Bitcoin System

Article · June 2017
DOI: 10.18267/j.aip.97

1 author:

Jan Lansky
The University of Finance and Administration
23 PUBLICATIONS **84** CITATIONS

SEE PROFILE

Acta Informatica Pragensia, 2017, 6(1): 20–31
DOI: 10.18267/j.aip.97
Peer-reviewed paper

Bitcoin System

Jan Lánský*

Abstract

Cryptocurrency systems are purely digital and decentralized systems that use cryptographic principles to confirm transactions. Bitcoin is the first and also the most widespread cryptocurrency. The aim of this article is to introduce Bitcoin system using a language understandable also to readers without computer science education. This article captures the Bitcoin system from three perspectives: internal structure, network and users. Emphasis is placed on brief and clear definitions (system components) and their mutual relationships. A new system view of the stated terms constitutes author's own contribution.

Keywords: Bitcoin, System, Transaction, Blockchain, Network, User.

1 Introduction

Cryptocurrencies are an alternative to fiat currencies that are issued and guaranteed by individual states. Cryptocurrency systems are purely digital and decentralized systems that use cryptographic principles to confirm transactions. Transactions in cryptocurrency systems are pseudoanonymous, yet also transparent, non-refundable, fast and cheap. Cryptocurrencies usually feature a fixed, maximum monetary stock and procedure of its release into circulation.

Bitcoin (Nakamoto, 2008) is the first and also the most widespread cryptocurrency. Currently, there are more than 600 different cryptocurrencies (Coinmarketcap, 2017), majority of which is derived from Bitcoin. Cryptocurrencies become a part of life of an increasing number of people; the number of merchandizers, who accept cryptocurrencies as a payment for their goods and services, has been expanding (Chokun, 2016). Bank regulatory authorities become increasingly interested in cryptocurrencies (European Banking Authority, 2014).

Bitcoin system has no central authority to perform transaction clearing. Transactions are cleared through a decentralized network of computers; each computer is called a node. Each network node independently verifies the correctness of transactions. Transactions are included in an accounting book called blockchain, designed by Haber and Stornetta (1997). The same copy of this book is kept up to date by each network node. In order for all network nodes to agree on one form of bookkeeping, the proof of work proposed by Back (2002) is used. In the proof of work, the solution of a difficult mathematical problem, belonging to the category of NP-complete tasks, is sought. To solve the problem, a large number of calculations are needed. Verifying the correctness of the solution is easy. The entry of proof of work is a block of transactions that the node considers to be correct. The node performs a complex mathematical calculation and publishes the resulting result. The other nodes will verify that

* Department of Computer Science and Mathematics, Faculty of Economic Studies,
University of Finance and Administration, Estonská 500, 101 00 Prague 10, Czech Republic
✉ zizelevak@gmail.com

the transactions were correct, and that the mathematical calculation result is also correct. At this point, transactions from the block become part of the accounting book. The node that made the correct calculation will receive a reward in the form of transaction fees and coins newly put into circulation.

Cryptocurrencies are a new issue, which is also very complex. To fully understand cryptocurrencies, one needs an extensive knowledge of computer science (cryptography and information security, algorithms and data structures, computer networks), finance and economics. University of Nicosia (2015) teaches masters degree programme focused exclusively on cryptocurrencies, which evidences how highly complex the issue of cryptocurrencies really is.

To understand the functioning of cryptocurrency systems it is necessary to study relevant literature. Currently, the articles on cryptocurrency require knowledge of computer science. As an alternative one can review books, which are designed also for general public. The disadvantage with respect to books is the amount of time one needs to study their contents, which can discourage many new users.

Article "Bitcoin: A Peer-to-Peer Electronic Cash System" (Nakamoto, 2008) contains a description of data structures and algorithms used for basic functioning of the Bitcoin system. The article uses terminology from the field of computer science and we cannot recommend it to cryptocurrency users - beginners. The book "Mastering Bitcoin: Unlocking Digital Cryptocurrencies" (Antonopoulos, 2014) begins with an explanation of the Bitcoin system's functions by practical examples and gradually transitions into implementation details. The book can be recommended to users-beginners and computer science professionals. The book "Bitcoin and Cryptocurrency Technologies" (Narayanan et. al., 2016) is a university textbook, contains mathematical definitions and implementation details, but does not contain the same depth of analysis as the previous book. The book "Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money" (Popper, 2015) deals with history of the Bitcoin system. The book's plot is composed of memories of important people who created this system. The book, however, does not get into details regarding the Bitcoin system's functionality.

The aim of this article is to introduce the Bitcoin system using a language understandable also to readers without computer science education. This article captures the Bitcoin system from three perspectives: internal structure, network and users. Each perspective is depicted in its own Figure. Emphasis is placed on definitions of terms (system components) and their mutual relations given the absence of clear and concise definition in the existing literature. New terms are defined using only the terms defined previously. The goal is to briefly describe the terms while maintaining their clarity. As a source of information, we use the book Mastering Bitcoin (Antonopoulos, 2014), but the concepts are defined in different ways. A new systemic view of the concepts presented constitutes the author's own contribution. A systemic approach ensues from the traditional concept of a system.

