laundering, which determines the relevance of this article.

2. Literature review

The study of using cryptocurrency for illegal activities is under the consideration of such scientists as Bezverbnyi K., Kasatkin A., Kornev I., Krylov G., Robbek A., and others. However, despite the significant contribution of the aforementioned scientists into considering the topic, the current situation with usage cryptocurrency for the commitment of economic crimes demands the deeper contemplation of it, especially regarding money laundering.

3. Brief characteristic of the virtual currency

The determination of money’s origin was always the issue of discussions. Paul Anthony Samuelson wrote that “money is an artificial social convention” (Samuelson, 1993). Consequently, if the social convention was created it must have a purpose. Aristotle suggested that exchange requires the emergence of the equivalent payment instrument (Bechler, 1995). Inasmuch as exchange can be considered as a social agreement, thus the establishment of the money can be seen as a social treaty.

However, there are a lot of supporters of another theory of money’s emergence. For instance, K. Marx laid the foundation of evolutionary theory, which later was finalized by Ludwig Heinrich Edler von Mises. He articulated that arise the inevitable tendency when means of exchange which were used became less exchangeable and were rejected one by one, until was laid the foundation of evolutionary theory, which later was expressed in “Virtual currency is a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency” (ECB, 2015).

Virtual currency is different than electronic money, which is a digital means of fiat currency and is utilized for electronic transfer of reflecting fiat currency cost and is considered as a legal means of payment (Karcheva and Nikitchuk, 2015). Furthermore, the distinction between virtual currency and other means of payment is the method of the emission of payment units and the organization of their storage and transfers system.

In addition, “unless gold or silver virtual currencies have no non-monetary use or value – they are just bits of data” (WSBI, 2014). Furthermore, the value of virtual currencies is based on the convention among system’s users, which are working via the Internet (Dziuba and Orzeszko, 2015).

According to the European Central Bank position which was expressed in “Virtual currency schemes – a further analysis” “virtual currency is a digital representation of value, not issued by a central bank, credit institution or e-money institution, which, in some circumstances, can be used as an alternative to money” (ECB, 2015). Moreover, in report of the Financial Action Task Force, virtual currency is considered as a “digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction. It is not issued or guaranteed by any jurisdiction and fulfills the above functions only by agreement within the community of users of the virtual currency” (FATF, 2014).

Thus, “virtual currencies represent both the emergence of a new form of currency and new payment technology to purchase goods and services” (Bolt and Oordt, 2016).
There are three types of virtual currency: closed, virtual currencies with the unidirectional flow, and virtual currencies with the bidirectional flow.

In fact, closed virtual currency does not link to the real economic sector. It is intended for payment for virtual goods or services, for instance, virtual games, and cannot be utilized out of the virtual community. As an example, World of Warcraft (WoW) Gold can be taken, which is used in the computer game with a similar name (Karcheva and Nikitchuk, 2015). All unconvertible virtual currencies are centralized: according to the definition, they are emitted by the central administrator, which controls system, sets the rules for using the virtual currency, maintains a centralized payment register, and has right to withdraw currency from circulation (Karcheva and Nikitchuk, 2015).

The virtual currency with unidirectional flow. Such currency can be purchased according to a specially set course by using “real” currency; however, it is impossible to comply with the same course to exchange it backward. Such currency can be purchased according to a specially set course by using “real” currency; however, it is impossible to exchange it backward in conformity with the same course. Its main purpose is the payment of virtual goods and services, nevertheless, some of them allow paying for real goods and services. As an example can be taken Facebook Credit, Amazon Coins, Nintendo Points, bonuses for passengers, who often enjoy the services of the particular airline (Badzym and Drevush, 2014).

Virtual currencies with the bidirectional flow. Such currency can be purchased and bought according to a certain exchange course, in other words, to convert it (Badzym and Drevush, 2014). The term “converted currency” does not mean its official convertibility (for instance in a case of the gold standard) but only indicates its “de facto” convertibility (for instance, due to the existence of the relevant market). Thus, virtual currency is “convertible” only until that time, while individuals and legal entities carry out transactions with it, and another except it as far as “convertibility” of virtual currency does not insur by the legislation (Karcheva and Nikitchuk, 2015).

