Annals of the University of Petrosani, Electrical Engineering, 20 (2018)

BRIEF ANALYSIS OF THE BITCOIN PHENOMENON BY PRIVATE USER

COSMIN RUS[1], ILEANA – SORINA RAKOŞ [2], NICOLETA NEGRU [3]

Abstract: This paper highlights aspects of the Bitcoin digital paradigm that use decentralized technology for secure payments and the storage of money that does not require banks or names of people. The main objective of the paper is to understand the bitcoin phenomenon both in terms of economic implications and in terms of the technical notions of the entire process of producing the virtual coins. Also, there are some clear remarks about the need to try to reduce the electricity consumption used in the virtual coin mining process or the more frequent use of renewable energy resources.

Keywords: bitcoin, mining, ledger, renewable energy resources, blockchain, technology

1. INTRODUCTION

In 2009, due to the increasing popularity of electronic payment systems, a person or a group of unknown people, under the pseudonym Satoshi Nakamoto, created Bitcoin. It can be defined as a decentralized electronic payment system, but also a digital coin. The purpose of this coin is to ensure security and transaction anonymity, free business finance, and investment protection without resorting to public or private financial institutions, thus excluding dependence on a certain financial structure. As we know, the world currencies have a special issuer: The dollar is issued by the US Federal Reserve System, the Euro is issued by the Central Bank of Europe, etc. Unlike these coins, Bitcoin does not use a central issuer, being totally decentralized. Economically speaking, Bitcoin has no value, and is used as a measure of the value of traded items, basically fulfilling the original money function. Bitcoin's value is based on the confidence of all participants in this coin's trading network.[1],[5]

Next we will address the technical aspect of this coin, because without it, we can not understand its principle of operation. It's a bit heavy, but we'll try to make it as suggestive as possible. Due to its construction, the Bitcoin can be anonymously transmitted, and saved on the user's computer as a portfile. In order to make a transaction,

[1] Ph.D. student, Eng., University of Petroşani, cosminrus@upet

[2] Ph.D, Associate Prof.,University of Petroşani, nihilsinedeo_68@yahoo.com

[3] Ph.D. student, University of Petroşani, negru.ioananicoleta@yahoo.ro

users need two "keys", a public one, which is used to encrypt the transaction code and BitTorrent, and a private one, with which the code is decoded, and finalizing the transaction, offering anonymity and security.[2],[3],[7]

In our opinion, the concept of crypto-labeled is perspective, but Bitcoin does not have a high practical capacity, because of how paradoxically it would be, its main plus: decentralization. Because of this facility, this currency can not be controlled by the state, it does not depend on any bank, it can not suffer inflation (the number of bitches being controlled), what is the problem then? The problem is the financial value of a Bitcoin coin. The course of this cryptocurrency is very unstable, sensitive to crises in economic life and investor actions.[7]

2. BITCOIN MINING

Bitcoin is a digital currency (also called cryptocurrency) that is not backed by any country's central bank or government. Bitcoins can be traded for goods or services with vendors who accept Bitcoins as payment. Mining is the process of adding transaction records to Bitcoin's public ledger of past transactions (and a "mining rig" is a colloquial metaphor for a single computer system that performs the necessary computations for "mining"). This ledger of past transactions is called the block chain as it is a chain of blocks. The blockchain serves to confirm transactions to the rest of the network as having taken place. Bitcoin nodes use the blockchain to distinguish legitimate Bitcoin transactions from attempts to re-spend coins that have already been spent elsewhere.[5]

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 set the history of transactions in a way that is computationally impractical to modify by any one entity. By downloading and verifying the blockchain, bitcoin nodes are able to reach consensus about the ordering of events in bitcoin.

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. This both serves the purpose of disseminating new coins in a decentralized manner as well as motivating people to provide security for the system. Bitcoin mining is so called because it resembles the mining of other commodities: it requires exertion and it slowly makes new units available to anybody who wishes to take part. An important difference is that the supply does not depend on the amount of mining. In general changing total miner hashpower does not change how many bitcoins are created over the long term.

Mining a block is difficult because the SHA-256 hash of a block's header must be lower than or equal to the target in order for the block to be accepted by the network. This problem can be simplified for explanation purposes: The hash of a block must start with a certain number of zeros. The probability of calculating a hash that starts with many zeros is very low, therefore many attempts must be made. In order to generate a new hash each round, a nonce is incremented.