View of the internal structure of the Bitcoin system describes the whole process of executing transaction. We deliberately conceal the existence of data structures (*e.g.* Merkle Tree), for the understanding of which we would require knowledge of computer science. A network view represents different types of nods, their functions, and limitations. A user view deals with possible users' roles within the Bitcoin system.

2 Internal Structure of the Bitcoin system

On the basis of a systemic approach internal structure of Bitcoin system can be identified with basic concepts: bitcoin, satoshi, private key, owner, address, multisig address, transaction, input, output, UTXO, transaction fee, common transaction, aggregating transaction, distributing transaction, block, verified transaction, mining, nonce, hash, coinbase transaction, blockchain.

Bitcoin is a monetary unit of the Bitcoin system. Bitcoin exchange rate against the US dollar is 1 BTC = 1800 USD (14th May 2017), see Coinmarketcap (2017). The total maximum number of Bitcoins in circulation is fixed and amounts to 21 million, which will be achieved in 2140. The current number of Bitcoins in circulation is 16.1 million, see Coinmarketcap (2017). Similarly as dollars are divided into smaller units - cents - Bitcoins are divided into smaller units - satoshi. One Bitcoin is made of hundred million satoshi. Writing about the currency amounts expressed in Bitcoins in the article, we do not usually mean entire Bitcoins, but an amount rounded up with a precision to individual satoshi.

Private key is a 256-bit random number. Private key can be created, for example, by means of a coin, paper and pencil. Gradually, we toss a coin 256 times and write the results of individual coin tosses on a piece of paper. If you get a reverse (tails), write 1 bit, if you get an obverse (heads), write 0 bit. In practice, private keys are created by software using cryptographically secure pseudo-random number generator (CSPRNG), for example, by means of ISAAC designed by Jenkins (1996). Private key so created can not be possibly derived by a potential attacker, nor can be deduced the rest of the key from knowledge of the part of the key. Private key is used to prove ownership of Bitcoin. Imagine the private key as a specimen signature at bank.

Owner is a person who knows a private key. Only one person should know each private key. This person may dispose of Bitcoins, the property of which he/she proves using the private key. If more people know the private key, it is impossible to distinguish, which of them disposed of Bitcoins. The situation, where more persons know the private key, occurs rarely in practice; most often an attacker, who lured the owner to revealing the private key, is the other person. In case of obtaining a private key by an attacker, an owner and attacker cannot be distinguished from each other, which an attacker usually uses to steal Bitcoins. If the owner forgets the private key, or medium, on which the owner has stored the private key, is destroyed, it can no longer prove ownership of respective Bitcoins and these are irrevocably and forever lost; no one can dispose of these Bitcoins.

Address is usually derived from one private key using complicated mathematics method called elliptic curve cryptography using secp256k1 standard created by Certicom Research (2010). The derivation process is a one-way process; the private key cannot be recovered from the address, which is important for security. The owner of the private key disposes of Bitcoins stored at this address. Imagine the address as a bank account number and Bitcoins as funds on this account. Multisig addresses are special types of addresses that are derived from *k* private keys. The consent of owners holding at least *n* private keys is necessary for the disposal of Bitcoins stored at this address. The $n \leq k$ condition applies. The most common type of multisig addresses are 1 of 2, whereas at least one of the two owners of the respective private keys has to give consent with the disposal of Bitcoins stored at this address.

Transaction transfers transaction inputs owned by Bitcoins in favour of transaction outputs. Each transaction output consists of a pair - address and Bitcoin amount - transferred in favour of this address. The transaction output can be used as an input to another transaction, but can

be used at most once. The transaction output, which has not been so far used as an input to another transaction, is called unspent transaction output, abbreviated as UTXO. The transaction shall be signed by owners of private keys of all addresses forming transactional inputs. The owners thereby express their consent with the transfer of Bitcoins they own in favour of the transaction output. If it were a bank transaction, this moment would correspond to giving instructions to the bank to execute transaction.

The sum of Bitcoins transferred in favour of the outputs of a given transaction decreased by the sum of Bitcoins owned by the inputs of this transaction is called a transaction fee. The amount of the transaction fee is not fixed; it can be set up by owners of private keys from the addresses forming transactional inputs. The transactional fee cannot be negative; the transaction cannot spend more Bitcoins than what has been entered in the transaction. Transaction fee may be zero, but with the increasing amount of the transaction fee the transaction will be processed sooner by the Bitcoin system. If the fee is lower, on the contrary, there is a possibility that the transaction will never be processed.

Transactions in the Bitcoin system are more complicated than banking transactions; they are more similar to transactions with gold. Transactional inputs and outputs correspond to pieces of gold, which their owner melted and casted pieces of gold of different sizes from them. Each transaction input must be spent entirely within a transaction, by the same token, the entire piece of gold shall be used after melting.

