Research on Bitcoin's Working Mechanism and Monetary Attributes

Shengye Tao [1, a] and Zhen Li[2, b*]
[1]*Hohai University, School of Marxism, Nanjing, Jiangsu, China*
[2]*Jining University, Jining, Shandong, China*

Keywords: Bitcoin, Monetary, Attribute.

Abstract: This paper analyses the currency attributes of bitcoin starting with the operation principle of bitcoin. This paper argues that 1. Bitcoins are automatically generated by computer algorithms and do not involve social labor; 2. transaction confirmation time is so long, block capacity is so small, that bitcoin has difficulty in dealing with the huge amount of transaction payment information; 3. the total amount fixed and high concentration make the bitcoin unable to perform the function of storage means; 4. the bitcoin is difficult to conduct credit transactions and financing activities because of highly anonymity; 5. unstable transaction value and the number of issues of bitcoin does not match the growth of international trade make it difficult to be an international currency.

1 INTRODUCTION

On November 1, 2008, Satoshi Nakamoto, the inventor of Bitcoin, published a paper entitled *Bitcoin: A Peer-to-Peer Electronic Cash System* on the Internet. Nakamoto introduced an electronic cash system based entirely on Point to Point (P2P). In such a system, blockchain technology and distributed database are utilized so that both parties of the transaction can get rid of a third-party intermediary (commercial banks, for example) and conduct payment directly, hence creating a brand new decentralized monetary payment system. This is the birth of Bitcoin, a digital currency that is not controlled by central banks and any financial institutions. The first transaction using Bitcoin took place in 2010 when an American programmer managed to exchange 10,000 Bitcoin for two slices of pizza. At that time. 10,000 Bitcoins were only worth 30 USD. Earlier in 2021, the price of Bitcoin hit its highest in history, at 46,000 USD. However, it fell back to 30,000 USD in a few days. Bitcoin's price has been soaring since its birth, creating a wave of digital currency in the world financial sector. Bitcoin has received wide attention from governments, investors, and consumers around the world. Germany has become the first country in the world to recognize the legal status of Bitcoin. Canada installed its first Bitcoin ATM, through which citizens can exchange Canadian dollars and Bitcoins in both directions. The United States and Singapore are supportive of Bitcoin trading. The governments of Russia and Thailand, however, have completely blocked Bitcoin. India, Norway, and South Korea, on the other hand, are prudent towards the use of Bitcoins, and have issued some regulations to restrict the cryptocurrency's development. Five Chinese Ministries and Commissions, including the People's Bank of China, jointly issued the Notice of Preventing Bitcoin Risks in 2013, refusing to recognize the monetary attributes of Bitcoin and banning its circulation in the domestic market.

At present, major controversies still exist in the academic community concerning the monetary attributes of this cryptocurrency. Scholars with a supportive attitude believe that Bitcoins can be used as a universal equivalent that participates in commodity exchanges. By analyzing the five functions of a currency, Hong concluded that Bitcoin is the same as other currencies such as gold and silver in serving the functions of currency (Hong, 2011). McHugh described Bitcoin as "another form of currency" and "a kind of private currency." (McHugh, 2014) Chowdhury and Mendelson hold the belief that as more and more people came to recognize virtual currencies, it is only a matter of time before virtual currencies go mainstream (Chowdhury, 2014). Jia believes that Bitcoin is a brand new decentralized virtual currency that can serve as a measure of value, an exchange medium, the means of payments, and a

Tao, S. and Li, Z.
Research on BitcoinâĂŹs Working Mechanism and Monetary Attributes.
DOI: 10.5220/0011733200003607
In *Proceedings of the 1st International Conference on Public Management, Digital Economy and Internet Technology (ICPDI 2022)*, pages 208-214
ISBN: 978-989-758-620-0

store of value, forming an independent currency system. Based on the current challenge facing the Bitcoin market, Jia also proposed that we should improve the supervision of Internet financial institutions and establish a coordinated supervision mechanism. (Jia, 2013)

However, some scholars hold a dubious attitude towards Bitcoin's monetary attributes and durability. Surda believes that without intrinsic value or government endorsement, Bitcoin's circulation depends entirely on users' confidence and markets' acceptance. (Surda, 2014) Wang proposed that there are four major risks in the use of Bitcoin: the uncertain legal status, the vulnerability of trading platforms, price fluctuations and Ponzi schemes, as well as value abrasion. (Wang, 2013) According to Wu, problems and risks of Bitcoin include excessive speculation, cybercrime, huge price fluctuations, waste of social resources, etc. (Wu, 2013) Li proposed that Bitcoin is a kind of virtual speculative asset. It is neither a commodity currency nor a credit currency, which means it can never be a real currency in China. Bitcoin's decentralization nature, fluctuating exchange values, and the fixed amount that cannot be able to keep up with the international economic development mean that this cryptocurrency will never become an international currency. The fate of Bitcoin depends on how the central banks view it and the merchants' willingness to accept it. (Li, 2015)

Bitcoin is generated by computer algorithms, a great difference from any previous currency. The author of this paper will start with Bitcoin's working mechanism, and then conduct an economic analysis of Bitcoin before he finally reaches a conclusion.

2 BITCOIN'S WORKING MECHANISM

By using blockchain technology and a distributed database, Bitcoin forms a P2P electronic cash transaction system. No third-party intermediary would be involved in the transaction process. The transaction will be carried out solely by the two parties. It would be a brand-new decentralized currency payment system.

2.1 Bitcoin's Payment Mechanism

In traditional centralized payments, financial institutions such as commercial banks serve as third-party intermediaries and transfer the money from Client A's account directly to Client B's account. They use their ledger which stores the balances of all depositors to make these transactions happen. The commercial banks lie at the center of the payment. They have to ensure that the amount in each client's account could not be changed for no reason. Commercial banks set up their computer rooms, build independent network environments, purchase advanced servers and hire senior experts for security reasons.

Bitcoin, however, adopts a decentralized ledger storage solution. All computers connected to the Bitcoin system (or the "nodes") store a ledger that records all payments up to this point. Since the ledger is stored at each node, if problems occur at one of these nodes, the correct data can still be accessed from other nodes on the network. When the ledger is updated at a certain node, other nodes would be notified to change their ledger records.

Bitcoin Payment not only involves paying with Bitcoin, but also the recording of corresponding payment information. Such information includes 1. Bitcoin addresses (id); 2. source of the fund, the Bitcoin addresses (id) of the previous payment where you receive these Bitcoins; 3. payers' electronic signature in the previous payment where you receive these Bitcoins for other nodes to verify the authenticity of the source; 4. destination of the funds, and the account (public key) of the Bitcoins' recipient; 5. amount of the fund; 6. payers' signature for this transaction to prove that he/she is the issuer of the payment. Since each transaction order records the previous owner, current owner, and the future owner of the funds, we will be able to trace the entire process of the transaction based on this information. This is also one of the characteristics of Bitcoin. Finally, when each transaction is completed, the system would inform all users of the execution of this payment. (Yao, 2013)

All information of Bitcoin payments that abide by the system rules will be packed and stored. The package they form is what we usually call a "block". Currently, the Bitcoin system generates a block every ten minutes, and each block records the parameters of the previous block. In this way, each block can be traced back to its previous block, and even all the way to Block #0 (or the Genesis Block), hence forming a complete transaction chain, also a now-famous blockchain. This blockchain will announce to the whole network each time a new block is added so that every "node" in the Bitcoin system could have a copy of the record. The highly decentralized storage of transaction information makes it almost impossible for us to completely lose the Bitcoin blockchain.

We can see from the above introductions that once

payment information is stored in a blockchain. Theoretically speaking, it cannot be modified or deleted. With its unique technical characteristics, Bitcoin provides us with a new payment mechanism.

2.2 Bitcoin's Generation

Once a Bitcoin transaction occurs, the system will first verify the transaction information throughout the entire network to ensure that the source and destination of the Bitcoins are authentic and valid to prevent false payments and double payments. If the verification succeeds, these transactions will be temporarily stored in a valid transaction pool; they are called "unconfirmed transactions". Eventually, the unconfirmed transactions will be loaded into a block. Only when the newly formed block is added to the entire blockchain, can the transaction be declared settled. From that moment, the transactions can no longer be modified or deleted anymore. On the other hand, if the verification fails, the transaction will be deemed as an "invalid transaction."

As was mentioned earlier, in times of a new block being added to the chain, the blockchain will announce the whole network, so that every computer connected to the Bitcoin system could make a copy of the record. The more computers connected to the Bitcoin system are, the more secure the transaction information, i.e., the blockchain will be. To encourage more people to connect their computers to the Bitcoin system and make use of their idle computing power for accounting, certain rewards are provided for each computer node that gains the power to add a new block for the first time. Those rewards are today's well-known Bitcoins. The newly generated information of Bitcoin is also stored in the new block. In January 2009, the first block, Block #0, or the Genesis Block, was included in the public ledger at 6:15 p.m. at server time. The reward was 50 Bitcoins. Besides a certain amount of Bitcoin, these nodes that have the right to add a new block will also be rewarded some "transaction fees" from the transaction orders in the new blocks.

So far, as Bitcoin continues to enter the public eye, more and more people (or computers) are connected to the Bitcoin system. Every node on the system is vying for the power to add a new block so that they can gain more rewards. The process is vividly called "mining". Users participating in the Bitcoin system would install mining software on their computers and use them to solve complex problems that are automatically generated by the system. In fact, what these computers need to do is to calculate the hash value generated by the Hash function with the parameters of the previous block. The first node solving the problem will be granted the right to add a new block and at the same time, gain a certain amount of Bitcoin for rewards, while other nodes can only copy the newly added block without any rewards.

According to the setting of the Bitcoin system, the Bitcoins rewarded for each added new block are halved every four years. When the year 2009 first started, the reward was 50 Bitcoins for each new block added. It was 25 Bitcoins for 2013-2016; 12.5 for 2017-2021. The ultimate setting is that the total amount of Bitcoin in the system will reach the upper limit of 21 million in 2140. (Yang, 2014)

Since the number of miners mining simultaneously is uncertain, the Bitcoin system will automatically adjust the problem difficulty based on the total computing power of all nodes, which means if the total computing power is bigger in the system, the problem difficulty will be increased, and vice versa. This rule ensures that the generation rate of new blocks (Bitcoin) remains within an acceptable range. The current rate is one new block generated every ten minutes. As more netizens are interested in mining Bitcoins and invest their computing power in the Bitcoin system, the mining also gets significantly difficult. Now the miners have already formed groups, connecting their computers with each other's and joining their computing powers, forming a so-called "mining pool" to get the ability to solve more difficult mathematical problems and increase the odds of gaining Bitcoins. The Bitcoins then gained will be handed out to the group members based on their contributions.

2.3 Bitcoin's Characteristics

Based on the above analysis of Bitcoin's working mechanism, we can conclude that Bitcoin with the following characteristics:

2.3.1 Decentralization

Most existing currencies are issued by a country's central bank. They receive endorsement from the local governments, and their circulation is guaranteed by the law. Bitcoin, on the other hand, is automatically generated by computer algorithms. Its generation rate and total supply have already been determined at the time of its birth, not subject to the influence of any institution or individual.

2.3.2 High Anonymity

The forming of Bitcoin addresses (id) does not require real-name authentication. All the users need

to do is to submit applications on related websites, and then they can get one or more Bitcoin addresses. These Bitcoin addresses are merely some irregular character strings made of letters and numbers, whose only function is to accept or pay Bitcoins. Therefore, no owner information could be drawn from these addresses. Also, no connection could be seen between different accounts of the same owner, so others would not be able to calculate the total amount of Bitcoins owned by a particular user.

2.3.3 Perfect Traceability

The blockchain records all the transactions that have ever happened in history. Each Bitcoin can be traced back to the time when it was first generated. Every node in the Bitcoin system keeps a complete copy of the transaction history, which means anyone could have access to the transaction records of every account. This puts the whole network under supervision to ensure a fair and transparent market order.