The main propose of it is payment for real and virtual goods and services (Badzym and Drevush, 2014). As an example of “converted currency,” cryptocurrency can be taken.

4. The stages of cryptocurrency creation

Despite the significant popularity of cryptocurrency in Ukraine and other European countries, its particular definition still has not been articulated. We support the viewpoint that “cryptocurrency is a digital decentralized currency, a unit of which is a coin cryptographically protected against tampering since it is an encrypted information that cannot be copied, while all information about transactions is stored in the blockchain system” (Inshyn, Mohilevskyi, Drozd, 2018).

Very often the creation of cryptocurrency correlates with the replication to the social demand for a currency independent from banking and governmental institutions, after economic crises in 2008 when they lost their reliability.

However, the idea of private money is not new; it was articulated in the book of Austrian economist Friedrich August von Hayek “The Denationalization of Money.” His main idea was that government should be deprived of the money’s emission monopoly with a target to prevent the inflation process (Hayek, 1976). Furthermore, Milton Friedman in 1999 during the interview admitted that “…the Internet is going to be one of the major forces for reducing the role of government. The one thing that’s missing, but that will soon be developed, is a reliable e-cash, a method whereby on the Internet you can transfer funds from A to B without A knowing B or B knowing A, the way I can take a USD 20 bill and hand it over to you and then there is no record of where it came from” (WSBI, 2014). His prediction was precision because progressive instruments and systems are establishing neoteric paradigms for transactions and new channels of capital (Hileman and Rauchs, 2017).

It should be noticed that the roots of cryptocurrency go to the end of the previous century, in particular, in 1983 David Chaum offered the idea of combining transparency and anonymity of transaction for all users by utilizing “Blind signature” (Chaum, 1982).

Then in 1990th, the movement of crypto-anarchists was formed – cypherpunk whose idea was the usage of cryptography and other similar tools for changing the social order. In 1993, one of the founders of the cypherpunk Eric Hughes announced the confidentiality of transactions by using multi-step encryption and published.

In 1994, Timothy C. May published the work “The Cyphernomicon: Cypherpunks FAQ and More, Version 0.666” where he described safe untraceable encrypted transactions, which would use the P2P system which does not need verification by third parties and would cause the independent from the government (May, 1994).

In 1998, Wei Dai offered cryptocurrency “b-money”. He wrote “I am fascinated by Tim May’s crypto-anarchy. Unlike the communities traditionally associated with the word ‘anarchy’, in a crypto-anarchy, the government is not temporarily destroyed but permanently forbidden and permanently unnecessary. It’s a community where the threat of violence is impotent because violence is impossible, and violence is impossible because its participants cannot be linked to their true names or physical locations” (Dai, 1998).

In 2005, Nick Szabo created “Bitgold”. As a libertarian wing of cypherpunk inspired by the novel of Ayn Rand “Atlas Shrugged” he wanted to create “Galt’s Gorge” in the cyberspace – free trade zone. Firstly he came to the idea of creation smart-contracts, which was based on blockchain system in 1990th, and later on invented cryptocurrency.
5. The analyses of Bitcoin as a cryptocurrency

Currently, the most popular cryptocurrency which is used by bidirectional flow is Bitcoin. Bitcoin is decentralized P2P (Person to Person) payment network, which serves its users without central bodies and agents. From the users’ point of view, Bitcoin is analogue of cash but only for the Internet (In Bitcoin information site). The maximum amount of Bitcoin in the world is restricted and cannot be more than 21 million.

The creation of Bitcoin is correlated with the name of Satoshi Nakamoto, who on September 3, 2009, via the Internet published an article “Bitcoin: A Peer-to-Peer Electronic Cash System” (Nakamoto, 2009), in which he described the main principals of new cryptocurrency. The main characteristics, which distinguish Bitcoin from traditional electronic money and cashless settlements, that Bitcoin is not debt obligations of the issuer.