In practice, three types of transactions occur most frequently: common, aggregating funds and distributing funds. The common transaction is an equivalent to a standard transaction with a retailer when the customer pays with a banknote and a retailer returns a change. Banknote as well as transactional input must be spent entirely. The common transaction has one input and two outputs. Input corresponds to a banknote payment; one output falls upon a merchandizer; the second output is a refund of change to a customer. Aggregating funds have many inputs and one output. It is similar to exchanging many small coins for one banknote. Distributing funds have one input and many outputs; it is used for mass payments to many recipients, for example, in case of payment of wages to employees.

Block contains transactions. Block of a maximum 1MB permit usually contains 1000-2000 transactions depending on the size of these transactions. Transactions for inclusion in the block are selected from pending signed transactions. Transactions with the highest value of transaction fee divided by the data size of the transaction are classified in the block. The transaction fee value is not dependent on the transaction value. In case of common transactions with the size of about 0.25 kB the fee is about 10,000 satoshi, see Blockchain.info (2017). Big transactions with many inputs and outputs must pay a much higher fee than common transactions. The transaction included in the block is called verified. In case of bank transaction this moment would correspond to its execution by a bank.

A block is formed during the process called mining. During mining it is necessary to perform a large number of mathematical operations. First, a candidate block is created from the available transactions. A hash function is applied to this candidate block to create a 256-bit number called hash. There is a requirement for this hash to contain a value of zero on a given number of first bits. The required number of zeros is dynamically adjusted so that the right solution in the entire Bitcoin system is found on average once every 10 minutes, regardless of how much the computing power of the entire Bitcoin system is growing. The block is considered to be mined, if its hash starts with the required number of zeros. If the candidate block has not been mined, it is necessary to modify its content slightly, re-count the hash. We modify this block until we get a hash that fulfils the condition for an initial zero. Changing the

contents of the block is done by changing two 32-bit numbers called nonce. Because of the hash function properties, a small change in the block leads to a completely different hash.

Each block contains one special transaction called coinbase, which has no inputs. This transaction is a reward for a successfully mined block. Mining is important for achieving consensus in the Bitcoin system; thus, its performance is motivated by a reward for its successful implementation. Through coinbase transactions new Bitcoins contribute to the Bitcoin system according to the predetermined schedule. The amount of remuneration begins at 50 BTC and every four years decreases to half; currently it amounts to 12.5 BTC. Besides the predetermined reward for the mined block the coinbase transaction contains variable fees for all transactions that the block contains.

Blockchain is a sequence of blocks, which extends with each mined block. Each block includes a hash of the previous block; the sequence of blocks leads to the genesis of a block, which is the first block of a blockchain. This sequence of hashes ensures it is impossible to change the contents of any of the previous block without altering the contents of all subsequent blocks. Due to the high computational cost of block mining it is realistically possible to change just one or two blocks that have been created most recently; older blocks, however, are no longer immutable. According Blockchain.info server (2017), blockchain has about 450,000 blocks and about 100 gigabytes of disk space is required to save it.