2.3.4 Irreversibility of Bitcoin Transactions

Sustainable right to add a new block would be guaranteed, unless a certain node possesses more than 51% computing power of the entire system. Once a transaction is recorded on the blockchain, other nodes would copy and save the record immediately. It would be impossible to cancel the change or delete the record. This design prevents the payer from infringing the payee's interests by canceling any operations.

2.3.5 No Inflation Will Be Seen in The System

As was mentioned above, the total amount of Bitcoin would be 21 million, and the generation rate of new Bitcoin halves every four years. The new Bitcoin is automatically generated by computer algorithms, so no sudden will increase or decrease in circulation.

2.3.6 Bitcoin Knows No Borders

Anyone who possesses a Bitcoin address (id) with a password (or private key) can receive or pay with Bitcoin on any computer in every corner of the world, without government supervision.

2.3.7 The Transaction Fees of Bitcoin Are Low

Only 1 bitcent would be charged for each transaction. No exchange rate exists in cross-border transactions. (Jia, 2013)

3 BITCOIN'S CURRENCY ATTRIBUTES

From Bitcoin's working mechanism, we can see that Bitcoin has unique characteristics compared to any traditional currencies. Both western economics or Marxist economics agree that a currency should have the following five functions: a measure of value, an exchange medium, means of payments, store of value, and universal currency. The author believes that Bitcoin is still sufficient in fulfilling its functions.

3.1 A Measure of Value

The value of a commodity depends on the relative quantity of labor that is necessary for its production. Here the socially necessary labor time serves as the intrinsic measure of commodity value. Currency is a kind of universal equivalent. The reason why it can be a measure of value is that currency itself also possess value. Therefore, the value contained in other commodities can be measured with the currency as the scale.

Bitcoin was first created to encourage more "nodes" to connect themselves to the Bitcoin system and devote their idle computing power to solving math problems. Bitcoin is entirely generated by computer programs automatically, with no social labor involved in this process. Some believe that the computing hardware and electric power invested in the "mining" process can be seen as the value of Bitcoin. But the truth is, to raise or decrease such investment has little impact on the speed of Bitcoin generation. No matter how many people are engaged in the "mining", Bitcoin will be always generated at a set rate. It is worth noting that to maintain this rate, the Bitcoin system will automatically adjust the problem difficulty based on the sum of computing power in the systems. In other words, if there is more computing power in the system working on the same problem simultaneously, the problem gets more difficult, and vice versa. As the number of "miners" gradually increased, the problems also get more and more difficult, leading to a serious waste of social resources. According to the statistics of the Bitcoin Energy Consumption Index, by the end of 2020, the electricity consumption devoted to Bitcoin mining in 2020 reached 29.51 Terawatt Hours (TWh), accounting for about 0.13% of global electricity

consumption. This figure was higher than the yearly power consumption of nearly 160 countries or regions, including Iceland and Nigeria. If all the Bitcoin miners around the globe were to form a new country, its power consumption would rank 61st in the world. ((Sources: power compare)

3.2 An Exchange Medium

Currency serves as a medium of commodity exchange. In the exchange process, the sellers convert their goods into money, and then use the money they received to purchase new goods. Here, currency serves as the exchange medium that enables goods circulation.

