INSIST Vol. 4 No.1, April 2019 (191–194)
http://insist.unila.ac.id/
DOI:10.23960/ins.v4i1.191
eSSN: 2502-8588
Received: 22/07/2018
Accepted: 05/01/2019
Published online: 01/04/2019

Bitcoin mining, the way to process transaction information or the way to make money?

Jiangdong Cao[1,*], Wei Cao[2]

Abstract—Bitcoin is a crypto currency introduced by Satoshi Nakamoto in 2008. It has the features of decentralization cross-border and fixed total amount and has become one of the most widely used crypto-currencies. Bitcoin, as a new digital currency system, innovatively makes the use of cryptographic elements and consensus mechanisms and builds up a secure decentralized system. The Blockchain, as the core of Bitcoin, uses peer-to-peer network communications and backs up transaction data in every node of the system, thus creating a huge distributed public book. It is essentially a decentralized distributed ledger database, and the decentralization means that the transaction is broadcast to the entire network, where everyone is involved in book keeping. In order to make every participant in the Blockchain willing to participate in the bookkeeping, the reward mechanism of the Bitcoin system is mining. This article first introduces the concept of Blockchain technology, then expounds the principle and the operation mechanism of the Bitcoin and the Bitcoin mining principle, introduces an example of Bitcoin mining in-depth study and analysis, finally, summarize and prospect the development of the Bitcoin mining.

Keywords—Blockchain, Bitcoin mining, Decentralization

I. INTRODUCTION

BITCOIN was born in a global economic environment that was just beginning to be hit by the US subprime crisis. It integrates distributed technology, cryptography and game theory, which are not new fields of knowledge, and realizes a consensus mechanism called "Blockchain". Traditional monetary system typically consists of a unified agency or a dominant third party as a central node and the Bitcoin overturns this kind of design. It uses consensus and incentive mechanism to maintain a distributed public account book in the peer-to-peer network, and the data in the book is secured and legalized by cryptographic algorithm [1]. Blockchain is the data structure of distributed account books in Bitcoin. It is composed of many blocks connected head to tail with decentralized feature, each recording the trading data of the system over a period of time. The decentralization of Blockchain means that the transaction is broadcast to the entire network, where everyone is involved in bookkeeping. In order to make every participant in the Blockchain willing to participate in the bookkeeping, the reward mechanism of the Bitcoin system is Bitcoin mining. This task is similar to the "gold rush" in real life, many people call it mining. The paper is organized as follows. Section 2 introduces Blockchain and its features. Section 3 expounds the most primitive application of digital currency in Blockchain Bitcoin. The process of Bitcoin mining is studied and analyzed through theory and examples in Section 4. The paper is briefly concluded in Section 5.

[1]Department of Computer Science, China University of Geosciences, NO.388, Lumo Road, Wuhan, P.R.China.
[2]Department of Computer Science, China University of Geosciences, NO .388, Lumo Road, Wuhan, P.R.China.
[*]Correspondence to Jiangdong Cao, email: galtoncao@gmail.com.

II. WHAT IS BLOCKCHAIN ?

Although Blockchain is a new concept, it relies on technologies that are not new at all, such as asymmetric encryption technology, P2P network protocol, etc. Like lego bricks, blocks are finite, but different combinations can produce very interesting things.

A Blockchain is a continuously growing list of records, called blocks, which are linked and secured using cryptography. In a narrow sense, Blockchain is a decentralized distributed database [2]. The data blocks as a number of transaction records arranged in chronological order are stored in the database, which are stored in each block, which are generated by cryptographic methods to ensure that data cannot be falsified, cannot be forged, and can be verified; With the consensus algorithm, all the nodes of the whole network can complete the recognition of the block. Broadly speaking, the Blockchain technology is a whole process of using cryptographic chain block structures to test and store data, to generate and update data using distributed node consensus algorithms to generate and update data and to use automated scripting code to program and manipulate data. This is a new way of decentralized infrastructure and distributed computing paradigm. It has two main features as follows:

1) *Decentralization*: Blockchain is a distributed data storage structure. There is no central node, and all nodes keep all the same block information, it is fully decentralized. It is an open and distributed ledger that can efficiently record transactions between two parties in a verifiable and permanent way. For use as a distributed ledger, a Blockchain is typically managed by a peer-to-peer network which collectively adhere to a protocol for inter-node communication and validating new blocks. After the agreement is reached between the nodes, the transaction is written into the block, and there is no third-party certification authority to handle the application and operation.
2) *Tamperability*: Each of the transaction information stored in the Blockchain has a corresponding Hash value. The Hash value of each record is used as the leaf node to generate the binary Merkle tree. The root node (Hash value) of the Merkle tree is stored in the bulk part of the block. Besides the root node of the Merkle tree of the current block, the time stamp and the identifier (Hash pointer) of the previous block are also saved to form a chain structure. Therefore, to tamper a record in the Blockchain, you need to modify not only the Hash value of this block, but also the Hash value of all subsequent blocks. In fact, it's hard to do.

