

PRODUCING OF CRYPTOCURRENCIES

Natalija Tomić, Danijel Bogosavljević

*University of Belgrade, Technical faculty in Bor, Engineering Management Department
Bor, Serbia*

Abstract

The basic terms and concept of cryptocurrencies were described in this paper. In the first part will be presented a brief description and explanation of how the cryptocurrencies can be created, how the crypts work, and something about their production. This paper also involves the research and the interviews about that how cryptocurrencies can have positive or negative effect on the standard and the opinions of the people who dealing with cryptocurrencies and who are informed in that area.

Keywords: *cryptocurrency, digital money, production, interview, bitcoin*

1. INTRODUCTION

Due to the anonymity in the night market, the exchange of goods necessitates a means of payment which we assume is a cryptocurrency. A cryptocurrency is a digital record-keeping device that uses balances to keep track of the obligations from trading and that is publicly known to all traders. [1]

Crypto-currencies are virtual payment systems that do not rely on a central authority to generate currency supply or to verify, track, and record transactions. Instead, crypto-currencies rely on a distributed ledger to determine, verify, and track ownership of monetary units without the need for merely as digital records with a tiered structure of clearing institutions culminating in the central bank. The technology behind the crypto-ledger enables the bypassing of this centralized clearing structure to record the ownership to financial assets. [2]

As cryptocurrencies gain popularity, the issue of how to regulate them becomes more pressing. The attractiveness of cryptocurrencies is due in part to their decentralized, peer-to-peer structure. This makes them an alternative to national currencies which are controlled by central banks. Given that these cryptocurrencies are already replacing some of the “regular” national currencies and financial products. [3]

In the first part will be presented a brief description and explanation of how the cryptocurrencies work, how the crypts can be created, and something about their production. In second part of this paper will be presented interview with two respondents who works with Cryptocurrencies and their explanation about that how actually that business works.

2. DEVELOPMENT OF CRYPTOCURRENCIES

Since the creation of Bitcoin in 2009, numerous private cryptocurrencies have been introduced. Bitcoin is by far the most successful one. It has been getting a lot of media attention, and its total market value has reached 20 billions USD in March 2017. More importantly, a number of central banks started recently to explore the adoption of cryptocurrency and blockchain technologies for retail and large-value payments. For example, the People's Bank of China aims to develop a nationwide digital currency based on blockchain technology, the Bank of Canada and Monetary Authority of Singapore are studying its usage for interbank payment systems, the Deutsche Bundesbank has developed a preliminary prototype for blockchain-based settlement of financial assets. Many proponents believe that cryptocurrency and blockchain technology will have a significant influence on the future development of payment and financial systems.

While policy makers concern about the opportunities and challenges brought about by these technological advances, there is very little guidance provided by economic theory regarding the appropriate usage of these technologies and the optimal design of these systems. This paper attempts to provide an economic theory to help us understand the fundamental economic tradeoffs and address relevant policy issues. Most existing models of cryptocurrencies are built by computer scientists who focus mainly on the feasibility and security of these systems. This line of research often ignores the incentives of participants and the endogenous nature of key variables. The economic literature on cryptocurrencies is very thin. So far, there are only a few economic models developed to study this new payment technology. [1]

3. PRODUCING OF CRYPTOCURRENCIES

The human innovation in the field of monetary freedom takes shape in the virtual communities. Developed and implemented through a decentralized algorithm, the bitcoin project has so far proved itself a success in the field of virtual currency. [4]

As bitcoin becomes more important as a worldwide financial phenomenon, it also becomes important to understand its sources of value formation. There are three ways to obtain bitcoins: buy them outright, accept them in exchange, or else produce them by 'mining'. Mining employs computational effort which requires electrical consumption for operation. The cost of electricity per kWh, the efficiency of mining as measured by watts per unit of mining effort, the market price of bitcoin, and the difficulty of mining all matter in making the decision to produce. Bitcoin production seems to resemble a competitive market, so in theory miners will produce until their marginal costs equal their marginal product. Break-even points are modeled for market price, energy cost, efficiency and difficulty to produce. The cost of production price may represent a theoretical value around which market prices tend to gravitate. As the average efficiency increases over time due to competition driving technological progress – as inefficient capital becomes obsolete it is removed while new capital replaces them – the break-even production cost of bitcoins denominated in dollars will fall. Increased efficiency, although necessary to maintain competitive advantage over other miners could serve to drive the value of bitcoin down, however adjustments in the mining difficulty and the regular halving of the block reward throughout time will tend to counteract a decreasing tendency in cost of production. [5]

For the purpose of making easier transactions, the world, throughout history, has assigned pressed coins in old times to trade products and in present, printed currency was invented. However, this has increased the number of countries that are getting trapped into

debt or for sure are facing the difficulties in meeting the needs of their fiscal targets in modern era's functions.

It is a system of payment that eliminates the requirement of a financial intermediary between two parties wanting to transmit money using the internet. It is a less costly method and at times, it is totally free.

