

Artículo de investigación

Bitcoin blockchain: Participants typology

БЛОКЧЕЙН БИТКОИН: Типология участников

Cadena de bloques de bitcoin: Tipología de los participantes

Recibido: 15 de mayo del 2019

Aceptado: 6 de julio del 2019

Written by:

Vladimir I. Glotov⁷⁵https://elibrary.ru/author_items.asp?authorid=1012498**Dmitri M. Mikhaylov**⁷⁶**Alexey A. Yurov**⁷⁷**Dmitri O. Uglov**⁷⁸**Maxim V. Taranov**⁷⁹**Abstract**

The paper describes the classification and criteria for blockchain environment participants. The overview of the main types of blockchain participants is essential for the understanding of blockchain social and economic behaviour. It structured in the description of the several patterns which is often generated inside the Bitcoin blockchain and the list of the economic entities with the criteria of their behaviour. The paper gives the view on the different types of blockchain entities both from outside and inside the blockchain. Also, the paper lists the possible risks of criminal behaviour corresponding to every entity.

Key words: Blockchain, identification pattern, the pattern of a massive structure, miners, mining pools, markets, aggregators of exchangers, OTC, exchange offices, AML/CFT

Аннотация

В статье описывается классификация и критерии классификации участников блокчейн среды. Обзор основных видов блокчейн участников имеет важное значение для понимания социального и экономического поведения в блокчейн. Статья структурирована как описание нескольких моделей, которые часто возникают внутри блокчейн Биткоин и перечень хозяйствующих субъектов с критериями их поведения. В статье дается представление о различных типах блокчейн структур со взглядом как снаружи, так и внутри блокчейн. Кроме того, в документе перечислены возможные риски преступного поведения, соответствующего каждому объекту.

Ключевые слова: блокчейн, модель идентификации, модель крупной структуры, майнер, майнинг пул, биржи, агрегатор обменных пунктов, OTC деск, обменные пункты, ПОД/ФТ

⁷⁵ Candidate of Sciences in Economics, Professor, I.E. Tamm Theory Department, Lebedev Physical Institute of the Russian Academy of Sciences, Moscow. glotovvi@lebedev.ru

⁷⁶ Candidate of Sciences in Technology, Senior Researcher, I.E. Tamm Theory Department, Lebedev Physical Institute of the Russian Academy of Sciences, Moscow. mikhaylovdm@lebedev.ru

⁷⁷ Leading Researcher, I.E. Tamm Theory Department, Lebedev Physical Institute of the Russian Academy of Sciences, Moscow. yurovaa@lebedev.ru

⁷⁸ E. Tamm Theory Department, Lebedev Physical Institute of the Russian Academy of Sciences, Moscow. uglovdo@lebedev.ru

⁷⁹ Engineer, I.E. Tamm Theory Department, Lebedev Physical Institute of the Russian Academy of Sciences, Moscow. taranov.maksim.work@gmail.com

Resumen

El artículo describe la clasificación y los criterios para los participantes del entorno de blockchain. La descripción general de los principales tipos de participantes de blockchain es esencial para la comprensión del comportamiento social y económico de blockchain. Se estructura en la descripción de los diversos patrones que a menudo se generan dentro de la cadena de bloques de Bitcoin y la lista de las entidades económicas con los criterios de su comportamiento. El documento ofrece una vista de los diferentes tipos de entidades de blockchain tanto desde fuera como desde dentro de blockchain. Además, el documento enumera los posibles riesgos de comportamiento criminal que corresponden a cada entidad.

Palabras clave: Blockchain, patrón de identificación, el patrón de una estructura masiva, mineros, grupos mineros, mercados, agregadores de intercambiadores, OTC, oficinas de cambio, ALA / CFT

Introduction

Since the creation of bitcoin in 2008 by Satoshi Nakamoto (Nakamoto, 2008), the ecosystem of the crypto-currency world has grown to unprecedented sizes, and it has now a similar infrastructure to Fiat money. However, to date, bitcoin occupies a leading position among all cryptocurrencies.

The turnover of cryptocurrencies is experiencing ups and downs but has already become a reality of the economy, large banks have opened cryptocurrency desks, and the big four companies advise the use of blockchain and cryptocurrencies. These activities are poorly regulated, and this is a concern for both regulators and the rest of the financial industry, as increases the likelihood of money laundering and other fraudulent activities.