Based on the previous analysis of Blockchain and refer to the literature [3], Blockchain has the structure as shown in Fig.1.

INSIST Vol. 4 No.1, April 2019 (191–194)
http://insist.unila.ac.id/
DOI:10.23960/ins.v4i1.191

Received: 22/07/2018
Accepted: 05/01/2019
Published online: 01/04/2019

III. BITCOIN, THE MOST PRIMITIVE APPLICATION OF DIGITAL CURRENCY IN BLOCKCHAIN ?

A. *What is Bitcoin?*

Talk about Blockchain around the currency, however, like to talk about economics but trading. As the most original and purest application of digital cryptocurrency in Blockchain [4], Bitcoin has become the most specific research case of Blockchain. So,what is Bitcoin?

Some people think it as a speculative bubble, while others call it a digital revolution. Everyone has a point about the world's first cryptocurrency, Bitcoin.

Bitcoin is a decentralized digital currency. Digital currency is a new type of currency that does not rely on credit or physical goods, and its value is determined by consensus. Decentralization means that all transactions are conducted directly between users, without any agents, such as Banks, payment systems, or government control. Digital mean that Bitcoin exists as a record of transaction data. It's a virtual currency that we call it Bitcoin.

B. *The principle and the operation mechanism of Bitcoin*

Bitcoin is a digital document that lists accounts and amounts, like a ledger, and a copy of the document is stored on every computer in the Bitcoin network. In fact, in the real world, these numbers don't make any sense, they are valuable because people are willing to trade them for real goods and services, and believe others will do the same.

When you transfer money to someone else, you need to send a message to the entire network, and then the amount of your account will decrease and the recipient's account will increase. At the same time, nodes or computers in the Bitcoin network update their account copy information, and then continue to pass the transaction information to other nodes. Based on the security mechanism, this digital computing,which forms the Bitcoin trading network itself, is a system that allows a group of computers to jointly keep a copy of a ledger.

Bitcoin adopts an internet-based peer-to-peer (P2P) distributed network architecture which is shown in Fig.2, P2P network refers to that every computer in the same network is equivalent to each other, and each node provides network services together. There are no "special" nodes, and each network node is connected with each other in a flat topology, and a Bitcoin network can be thought of as a collection of nodes running on a peer-to-peer basis.

Because of this network mechanism, unlike in a bank where only you know your trading information, in a Bitcoin trading network, everyone knows everyone's trading information. But in real life, if some trade goes wrong, you can trust the bank also has the right to prosecute it, but in the Bitcoin network, every time you are dealing with a stranger all the time, so you can't trust anyone. Based on this reason, the Bitcoin system is designed to make "trust" unnecessary, the special digital function ensures that every aspect of the system is running normally. So, how does Bitcoin work?

Well it's pretty simple, for example, when transferring 5 BTC from Alice account to Bob account, she only needs to broadcast a message to the Bitcoin network, indicating the account and amount information, Every node receiving this message will update their account copy information, and Alice

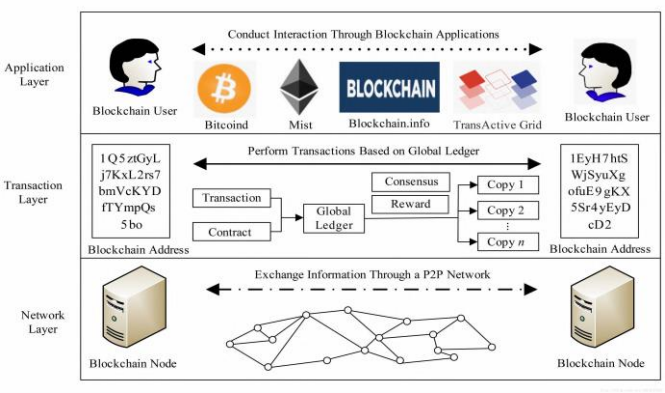

Fig. 1. A three-layer architecture of Blockchain.

