Journal of Theoretical and Applied Information Technology
20th January 2016. Vol.83. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

INVESTIGATION OF MONEY LAUNDERING METHODS THROUGH CRYPTOCURRENCY

[1]DIANA MERGENOVNA SAT, [2]GRIGORY OLEGOVICH KRYLOV, [3]KIRILL EVGENYEVICH, [4]BEZVERBNYI, [5]ALEXANDER BORISOVICH KASATKIN, [6]IVAN ALEKSANDROVICH KORNEV

[1]National Research Nuclear University MEPhI (Moscow Engineering Physics Institute)
Kashirskoe highway, 31, Moscow, 115409, Russia
[2]Financial University under the Government of the Russian Federation
[3]Leningradsky prospekt, 49, Moscow, GSP-3, 125993, Russia
[4]National Research Nuclear University MEPhI (Moscow Engineering Physics Institute)
Kashirskoe highway, 31, Moscow, 115409, Russia
[5]National Research Nuclear University MEPhI (Moscow Engineering Physics Institute)
Kashirskoe highway, 31, Moscow, 115409, Russia
[6]National Research Nuclear University MEPhI (Moscow Engineering Physics Institute)
Kashirskoe highway, 31, Moscow, 115409, Russia

ABSTRACT

The main issue of this work is to search of suspicious operations that were made with the use of cryptocurrency. The set tasks: creation of a database from received information; visualization of received results; analysis and conclusions of received results. The object of the research is money laundering and financing terrorism by means of cryptocurrency. Nowadays it is an actual term for research as for countries cryptocurrency is a new way of payments and each country decides differently how to deal with it. But new technologies provide us new possibilities in our live (especially in anonymous transactions as payments for goods and other purposes) and of course they can be used in illegal activity such as money laundering and financing of terrorism. Besides anonymity is one of the main features of cryptocurrency that helps to hide the source of income. This is the problem for countries because they have to combat such a threat as money laundering and financing of terrorism. So it is natural to find out ways of searching suspicious operations that can be directed to money laundering and financing of terrorism.

Keywords: *Bitcoin, Transaction, Bitcoin Address Of The Recipient (Addresser), Bitcoin Address Of The Sender (Receiver), Anti-Money Laundering, Combating Financing Of Terrorism, Financial Monitoring.*

1. INTRODUCTION

In modern world new technologies provide us new possibilities in our live (especially in anonymous transactions as payments for goods and other purposes) and of course they can be used in illegal activity such as money laundering (a process whereby the proceeds of crime are transformed into apparently legitimate money or other assets [1]) and financing of terrorism (provides funds for terrorist activity. The main objective of terrorist activity is to intimidate a population or compel a government to do something by killing, seriously harming or endangering one or more persons; causing substantial property damage that is likely to seriously harm one or more persons; or seriously interfering with or disrupting essential services, facilities or systems [2]).

If we are speaking about cryptocurrency (a medium of exchange like normal currencies such as USD, but designed for the purpose of exchanging digital information through a process made possible by certain principles of cryptography. Cryptography is used to secure the transactions and to control the creation of new coins [3]) for countries it is a new way of payments and each country decides differently how to deal with it. Besides anonymity is one of the main features of cryptocurrency that helps to hide the source of income. This is the problem for countries because they have to combat such a threat as money laundering and financing of terrorism.

So it is natural to find out ways of searching suspicious operations that can be directed to money laundering and financing of terrorism. For this

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

purpose it was decided to choose one of the most popular cryptocurrency – Bitcoin and figure out how we can find suspicious operations with appointed currency that are made via internet technology.

1.1. What is Bitcoin?

The bitcoin is the first decentralized P2P (peer-to-peer) payment network which is served by its users without the central governing bodies or agents. From the point of users' view, Bitcoin has similarity to cash but only for the Internet [4].

Anonymity is peculiar to Bitcoin as a result of decentralization of system and existence of properties of cash and there is a risk of its use for laundering of criminal income and financing of terrorism.

As accounts of Bitcoin-addresses do not contain names in their structure or other identification information about clients and there is no central server or provider of services in the system. The bitcoin protocol does not demand and provide establishment and check of persons of participants or formation and maintaining data on operations for past period which have been done in the real world. Besides there is no central supervisory authority and nowadays there is no software for anti-money laundering and combating financing of terrorism (CML/FT) using which it would be possible to trace and reveal schemes of suspicious operations. In total it provides the high level of anonymity which is simply impossible in case of credit and debit cards and electronic payment systems (e-wallets).

Nearly the main issue concerning virtual currencies from the point of view of proofs of intention of commission a crime is concealed in the essence of virtual currencies, namely: virtual currencies are out of the established financial institutions and at total absence of regulation that can be presented as a conscious choice [5].

Cryptocurrencies provide anonymity of operations: after virtual currency, for example, Bitcoin, is placed to a certain wallet, further operations with it in a chain of blocks (the unified on-line register of payments of the Bitcoin network) can be anonymized that excludes opportunity to trace the real owners of wallets.