Bitcoin is favored by users due to its decentralization, high anonymity, transaction irreversibility, perfect traceability, and low transaction fees. Many people regard it as a safe and effective means of payment. But we still need to remind you that Bitcoin still poses some concerns: First, the Bitcoin system generates a new block every ten minutes and only at this time, the transaction record loaded on the blockchain will be preliminarily confirmed. The transaction will be further confirmed once the new block is connected to the previous block. Based on the technicality of the Bitcoin system, the transaction could be truly and irreversibly confirmed only after the confirmation of six new blocks. The means to truly confirm a Bitcoin transaction takes about an hour, which is too slow compared to the current centralized payment system that only takes seconds. The slow transaction speed is closely linked to the underlying technical design of the Bitcoin system. Second, a block is 1 M in size, which is big enough to contain around 1,000 pieces of transaction information. This means that a large amount of transaction information will be temporarily stored in the transaction pool to be confirmed. This would prolong the transaction time, posing great limits on the number and scale of transactions being conducted simultaneously. Third, every node in the Bitcoin system must keep a copy of the entire blockchain, and this chain is still getting longer, with one new block added every ten minutes. Currently, its size is even bigger than the storage capacity of any personal computer. Many Bitcoin users have to seek help from the supercomputers in large institutions, which contradicts Bitcoin's decentralization nature. Since deficiencies like this were developed out of Bitcoin's decentralization nature, they cannot be fixed by merely upgrading the central hardware or software just like what has been done on a centralized trading system. The solutions to those problems are still unknown and under discussion.

3.3 Store of Value

Currency as a store of value refers to its being preserved as a symbol of social wealth when it is no longer circulated on the market. It can adjust the amount of currency being circulated. Only authentic and pure gold and silver, in the forms of coins and bars, can be kept as a store of value. When kept in banks, paper money can be seen as the symbol of one's assets, but it can never be a store of value. People will only keep paper money only when its value could remain stable for a long time.

Bitcoin does not possess any value in itself, so it can never be a store of value like gold and silver. Though the total amount of Bitcoin was set to be 21 million, some people insist that it has high resistance to inflation. However, two shortcomings that exist with Bitcoin make it almost impossible for this cryptocurrency to become a store of value. On the one hand, there will be only 21 million Bitcoin in this world, but our total economic and social production capacity is far greater than this. We all know that Bitcoin can be divided into eight decimal places, so it seems possible for it to satisfy the transactions of the whole society. However, owners of Bitcoin, seeing the rising trend of Bitcoin prices, would not use their Bitcoin for transactions. Instead, they will hoard them and wait for them to appreciate. An American economist, Paul Krugman, once wrote: "What we want from a monetary system is not to make people holding money rich; we want it to facilitate transactions and make the economy as a whole rich." "Due to the expectation that Bitcoin economy will grow, people will tend to hoard the virtual currency rather than spending it," resulting in "money-hoarding, deflation and depression." On the other hand, when Bitcoin first appeared, only geeks [1] would collect this virtual currency, leading to today's excessive concentration of Bitcoin. As reported by Bloomberg, nearly 40% of the world's Bitcoin is owned by a thousand users. "They have a great impact on the Bitcoin market. They are known as whales." If Bitcoin can serve as a store of value, it means nearly 40% of the social wealth would be in the hands of these one thousand people. Obviously, it is unacceptable to almost any economy or society.

[1] Geek: With the rise of the Internet culture, geeks refer to those who show passion for computing and Internet technologies and are willing to devote much of their time in learning such technologies.

Figure 1: Bitcoin's Price History in the Previous Year (Sources: www.price.btcfans.com).

Even though Bitcoin cannot be a real currency enabling economic and social circulation, such a high concentration still contradicts Bitcoin's decentralized nature.

3.4 Means of Payments

Currency serves as a means of payment during debt repayment. In fact, commodity exchange can be done without cash. Deferred payment can be possible, where the cash will be paid after a certain period. Here currency serves as a means of payment. Its function as a means of payment was first seen in commodity exchange, and later expanded outside of it. With the rise of deferred payment, various credit currencies also appeared, such as promissory notes, checks, money orders, banknotes. These diverse credit currencies also function as means of payment. In the meantime, the debts they represent can offset each other, which has significantly reduced the amount of currency being circulated in the market.