Any person, who has access to the Internet and enough amount of computer memory, can be a user of Bitcoin. For this purpose, utilizor has on the official website to choose “wallet” and to install it. The wallet can be installed on the personal computer, mobile phone, or can be available via the Internet. It should be noticed that wallet has the specific address and it contains information about closed keys “seed” for all Bitcoin, which belongs to the particular user. By utilizing the aforementioned wallet user can do any transactions.

Essentially, all owners of Bitcoin’s accounts, wallet, as well as participants of transactions, are holders of individual accidentally generated numbers, which become key or “password” for that element or activity. Any key or “password” is absolutely unique and anonymous because does not need user’s personal data and owner of that key becomes the owner of the account, wallet or transaction. Peer-to-peer system which is utilized by Bitcoin allows users to do transactions between themselves without interruption of the third party. Operations are checked by network nodes and records to a distributed ledger database – blockchain.

Blockchain automatically gives information to one party that another party of the treaty legally has paid for goods or services. In the aforementioned transaction, there isn’t a third party. The system literally is controlled by all participants. Any person who participates in cryptocurrency commerce has the same capability to control the movements of cryptocurrency. All verified transactions are included into blockchain.

The transaction is a transfer of value between Bitcoin’s wallets which are included into blockchain. Bitcoin’s wallet applies the key to sign a transaction. Key provides mathematical proof that Bitcoin comes from the owner of the “Wallet”. All transactions are transmitted between users and commonly begin to be confirmed by the network during the next 10 minutes through the certain process – “mining”.

“Mining” is a process of producing electronic money with aid of solving by the computer, certain the cryptographic algorithms (Lyubshina and Zolotaryuk, 2016).

Bitcoin is mined by blocks, the initial size of one block is 50 Bitcoin, however, after every 250000 blocks, and their amount is declining twice. On the average, each block is mined in 10 minutes. To save the aforementioned parameter after any 2016 mined blocks, the complexity of their mining is adjusted. Since the amount of equipment, which is used for mining constantly increase, thus the share of mined blocks for each of them constantly decrease. By simple calculation can be determined the amount of Bitcoin which is generated per day: $25 \times 24 \times 6 = 3600$. Thereby, the amount of emission is known in advance (Robbek, 2014).

It should be noticed that governments of different states of the world have a different opinion about the legalization of Bitcoin inside their countries. For instance, the new law, which has come into a force in Japan, allows utilizing Bitcoin as a legitimate means of payment.

As for Ukraine, according to the explanation of National Bank of Ukraine regarding the legality of “virtual currency/cryptocurrency” Bitcoin usage in Ukraine – Bitcoin is a monetary surrogate, which does not have provision by the real cost and cannot be used by individuals and legal entities on the territory of Ukraine as a means of payment, as far as it contradicts norms of Ukrainian legislation (Natsionalnyi Bank Ukrainy, 2014). It should be noticed that the explanation of the National Bank of Ukraine cannot be considered as a norm as far as it does not provide any responsibility; therefore, it can be utilized as a kind of notification or warning (Drozd, Lazur and Serbin, 2017). It should be noticed that “an ambiguous approach to cryptocurrency in different countries of the world creates additional problems for determining the legal status of cryptocurrency” (Drozd, Basai, Churpita, 2017).

The aforementioned position of National Bank of Ukraine was formed because transactions with Bitcoin does not allow to identify persons who realized them and it opens significant opportunities for crimes commitment, which correlate, in particular, with money laundering. For instance, FBI reported that if Bitcoin becomes more widely accepted among vendors and users, the FBI anticipates seeing increased Bitcoin money laundering activities (FBI, 2012).