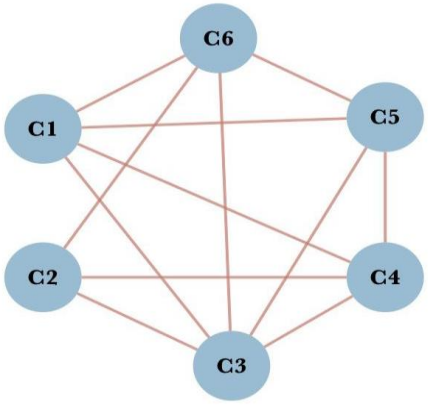

Fig. 2. A peer-to-peer network.

will update her total account (5 BTC reduced), and Bob will update his total account (5 BTC increased). But how can a node determine that this message is credible?

In fact, Bitcoin has a set of cryptographic rules for unlocking and managing currency transactions called "digital signatures." Like a signature in real life, it can prove the authenticity of a transaction and is implemented by a digital algorithm. This algorithm can prevent data replication or forgery. Only true owners has the right to send this message.

In the Bitcoin trading network, the ownership of currency is verified by verifying historical transaction information. For example, in order to send 5 BTC to Bob, Alice must refer to the historical transaction information that received these 5 BTC before. These quoted transaction records are called "incoming accounts", and the nodes in the network that verify the transaction information will check those "incoming accounts" to ensure that Alice is the true receiver, and ensure that the amount received is 5 BTC. One can easily understand this process through Fig.3.

From here, we can see that Bitcoin does not use the way of recording account balance, but uses the way of recording transaction information, forming a huge transaction record table. Well, Bitcoin uses the UXTO model (Unspent Transaction Outputs model), this model expresses the concept of transfer, that is, any generated new currency, in the subsequent life cycle, only transfer, not extinction, is essentially controlled by the signature and verification of the encryption algorithm. The model diagram is shown in Fig.4.

INSIST Vol. 4 No.1, April 2019 (191–194)
http://insist.unila.ac.id/
DOI:10.23960/ins.v4i1.191

Received: 22/07/2018
Accepted: 05/01/2019
Published online: 01/04/2019

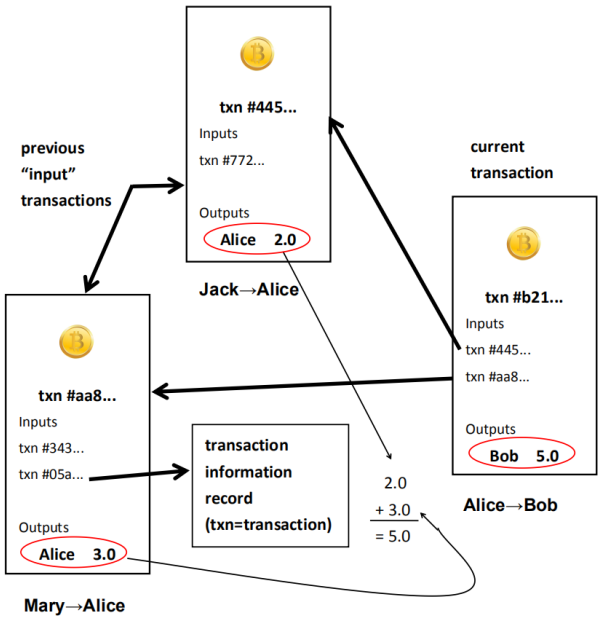

Fig. 3. Quoting historical trading information.

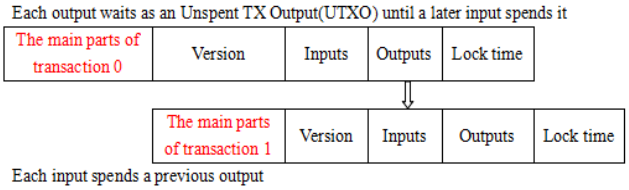

Fig. 4. UTXO model diagram.

IV. BITCOIN MINING

A. *The way to process transaction information*

Blockchain underlies cryptocurrencies such as Bitcoin, which is traded as units called Bitcoins with a lowercase 'b. It is created by a community of 'miners, who run Bitcoin software on their hardware and compete to discover a hard-to-find number by trial and error. The victor of this contest adds an encrypted block of transactions to the chain and earns a financial reward. They communicate the extended Blockchain to all other miners, and the process starts again, Andy Extance says [5]. In fact, this is the Bitcoin mining process.