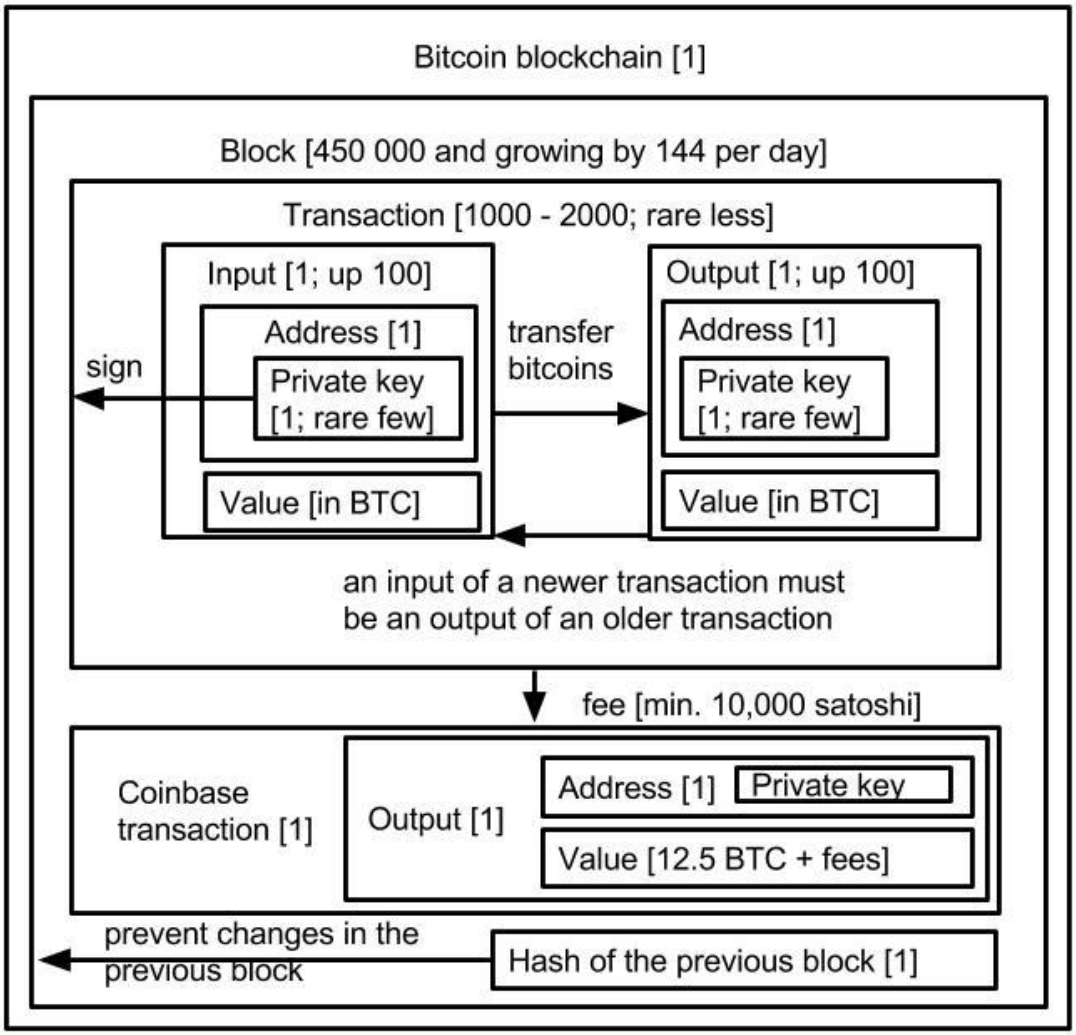

Figure 1. *Internal structure of the Bitcoin system. Source: Author's own.*

The internal structure of the Bitcoin system is captured in a simplified way in Figure 1. Blockchain consists of a chain of blocks linked together via a hash of the previous block. The blocks consist of transactions. Transaction shifts Bitcoins from inputs in favour of outputs. Transaction input is an output of a previous transaction. The transaction output contains address of the transaction and the amount in Bitcoins. Transaction shall be signed by the owners of private keys for all transaction inputs. There is usually one private key for the address, but, theoretically, there may be more. Each block has a special coinbase transaction that has no input; it has only output. Coinbase transaction is a reward for a successfully mined block.

3 Structure of the Bitcoin Network

The structure of Bitcoin network can be based on a system approach identified with basic concepts: full node, full wallet, lightweight wallet, solo miner, mining pool, pool mining administrator and a pool miner.

Full node contains a full copy of blockchain performance and verifies its accuracy. This copy of blockchain is updated based on new information about the transactions and blocks. It obtains new information from its neighbouring nodes and by algorithm waves spreads this new information to all remaining neighbouring nodes (from which the information has not been received). This mechanism ensures rapid expansion of new information throughout the entire network. The Bitcoin network consists of over 5000 full nodes according NodeCounter (2017). Full nodes are a backbone of the Bitcoin network, the high number of which ensures security and independence.

Full wallet is a type of full node, which additionally offers also service of creation and storage of private keys and addresses derived therefrom. It enables you to create and sign transactions. Lightweight wallet is a type of node that similarly as a full wallet offers creation of private keys, addresses and transactions, but unlike a full wallet does not offer a full node services. From blockchain it stores only small parts of each block, the so-called headers. If necessary, it collects information about the transactions requested from full network nodes by asking questions using the Simplified Payment Verification (SPV) protocol. The advantage of a lightweight wallet is less demand on used disk space, several tens of MB instead of 100 GB needed to run a full wallet. The disadvantage of a lightweight wallet is the necessity to rely on the accuracy of information derived from its neighbouring nodes and the inability to independently verify this information. While there are thousands of full wallets, there are tens of millions of lightweight wallets, see Blockchain.info (2017).

Solo miner is a type of full node, which, in addition, also tries to mine blocks. From its neighbouring nodes it acquires new transactions, verifies their accuracy, assembles blocks from them, in which he tries different nonce values. It attempts to find such a block whose hash meets the condition for inclusion of a block into blockchain. In case of success it obtains a reward in the form of coinbase transaction. The process of block mining is affected by a coincidence. With the increasing computing power of the Bitcoin system it is currently extremely unlikely for a solo miner to independently mine a block.

Mining pools constitute an alternative to a solo mining. Currently, there are 20 mining pools, which are able to mine at least one block per day, see Blockchain.info (2017). In the mining pool, there is one node called a mining pool administrator and usually several thousands of nodes called pool miners. The oldest mining pool in the world Slushpool (2017) has nearly 5,000 active pool miners. The mining administrator must run a full node similarly as a solo miner. Similarly as a sole miner it compiles blocks. The pool miners then look for the right

nonce, for which the block hash will meet the inclusion into blockchain. Pool mining administrator monitors the amount of work done by individual pool miners and accordingly distributes them rewards from coinbase transactions that the mining pool received for the mined blocks. For pool miners, regularity of smaller payments corresponding to the work done by it is an advantage over solo mining when it would receive one large payment for many decades. The pool miners also need not run the full nodes, which is another advantage.

The Bitcoin network is shown in Figure 2. Foundations of the network consist of full nodes that accept new transactions and blocks, verify them and spread them among the other full nodes. Full wallet is an extension of full node by the service of private keys and addresses management. Lightweight wallet offers also private keys and addresses management, but if necessary, it must obtain relevant transactions from full nodes by asking questions. Solo miner is an extension of the full node by the possibility of building new blocks and receive rewards for their mining. Pool mining administrator also compiles new blocks, but delegates the actual process of mining to pool miners who belong to the mining pool.

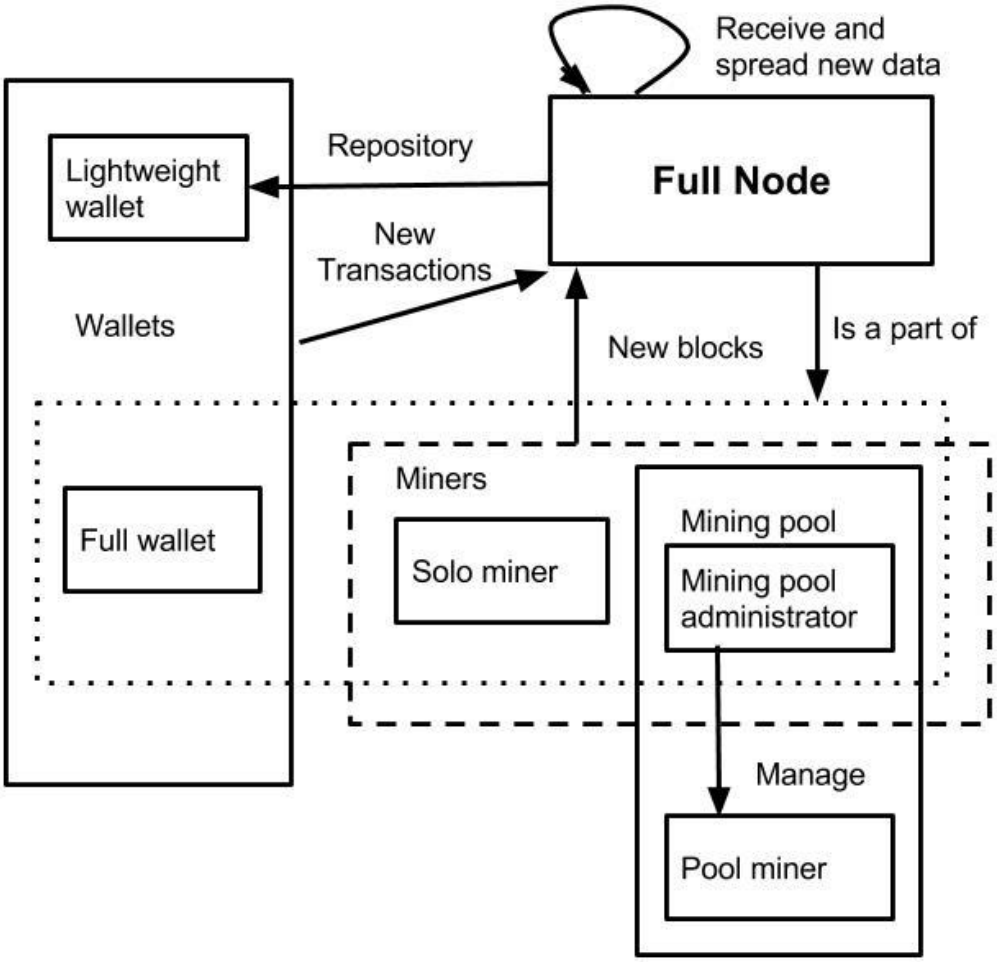

Figure 2. *Bitcoin network. Source: Author's own.*

4 Structure of the Bitcoin System Users

The structure of Bitcoin system users can be based on a systemic approach identified with basic concepts: Bitcoin user, propagator, developer, merchandizer, exchange, customer, miner and investor.

Bitcoin user can be distinguished by roles they assume in the Bitcoin system; one user can hold multiple roles. Individual roles are usually held by several thousand users, of which several dozens have a major say in the given role. Two roles that in their unification include almost all Bitcoin users are an exception. For individual groups estimates of the number of users are given. If data is missing for a given source, it was created by the authors of this article based on their own experience gained from many years of newsgroups and community websites studying.

Propagators expand awareness of the Bitcoin system and its advantages compared to fiat currencies. By its effect on general population the Bitcoin system obtains additional users. There are tens of propagators at the global level; in particular, we will mention two of them. Andreas M. Antonopoulos became famous, among others, as an author of the book Mastering Bitcoin, see Antonopoulos (2014). Roger Ver is known under a nickname Bitcoin Jesus. Thousands more propagators are active at the level of individual states or smaller units, for example cities. The authors of this article estimated the number of propagators on the basis of their own experience gained by studying discussion groups and community websites.