In order to highlight the probable criminal actions, it makes sense to identify the types of participants in the crypto-currency market, try to determine the essence of their economic activity and assess the likelihood of participation and role in criminal actions. It is important to highlight not only transactions that can carry criminal transactions, but also the law-abiding and honest members of society, as well as such activities that can serve as a cover of criminal activity and a contribution to it, do not have the same sense.

Bitcoin blockchain is the first, according to the industry, investors and all community members still rely on it. The bitcoin blockchain still has the largest capitalization. Since bitcoin is still an

economic standard of cryptocurrency, it can be used as a model to identify the types of participants and train the formal criteria to attribute participants to a particular type of activity. The researcher can also reveal patterns in transactions for further identification. Methodological base.

In the process of the current job, the team uses the observation of the transactions of the available blockchain bitcoin resources in the blockchain. The conduction of the desktop research gives the collection of the data of the self-representation of the mentioned entities on the Internet.

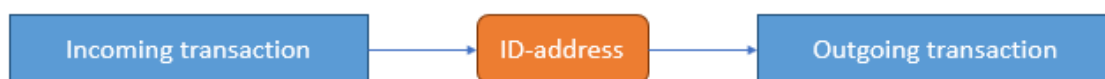
Using the risk approach based on FATF recommendations gives the possibility to execute the statements on risk evaluation. The analysis of the collected information gives the possibility to systematize the participants of the blockchain bitcoin ecosystem and to propose a kind of classification.

Results.

Technical patterns

Technical patterns
In order to describe the diversity of participants in the bitcoin blockchain environment, it is necessary to highlight the common elementary types of transactions. These types of transactions are often elements of larger structures and define specific characteristics of interactions.

Identification pattern

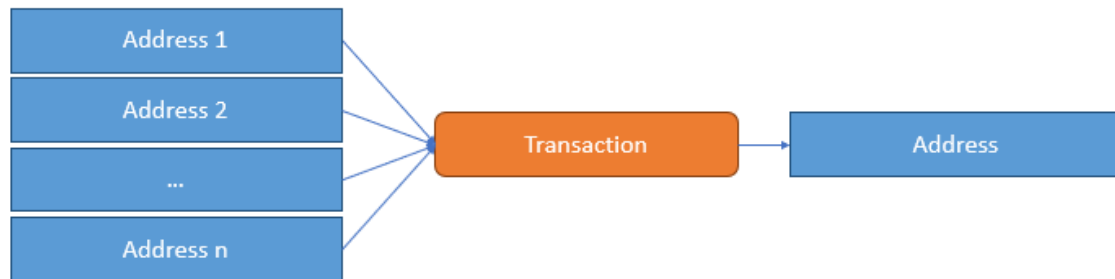


Pic 1. Identification pattern.

The primary descriptive attribute of this pattern is the fact that bitcoins are transferred to a previously unused address. This transaction is an identifier of a particular payment, after the transaction bitcoins are immediately (in one of the following blocks) formed in the next

transaction, for further work with them. It is also possible that the owner of an address has been waiting for an event and only then makes further transactions.

The pattern of a massive structure (input)

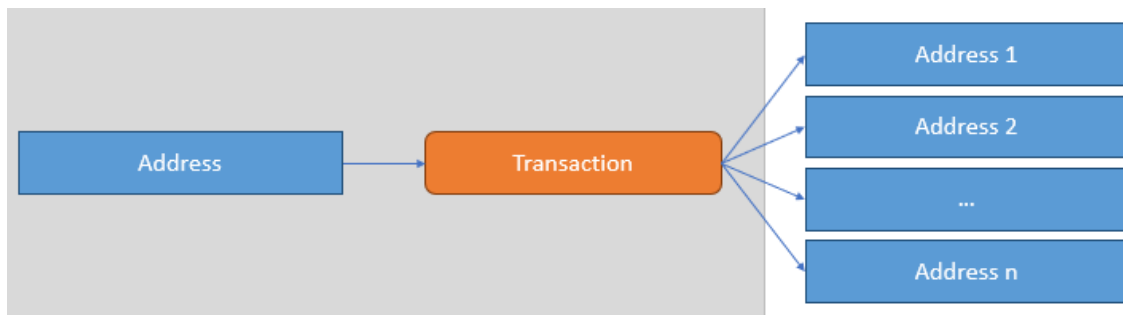


Pic 2. The pattern of a massive structure (input).