6. The place of Bitcoin in the money laundering process

Money laundering can be defined as a financial transaction and other activities, which are committed for a particular target of concealment the real origin of the revenue. It should be noticed that “money laundering begins with the fruits of a crime – the underlying or “predicate” offense – and ends with funds that can be used safely or at least with minimal risk, for any purpose” (Levi and Reuter, 1997).
In the world practice, the biggest case in the history of online money laundering is Liberty Reserve. In May 2013, the U.S. Department of Justice has pressed charges against the company “Liberty Reserve” (which was the system of electronic transactions and located in Costa Rica) and seven its managers and employees. They were accused of commitment unregistered commercial activity with the provision of money transfer services and money laundering by the assistance of transactions of illegal income more than 6 billion US dollars. This system was functioning in colossal dimensions, counted millions of users all over the world, including 200000 users in the USA. In its framework, approximately 55 million transactions were carried out; almost all of them were illegal. Inside the system, their own virtual currency “Liberty Dollars” or LD was used, however, in the initial and end point of transaction money were converted and stored in fiat currency (USD). As a result of conducted well-coordinated actions, the Ministry of Finance of the USA determined “Liberty Reserve” as the financial agency, which triggered concern in terms of money laundering comply with Chapter 311 US Anti-Terrorism Act (Patriot Act) and completely deprived its access into the financial system of the USA (FATF, 2015).

As an example of the utilizing Bitcoin cryptocurrency for criminal activity, successful functioning of hiding website “Silk Road” can be taken. It was the biggest virtual market of drugs trading. All transactions via that website were conducted with aid of Bitcoin and anonymity for users was given through the functioning in Darknet, which viability was carried out by using the TOR software.

“Silk Road” was functioning as a peculiar Bitcoin’s bank, where any user had to have account for conducting transaction via the website, if it was possible not less than one (or even thousands) Bitcoin address “Silk Road”, which were attached to user’s account on the website and were stored on the server, which was controlled by “Silk Road”. For purchasing, a user sent mined Bitcoin to the Bitcoin address of “Silk Road” which was attached to his account on the website. After the realization of purchasing, the user’s currency transferred in the system of escrow account until the complete end of the transaction, then Bitcoin of user/customer transmitted from escrow account to Bitcoin address of the Silk Road’s seller. Furthermore, “toggle-switch” was used for any buyer which directed all payments with aid of complicated series quasi-random fake transactions … almost excluding the opportunity to binding payment to any Bitcoin, which was sent from the website (Mergenovna, Krylov, Bezverbnyi, Kasatkin and Kornev, 2016).

Currently, the aforementioned website “Silk Road” has shut down, and persons who governed it were brought to criminal responsibility.

7. Conclusions

To sum up, it should be emphasized that modern technologies facilitate using cryptocurrency, in particular, Bitcoin for money laundering. This process has become more complicated and intelligent, as far as elaboration allows:

- **firstly**, to eliminate bonds between real person and account of virtual currency because Bitcoin address and protocols do not require the client’s identification;
- **secondly**, to conduct conversation by utilizing simplified system, which does not need a person. Whereas, virtual currencies’ exchange does not have strict regulation, as those, which work with fiat currencies and according to the law have to store particular documentation about clients;
- **thirdly**, to create unlimited amount of account, which objectively makes it impossible to control all transactions;
- **fourthly**, to utilize tools which block the opportunity to track back particular activity (anonymizers etc.). For instance, Dark Wallet, which mixes together several transactions and complicates the opportunity to track back the particular address of Bitcoin wallet, which sends Bitcoin. In addition, transactions can be done through the TOR network, which directs particular web-traffic through several relays, in that way hiding the real user’s IP-address.

Thus, Bitcoin allows conducting different schemes of money laundering, which almost block the possibility of the criminals’ identification. This feature triggers new challenges for law enforcement agencies to seek out new forms and methods of money laundering investigation. Moreover, the aforementioned characteristics of cryptocurrency are pushing lawmakers all over the world to unify the legislative system regarding utilizing cryptocurrency as a means of payment. Without its recognition by government, it is almost impossible to combat and prevent the commitment of money laundering.

References:


