Cryptoeconomics

Dajsinani, Madrid
RezzyTech Inc.

***Abstract*—Bitcoin is the most used cryptocurrency in the world, which revolutionize our financial and monetary system. The main characteristic of any modern cryptocurrency is their decentralized nature, where one party can send money to anther party without going through a central institution control. The real challenge in decentralized peer-to-peer system is the avoidance of central authority, one must expect that there will be bad participants hoping to disrupt the network. Cryptoeconomics is the combination of two disciplines: cryptography and economics. They contribute to create a robust distributed peer-to-peer networks that flourish over time regardless of endeavoring to disrupt them. Cryptography technologies are used to provide a secure peer-to-peer communication within network and economics incentives to motivate all participants to contribute to the network.**

Contents

1. Introduction

The world of cryptocurrency started in 2008, where a pseudonym person named himself Satoshi Nakamoto published a white paper about Bitcoin. It is a system that is totally decentralized peer-to-peer version of a cash-system, where one party can transfer money to another party without the permission or going through a central financial authority. Some time after the publication of Bitcoin white paper, it took the attention of traders, investors and developers, that wanted to sell it, buy it or invest on it. The underlying concept behind any cryptocurrency is Cryptoeconomics, which is the combination of cryptography and economics. The combination of these two has formed a new way of storing and interaction with data. This paper describe the function and problem of our traditional monetary system and how cryptocurrency try to solve those problems with combination of mathematics and computer science.

2. Fiat Currency

2.1. Definition

Fiat money has made appearance on the world economic scene on several occasions but it was not until the beginning of the 20th century that its universal application became a topic of serious debates [6]. By this period, most nations already had a government monopoly on printing money, which were to be redeemed in gold upon request [6]. Fiat money is the most utilized money around the globe. It is a kind of cash that enables us to purchase things when there are required or a demand emerges. Fiat money is currency that money play the role as a storage medium [7] and a substitute for the barter [19]. The government has accept it for payment of taxes and debt, therefore fiat money has value, so it is a declared currency from government to be a legal tender. It is the opposite of commodity money that is backed by valuable commodity which means fiat money is not backed or guaranteed by a physical commodity like silver or gold.

2.2. Central Banks

Central bank is a financial institution, that managed and administrate the operations of the banking system. It has many several functions like controlling of country's monetary policy [17], monitoring and maintaining the value of currency to ensure price and financial stability, serving as a last-resort lender [14] to other banks and acting as government's bank [9]. It also regulates the flow of credit, since the creation of loans by other banks, the supply of money can be diminished or inflated, which can have a negative impact on the supply of money. Monetary policy enforced by a central bank is used in general to influence the economic activity and control inflation [9].

Central bank is an independent authority, that means there is no political influence on its policy, but in reality that is not always the case [9].

2.3. Commercial Banks

A commercial bank is a financial institution that is also part of our banking system, which has a direct interaction with the general public. It is part of money distribution by offering various financial services to general public, businesses and companies. Accepting credit is one of prime function, but it also grant loans and provides financial service to customers [10]. The bank earns profit by paying interest at a low rate to the depositors and charges a higher rate of interest to the borrowers [10]. To operate within our banking system, commercial banks must act according to certain rules, which are set by central bank. In this way commercial banks operate under the supervision of the central bank [10].

2.4. The Problems with Fiat Currency

One of the major risk of fiat currency is the confidence that people have in the currency and in the authority backing it. But there have been many cases in different countries that a financial situation like hyperinflation or inflation destroying this faith of national currency. Hyperinflation is a financial situation, where prices of goods and services rise every day or month. The most recent episode of Hyperinflation is Venezuela. Venezuela's economy and the value of the Venezuela's currency, the Bolivar, are heavily dependent on exports. Oil comprises 95% Venezuela's exports and 25% of its gross domestic product (GDP), so high prices provide a boom to the country's economy [11]. The government used that earning to pay social programs to fight against poverty and inequality [21]. At the end of 2014 the oil price collapsed, which also put the Venezuelan economy in crisis. In this situation the government has to spend more money than they accrue from taxes and other income streams like oil exports, by their own power, they print money for their needs and put into economy [21]. Because this money is not backed and not limited the process of printing is not expensive, its cheap. The effect of printing more money is the decrease in value of money already in circulation.

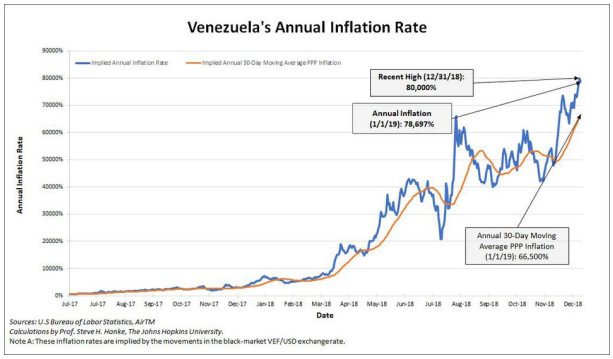

Figure 1. Venezuela's Annual Inflation Rate [**SpecialT31:online**]

The figure 1 shows the annual inflation rate of Venezuela, which is the highest inflation rate. This situation comes from bad decisions of government and financial authorities like: economic mismanagement, corruption of high level and absence of central bank independence [21]. In a hyperinflation case the faith, confidence and trust between people and government or financial authority are destroyed, which make the money no more valuable and worthless. Due to no more worthy currency people try to exchange Bolivar with another stable currency like dollar. It means, the government and central bank make the currency Bolivar worthless and useless. That differs from currency backed by gold it is that it has value because of the demand for gold and its scarcity. Generally speaking, governments have created monetary systems that allow them to manipulate the supply of their country's money, assuring its value is backed by their word that it will always be worth something causing price instability and increases economic volatility.

3. Cryptocurrency

3.1. Principles

History has shown us that crises in the financial and banking system occur all over the world. The occurrence of this situation, these financial institutions should be rescued from their government, therefore they arise indirectly from taxpayer's money. With time and the lessons of financial crises, it becomes increasingly clear that our financial system is not only unstable, insecure, unbelievable and fragile, but perhaps also flawed. As a result of these problems in our monetary system, the research and interest aroused in cryptographic technology, the creation of an alternative currency has turned from deep dissatisfaction with traditional banks and financial institutions. Cryptocurrency is a digital currency, which is based on cryptic protocols. These protocols are built on the principles of mathematics and computer engineering that practically makes it difficult or impossible to duplicate either falsification of currency and transactions. One of the main features of cryptocurrencies is avoiding control of one central authority, meaning decentralization of the system. The decentralized nature of blockchain make cryptocurrency immune to the old way of government control and interference. Most digital currencies mask the identity of the user, making it difficult to attribute transactions to specific persons or groups. The first decentralized digital currency that allowed money to be transferred to anyone and anywhere in the world is Bitcoin [18]. It is a system that uses peer-to-peer technology in order to operate without having a control center. Transaction management, currency security and other tasks are collectively managed by the network [18]. Cryptocurrencies facilitate the execution of transactions by simplifying transfers through the use of public and private keys for security and privacy purposes [18]. These transfers can be made with minimal processing fees, allowing users to avoid the high fees of traditional financial institutions [18].

Figure 2 shows the comparison of transaction processes between traditional fiat currency and cryptocurrency. Fiat currencies (banknotes or coins) are usually government-issued in any country, currencies that are circulated by medium of exchange. Comparing the cryptocurrency, encryption techniques are used to generate

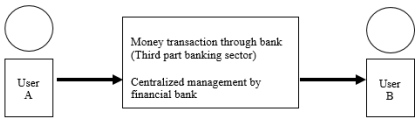

Figure 1: Money transaction procedure

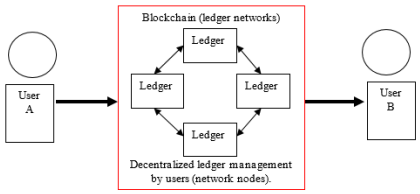

Figure 2. Procedure of cryptocurrency transaction. [12]

the units of currency which is virtual, with no physical evidence.