Smaller transactions from multiple wallets are collected in one for further transactions. The inputs of such a transaction number typically in

tens or hundreds, which can mean a massive infrastructure object of the blockchain.

The pattern of a massive structure (output)



Pic 3. The pattern of a massive structure (output).

One gross transaction splits into many smaller outputs. In case of exchanges, this pattern is often used to deliver bitcoins directly to end users (via a cascade of wallets or directly). Unlike the input pattern where multiple incoming addresses belong to a structure, this pattern is not absolutely mirrored because output addresses are likely to have already other owners.

as they are responsible for grouping unconfirmed transactions into new blocks and adding them to the global Ledger (Ankalkoti, 2017). They provide the necessary computing power for the blockchain by calculating a considerable amount of hashes to find a valid one for closing the next block. Each valid block added by miners to the blockchain generates a reward (Rosenfeld, 2011) for them. The difficulty they overcome in picking up a valid hash makes it difficult to attack registry reorganization and double-spend (Kroll, 2013). There are the following types of participants in the miner sector:

Infrastructure participants

At the moment there are many different participants (Bahn, 2014) in the cryptocurrency market. They can be divided into groups according to specific criteria of their behavior and functions (Lischke, 2016).

- miners
- mining pools.
- Cloud mining, which refers to fraud rather than to real economic activity.

Miners and mining pools

Miners play a crucial role in the bitcoin system

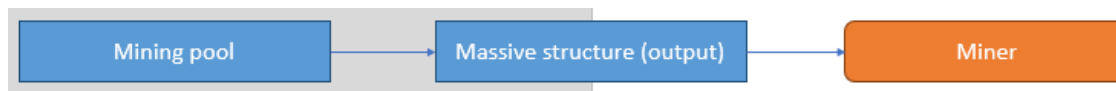
Miners

Miners are individuals and organizations that use their mining hardware for transaction processing and receiving rewards for mining and commissions. Usually, these are people and groups of people with specialized equipment (Malone, 2014).

Criteria:

- Own website: none
- The size of the deals: they get the reward for mining the block by way of the coinbase transaction of the block or now mainly through distribution such transaction inside of a mining pool;
- Work on behalf of: owners of equipment on which mine: video cards or specialized cards(ASIC)
- Miners are not usually registered in any way, although they may have legal entities necessary for the purchase of equipment, payment of electricity and payment and maintenance of premises.
- The size of assets varies over a broad

Patterns:



Pic 4. Miner pattern.

Mining pools

As the chance of mining a new block has dramatically decreased over time, miners combine in mining pools (Cong, 2018).

Mining pool is combined compute resources from many miners to increase the probability of finding a new block. After finding a new block, the reward is distributed among the pool members by the provided computing power. About 58% of mining pools are located in China.

Top mining pools in the world:

[BTC.com](#),
[Antpool](#),
[ViaBTC](#),
[Slushpool](#),
[F2pool](#),
[BTC.TOP](#),
[Poolin](#),
[Bitfury](#),
[BitClub](#),
[Dpool](#)

range, but the current bitcoin blockchain economy leads to the shutdown of small miners due to negative profitability.

Description of possible risks for AML/CFT:

Miners in the PRC were used to withdraw funds outside the PRC according to the following scheme: in the domestic market, equipment was purchased that produced bitcoins that were sold on the foreign market.

It is also necessary to understand that in any country, most miners, although not everyone need to pay for overhead costs and part of the cryptocurrency is sold on the domestic market. The source of funds is legal, because the newly mined bitcoins have not participated in any turnover, and payment transactions make up a smaller part is paid for work performed, in case miners carry out the laws of the jurisdiction where established mining equipment on payment of taxes exists.

Criteria:

- Own website: Yes
- Mining pools mine blocks much more often than individual miners, and today it is almost impossible for individual miners to mine a block.
- A commercial company
- Terms of service: an intermediary between the miners and coinbase transaction
- Size of transactions: income is distributed among the members of the pool according to put power; there are several basic approaches to income distribution option (Cryptocurrency mining, 2019).
- They receive funds from the Coinbase transaction and distribute them among miners

Description of possible risks for AML/CFT:

From an AML / CFT perspective, mining pools are a veil and at the same time they have access

to individual miners and organizations. However, again, the source of income in bitcoin mining pools as well as miners is utterly

transparent.