One of the initially invented digital modes of exchange is cryptocurrency, and interest has increased rapidly since last year over cryptocurrency. Digital mode of exchange like cryptocurrency is a currency that is anonymous in all aspects. Because there isn't any central government who controls the supply of cryptocurrency, that's why its transactions are untraceable.

The decentralization of cryptocurrency is in its early stages and still not fully implemented. This project is an open source concept known as CRYPTOCURRENCY, which was invented to prove that financial transactions could be conducted without authorization from a central bank.

Cryptocurrency technology has become more and more popular and much important to the public as a medium of storing and transferring wealth. Like any other new technologies that attract swift global attention, cryptocurrency has been under attack by malicious actors trying to exploit the trial nature of the cryptocurrency protocol.

Cryptocurrency is a good example of peer-to-peer networks that relies on users active involvement to enhance successful dependable data exchange. Every transaction is verified through numerous codes that are confirmed in the network prior to getting its destination. This verification process assures the reliability of data transfer. [6]

Suppose a public ledger is given as an oracle. Now it is easy to create a crypto currency based on it. We call a bank account a key pair from a digital signature scheme. More precisely, the public key is the account number (called address). Furthermore, some mechanism is required to distribute some money (called emitting money) i.e. assign or add different amounts to accounts, so that some money is there to deal with. [7]

Bitcoin is a "crypto currency", a decentralized electronic payment scheme which has recently gained excessive popularity. Scientific research on bitcoin is less abundant. Optimizations enable bitcoin miners to save tens of millions of dollars per year in electricity bills. Miners who set up mining operations face many economic uncertainties such as high volatility. In this paper we point out that there are fundamental uncertainties which depend very strongly on the bitcoin specification. The energy efficiency of bitcoin miners have already been improved by a factor of about 10,000, and we claim that further improvements are inevitable. Better technology is bound to be invented, would it be quantum miners. More importantly, the specification is likely to change. A major change have been proposed in May 2013 at Bitcoin conference in San Diego by Dan Kaminsky. However, any sort of change could be flatly rejected by the community which have heavily invested in mining with the current technology. [8]

Bitcoin uses cryptography to control the production of Bitcoins in the system and a public ledger scheme to validate transactions. With respect to Bitcoin production, Bitcoins enter into circulation once they are uncovered through a process called mining. Mining refers to using a computer's processing power to solve complex, dynamic, cryptographic problems. The difficulty, or attendant computer processing power that is required to solve the problems, adjusts dynamically in response to the number of Bitcoins that have been mined. This ensures that Bitcoins will be discovered at a limited, controlled pace. Indeed, there are about 12.5 million Bitcoins in circulation today and the maximum circulation of 21 million is not expected to be reached until 2140. This method of controlling the supply of Bitcoins eliminates the need for a central banking authority that sets monetary policy for the currency. From another perspective, the monetary policy of Bitcoin is hard-coded into the Bitcoin protocol. Other notable aspects of Bitcoin include how Bitcoins are stored and

how they are exchanged once in circulation. In order to connect to the Bitcoin network, users must first download the open-source Bitcoin software. [9]

Bitcoin mining, a process which results in the generation of new Bitcoins, is performed by miner operators for reception of incentives in the form of Bitcoins. This mining process is essentially operations of SHA-256 hashing of values in search of a hash digest smaller than a specific value. Once this winning hash has been discovered, a new block to Blockchain is added and BTC incentives are furnished by the Bitcoin network to the miner. [10]

4. BITCOIN MINING

With Bitcoin, miners use special software to solve math problems and are issued a certain number of bitcoins in exchange. This provides a smart way to issue the currency and also creates an incentive for more people to mine. Bitcoin miners help keep the Bitcoin network secure by approving transactions. Mining is an important and integral part of Bitcoin that ensures fairness while keeping the Bitcoin network stable, safe and secure. Bitcoin mining is the process of adding transaction records to Bitcoin's public ledger of past transactions or blockchain. This ledger of past transactions is called the block chain as it is a chain of blocks. The block chain serves to confirm transactions to the rest of the network as having taken place. Bitcoin nodes use the block chain to distinguish legitimate Bitcoin transactions from attempts to re-spend coins that have already been spent elsewhere. Bitcoin mining is intentionally designed to be resource-intensive and difficult so that the number of blocks found each day by miners remains steady. Individual blocks must contain a proof of work to be considered valid. This proof of work is verified by other Bitcoin nodes each time they receive a block. Bitcoin uses the hashcash proof of work function.

The primary purpose of mining is to allow Bitcoin nodes to reach a secure, tamper-resistant consensus. Mining is also the mechanism used to introduce Bitcoins into the system: Miners are paid any transaction fees as well as a "subsidy" of newly created coins. As more miners join, the rate of block creation will go up. As the rate of block generation goes up, the difficulty rises to compensate which will push the rate of block creation back down. Any blocks released by malicious miners that do not meet the required difficulty target will simply be rejected by everyone on the network and thus will be worthless.