3.2. Decentralization - Blockchain

One of the key innovation in Bitcoin, compared to other digital or virtual currencies, is its decentralized core technology. Accordingly, by definition decentralization is "the process by which the activities of an organization, particularly those regarding planning and decision making, are distributed or delegated away from a central, authoritative location or group" [4]. In opposite to traditional banking system, most of cryptocurrencies are decentralized on distributed network, which consist in group of computer that are spread around the world, also know as nodes. So, it avoids concentrations of power that could let a single person or organization take control. It often promotes availability and resiliency of a computer system, avoiding a central point of failure [23]. Because the system is not managed by a single point it makes more expensive to attack, destroy or manipulate the system [23]. In Bitcoin and as well as in other cryptocurrencies, the transactions are processed and validated by a distributed and open network, that is owned by no-one. The blockchain is the mechanism of decentralized control of each cryptocurrency. Accordingly, by definition blockchain is "an incorruptible digital ledger of economic transaction that can be programmed to record no just financial transactions but virtually everything of value" [8]. Blockchain is a distributed data structure comprising a chain of blocks. It acts as a distributed database or a global ledger which maintains records of all transactions on a Blockchain network. The transactions are time stamped and bundled into blocks and executed on all the participating nodes where each block is identified by its cryptographic hash [18]. A block contains a transaction list, the most recent state, a block number and a difficulty value. If there are conflicting transactions on the network only one of them is selected to become a part of the block. The blocks are added to the Blockchain at regular intervals [8]. The blocks form a linear sequence where each block references the hash of the previous block [18]. All nodes keep a copy of blockchain, maintain it and execute and record the same transactions. Blockchain is public, it means everyone and node of network can read the transactions.

3.3. Consensus Algorithm

An essential challenge within the distributed computing and multi-node systems is the consensus problem. This problem highlights the difficulty that a number of processes or nodes attempt to reach an agreement on some data value that is needed during the computation [16]. Some nodes, that are part of this distributed system may fail or may not be unreliable, which can effect in the reliability of the network, meaning it would result in an unreliable network. Consensus algorithms are mechanisms that are used to achieve the agreement on a single data value, also when unreliable participants (nodes) are involved in that reliable network [16]. Blockchain is also a distributed computing and multi-node system, that need a way for these nodes to reach a agreement for the shared state of data stored in blockchain. This agreement or consensus within the blockchain network is achieved by use of consensus algorithm. Consensus within distributed system has been always an problem and researchers have study for many years in consensus algorithm in distributed system. Nowadays are some consensus algorithm applied in blockchain.

3.3.1. Proof-of-Work. PoW (Proof-of-Work) [18] is the first implementation of a distributed and trustless consensus algorithm used in Bitcoin. With the PoW method, participants are rewarded for solving complicated cryptographic tasks competition among the nodes. The solution to the tasks is marked in the blockchain by generation of a new block that is based on information of previous block.

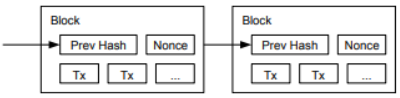

Figure 3. Block model [18]

This process is called "mining" [18]. The PoW takes also the role of safeguard. All block depends on hash of previous blocks and the length of chain is proportional to workload [16]. The first node that solves the problem get rewarded with an amount of Bitcoin [18]. All nodes trust the longest chain, which has the greatest PoW effort invested in it [18]. In case that someone wants to tamper the blockchain, he has to control more than 50% of the world's hashing power to ensure that he can become the first one to generate the latest block and master the longest chain [16]. All of that work effect in electricity and hardware cost that make tampering more expensive then cost to be honest node. So the PoW can guarantee the safety of the blockchain. Through this process Bitcoin guarantee the safety of blockchain.

3.3.2. Proof-of-Stake. PoS (Proof-of-Stake) is another way of reaching consensus within distributed network and validating transactions. The goal is the same of PoW, but the process to reach it is quite different. In PoS, there is no mathematical puzzle to solve in order to keep the network secure and validating transaction but the creator of a new block is chosen in a deterministic way based on their stake [16]. This means there is there is no block reward. In order to build economic incentives, in PoS trusted nodes get

payed by transaction fees [16]. The trusted entities work together to add records in PoS protocol and there is the voting process for accepting the block on the blockchain [8].

3.4. Smart Contracts

Blockchain not only enables the decentralization of transaction management, but also the automation of processes, regulations and organizational principles. The transactions can be supplemented by rules for preserving consistency and then become so-called smart contracts [22]. Smart contracts are similar to normal contracts in the real world, but the only difference is that they are completely digital based on the new technology blockchain. It is computer program that is stored remotely in a blockchain and run automatically when the conditions are met. It enable trusted transactions and agreements to be conducted between different anonymous parties and without the need for a central authority, legal system or external enforcement mechanism. The idea of Smart Contracts came from an American lawyer, computer scientist and cryptographer named Nick Szabo about twenty-two years ago [22]. A smart contract is a flow of conditions that have to be fulfilled, which leads to consequence. The principle is: Code is law. An example of a blockchain platform offering smart contracts is Ethereum [2]. The Ethereum platform builds on Bitcoin's peer-to-peer transaction system. Ethereum does the same as Bitcoin, but with smart contracts, which makes them especially secure. Ethereum uses the Solidity programming language to create Smart Contracts that is developed by Co-Founder of Ethereum.

3.5. Privacy

The privacy in our banking model is guarantee from banks. Through limiting access to information to parties involved and the trusted third party, banks achieve a level of privacy [18]. This kind of information hiding make them a nontransparent system to the public. In order to make it transparent or notify all transactions this method is excluded, but privacy should be achieved by changing the method.

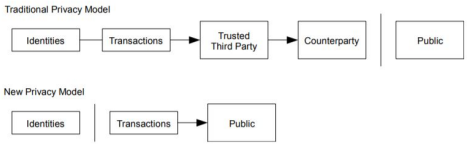

Figure 4. Privacy Model [18]

Through changing the flow of information, so by keeping public keys anonymous. In public key infrastructure anyone can see the participants of a transaction, but no information linking to real identity [18]. The achievement of privacy between two model is shown in figure 4.

3.6. Anonymity

Most of people think that Bitcoin and other cryptocurrencies are developed for criminals who use it to conduct their illegal business. Bitcoin's reputation has been built primarily on the fact that cryptocurrency was the official currency of the virtual black market Silk Road [20], launched by FBI in 2013. Bitcoin is not Anonymous, but Pseudonymous. Transactions are written under a pseudonym. All transactions are permanent and public, anyone can see how much credit is hidden behind the public address and what transactions have already been made with it. Bitcoin addresses are anonymous, but if an address can somehow be linked to a real-world identity, Bitcoin offers no privacy [18]. There are a number of techniques to connect address to real-world identities. To achieve privacy in Bitcoin, it is recommend to use a new address for each new transaction to avoid the transactions being linked to a common owner [18]. Although this is still a good practice, it is not enough to ensure full anonymity through multiple-input transactions [18].

4. Economic Factors

4.1. Limited Supply & Scarcity

Scarcity occurs when a product is available in smaller quantities than desired [5]. From an economic point of view, a good is scarce if there would be more demand than available at a price of zero. Scarcity is thus to be regarded as the cause of economic activity. The scarcity of goods presents an economy with the challenge of allocating the available goods optimally among the various competing users. As a rule, the coincidence of supply and demand on a market results in an equilibrium price for the good, which can be interpreted as a measure of the scarcity of the good [5]. Scarcity of a resource make it valuable. In general, scarcity limits the growth path of the monetary base and facilitates price stability [5]. In modern economies, where money is stored in electronic form, scarcity is preserved by legal provisions that ensure the accuracy of accounting: that is, e-money is a financial system in which transactions trigger a credit to one account and a corresponding debit to another [5]. Traditional currencies like USD, EUR, GBP etc. that are fiat currency are inflationary. This means that there is no limit to how much currency is created and can be on the market at any time. If a system needs more currency, the central bank will issue more bills and coins, helping the economy using that particular currency. However, the main problem with inflationary currencies is that their value decreases as foreign exchange supplies increase. The consequence of this is that the value of currency is hard to estimate as its supply could increase daily. Bitcoin is scarce asset [18]. The only way that new Bitcoin is created is through mining [18]. Each time a miner solves Power of Work algorithm a new block is created. The miner or mining pool that mines a block is rewarded through the block reward. The rate of block creation is adjusted every 2016 blocks to aim for a constant two week adjustment period [3]. The number of bitcoins generated per block is set to decrease geometrically, with a 50% reduction every 210,000 blocks, or approximately four years [3]. There are 21 million Bitcoin that are to be mined, until now are 17 million Bitcoin mined.

As number of created coins get closer to its limit the generation of new coin is progressively harder and

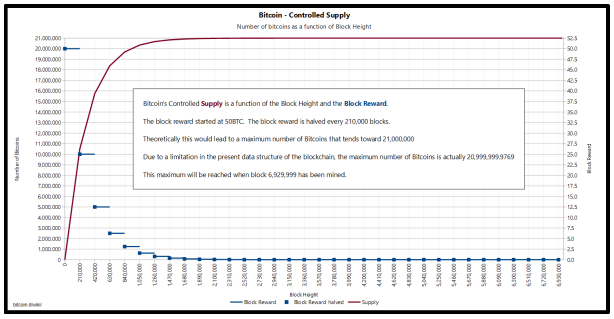

Figure 5. Bitcoin Controlled Supply [3]

harder [18]. While comparable goods such as gold or silver are responding to a supply response in response to increased demand (with higher gold demand, gold mines are increasingly digging up the precious metal and thus increasing supply), Bitcoin's offer is stiff. One speaks of the so-called price elasticity of the offer - and that is with Bitcoin as less as nowhere else. An increased demand is thus certainly on the course, because even if in a demand shock more miners go to the net, the quantity can not inflate. There are also other currency that are not based on that scarcity theory. Ethereum [2] is a type of cryptocurrency that is not supply limited, new coins can be created every time.

4.2. Block Rewards

Lacks a centralized authority makes processing transaction and issuing coins a more difficult than in our monetary system. Bitcoin mining is the process, that secure the network and processing transaction. Each day countless thousand watts of electricity are used to mine Bitcoin. People mine Bitcoin because it is the most expensive currency in the market, has value, and can be bought and sold in various market. Mining is an expensive process that cost a lot of electricity and CPU power [18]. Satoshi Nakamoto [18] wanted to create a system that is able to support itself and closer to gold mining. Each mined block contains a reward. So as to mine, this reward must be sufficiently high to give a solid motivation to mine. Be that as it may, the reward can't be an excessive amount of either. A major reward would cause an oversupply and lower value of the currency. After some time, mining would turn out to be progressively troublesome and the prizes gathered would gradually diminish to control supply. Nakamoto's answer for this issue is to present a Bitcoin halving mechanism. That is the way it works. At the point when Bitcoin began, the block reward was an incredible 50 Bitcoin at regular intervals [18]. The Bitcoin code contains an explanation that this reward ought to be divided after 210,000 blocks (or around four years at 10 minutes for each block) [18]. After the last two Bitcoin parts, the present block reward is currently 12.5 Bitcoin. In 2020 it will be 6.25, etc. Along these lines, the Bitcoin halving has various significant impacts on the system. To start with, it expands the life of the reward mechanism. If we somehow happened to discharge 50 Bitcoin at regular intervals, we would achieve the greatest conveyance cutoff of 21 million Bitcoin before long. Truth be told, the mining rewards would be eliminated in around 8 years. In the event that you gradually diminish the reward rate after some time, the period wherein the mining prompts a block reward will be longer. Also, halving Bitcoin causes Bitcoin to record a consistent cost increment after some time. This is on the grounds that the quantity of new Bitcoin coins that seem every year is diminishing. This constrained supply prompts an expansion in Bitcoin costs as their deficiency increments relatively. The Bitcoin halving was additionally planned to imitate gold-mining, as gold-mining definitely turns out to be increasingly costly and troublesome after some time, as increasingly more of the Earth's gold stores are mined out [18]. In addition to the fact that it gets increasingly costly, however not as much as veil new gold enters the gold commercial center every year. It also keeps Bitcoin costs relentlessly moving upward over extensive stretches of time. In the event that it were not for the Bitcoin splitting, Bitcoin today may just be worth 50 or hundred dollars each rather than the thousands that it's value now.

4.3. Transaction Fees

The miners still have clear motivations to proceed with their tasks right now, as they are as of now profiting by the expanding estimation of the Bitcoin, which are paid out as rewards as long as the offer amount has not yet been completely depleted. However, when the 21 million imprint is achieved, miners will never again have the option to get Bitcoin reward. In any case, transactions should at present be approved and stored in blockchain. Miner have a moment potential source of income. When posting a transaction, the buyer and dealer can moreover offer to pay a transaction fee, which may be a reward installment to anything miner solves the mathematical tasks that confirms the transaction [18]. The difference is a transaction fee that is included to an incentive of the block containing the transaction [18]. When a predetermined number of coins have entered flow, incentive can progress altogether to transaction fees and be totally inflation free [18]. The incentive may help urge nodes to remain legit. On the off chance that a covetous assailant can collect more CPU control than all the honest nodes, he would need to pick between utilizing it to dupe individuals by taking back his payments or utilizing it to produce new coins [18]. He should think that it's increasingly productive to play by the guidelines, such decides that favour him with more new coins than every other person joined than to undermine the framework and the validity of his own wealth [18].

4.4. Deflationary nature of Bitcoin

Traditional economists have associated the term deflation largely with under-performance or economic crisis, which usually causes people to move to liquid currencies [5]. Without minting new coins, however, existing coins should gain in value as they are now harder to obtain. Some cryptocurrencies, such as Ethereum [2] and some other have opted for the inflationary currency model by enabling the continuous creation of new coins. While other coins like Bitcoin and Litecoin [15] have chosen to limit the money supply, they eventually become deflationary.

Deflation is commonly characterized as the general decrease in the cost of products and enterprises when the inflation rate achieves a negative value. While inflation diminishes the value of cash after some time, deflation builds it due to having a fixed supply, which makes a type of scarcity for the money. The block reward and transaction fees are two factors that impact to Bitcoin price. Block reward for miners is the only way for supplying the network with new Bitcoin. The block reward is periodically halved, as shown in figure 6. The motivation why the linear supply is not offered is to avoid inflation [13]. Although the network is still in a temporary low-inflation state, Bitcoin is eventually meant to be deflationary [13]. Predetermined control of Bitcoin supply as part of rules is to diminish inflation shortly after the initial launch [13]. Figure 6 demonstrates also the relation of created blocks over time and the inflation rate. The inflation rate of Bitcoin is identified with available number of bitcoins in circulation and interest for buying and selling it. So Bitcoin will remain a inflationary currency until it reaches the predefined limit of coin. After the entry of all Bitcoin in circulation inflation will be replaced by deflation and block reward by transaction fees [18]. The significant scarcity in supply can see as a negative feature of Bitcoin, because block reward is a huge incentive to keep the system work. But its scarcity and block reward halving will not effect the incentive of miners because the higher value in price as the price of Bitcoin is dramatically increasing.