Patterns:



Pic 5. Mining pool pattern.

Markets

The exchange sector was the first in the cryptocurrency industry and remained the central sector in terms of the number of companies and employees. The first official exchange, the Bitcoin Market, was opened on February 6, 2010 as a project allowing users to trade bitcoins and set the market price themselves.

Centralized exchanges (CEX) are intermediaries that facilitate trading on their platform, similar to traditional stock exchanges. In exchange for providing this service, intermediaries charge a Commission for trade. Centralized exchanges often act as a point of the first contact for beginners who are interested in trading cryptocurrencies. Many of them seek to have an interface that can link to both cryptocurrency trading and real economy. Centralized exchanges provide this. Largely centralized exchanges conduct KYC and Compliance procedures (procedures for identifying and verifying the reputation of their clients) with varying degrees of care depending on the jurisdiction of the exchange.

The advantages of centralized exchanges are advanced features and tools, ease of use, high liquidity and fast transaction speed.

There are two main types of exchanges:

- the one allows you to convert Fiat money into cryptocurrency;
- The cryptocurrency exchange only for cash (C2C).

Centralized CEX exchanges Fiat/crypto:

- Bitmex (USD)
- Bithumb (Korean Wong)
- Bitfinex (USD)

- Liquid (Yen, USD)
- Coinbase, (USD)
- Bitbank (Yen)
- Bitterex (USD)
- Kraken (Eur, USD)
- Gemini (USD)
- BitStamp. (USD)Crypto/crypto:
- Binance,
- Huobi,
- Kucoin,

Criteria:

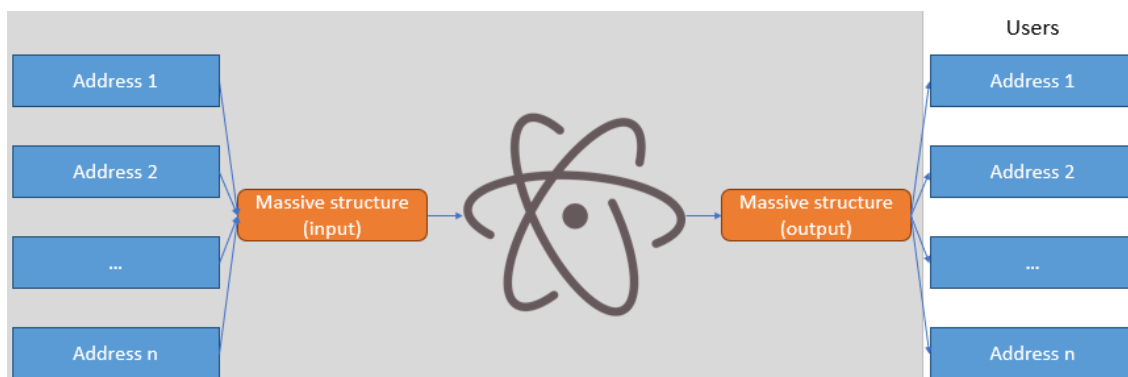
- Have their website with a developed graphical interface, graphics
- The large size of assets
- Make transactions of any size
- Identify their client
- Provision of services: users send their bitcoin to the exchange trusted storage; the exchange happens through a standard financial exchange
- Have legal registration

Description of possible risks for AML/CFT:

The risks are similar to those associated with classic exchanges, provided that the exchanges are located in different jurisdictions and have different requirements for the identification of their clients. The willingness to respond to requests depends on the jurisdiction.

At the same time, except for identification, exchanges and exchange offices are almost ideal anonymizers because the movement of transactions in them is interrupted.

It should also note that at least one-time transactions related to illegal funds of the exchange are easily missed, so it is necessary to carefully analyze the quality of work of compliance officers of the exchange by the number of "dirty bitcoins passed through them.

Patterns:

Pic 6. CEX exchange pattern.

OTC

Participants in the OTC market are investors with significant assets - crypto funds, the first buyers of bitcoin, people with significant capital. They use OTC brokers among themselves, not on exchanges. Investors in this category hold millions in bitcoin and are members of the so-called bitcoin rich list club, a list of BTC wallets with the most significant assets. In the report of the consulting company TABB, the author claims that based on surveys of industry participants, cryptocurrency trading in the OTC market can exceed the size of daily stock exchanges.