Simply, through the knowledge of the mechanics of the Blockchain and Bitcoin, we know that the trade of Bitcoin is the transaction of information records, and all the transaction record data blocks are added together to form the Blockchain. When the user posts the transaction information, someone needs to confirm the transaction and write it into the blockchain to form a new block. In a system of mutual distrust [6], who should do this work? The Bitcoin network has taken a "mining" approach to solve the problem. Therefore, mining can be said to be the processing of the transaction information of the Bitcoin system, that is, the bookkeeping process of nodes. In short, the process of processing transaction information in the Bitcoin system by consuming the computing power of a computer is Bitcoin mining.

As more and more people and institutions joined the decentralized mining, it was discovered that no one or organization could monopolize the Bitcoin mined. According to the system's design, if any person or organization wants to monopolize the mining of Bitcoin, it must master more than half of the mining computers and equipment, but this is impossible to achieve, so that the Bitcoin system becomes stronger and safer. If the system is attacked by hackers, only a small number of nodes will be affected, most of them will continue to process transactions, continue mining, will not be affected at all. Mining profits come from Bitcoin rewards and transaction fees. The mining reward mechanism for the Bitcoin system just solved the problem of each of the nodes equal and no obligation to serve the people, because as long as you pay the resources and computer resources, you will get the reward of the system. More pay for more work, and the system is run automatically, no one can tamper with it, this is fair, everyone can make a profit through their own work, and, yes, the reward is the source of power, motivating more people to join in building and maintaining the system. It is the mining that lead to the massive numbers of miners that keep the system alive.

Speaking of that, you can see that Bitcoin mining is also a money-making process.

B. *The way to make money*

Now more and more people put the Bitcoin mining as a investment method is not unreasonable. First of all, we can see through the Fig.5, there are quite a few stores in the world that can use Bitcoin, and the number of stores is still increasing. Moreover, Bitcoin has become the actual hard currency in the whole cryptocurrency and Blockchain industry, and become the real digital gold. The entire cryptocurrency industry as a whole is worth only a few hundred billion dollars, and gold's global value is seven trillion dollars. The value of Bitcoin and cryptocurrencies has only just emerged, and there is no limit to how much space they can rise. Based on this, the fact that Bitcoin is an investment object is in place.

As mentioned earlier, Bitcoin is essentially a public, untamable, distributed book of accounts. Mining is actually accounting through mathematical calculations, while a large number of mathematical cryptographic operations are used to ensure that this account book will not be tampered with. Accounting costs a lot of computing power, hardware and electricity, and as a reward, the new Bitcoin is owned by the miners.

There are several factors that affect the income of mining. First, the value of Bitcoin, the higher the price of Bitcoin, the more profitable mining. Second, the difficulty of mining, the more slowly the difficulty of mining increase, the more profitable mining. The lower the cost, the more profitable the mining. Of course, the cost here refers to the cost of purchasing power and operating costs, including labor, network fees, construction cost, electricity, and so on. The lower the cost, the better.

Let's discuss an example: Suppose you buy an Antminer S9 14T miner, as shown in Fig.6. Through the online computing platform, we can do a rough calculation of the returns [7], and we can see from Fig.7 that the revenue cycle is still very long. Does Bitcoin mining make money or not now? It's worth thinking about.

INSIST Vol. 4 No.1, April 2019 (191–194)
http://insist.unila.ac.id/
DOI:10.23960/ins.v4i1.191

Received: 22/07/2018
Accepted: 05/01/2019
Published online: 01/04/2019

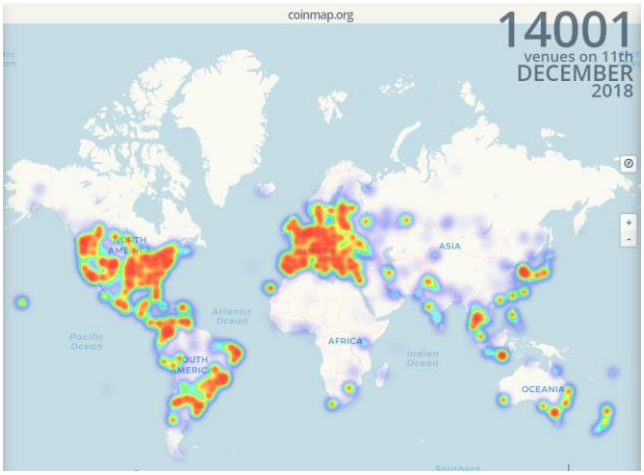

Fig. 5. Map showing places where Bitcoin is accepted.(The more red the color,the more concentrated the Bitcoin transactions)

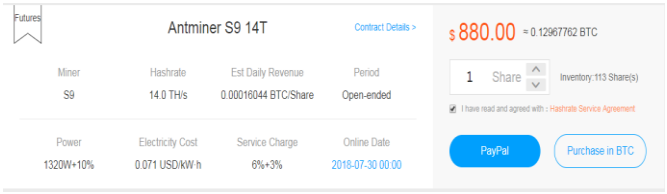

Fig. 6. The cost of an Antminer S9.