Based on Bitcoin's trading mechanism, deferred payments or credit behaviors are still impossible in transactions of Bitcoin. First of all, the irreversibility of Bitcoin transactions can effectively protect the recipients' privacy, but not the interests of the payers. A third party, for instance, Alipay, is required to protect their interests. To this end, one or several centralized nodes could be generated to ensure the smooth progress of transactions, which will also contradict the decentralized nature of Bitcoin. Secondly, whether it is direct financing or indirect financing, the borrower's identity needs to be confirmed and the borrower's credit information is needed as the basis for risk evaluation. However, Bitcoin's high anonymity makes it almost impossible for relevant information to be collected. If an intermediary institution like a bank is brought in to bridge the borrowers and lenders, it means another central node has to arise. All these mean that although it is technically feasible to finance through Bitcoin, the action will undermine the virtual currency's decentralized nature. Financing difficulties will become a major obstacle to Bitcoin's development. Thirdly, even if financing becomes possible in the Bitcoin system, credit instruments like promissory notes, checks, money orders, banknotes will be created. The excessive use of credit instruments could result in the forming of a central banking system, also contrary to Bitcoin's decentralization.

3.5 World Currency

When a currency serves as a universal equivalent in the world market, it is also called a world currency. Bitcoin knows no borders. Anyone can receive and pay Bitcoin on any computer in every corner of the world without government supervision. However, as it is pointed out by Li, Bitcoin could never become a world currency. If we want Bitcoin to become a world currency, its "decentralization" has to be replaced by "centralization"; its exchange value must remain stable; its total amount shall be able to meet the requirements of global economic development (Li, 2015). At present, Bitcoin is not able to serve the function of being a world currency.

4 CONCLUSIONS

Bitcoin is a major breakthrough in currency development. The devising of a reliable electronic payment system provides valuable experience for designing future payment systems and virtual currency systems. Bitcoin's inherent advantages

provide a series of innovative ideas and methods for solving the currency-related problems faced by all countries around the globe, especially inflation. Financial institutions of all countries can learn from Bitcoin's design concept. However, though Bitcoin presents technical innovations and solutions to traditional problems, it also brings some new and serious problems that are not easy to be fixed, which casts a shadow over its long-term development. As the concept of Bitcoin went viral in recent years, people's attention has been shifted from this technological innovation to its possible price bubble. it is concluded that, instead of Bitcoin itself, we should focus more on its underlying techniques, namely blockchain technology and distributed storage technology. The latter will surely play a bigger role in future economic development and provide more feasible solutions and technical support for solving practical problems.

REFERENCES

Chowdhury A, Mendelson B K. Digital Currency and Financial System. (2014) The Case of Bitcoin[J]. Investments & Wealth Monitor.

Hong S. Bitcoin. (2011) A Cryptocurrency's Challenge to the Financial System [J]. China Credit Card, 2011(10): 61-63

Jia L. Theories. (2013)Practices and Influence of Bitcoin [J]. Studies of International Finance, 2013(12): 14-25.

Jia L. (2013) Theories, Practices and Influence of Bitcoin [J]. Studies of International Finance, 2013(12): 14-25.

Li C.(2015) Will Bitcoin Become a Currency? [J]. Contemporary Economic Research, 2015(4): 60-65.

Li C. (2015) Will Bitcoin Become a Currency? [J]. Contemporary Economic Research, 2015(4): 60-65.

McHugh S, Yarmey K. Near field communication. (2014) Recent developments and library implications [J]. Synthesis Lectures on Emerging Trends in Librarianship, 2014, 1(1): 1-93.

Surda P. (2014) The Origin, Classification and Utility of Bitcoin[J]. Classification and Utility of Bitcoin (May 4, 2014), 2014.

Wang G., Feng Z. (2013) Risks, Current Regulations and Policy Recommendation of Bitcoin [J]. Finance and Economy, 2013(9): 46-49.

Wu H., Fang Y., Zhang Y. (2013) A Crazy Digital Currency: Nature of Bitcoin and its Enlightenment [J]. Journal of Beijing University of Posts and Telecommunications, 2013, 15(3): 49-50.

Yao Y. (2013) Easy Understood Bitcoin Mechanism. www.btcl23.com/data/docs/easy_understood_Bitcoin_mechanism.pdf

Yang C., Zhang M. (2014) Dynamics, Characteristics and Prospects of Bitcoin [J]. Chinese Review of Financial Studies. 2014(1): 38-53.