Cryptocurrencies rely on cryptography the value is attached to the distributed network of the calculations which are carried out by miner for the solution of cryptographic task. It also, in addition, complicates possibility of tracking and establishment of the facts of illegal use of virtual currencies.

1.2. Principle of usage Bitcoin

From the point of view of the user, Bitcoin is a system of electronic cash. Any person having access to the Internet and necessary amount of memory on his or her computer can become a user of this electronic cash. The first step to start using bitcoins is a choice of a wallet on the site "bitcoin.org" [4] and its subsequent installation. The wallet can be desktop (is established on the computer), mobile (phone wallet) and Internet wallet. Bitcoin-address is generated automatically after creating a wallet. Using this wallet a user can make any transactions. Transfer of bitcoins from one user of the network to another is made by means of the transfer of bitcoins from one address to another. This address provides full anonymity to his owner as it looks like a combination of figures and letters, for example: "1D5wZqCjxNuPqfUN3RMFsxxxtqRBwiAeTZ". Every bitcoin wallet contains the classified information about private keys to everyone bitcoin-address which is owned by the specific user. Therefore, you can make transactions if you own a private key from a bitcoin-address intended for the transaction [6]. In spite of the fact that this system is rather safe, site administrators recommend to use as many bitcoin-addresses as possible, namely a new bitcoin-address for each transaction. It is caused that a function of restoration of a private key, in Bitcoin system is absent. Therefore, in case of loss of the private key the user will lose all funds which are stored on this address. Theft of a private key will also lead to loss of the stored bitcoins. The interesting fact is that for receiving bitcoins to the address the user should not be connected to the Internet, this need is presented only at that user who pays bitcoins.

Data on transactions are stored in the distributed database which is in open access, however, without disclosure of information about the user of the address as it was earlier mentioned. For prevention of situations when the same bitcoins can be spent twice, Satoshi Nakamoto (a nickname of the person in the Internet who published the file "Bitcoin: Peer-To-Peer Electronic Cash System" where described the protocol of Bitcoin system and the principle of this P2P network) developed a system of tags of time ("timestamp server") where the database is broken into a chain of special blocks [7]. Each block contains hash (checksum) of the previous block and the serial number. The new block is created by means of confirmation of

Journal of Theoretical and Applied Information Technology
20th January 2016. Vol.83. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

accomplishment of transactions and contains information about this and the previous transactions made with concrete bitcoins. In other words, each bitcoin has information how it was used earlier, and users leave "digital signatures" and a public key of the following owner when receiving bitcoins. The scheme of commission of transactions is given below.

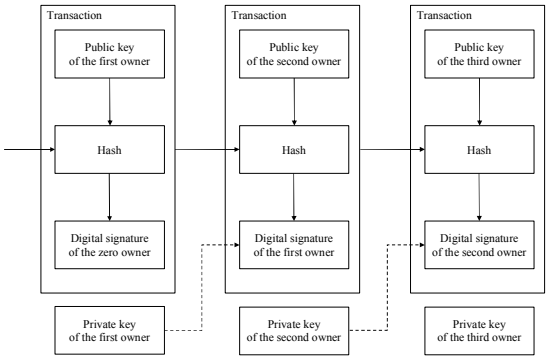

Figure 1.Creation Of New Transaction

All transactions have connection with Bitcoin-addresses and remain in a chain of Bitcoin blocks which can be found in the Internet. Thus, the information of Bitcoin-addresses found in the suspect's computer can be in addition studied regarding establishment of what transactions preceded and followed after transfers from/to the Bitcoin-addresses connected with the suspect.

On the site blockchain.info [8] it is possible to consider the full structure of transaction presented in the form of a tree which can be seen in the corresponding figure.

(SEE IN THE APPENDIX)

Figure 2. Structure Of Transactions In The Form Of A Tree

1.3. Tools to obstruct tracking

The central payment register known as a chain of blocks is the basis of functioning of the Bitcoin network. The register contains information on all ever executed operations and is used for checking the legitimacy of transactions. To confuse transition of money from the buyer to the seller is very easy. It is possible to carry out it by means of so-called blenders/mixers ("Tumbler") for a certain commission. The schematical image is shown on the corresponding figure.

Figure 3. The Centralized Mixer

The centralized mixing services

Bitcoin mixers, belonging to the first generation, worked as the centralized services for mixing. It was possible to send bitcoins there, to pay the commission for this service, and to receive the sum of absolutely other bitcoins. These were the earliest and most primitive services of bitcoin-mixing [9].

The success of anonymization of currency by means of such provided services depends on number of the user and bitcoins. Because of it such specialized services are not so popular. For the similar purposes the bitcoin exchange and other trade platforms are more often used. If the mixer was rather big (like Mt. Gox) [10], the deposited funds at a conclusion would turn into absolutely other bitcoins, and it is even not obligatory to sell them and to buy. Thus, without the commission bitcoins effectively mix up.

It is necessary to trust such service it should not steal our bitcoins and the currency has to be protected by technical service from thefts and breakings. Besides, we have to trust that service does not save reports of the passed mixing operations and will sell or give nobody such records. It is very problematic to verify listed above even if service assures of the return.

Peer-to-peer mixers

With the purpose to optimize the first generation of mixing services, the following one was based on "peer-to-peer groups" of bitcoin users, interested in mixing currency, gathering in certain time. Such mixers (instead of transferring and getting currency) operate as the meeting place of users who will organize mixing independently on a certain platform.

Journal of Theoretical and Applied Information Technology
20th January 2016. Vol.83. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

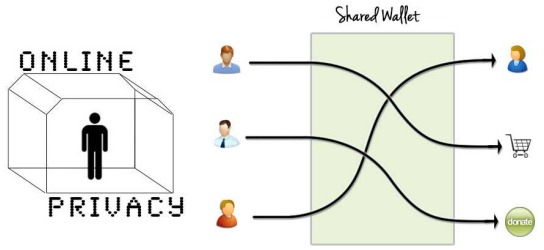

Figure 4. Peer-To-Peer Mixer

There is no agent holder in such model that's why there is no danger of losing coins. Therefore, the theft problem is solved. The CoinSwap [11], CoinJoin [12] and SharedCoin [13] protocols allow users to gather and create a general bitcoin transaction in some stages. Being created, bitcoins go to destination of one transaction. Until transaction is created completely there is no chance of loss of currency.

Nobody, except the mixing server, knows links between senders and recipients (initial and final addresses) of coins. To complicate the analysis of a chain through blockchain even more, this operation can be performed in some circles.

Also according to the researcher Christoph Atlas peer-to-peer mixing can solve the record-keeping problem by mixing-service, as: "addition to peer-to-peer mixers of such cryptographic primitives as cryptographic blinding (crypto-blinding), zero knowledge proofs (ZKP) and Succinct Non-interactive Arguments of Knowledge (SNARK) can improve anonymity to the level when neither participants of the process nor the service organizing mixing knows what address what coins went in the upshot" [14].

Mr. Atlas calls this advanced option of the peer-to-peer mixers as "blind mixing".

Anonymous Altcoins

Due to the developed currencies it becomes possible to complicate transactions even more.

Christoph Atlas considers that exchangers of cryptocurrencies with participation of various Altcoins (so-called alternative to Bitcoin, created on the basis of Bitcoin code) [15] can be included in BlockChain-technologies for receiving completely peer-to-peer exchange mechanism. As soon as new anonymous exchangers are completely developed, we will see how through these exchangers the exit will be done from bitcoins to anonymous Altcoins and the entrance to them in essence, such exchangers will act as reliable mixers.

This introduction will allow to improve a bitcoin mixers and to expand a process decentralization framework. The mixing is given on the distributed network of Altcoins, and it considerably increases the general anonymities size, and complicates tracing of operations of the user.

The leader in development of completely anonymous Altcoins is the Zerocoin team [16].

In the conditions of the adverse relation of regulators to cryptocurrency the main bitcoin developers watch with a reluctance at idea of merge of currencies. And whether it is necessary these are excess overhead costs, complication of the main protocol.

As one of the main bitcoin developers Mike Hern tells, the forthcoming bitcoinj version will direct all connections to a bitcoin network via the Tor anonymizer by default [17].

Use of "laundries" in criminal intents

Criminals use "laundries" (a set of services which generates a huge number of wallets and sends currency between them in a casual order) for bigger complication of their actions and complication of traces.

At the forum Runion [18] one man advises the rest ones to write such program for complication of investigative actions.

Signs of use of virtual "laundries" are very similar to that are used in real "laundries".

On the site http://blockchain.info there is a service of the anonymous transfer between bitcoin wallets (take 1.5% commission), which as write at forums, works banal. And thus the probability is high that the made operations of mixing register on the server.

1.4. On-line black market "Silk Road" as an example of bitcoin usage

The hidden website "Silk Road" (a criminal case has been instituted proceedings against the owners of the website because of selling drugs, weapons, etc.) [19] worked only with virtual currency Bitcoin and provided anonymity due to functioning in the hidden TOR network.

Journal of Theoretical and Applied Information Technology
20th January 2016. Vol.83. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

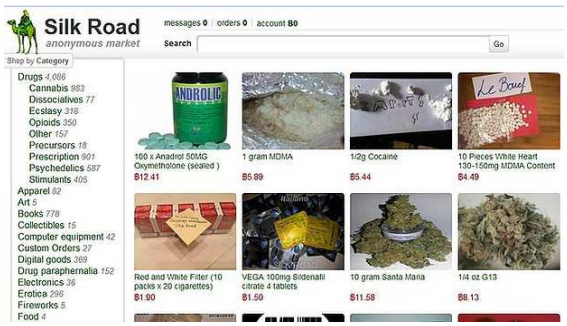

Figure 5. Structure Of The Site "Silk Road"

Using of Bitcoin as the only currency on the site "Silk Road" allowed users of the site (buyers, sellers) to hide their personalities at the expense of anonymous bitcoins addresses/accounts. It is not difficult to acquire currency on the site at all.

Users could create a huge number of addresses, could also use additional "anonymizers", besides service of "mixing" (tumbler) which was built in the operations which are carried out through the site [20].

"Silk Road" functioned as the Bitcoin bank where each user had to have the account for fulfilling operations on the site, possible not less than one (or even thousands) Bitcoin addresses of "Silk Road", attached to the account of the user of the site, stored in wallets on the servers controlled by "Silk Road". For purchase the user got bitcoins and sent them to the Bitcoin address attached to its account on the site. After purchase fulfilling currency of the user was transferred within system to the target deposit account before full completion of operation then bitcoins of the user/buyer were transferred from the target deposit account on the Bitcoin address of the seller of "Silk Road". Also, at each purchase "toggle-switch" was used which "directs all payments by means of a difficult series of quasi-random fictitious operations … practically excepting possibility of a binding of your payment to any bitcoins sent from the site" (it was so specified on the site).

At the moment the site http://silkroadvb5piz3r.onion/ is blocked.

Figure 6. The Maintenance Of The Blocked Silk Road Resource

2. METHOD

2.1. Signs Of Money Laundering

Let's remind that the process of tracking cash flows through bitcoin becomes difficult and more confused due to the following factors [21]:

- Lack of communication between real people and accounts of virtual currency;
- Obstacle tools for tracking (mixers, tumblers, anonymizers);
- Possibilities of creation of unlimited number of accounts.

The signs (examples of red flags/indicators) of money laundering in the Internet are:

- A large number of the bank accounts belonging to one administrator of the virtual currency or the company which is engaged in an exchange of virtual currencies (they are sometimes in different countries) which, likely, are used as suspense accounts (so-called "stratification" - the second stage of money laundering).
- The administrator of the virtual currency or the company which is engaged in an exchange of virtual currencies is in one country, but has accounts in other countries where they have no essential client base (illogical justification of such business activity that can be suspicious)
- A roundabout of the money between bank accounts which are in different countries and belong to different administrators of virtual currency or the companies, engaged in an exchange of virtual currencies (can testify to "stratification" if such activity of the company is unusual);
- The volume and frequency of operations with cash (often the sums are lower than a

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

threshold of providing the reporting), which are performed by the owner of the administrator of the virtual currency or the company which is engaged in an exchange of virtual currencies and do not make economic sense.

Criminals use the correspondence nature of virtual currencies for laundering of the criminal income:

- The majority of operations with virtual currencies assume minimum or do not assume any contact "face to face". Such state of affairs promotes that virtual currencies are used by criminals for money laundering.
- One category of cases of using virtual currencies in the criminal purposes includes the scenario which criminals receive control over accounts of lawful users and opportunity to carry out on them operations.
- The second category of cases of use of the correspondence nature of accounts of new payments methods is connected with use of anonymous character of some such services.

2.2. The Increasing Complexity Of Schemes Of Money Laundering

Lack of communications between accounts in virtual currencies and real people in combination with opportunity to have any number of accounts allows to create new difficult schemes for the purpose of concealment of an illegal source of an origin of means.

Thus virtual currencies represent additional opportunities for creation of new methods of money laundering. It is quite natural to expect that criminals will continue to develop ways of laundering of the criminal income, using for this purpose virtual currencies. Emergence of more intricate schemes with wide use in criminal intents the speech about which went above will become the result of it.

Let's give an example where the scheme of money laundering of illegal income by means of virtual currencies and prepaid cards is presented:

When the investigation was carrying out it was established that the international criminal group used one of providers of financial services for transferring illegal money to the East European countries which members of this group cashed and turned the specified means into electronic money in offices on an exchange of electronic currencies. Electronic money was transferred into the accounts opened by the members of this group at one of providers of financial services who was engaged in operations with virtual currency in the specified countries. The mentioned provider of financial services let out together with one offshore bank the MasterCard Cirrus prepaid cards which could be got anonymously and deposited on them the sums of electronic currency. Such cards could be used in any countries in ATMs and at payment of purchases via the terminals accepting the Cirrus cards. This scheme allowed criminals to hide effectively illegal money and provided fast and anonymous access to such means.

2.3. Search Of Suspicious Operations

From all above-mentioned, it is possible to create a hypothesis that for complication of movement of cash in the virtual environment the criminal (in most cases, most likely, the robot) creates a huge number of purses and sends between them currency. Thus it aggravates investigation process which is already difficult. After that the raised funds merge on one purse and further necessary actions with them are made (removal from the ATM, transfer, payment of goods/services).

To check this hypothesis, the website "blockchain.info" [22] was chosen for searching suspicious operations where the latest committed transactions were reflected online and also other information.

The transactions from the list of the latest transactions with weighty sums were chosen by random and were studied regarding suspiciousness.

Finally, the choice was made on a bitcoin address "19HGYSRWiSKrRCybsMbcWDqZpSRj5GQ5bm" where on April 30, 2015 at 7:35 am there was incoming transaction with the sum aggregated of 32.8710217 BTC equal $ 7,755.59 for the transaction commission moment and at 7:37 am at the same day there were transactions from this address to two others with the sums of 32.80110338 BTC = $ 7,739.09 and 0.0698 BTC = $ 16.47 [22].

These actions were seemed suspicious as here we could obviously see the splitting of a large sum on a big and smaller ones which went further on the next bitcoin addresses and so on.

For making general and fuller data base in respect of a chain but not in respect of amount it was decided to go through the chain of transactions with the bigger sum. Thus the starting point of transactions would be a bitcoin address "19DU7YCz3dBerGeTievE4WaDYaCU4zPFnu". 32.80110338 BTC were sent from the investigated address to this [23].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

As a result, 98 transactions were looked through from this chain which created a small but quite informative database.

3. RESULTS

3.1. Creation of a database from the received information

There was used MS Excel (fig. 3) in creation of database in which there were created 7 columns:

- number of record (Line number(Line ID));
- bitcoin address of the sender (Addresser);
- bitcoin address of the recipient (Receiver);
- number of transaction (Transaction);
- sum of transaction (Amount of transaction (BTC));
- date of transaction (DD.MM.YYYY);
- time of transaction (HH:MM:SS).

(SEE IN THE APPENDIX)

Figure 7. The Table In MS Excel

After creation of columns records of transaction were placed from the start point till the other 97 ones. The chains of transaction with big sums were placed as well as with smaller ones but only to the first knee if further record did not make sense. The recording of chains would stop if the chain broke (logically came to an end), lost (by mixing various sums and absence of opportunity to trace the studied sum) or lost the meaning.

It is possible to add that the bulk of operations was carried out in the same day, with a difference in a chain between two next operations in some minutes, and sometimes in a few seconds. All studied chain occupies a period of 5 days – from 30.04.2015 till 04.05.2015.

3.2. Visualization

For visualization of a chain of presumable money laundering the IBM i2 Analyst's Notebook 8 program was used.

The scheme of visualization "one to one" was chosen where Addresser and Receiver through Transaction were connected [24].

(SEE IN THE APPENDIX)

Figure 8. Visualization Example Of The Scheme

At first let's try to make out in details what this scheme represents. The initial point, i.e. that bitcoin address which studying of the scheme was begun with, is on the scheme:

(SEE IN THE APPENDIX)

Figure 9. Initial Bitcoin Address. Visualization Of The Scheme

Further the chain goes, branches, splits on some, becomes "distributive knots" where a mixing of money is and also there are other metamorphoses of this scheme.

For an example of money laundering methods, there are operations without economic or other sense when money from one account passes on some and from all of them back to another account.

Further, main chain represented roughly and more specifically its branches which it is possible to follow from a starting point.

(SEE IN THE APPENDIX)

Figure 10. Reflection Of The Main Chain Of Transactions

4. CONCLUSION

In this article the scheme of money laundering and financing of terrorism using cryptocurrency is considered by the example of transactions of the most famous currency Bitcoin and an approach is suggested for identifying the "laundry" cryptocurrency.

In the analysis of money laundering schemes using cryptocurrency bitcoin it is necessary to generate the function the result of which is a probabilistic assessment of the transactions involved in the activities of money laundering and financing of terrorism. This allowed the hypothesis of the compactness of the set studied: cryptocurrency Bitcoin transactions are considered, database of transactions is researched at the time of the study, assignment to transactions for money laundering and financing of terrorism makes a complete group of events.

The search and collection of data on transactions cryptocurrency bitcoin was carried out during the research. A relational database was designed and implemented for storage and processing. To form the feature space signs of suspicious transactions have been formalized and automated to the typologies of money laundering using the classical banking system and the article about the analysis of the transaction reports cryptocurrency of FATF has been used. According to it, data analysis methods were used in particular, methods of cluster analysis

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

and principal component analysis. As a result, suspicious transactions have been identified using the "laundry". Using algorithms to detect suspicious financial transactions signs of transactions used to launder were identified. The study results allow to develop tools that can be used to monitor suspicious transactions.

According to this article, the hypothesis of the existence of signs of identification of money laundering using cryptocurrency was proposed and verified on the basis of the results of analysis, property transactions were formalized in the feature space related to money laundering and financing terrorism.

The analogues of data analysis methods can be investigated to find optimal performance and resource intensity of the algorithm in future work. And it is also advisable to extend the feature space due to the signs of the derivatives based on the activity of the wallets.

REFERENCES:

[1] What is Money Laundering? In Duhaime's Financial Crime and Anti-Money Laundering Law. Retrieved March 30, 2015, from http://www.antimoneylaunderinglaw.com/aml-law-in-canada/what-is-money-laundering.

[2] What is Terrorist Financing? In Duhaime's Financial Crime and Anti-Money Laundering Law. Retrieved March 30, 2015, from http://www.antimoneylaunderinglaw.com/aml-law-in-canada/what-is-terrorist-financing.

[3] What is Cryptocurrency? In CCN. Retrieved March 30, 2015, from https://www.cryptocoinsnews.com/cryptocurrency/.

[4] FAQ (n.d.). In Bitcoin information site. Retrieved April 25, 2015, from bitcoin.org/ru/faq#what-is-bitcoin.

[5] Phenomenon of cryptocurrency Bitcoin as a means of payment and earnings (n.d.). In Prostoinvesticii. Retrieved March 30, 2015, http://prostoinvesticii.com/o-dengakh/fenomen-kriptovalyuty-bitkoin-kak-sposoba-raschetov-i-zarabotka.html.

[6] Bitcoin. How it wokrs (2011, February 28). In habrahabr. Retrieved April 25, 2015, from http://habrahabr.ru/post/114642/.

[7] Vlasov, A.V. (2012). Virtual currency and the evolutionary theory of the origin of money. *Science and Education: Agriculture and economics; entrepreneurship; law and governance*, 12, 17.

[8] Home. Blockchain (n.d.). In Blockchain. Retrieved March 24, 2015, from https://blockchain.info/.

[9] Taxonomy bitcoin-mixers (n.d.). In Bitnovosti. Retrieved March 30, 2015, from http://bitnovosti.com/2014/03/18/taxonomia-bitcoin-mixerov/.

[10] The history of bitcoin and reasons for instability problems of currency (2014, March 13). In Vesti.Finance. Retrieved May 3, 2015, from http://www.vestifinance.ru/articles/40536/.

[11] CoinSwap: Transaction graph disjoint trustless trading (2013, October 30). In Bitcoin Forum. Retrieved March 30, 2015, from https://bitcointalk.org/index.php?topic=321228.

[12] CoinJoin: Bitcoin privacy for the real world (2013, August 22). In Bitcoin Forum. Retrieved March 30, 2015, from https://bitcointalk.org/?topic=279249.

[13] Randomised Consensus Shared Coin Protocol (n.d.). In PRISM. Retrieved March 30, 2015, from http://www.prismmodelchecker.org/casestudies/consensus_prism.php.

[14] The first three generations of bitcoin mixing technology (n.d.) In The LTB Network. Retrieved March 30, 2015, from https://letstalkbitcoin.com/the-first-three-generations-of-bitcoin-mixing-technology/#.Uya-jc5GbIs.

[15] What is an Altcoin? (2014, September 12) In CCN. Retrieved March 30, 2015, from https://www.cryptocoinsnews.com/altcoin/.

[16] Zerocoin is the project for 100 % anonymity of digital currency (2014, January 16). In BitNovosti. Retrieved Aprel 30, 2015, from http://bitnovosti.com/2014/01/16/project-zerocoin/.

[17] Five bitcoin projects that can make payments more anonymous (2014, May 11). In Hi-News. Retrieved March 30, 2015, from http://hi-news.ru/technology/pyat-bitkoin-proektov-kotorye-mogut-sdelat-platezhi-bolee-anonimnymi.html.

[18] Forum RUnion in the TOR net (n.d.). In Forum RUnion. Retrieved March 30, 2015, from http://r2d2akbw3jpt4zbf.onion/.

[19] Summary: Digital "laundry" on money laundering, the analysis of virtual currencies and their use in cybercrime (n.d.). In McAfee. Retrieved March 29, 2015, from http://www.mcafee.com/ru/resources/white-papers/wp-digital-laundry.pdf?view=legacy.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[20] How to launder stolen bitcoins (2015, January 7). In CCN. Retrieved May 3, 2015, from https://www.cryptocoinsnews.com/launder-stolen-bitcoins/.

[21] UNODC (2014). Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies, June 2014.

[22] Bitcoin Block Explorer (n.d.). In Blockexplorer. Retrieved March 24, 2015, from http://blockexplorer.com.

[23] Information "About using of "virtual currencies", in particular, Bitcoin" (2014, January 27). In The Central Bank of the Russian Federation. Retrieved April 24, 2015, from www.cbr.ru/press/pr.aspx?file=27012014_1825052.htm.

[24] Abe: block browser for Bitcoin and similar currencies (n.d.). In GitHub. Retrieved March 24, 2015, from https://github.com/bitcoin-abe/bitcoin-abe.

Journal of Theoretical and Applied Information Technology
20th January 2016. Vol.83. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

APPENDIX

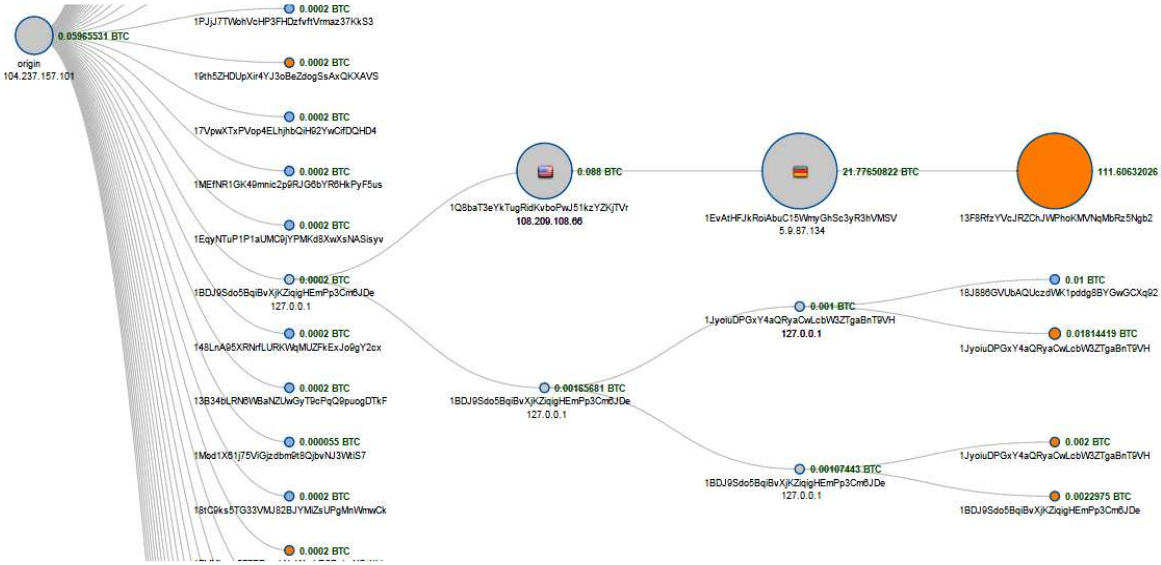

Figure 2. Structure Of Transactions In The Form Of A Tree

	A	B	C	D	E	F	G
1	Line number (Line ID)	Adresser	Reciever	Transaction	Amount of transaction (BTC)	DD.MM.YYYY	HH:MM:SS
2	1	19HGYSRWiSKrRCybsMbcWDqZpSRj5GQ5bm	19DU7YCz3dBerGeTievE4WaDYaCU4zPFnu	cccfb7f842c07a3c385017dd5152c9b7da9a186fce8288fa54c1170dde67ffc4	32.80110338	30.04.2015	7:37:16
3	2	19DU7YCz3dBerGeTievE4WaDYaCU4zPFnu	1DME4JWDWZsQ6B7JpDokRLt9vjFjEjmmXU	10b94e451dc01becc2dc7a8cfa2a865309f2acae18f3f8cc64d5c4a3874076078	0.12964548	30.04.2015	7:41:28
4	3	19DU7YCz3dBerGeTievE4WaDYaCU4zPFnu	1Kv7Cr9GRrs3hMRx9YqxuLHAkvR7efmfbY	10b94e451dc01becc2dc7a8cfa2a865309f2acae18f3f8cc64d5c4a3874076078	1	30.04.2015	7:41:28
5	4	19DU7YCz3dBerGeTievE4WaDYaCU4zPFnu	1FWfTPAQ3BTKtXhVW4DpC48HSRNfsMg1f	10b94e451dc01becc2dc7a8cfa2a865309f2acae18f3f8cc64d5c4a3874076078	31.67132178	30.04.2015	7:41:28