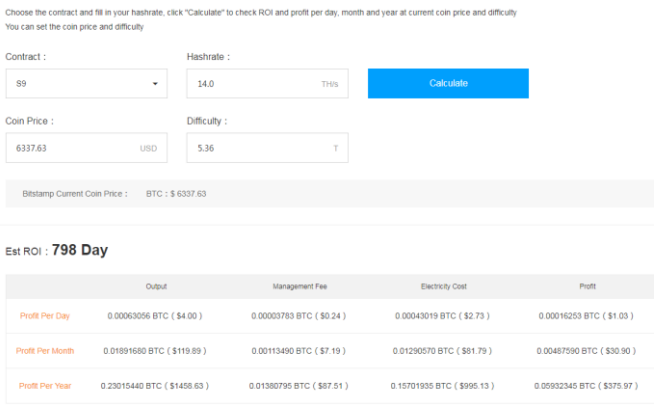

Fig. 7. Simulated revenue calculation.

The Bitcoin network now produces one block every 10 minutes, and each block will reward the miners with 12.5 Bitcoins, including transaction transfer fees for the block, which now account for about 15-20% of the block rewards. The total number of Bitcoin is 21 million, and every four years of the block rewards is cut in half, and by 2140 virtually all of the Bitcoin is produced, so the total amount of Bitcoin is constant, and it's not going to increase. As can reflect the Bitcoin design ideas of Satoshi Nakamoto, and all of the foundations of the currency system security, the mining industry will continue to exist. However, the reversion cycle will gradually become longer, so it is unlikely to return to the original period in the first few decades or even ten days. The revenue cycle over one year will be the normal state.

In view of this, the return on investment from individual mining will not be obvious. In the future, mining will be highly intensive and some super-large mines will be built.

V. Conclusion

This paper introduces the operation principle of Blockchain and Bitcoin, and through the promotion of the concept of progressive layer by layer and the introduction of an example, one can have a deep understanding of the purest application in Blockchain Bitcoin. The connotation of Bitcoin transaction and the essence of Bitcoin mining are mainly explained in this paper. Especially Bitcoin mining, now more and more people are engaged in it, everyone wants to gain benefits through the incentive mechanism of Bitcoin. But we need to spend a lot of manpower and material resources on it. Often, the process of benefit is very long, so we need to deeply understand the principle and combine all aspects to decide whether to join the miners. But as a trading method alone, Bitcoin has its own unique advantages, which is undeniable.

Acknowledgment

This research is supported by China University of Geosciences (CUG) funds.

References

[1] S. Nakamoto. (2008, October). A Peer-to-Peer Electronic Cash System . Available: https://Bitcoin.org/Bitcoin.pdf
[2] Y. Yuan , F. Y. Wang,"Blockchain: The State of the Art and Future Trends," Acta Automatica Sinica , vol. 4,pp. 481-494 , Apr.2016.
[3] L. H. Zhu, F. Gao , M. Shen ,Y. D. Li ,B. K. Zheng , "Survey on Privacy Preserving Techniques for Blockchain Technology," Journal of Computer Research and Development, vol.54, pp. 2170-2186 , Apr.2017.
[4] W. T. Tsai ,L. Yu ,W. Rong ,N. Liu ,E. Y. Deng ,"Blockchain Application Development Techniques," Journal of Software, vol.28, pp.1474-1487, Jun.2017.
[5] A. Extance,"Could Bitcoin Technology Help Science?," Nature , vol.552, pp.301 , Dec.2017.
[6] R. Beck ,J. S. Czepluch ,N. Lollike , "Blockchain – The Gateway To Trust-free Cryptographic Transactions," in Twenty-Fourth European Conference on Information Systems, Turkey, 2016, pp.1-14.
[7] Mining Calculator, https://www.suanlitou.com/calculator?l=en-us.
[8] B. Qin ,L. C. Chen,Q. H. Wu, "Bitcoin and digital fiat currency," Journal of Cryptologic Research , vol. 4, pp.176-186 , Feb.2017.
[9] Map of Bitcoin accepting venues, https://coinmap.org