In addition to being the means of generating new bitcoin, bitcoin mining creates the blockchain that verifies bitcoin transactions. The block reward is gleaned by placing a new block on the blockchain, which acts as an advancing public ledger of verified transaction. This is an essential function for bitcoin's operation as it enables the currency to be safely and predictably created without the centralized regulation in the form of a bank or federal government. Blocks must to be a validated by a proof of work, which can only be obtained by expending a great deal of processing power. Once a block is obtained a message is broadcast to the mining network and verified by all recipients.

5. INTERVIEW

We wanted to have relevant information about the process of creating cryptocurrency, but also how to do the best business and earning, we contacted the people involved in this job. Through interviews, we came to interesting data which define and characterize the cryptocurrency itself, and everything about bitcoin. The interview was conducted with two respondents, one from Serbia, and the other one was from Turkey.

First, we had interview with respondent from Turkey and we asked him some questions. We started with question what is the basic meaning of the cryptocurrency, is a emergence of a

cryptocurrency revolution and can people earn quickly if they try to? Our respondent gave us an answer: "There is no gold foundation for any currency. Well, it can be said, because when we make money from nothing, the notion of money is not a banknote at all, but the point is something else. We go to the city and spend, we buy some things, and as long as people believe that you bitcoins worth something, we have nothing to worry about. So, such a story goes on. And yes, you can earn very quickly if u are ready to invest some money in that business, also you have to have some plans and you need to be patient".

Second respondent is from Serbia. We asked him is easy to do "mining", how much money have to be invested if you want to try mining, is that safe job and does he plan to do that his whole life. His reply was: "New equipmnt are constantly coming out and they are much better for mining and your can better earn with them, if you do not use new equipment you will get an average earning and that is unacceptable for me. I bought my initial equipment in Serbia for the amount of 6000 euros, first prepare money and then you will know what to do. When I collect enough money I will invest in a private business, mining is like another job, isn't safe and you can always make a loss".

6. CONCLUSION

The cryptocurrency, as a new concept, is still in the process of understanding and acceptance by the side consumers - traders, and financial institutions. With the development of Bitcoin and it's derivatives, as well as the general growth of interest in using them, it is certain that will be problems in the future. The addition to all controversies and skepticism that follows the crypts, it's clear that their appearance can and possibility survive in this period is marked the beginning of a new chapter in digital and financial world.

BitCoin can be called the digital signature chain, which is not controlled by a bank, government, or any central financial institution, but participants in the network. Transactions in bitcoin network are verified by users who reach a consenzus about validation of certain transaction. New bitcoins are created through a process called mining which includes finding a solution of a difficult mathematical problem.

It is concluded that cryptoworks, like any other business, require the investment of a certain amount of money, their time, space, but also you need to be patient and know that this is not a safe job, that the production of bitcoins and other cryptocurrencies are carried out by mining. Loss in this business is also possible.

STVARANJE KRIPTOVALUTA

Natalija Tomić, Danijel Bogosavljević

Univerzitet u Beogradu, Tehnički fakultet u Boru, Odsek za inženjerski menadžment
Bor, Srbija

Izvod

Sam koncept kriptovaluta, kao i osnovni pojmovi opisani su u ovom radu. U prvom delu rada biće dat kratak opis i objašnjenja kako kriptovalute funkcionišu, njihovu proizvodnju, ali i kako su nastale. Ovaj rad, takođe, obuhvata i istraživanje u vidu intervjua o tome da li kriptovalute u današnje vreme negativno ili pozitivno utiču na standard, kao i mišljenja ljudi koji se bave kriptovalutama i upoznati su sa njima na najbolji mogući način.

Ključne reči: kriptovalute, digitalni novac, proizvodnja, intervju, bitcoin

LITERATURA / REFERENCES

- [1] Chiu, J., Koepl, T.V. (2017). The economics of cryptocurrencies-bitcoin and beyond.
- [2] Rosov, S. (2015). Beyond Bitcoin. CFA Institute Magazine, 26(1), 37-47.
- [3] Jabotinsky, H.Y. (2018). The Regulation of Cryptocurrencies-between a Currency and a Financial Product.
- [4] Iavorschi, M. (2013). The bitcoin project and the free market. CES Working Papers, 5(4), 529-534.
- [5] Hayes, A. (2015). A cost of production model for bitcoin.
- [6] Davidson, J. (2013). The Digital Coin Revolution-Crypto Currency-How to Make Money Online, 10, JD-Biz Corp Publishing.
- [7] Carstens, T.V. (2017). How not to wait long.
- [8] Courtois, N.T., Grajek, M., Naik, R. (2013). The unreasonable fundamental incertitudes behind bitcoin mining. arXiv preprint arXiv:1310.7935.
- [9] Mittal, S. (2012). Is bitcoin money? bitcoin and alternate theories of money.
- [10] Dev, J.A. (2014). Bitcoin mining acceleration and performance quantification. In Electrical and Computer Engineering (CCECE), 2014 IEEE 27th Canadian Conference, 1-6.