Developers create software that is used by other users for their activities in the Bitcoin system. The most influential group is 15 Bitcoin Core Developers (2017), which is the most widespread software for operating a full node. Additional thousands of developers create software for lightweight wallets, group mining and various commercial applications using Bitcoin.

Merchandisers offer their customers the option to pay for goods and services using Bitcoin, or possibly they offer their employees the opportunity to receive payments in Bitcoin. There are more than 8,000 stores worldwide accepting Bitcoins, see Coinmap (2017). In addition to Bitcoins these stores accept also their national currencies. One of the exceptions is a cafe in Paralelni Polis (2017), Prague, Czech Republic, which does not accept payments in national fiat currency - Czech crown, but only in Bitcoins. In addition, there are estimated tens of thousands of web shops where you can pay by Bitcoins. Overview of several tens of major companies accepting Bitcoins during online payments is provided by Chokun (2016). According to this report, you can make a purchase with Bitcoin, for example, even in Windows store.

Exchanges intermediate an exchange of Bitcoin for fiat currency or other cryptocurrencies. There are approximately 100 online exchanges that every day trade Bitcoins worth hundreds of millions of dollars. In the biggest exchange Bitfinex about 20% of volume of all transactions is conducted, see Coinmarketcap (2017). Regular (currency) exchanges are also important due to their availability. Bitcoins and fiat currencies can be mutually exchanged at more than 35,000 exchange offices and in 1000 ATMs, see Bitcoin ATM Map (2017).

Customers use Bitcoins for purchasing goods and services, or possibly obtain Bitcoins as a reward for their work. Most Bitcoin customers use Bitcoins as a supplement and carry out the vast majority of payment transactions in fiat currencies. It is difficult to estimate of the size of this group. The largest provider of lightweight wallets Blockchain.info (2017) reports that it manages over ten million accounts. The question is how many of these accounts are active so they could be described as customer accounts. Because of pseudo-anonymity, it is also not

recognizable if one owner owns multiple accounts. Data from Bitcoin exchange called Bitstamp (2016), which states that it has over half a million registered customers, provides a better estimate. This exchange according to Coinmarketcap (2017) has about 7% share in the market with exchanges. The number of customers can be estimated to be around several million people, of whom an estimated hundreds of thousands are regular customers.

Miners utilize a computing power of its specialized hardware devices to create new network blocks and as a reward they receive rewards in the form of coins newly put into circulation and transaction fees. In the early years of the Bitcoin system's existence it was possible to operate mining also on personal computers. There are approximately tens of thousands of Bitcoin miners. We have made this estimate on the basis of the 5000 miners in the mining pool Slushpool (2017) and the share of this group in mining performance of the entire Bitcoin system, which is 7.3% according Blockchain.info (2017).

Investors hope that the price of Bitcoin against fiat currencies will rise and, to this end, they will keep a part of their savings in Bitcoin. The number of investors is the same as the number of customers, that is millions. A large number of customers are primarily investors who occasionally become customers.