Figure 7. The Table In Ms Excel

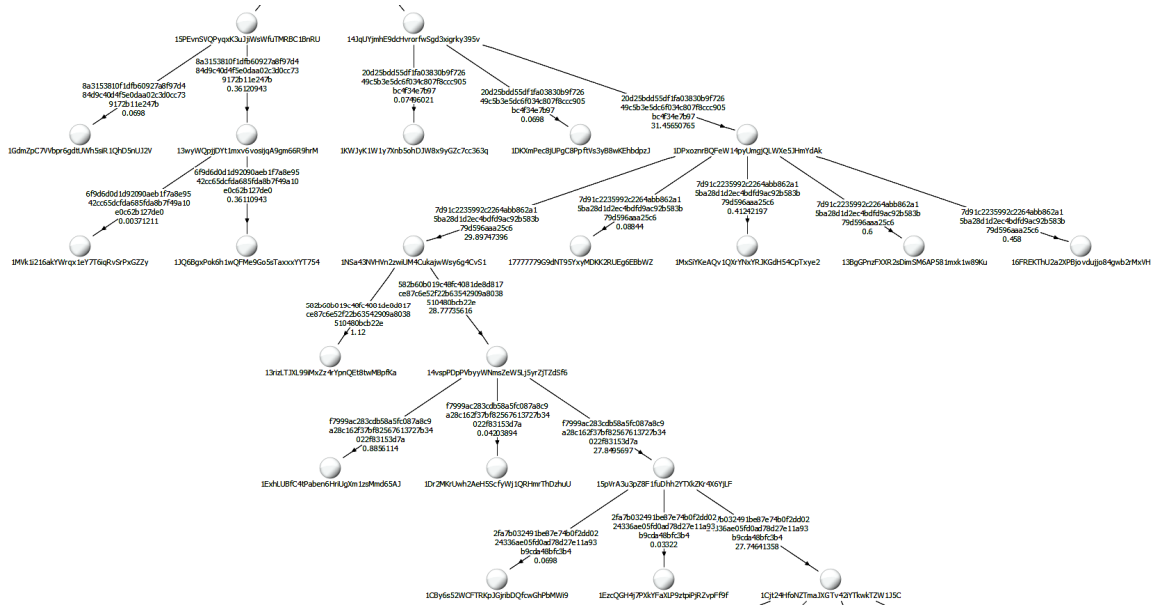

Figure 8. Visualization Example Of The Scheme

Journal of Theoretical and Applied Information Technology
20th January 2016. Vol.83. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

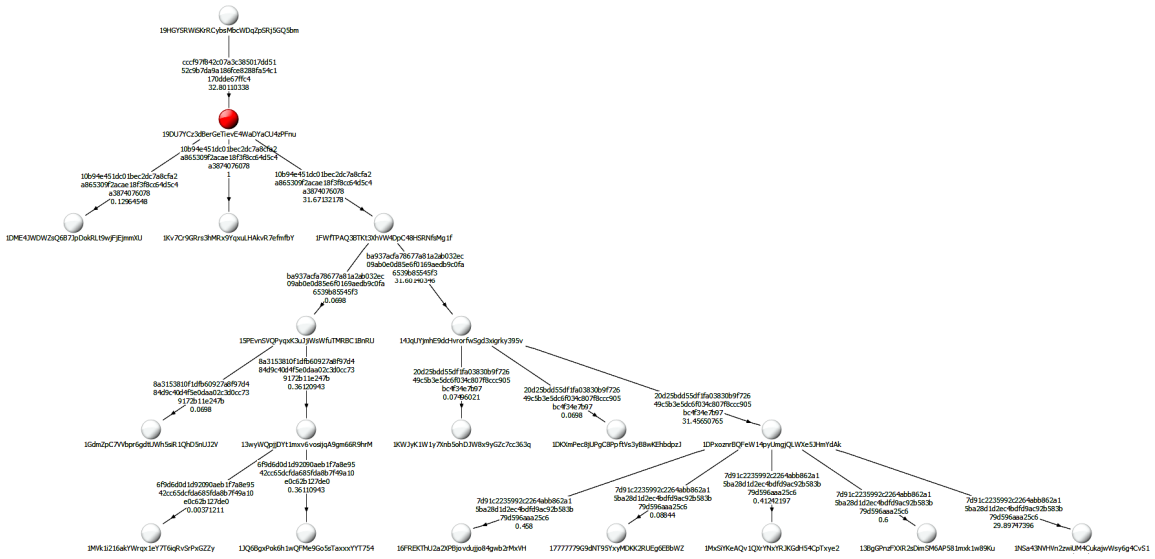

Figure 9. Initial Bitcoin Address. Visualization Of The Scheme

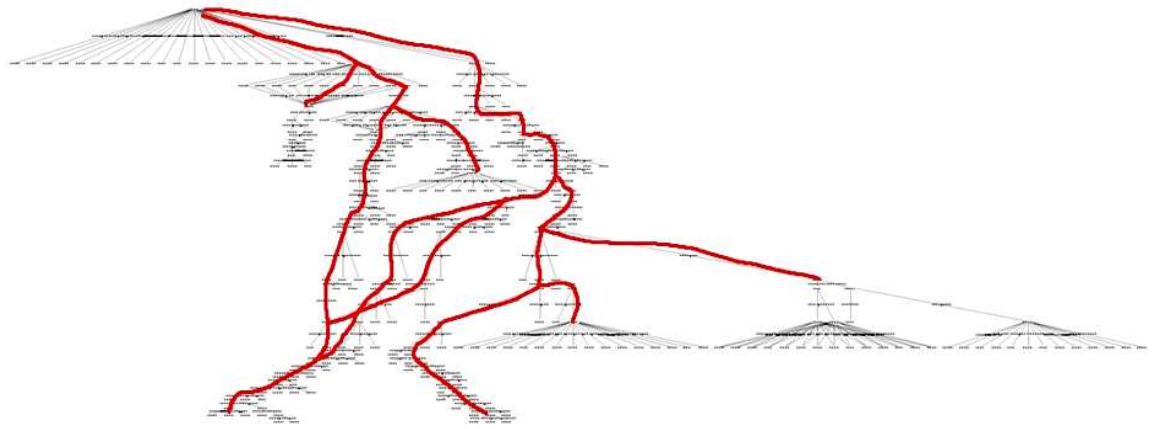

Figure 10. Reflection Of The Main Chain Of Transactions