The over-the-counter market attracts participants with great liquidity-exchanges do not supply great liquidity, and a single large order on the exchange can bring down the market, so for the implementation of large lots on the exchange, it is necessary to carry out a careful and painstaking work of a professional trader to realize the volume at a reasonable price;

Examples:

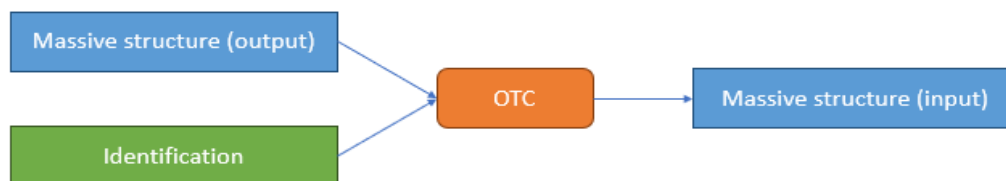
- [Circle](#)
- [OTCXN](#)
- [itBit](#)
- [HiveEx](#)

Criteria:

- Have their website
- Large transactions: conduct one-time transactions of at least \$ 100,000, the average transaction volume of \$ 1 million
- Major Asset
- Major players: private and institutional investors
- Provision of services: requires separate oral and written agreement; quotes about themselves; marketing Advisory services; broker-intermediaries; KYC compliance
- Small fees or already included in the sale and purchase price
- Not regulated by the state
- They are often at exchanges, therefore, have interaction with a large exchange structure at the transaction level
- Large transactions ~ 100 bitcoins and above

Description of possible risks for AML/CFT:

OTC desk is divided into large ones which conduct distinct KYC and are under the control of large system-forming banks. Moreover, small desks without any KYC can be accessed through friends or advertising on the Internet. Also, there is a high risk of using such structures for ML-FT schemes.

Patterns:


Pic 7. OTC market pattern.

Exchange office

Exchangers are an alternative to exchanges for retail customers who have their pros and cons (Kjaerland, 2018). The bitcoin exchange rate is often worse than on exchanges, and the spread can exceed 10%. This is because the owners of the currency set the prices, and on the exchange, prices are formed by supply/demand. In exchanges, there is not such a wide range of cryptocurrencies - usually, they work with the top 10 ones. Online exchanges allow you to change as Fiat in the crypt and the crypt to the crypt.

It should be noted that Fiat money can often be changed only to Bitcoin, Ethereum and Tether.

Exchange office ranking:

- [Ychanger](#)
- [60cek](#)
- [Trust-changer](#)
- [24xbtc](#)
- [Xchange](#)
- [F-change](#)
- [Alfacashier](#)
- [Bluecash](#)
- [Netex24](#)

Criteria:

- Have their website
- Size of transactions: small, but a lot (from 0.002 to 5 BTC)
- Average assets
- Work in retail
- Exchange offices should be registered as financial service providers, but this is not always the case.
- Services: currency exchange, a great choice of cryptocurrency, display their quotes, not quotes of participants, require mail

Description of possible risks for AML/CFT:

Exchange offices for anonymity are almost ideal points for risky schemes but have one limitation

- a small amount associated with the limits of banking operations.

Patterns:

Exchange offices are difficult to analyze, provided that the economic purpose of the user is to change to another currency, the movement within the exchanger is meaningless to analyze, it is essential to identify the boundaries using the identity of the types of addresses and the need to transfer the balance.

Aggregators of exchangers

Aggregators of exchangers collect offers of individuals, legal entities and individuals in the Board providing its users to choose with whom to make the exchange, the aggregator LocalBitcoin also performs the functions of escrow, conducting bitcoins through their addresses and being the guarantor of an honest transaction for which it takes its Commission.

- [LocalBitcoins](#)
- [Bestchange](#) site is an aggregator of data about the exchange offices and the exchange rates of cryptocurrencies. It does not participate directly in the transaction.
- [Cryptolocator](#), the website, is an aggregator of data about the exchange offices and the exchange rates of cryptocurrencies. It does not participate directly in the transaction.