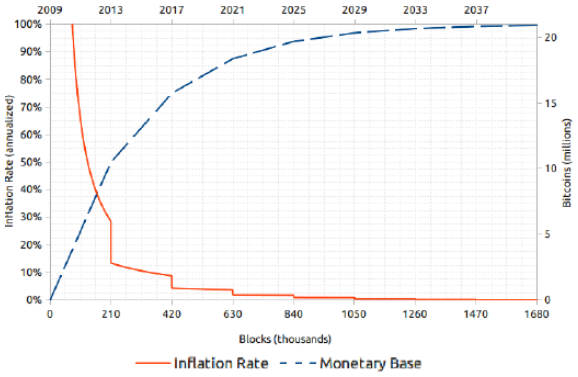

Figure 6. Bitcoin inflation vs time [13]

4.5. Initial Coin Offering

In association with modern cryptocurrencies in specific, there is regularly conversation of an ”ICO”. Recently, this term and the associated process have been discussed particularly critically. ICO stands for ”Initial Coin Offering”. This is the issue of coins to a certain circle of recipients, which is determined before the ICO [1]. Coins can be issued privately (private sale) and/or publicly (public sale). The term ICO is based on the initial public offering (IPO) of a company [1]. A company goes public during an IPO and offers shares to potential buyers. This enables the company to win money for itself and thus finance its projects and cover its costs. This is interesting for investors because an increase in value and the success of the company goes hand in hand with an increase in the value of the shares acquired [1]. In contrast to an IPO, which is subject to strict regulations, an ICO is more like crowdfunding [1]. An ICO invests in the company by buying a certain amount of newly produced crypto coins. Usually one has the possibility to pay the new coins with other cryptocurrency (Bitcoin, Ethereum) or Fiat money. The value of the tokens develops parallel to the project behind them.

5. Conclusion

Our monetary system has shown us that it is not the until now best created monetary system. The main problem is the central authority that has control of monitoring, maintenance and regulation of policies. The goal of any cryptocurrency is to create a system that is not controlled by a central financial institution. The concept behind Bitcoin is similar to gold, that means scarcity resource and deflationary currency. Inflation of Bitcoin is controlled through different mechanism like block reward halving mechanism and transaction fees. Like other systems also Bitcoin has shown some advantages and disadvantages. There are a number of advantages of Bitcoin like: decentralisation, peer-to-peer and encrypted communication between parties, secure, politically free, borderless money, low-transaction fees, limited money supply, irreversible transactions, fast transaction over the world in seconds. Although a lot of advantages, Bitcoin has shown some issues related to mining. China is biggest player in mining and using cryptocurrency, that has the risk of centralisation of hash rate power in one country. Blockchain, the underlying technology is the biggest innovation of Bitcoin, which took attention of start-up in finance ”FinTech”.

References

[1] *Bitcoin Magazine — Bitcoin Guide: What Is an ICO?* https://bitcoinmagazine.com/guides/what-ico. (Accessed on 06/26/2019).

[2] Vitalik Buterin. *Ethereum: A next-generation smart contract and decentralized application platform.* Accessed: 2016-08-22. 2014. URL: https://github.com/ethereum/wiki/wiki/White-Paper.

[3] *Controlled supply - Bitcoin Wiki.* https://en.bitcoin.it/wiki/Controlled_supply. (Accessed on 05/24/2019). May 2019.