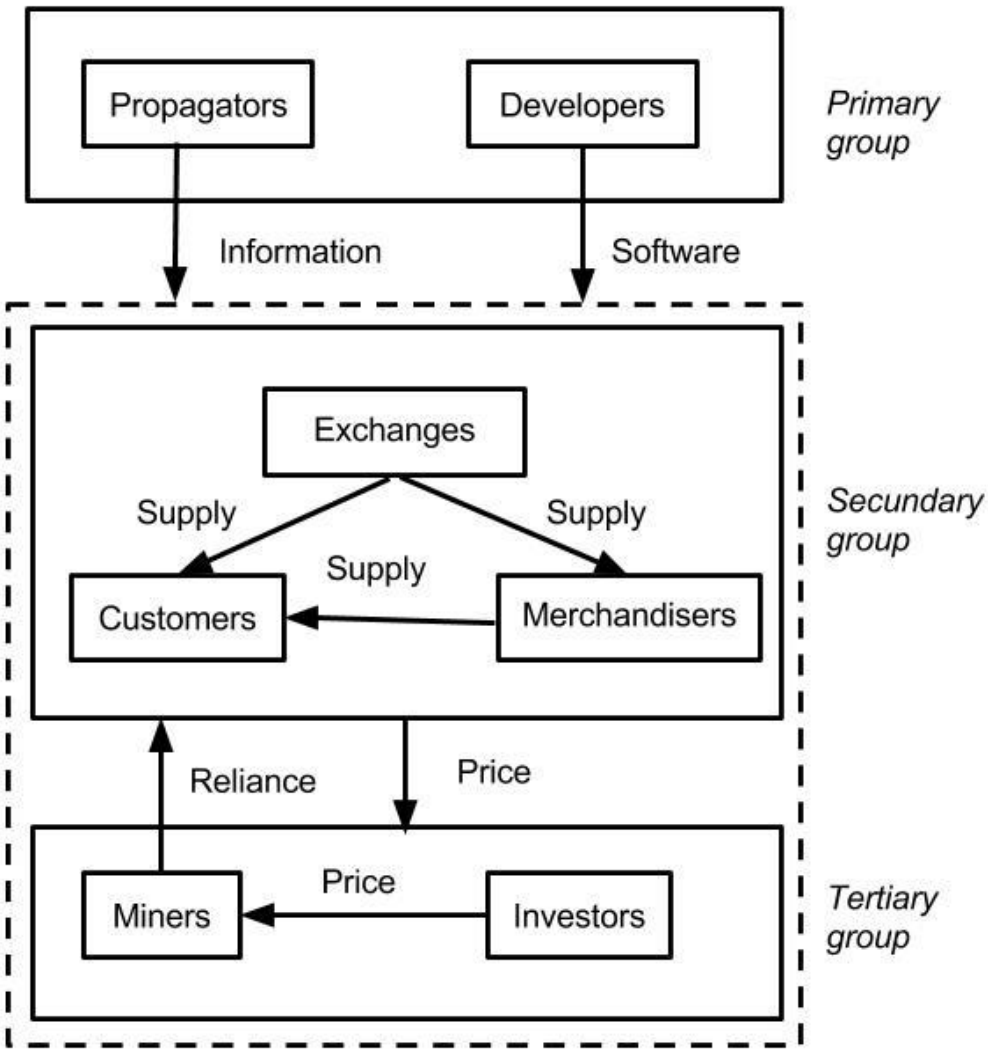

Figure 3. *Users of the Bitcoin system. Source: Author's own.*

The types of users in the Bitcoin network and their mutual relationships are shown in Figure 3. We have divided the types of users into three groups: primary, secondary and tertiary. Propagators and developers form the primary group. The primary group most influences the future direction of cryptocurrency and its effects lead to an increase in the number of users in other groups. Propagators through public education acquire new users of the Bitcoin system and with the existing users increase the level of their involvement. Developers create software that enables the users to work with the Bitcoin system. The secondary group is made of customers, merchandizers, and exchanges. Merchandizers make an offer for goods and services, for which customers can pay in Bitcoins. Exchanges offer merchandizers and customers the possibility of Bitcoin exchange for fiat currencies. The secondary group affects the growth in Bitcoin value, leading to a growth in the number of users in the tertiary group. Tertiary group comprises miners and investors. By performing a large number of mathematical calculations miners ensure the stability of the Bitcoin system and in return they acquire newly introduced Bitcoin into circulation and transaction fees. Investors believe in the long-term growth in Bitcoin value, they withdraw Bitcoins from the market and, thus, increase their cost.

5 Discussion

In the previous three chapters, we have presented three views of the Bitcoin system. In each view, we have identified system components and their mutual relationships. Within the discussion we will be seeking publications relating to individual relationships and identify the types of relationships that are yet to be solved in literature.

In the internal structure of the Bitcoin system their quantity was also provided with respect to some components and relationships. For example, one block contains on average 1000 - 2000 transactions and one coinbase transaction. Blockchain includes about 450,000 units. Numerical relationships between the components of the Bitcoin system are well analysed by publicly available servers, *e.g.* Blockchain.info (2017).

Miners are trying to mine new blocks and compete for reward for newly mined blocks. Due to the high value of this reward the competition is tough, which is widely documented in scientific literature. Vilim et. al. (2016) deals with hardware for mining, which does not calculate hashes flawlessly, but admits that some hash calculations will be flawed. This hardware improves earnings from mining by 30%. O'Dwyer and Malone (2014) deal with environmental aspects of miners' competition. Cocco and Marchesi, M. (2016) deal with economic modelling of mining in the Bitcoin system. Eyal and Sirer (2014) deal with the reliability of mining and warn that the Bitcoin system is vulnerable if the proportion of unfair miners exceeds 1/3.

Current scientific articles are also interested in the development of cryptocurrency prices and factors that influence this development. Lansky (2016) analyses, which cryptocurrencies have historically reached the largest price decreases and increases. Smith (2016) deals with the possibility that the price of Bitcoin is manipulated by a narrow group of speculators. Kancs et. al. (2015) deal with the question of whether Bitcoin performs the function of currency and, subsequently, analyse the factors affecting its price. Similarly as in the previous study, some price fluctuations cannot be explained without the influence of speculators.

In literature, by contrast, the issue of development of the number of Bitcoin network users and the factors that influence this development are not solved. How successful are the propagators and developers of software in attracting new users? How high is a proportion of investors

among Bitcoin holders? What is Bitcoin volume of customers' transactions with merchandizers? How often do customers purchase in Bitcoin?

6 Conclusion

This article introduces and provides closer account of the Bitcoin system and the relationships between its individual components to those newly interested in cryptocurrency. The issue of cryptocurrency is difficult in terms of input knowledge from many fields of science; this article, however, does not assume any input knowledge. The advantage of this article as compared to books is the clarity and brevity of definitions. In deriving new terms only the already defined terms are strictly used. New terms are not defined by means of terms, which will be defined later. A new system view of these terms is the author's own.