The difficulty is the measure of how difficult it is to find a new block compared to the easiest it can ever be. The rate is recalculated every 2,016 blocks to a value such that the previous 2,016 blocks would have been generated in exactly one fortnight (two weeks) had everyone been mining at this difficulty.

This is expected yield, on average, one block every ten minutes. As more miners join, the rate of block creation increases. As the rate of block generation increases, the difficulty rises to compensate, which has a balancing of effect due to reducing the rate of block-creation. Any blocks released by malicious miners that do not meet the required difficulty target will simply be rejected by the other participants in the network.When a block is discovered, the discoverer may award themselves a certain number of bitcoins, which is agreed-upon by everyone in the network.

Currently this bounty is 12.5 bitcoins; this value will halve every 210,000 blocks. Additionally, the miner is awarded the fees paid by users sending transactions. The fee is an incentive for the miner to include the transaction in their block. In the future, as the number of new bitcoins miners are allowed to create in each block dwindles, the fees will make up a much more important percentage of mining income.[10]

3. BLOCKCHAIN AND CRYPTOCURRENCY

We have to understand that creating cryptocurrency is not the only single use of Blockchain. In 2015, the Ethereum network was launched that generated far more modern technologies than Blockchain and other concepts such as smart-contracts. Ethereum was a Blockchain, but more technically advanced not only to perform currency transactions but also to initiate and process smart-contracts, create its own Token devices (identifies you as a user and authorizes your transactions) for use in any other (third) projects.[4]

Smart-Contracts is a new direction, which became known with the development of the Blockchain. Imagine a smart electronic contract that records all business conditions and cannot be changed by anyone. This technology will generate the complete disappearance of scams and lies, both from simple people and from the state. For example, you have created a smart contract for the sale of a good (your own house), you have scheduled the necessary conditions after which the smart-contract will create the necessary events (in our case the sale of the house (sale of the private-real estate)). Therefore, the buyer transfers the necessary amount of money to the smart-contract to the corresponding smart-contract, after which the smart-contract verifies daily the update in the State Property Register. As soon as the property registration letter is displayed after the new owner, the smart-contract will transfer to your account the amount equal to the price. If within one month this inscript will not be displayed, the smart-contract will return the buyer's crypt.

This is one of the simplest examples that make it clear that in front of Blockchain technology there is a big future. Blockchain and cryptocurrency are now like the Internet in 1993, everything that's more interesting is going to happen. And it is very important that we all understand this new direction, and if we have the opportunity, let us even take part in it.

4. THE HAZARDS ASSOCIATED WITH BITCOIN

As we know, the creator of Bitcoin is a person, or a group of people, known under the pseudonym Satoshi Nakomoto, who first launched the Bitcoin network. For testing and verification, around 7% of all Bitcoin coins were extracted, and today, in a few years, those 7% represent colossal amounts, approximately $ 20 billion, and after forecasts only 7% will almost equal $ 200 billion, and by 2050, these percentages will turn to $ 5-10 trillion. And it is very possible that at that moment to be the opposite of the present, ie the value of the dollar to be calculated in bitcoins, even if that sounds funny, this is likely to happen. So funny sounded for that boy who bought a 10,000 Bitcoin pizza in 2010, hearing that in 2018 the equivalent of that price would be $ 150 million. Ask a financial analyst or economist who you know about the danger of this phenomenon.

What will happen if 7% of all Bitcoins are extracted in a single day at cryptocurrency exchanges? We will see how soon Bitcoin, but also the other cryptocurrency, will be destroyed. Their value will decrease hundreds of times, creating such a catastrophe in the world that most financial organizations, traders and others will have to stop trading and sales. In fact, the entire world economy will stop in just two or three days. Stores, pharmacies, no trader will be able to accept payments, because everyone, a day ago, bought goods at a price hundreds of times higher.

Everyone will wait for clarifications, which they will not receive. Imagine that in your house there is a room that is full up to the bridge with $ 100 banknotes, so if you want to open the door, you will be covered with waves of money. And you have been living in that 9-year-old house, and in all these 9 years you've passed that room without taking even $ 1.[7]

Mining is a very wasteful electricity process, for the location of large mining devices, very cheap electricity access is needed, as is a favorable climate area. Mining equipment produces a large amount of heat that needs to be absorbed. After these clues, in your opinion, in which country are the capabilities and basic tools that Bitcoin is shuffling for? This is China. In the percentage ratio, it looks like this: China 81%; Japonia5%; Czech Republic 2%; Georgia1% etc. If most of Bitcoin's power is in a single country, it allows for a simpler connection between mining equipment owners, which causes danger. It is enough that these owners, uniting themselves, form 51% of the administrative equipment to make changes to the Bitcoin network. Mining pools already have their own brands and names, they have long known each other, and possibly keep in touch with each other.[10]

Today's modern cryptocurrency are no longer in need of mining. More secure and cheaper Blockchain projects have been designed and are already in place, where the role of mining is diminished, not much electricity is needed (Bitcoin currently consumes energy as a city with a population of 1 million people). Here too we can add accelerated demodulation of mining equipment, it will be an endless race. The equipment purchased yesterday, tomorrow, may be old and out of date with the release of new ones.[7][8]

I reviewed and analyzed the most important hazards that Bitcoin might pose. But what to do to avoid all this? Everything is simple and complicated at the same time. Cryptocurrency's company must not change Bitcoin's price higher than it has at present.

Most believe that $ 50-60 thousand is a reasonable limit for the Bitcoin value and safe for the cryptocurrency market, because if someone tries to destroy Bitcoin, the rest of the cryptocurrency will fall. We need to assess the situation correctly and not lift the Bitcoin up to those heights that may prove dangerous. We, society, can create a more positive future in this respect, which we will continue to talk about.[9]

5. CONCLUSIONS

We have approached Bitcoin from the multitude of cryptocurrency on the market because of its popularity, being the most used electronic money. From the ideas outlined above we can deduce that Bitcoin has no practical value, but it is not. Even if bitcoin use is somewhat more difficult because of its volatile course, the popularization of this coin has led to the development of cryptocurrency itself, which is economically important.

More stable and more practical cryptoscopes appear: Etherium, Litecoin, Yota, which, over time, may replace the concept of paper money, and move to electronic money.

Technologies are growing at an accelerated rate, and financial security is getting bigger every day, so implementation of cryptobodies might be an action that would provide economic prosperity in the future, yet they eventually meet the concept of money base: measuring the value of a product, and facilitating the exchange, that is money is a tool with which the exchange becomes effective.

Money presents our economic capacity, and cryptocurrency is a concept that attempts to implement this money feature in reality. As mentioned earlier, once and spices were considered "gold", which means that the nature of money is flexible, and what seems impossible now can be widely used in the future. Currently 12 TWh/year and rising will be consumed through Bitcoin Mining, and another 6 TWh/year by Ethereum Mining, this is the equivalent of 8 million average German households therefore in the context of smart city and sustainable development it is vital to step up efforts to increasingly use renewable energy sources in production of cryptocurrency (mining).

REFERENCES

[1]. Davis J., *The Crypto-Currency: Bitcoin and its mysterious inventor,* The New Yorker, pg. 93-96, 2011.

[2]. Detrixhe J., *The secret to crypto investing is there is no secret*, (https://qz.com/1321633/), 2018.

[3]. Jason M., *Cracking the Bitcoin: Digging Into a $131M USD Virtual Currency*, Daily Tech, 12 June 2011.

[4]. Timothy B., *An Illustrated History Of Bitcoin Crashe*, Forbes, 07 August 2011.

[5]. Antonopoulos M., *Mastering Bitcoin: Unlocking Digital Crypto-Currencies. O'Reilly Media*, 2014.

[6]. Merkle R.C., *Protocols for public key cryptosystems*, In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pg. 122-133, April 1980.

[7]. Nakamoto S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, www.bitcoin.org, 2008.

[8]. Nakamoto S. et al., *Bitcoin source code - amount constraints*, GitHub, 2016.

[9]. Wilson T., *Twitter and LinkedIn ban cryptocurrency adverts – leaving regulators behind*, Independent, 28 March 2018.

[10]. *** http://bitcoindaily.org/bitcoin-guides/what-is-bitcoin-mining/