[4] *Decentralization - Wikipedia.* https://en.wikipedia.org/wiki/Decentralization#cite_note-1. (Accessed on 05/13/2019).

[5] *Deflationary spiral - Bitcoin Wiki.* https://en.bitcoin.it/wiki/Deflationary_spiral. (Accessed on 06/26/2019).

[6] *Fiat Money.* http://www.centralbanksguide.com/fiat+money/. (Accessed on 05/15/2019).

[7] Scott Freeman. “Fiat Money as a Medium of Exchange”. In: *International Economic Review* 30.1 (1989), pp. 137–151. ISSN: 00206598, 14682354. URL: http://www.jstor.org/stable/2526554.

[8] Julija Golosova and Andrejs Romanovs. “The Advantages and Disadvantages of the Blockchain Technology”. In: Nov. 2018, pp. 1–6. DOI: 10.1109/AIEEE.2018.8592253.

[9] John B. Goodman. “The Politics of Central Bank Independence”. In: *Comparative Politics* 23.3 (1991), pp. 329–349. ISSN: 00104159. URL: http://www.jstor.org/stable/422090.

[10] Corporate Financial Institute. *Commercial Bank - What You Need To Know About Commercial Banks*. https://corporatefinanceinstitute.com/resources/knowledge/finance/commercial-bank/. (Accessed on 05/29/2019).

[11] Investopedia. *How does the price of oil affect Venezuela's economy?* https://www.investopedia.com/ask/answers/032515/how-does-price-oil-affect-venezuelas-economy.asp. (Accessed on 04/28/2019).

[12] M. R. Islam et al. “Cryptocurrency vs. Fiat Currency: Architecture, Algorithm, Cashflow amp; Ledger Technology on Emerging Economy: The Influential Facts of Cryptocurrency and Fiat Currency”. In: *2018 International Conference on Information and Communication Technology for the Muslim World (ICT4M)*. July 2018, pp. 69–73. DOI: 10.1109/ICT4M.2018.00022.

[13] Kerem Kaskaloglu. “Near Zero Bitcoin Transaction Fees Cannot Last Forever”. In: June 2014. URL: https://www.researchgate.net/publication/263617756_Near_Zero_Bitcoin_Transaction_Fees_Cannot_Last_Forever.

[14] *Lender of Last Resort*. http://www.centralbanksguide.com/lender+of+last+resort/. (Accessed on 05/16/2019).

[15] *Litecoin - Open source P2P digital currency*. https://litecoin.org/. (Accessed on 05/28/2019).

[16] D. Mingxiao et al. “A review on consensus algorithm of blockchain”. In: *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. Oct. 2017, pp. 2567–2572. DOI: 10.1109/SMC.2017.8123011.

[17] *Monetary Policy*. http://www.centralbanksguide.com/monetary+policy/. (Accessed on 05/16/2019).

[18] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Accessed on 04/04/2019. Dec. 2008. URL: https://bitcoin.org/bitcoin.pdf.

[19] Joseph A. Ritter. “The Transition from Barter to Fiat Money”. In: *The American Economic Review* 85.1 (1995), pp. 134–149. ISSN: 00028282. URL: http://www.jstor.org/stable/2118000.

[20] *Silk Road – Wikipedia*. https://de.wikipedia.org/wiki/Silk_Road. (Accessed on 06/26/2019).

[21] *Special Topics: Venezuela – Applied Economics, Global Health, and the Study of Business Enterprise*. https://sites.krieger.jhu.edu/iae/research-programs/special-topics-venezuela/. (Accessed on 04/26/2019).

[22] Nick Szabo. *The Idea of Smart Contracts — Satoshi Nakamoto Institute*. https://nakamotoinstitute.org/the-idea-of-smart-contracts/. (Accessed on 05/24/2019). 1997.

[23] *The Meaning of Decentralization – Vitalik Buterin – Medium*. https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274. (Accessed on 05/13/2019).