We have introduced the Bitcoin system from three perspectives. The first view is in terms of its internal structure. We have explained how transactions look and how they are organized in blocks and blockchain. The second view dealt with nodes of the Bitcoin network, their types, and their mutual relationships. Full nodes, wallet nodes and mining nodes were major nodes. A third view dealt with various types of users of Bitcoin network.

In the discussion, we have elaborated on available scientific literature with respect to certain relationships between the individual components of the Bitcoin system and drawn attention to topics that are not covered in literature.

Acknowledgement

This research was supported by the Czech Science Foundation as part of the project *New Sources of Systemic Risk on Financial Markets* (GA ČR 16-21506S).

References

Antonopoulos, A. M. (2014). *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. Sebastopol: O'Reilly Media.

Back, A. (2002). *Hashcash - A Denial of Service Counter-Measure*. Retrieved from http://www.hashcash.org/papers/hashcash.pdf

Bitcoin Core Developers. (2017). *Bitcoin Core Team*. Retrieved from https://bitcoincore.org/en/team/

Blockchain.info (2017). *Bitcoin Charts & Graphs*. Retrieved from https://blockchain.info/charts

Certicom Research. (2010). *Standards for Efficient Cryptography, SEC 2: Recommended Elliptic Curve Domain Parameters, Version 2.0*. Retrieved from http://www.secg.org/sec2-v2.pdf

Bitcoin ATM Map. (2017). *Find Bitcoin ATM, Online Rates*. Retrieved from https://coinatmradar.com/

Bitstamp. (2016). *BitStamp 1st Video 40 45.* Retrieved from https://www.youtube.com/watch?v=WHFhgSRTprA&feature=youtu.be

Cocco, L., & Marchesi, M. (2016). Modeling and Simulation of the Economics of Mining in the Bitcoin Market. *PLoS ONE*, 11(10),1–46. doi: 10.1371/journal.pone.0164603

Chokun, J. (2016). *Who Accepts Bitcoins as Payment List of Companies*. Retrieved from https://99bitcoins.com/who-accepts-bitcoins-payment-companies-stores-take-bitcoins/

Coinmap. (2017). *Map of Bitcoin accepting venues.* Retrieved from https://coinmap.org/#/world/64.09140752/-31.28906250/2

Coinmarketcap. (2017). *Crypto-Currency Market Capitalizations.* Retrieved from http://coinmarketcap.com/

Eyal. I, & Sirer, E. G. (2014). *Majority is not Enough: Bitcoin Mining is Vulnerable*. In Proceedings of the Financial Cryptography and Data Security conference (pp. 1–18). Retrieved from http://fc14.ifca.ai/papers/fc14_submission_82.pdf

European Banking Authority. (2014). *EBA Opinion on virtual currencies, EBA/Op/2014/08*. Retrieved from https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf

Haber, S. & Stornetta, W. S. (1997). Secure names for bitstrings. In: *Proceedings of the 4th ACM Conference on Computer and Communication Security* (pp. 28–35). New York: ACM. doi: 10.1145/266420.266430

Jenkins, R. J. Jr. (1996). ISAAC. In *Fast Software Encryption* (pp. 41–49). Berlin: Springer. doi: 10.1007/3-540-60865-6_41

Kancs, d'A., Ciaian, P., & Rajcaniova, M. (2015). *The Digital Agenda of Virtual Currencies: Can BitCoin Become a Global Currency? Report EUR 27397 EN*. Brussels: European Commission.

Lansky, J. (2016). Analysis of Cryptocurrencies Price Development. *Acta Informatica Pragensia,* 5(2), 118-137. doi: 10.18267/j.aip.89

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved from: https://bitcoin.org/bitcoin.pdf

NodeCounter. (2017). *Bitcoin Classic, XT, Unlimited Nodes, Blocks, Graphs, Charts, Statistics.* Retrieved from: http://xtnodes.com/#all_nodes

O'Dwyer, K. J., & Malone, D. (2014). Bitcoin Mining and its Energy Footprint. In *Proceedings of the 25th Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies* (pp. 280–285). New York: IEEE. doi: 10.1049/cp.2014.0699

Paralelni Polis. (2017). *Bitcoin Coffee - Paralelní Polis.* Retrieved from: https://www.paralelnipolis.cz/koncepty/bitcoin-coffee-en/

Popper, N. (2015). *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money*. New York: Harper.

Slushpool. (2017). *Statistiky – slushpool.com.* Retrieved from: https://slushpool.com/stats/

Smith, J. (2016). *An Analysis of Bitcoin Exchange Rates*. SSRN. Retrieved from: https://ssrn.com/abstract=2493797

University of Nicosia. (2015). MSc in Digital Currency. Retrieved from: http://digitalcurrency.unic.ac.cy/

Vilim, M., Duwe, H., & Kumar, R. (2016). Approximate Bitcoin Mining. In *The Proceedings of the 53rd Annual Design Automation Conference* (article no. 97). New York: ACM. doi: 10.1145/2897937.2897988