Criteria:

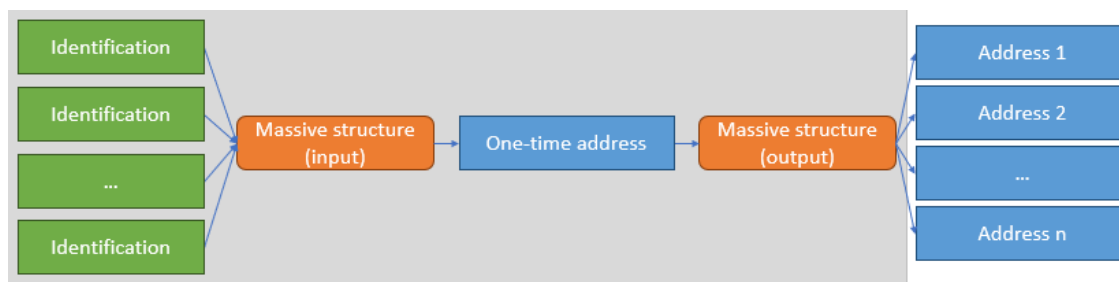
- Own site
- Deal size: small
- Major Asset
- Work for the most part with pros
- Legal registration
- Provision of services: act as a guarantor of exchange, provide information about the quotes of exchangers, provide a choice with whom to exchange, provide escrow(escrow)

Description of possible risks for AML/CFT:

Aggregators play an essential role in connecting private exchange entrepreneurs to their clients, but commonly known that the participants of the

do not follow the regulators' rules and don't pay taxes. So formally following the existing any jurisdiction legislation aggregators play a role of the framework of the grey market of cryptocurrency exchange services.

Patterns:



Pic 8. Aggregators of exchange pattern.

Discussion.

Understanding of the main participants of the bitcoin landscape is essential for further research of the social and economic behavior of the cryptocurrency industry. It gives the road signs for the navigation in the cryptocurrency world and is the ground step for the understanding of the relations of the different entities in the cryptocurrency world.

The internal structure of the leading cryptocurrency participant's types described very generally in the current paper. The request of the more detailed description for understanding the main participants still exists. Also, the current paper can be the ground for more detailed researches of every participant behavior.

The current research highlights the main, which forms serious distinguish between infrastructural participants and ordinary users. It also gives the background to review the risk of the transmitting of the toxic funds through the various types of cryptocurrencies industry participants. The main infrastructural participants' description limits the current study. Those kinds of participants form the primary landscape of the cryptocurrency operations.

Conclusion.

We have presented the main list of categories of participants in the bitcoin environment, which can be identified by type on different grounds. It

should be noted that the structure of transactions and the boundaries of ownership of private keys naturally differ from participant to participant within the same type and undoubtedly many of them require a more detailed approach in the description to highlight the boundaries and identify the ownership of addresses. At the same time, this description provides a basis for marking and further work on the risk assessment of participation in criminal activity and a basis for developing a methodology for risk infection, depending on the relationship of participants.

References

- Ankalkoti, P., & Santhosh, S. G. (2017). A Relative Study on Bitcoin Mining. *Imperial Journal of Interdisciplinary Research (IJIR)*.
- Bahn, J., Eaton A., Langone M. (2014). *THE CRYPTOECONOMY*. New York Law School, October.
- Cong, L. W., He, Z., & Li, J. (2018). Decentralized Mining in Centralized Pools. *SSRN*.
- Cryptocurrency mining. (2019). Information and analysis site. <https://mining-cryptocurrency.ru/luchshie-puly-dlya-majninga/>
- Kjærland, F., Krogstad, E., Khazal, A., Nordstrøm, F., & Oust, A. (2018). An Analysis of Bitcoin's Price Dynamics. *Journal of Risk and Financial Management*. <http://doi.org/10.3390/jrfm11040063>
- Kroll, J. A., Davey, I. C., & Felten, E. W. (2013). The Economics of Bitcoin Mining or, Bitcoin in the Presence of Adversaries. *Proceeding of WEIS*. <http://doi.org/June 11-12>.

Lischke, M., & Fabian, B. (2016). Analyzing the bitcoin network: The First Four Years. *Future Internet*. <http://doi.org/10.3390/fi8010007>
Malone, D., & O'Dwyer, K. J. (2014). Bitcoin Mining and its Energy Footprint. <http://doi.org/10.1049/cp.2014.0699>

Rosenfeld, M. (2011). Analysis of Bitcoin Pooled Mining Reward Systems. Retrieved from <https://arxiv.org/pdf/1112.4980.pdf>
Satoshi Nakamoto. (2008) Bitcoin: A peer-to-peer electronic cash system, <http://bitcoin.org/bitcoin.pdf>.