The Future of Bitcoins

Yaodan Zhang(✉)

Arts and Social Sciences, The University of Sydney, Sydney, NSW 2006, Australia
yzha2082@uni.sydney.edu.au

Abstract. With the outbreak of the Russian-Ukrainian war, more and more Western countries have imposed sanctions on the assets of the Russian people overseas, which have triggered a crisis of confidence in the world's currency, the dollar. At this time, the popularity of Bitcoin has also resurfaced. People are starting to think about the future of Bitcoin. This paper starts from the basic technical means of bitcoin and discusses the possibility of the future development of bitcoin by analyzing the characteristics of bitcoin. We believe that although Bitcoin cannot become a world currency in the future, it can become an investment asset and a convenient means of payment.

Keywords: Bitcoin · Blockchain · Decentralization · Anonymity · Functions of money

1 Introduction

This paper introduces the technology, principles, and characteristics of Bitcoin. The research purpose of this paper is to analyze how bitcoin will emerge in the future. Section 2 introduces the background of bitcoin. Section 3 is the definition and technology of bitcoin. Section 4 combines the characteristics of Bitcoin with its technical analysis. Section 5 explores the future of Bitcoin through the analysis of its characteristics. Section 6 makes a conclusion. The last section shows the limitations of the paper.

2 The Birth of Bitcoin in the Subprime Crisis

In the early 21st century, the U.S. government tackled the recession caused by "9.11" incident and the bursting of the IT bubble by introducing incentives for Americans to buy homes. The commercial banks and financial institutions continued to provide loans to low-credit groups to stimulate people to buy houses after the policy was issued. These loans provided to low-credit groups are sub-prime loans. Rising house prices have allowed unqualified people to mortgage their homes to pay off their loans. In this environment, the U.S. economy returned to growth. However, after the number of new homes in the US reached 2.3 m in January 2006, prices began to fall. The subsequent fall in house prices caused many unqualified lenders to default. Because of liquidity difficulties, these frequent default events have caused many financial companies' funds

F. Balli et al. (Eds.): ESFCT 2022, AEBMR 226, pp. 1087–1092, 2022.
https://doi.org/10.2991/978-94-6463-052-7_122

to draw on bank credit, which made the real estate bubble transmitted to the credit market, and the credit market bubble transmitted to the capital market. For more than a year, the subprime mortgage crisis began in the United States and then spread around the world. In this situation, many countries over-issued currency, causing the assets in the hands of the people to shrink continuously, and people have a credit crisis for centralized banks, which also stimulated the birth of Bitcoin.

On October 31, 2008, Satoshi Nakamoto released the Bitcoin White Paper, pointing out that Bitcoin is an electronic transaction system that does not rely on credit. Satoshi Nakamoto wanted Bitcoin to be a system without top-down control, managed by a decentralized crowd. Satoshi Nakamoto received 50 bitcoins for 'mining' the first block in January 2009. Satoshi later sent coins to Hal Finney [1], an early developer. Over time, Bitcoin's meteoric rise as the original cryptocurrency has made it a major concern for investors, media, economists, and technologists. In the process, the concept of Bitcoin and blockchain began to gain popularity among the general public.

3 What is Bitcoin?

Bitcoin is a peer-to-peer (P2P) form of virtual currency [2] and is not issued by a specific currency institution. It is generated by multiple calculations of a specific algorithm, using a distributed database of multiple nodes across the P2P network to confirm and record all transaction. Essentially, bitcoin is stored digitally in a database, and the system moves money from one account to another by transferring numbers. Bitcoin is the first distributed virtual currency, with an entire network of users and no central bank. Decentralization is the guarantee of Bitcoin's security and freedom.

As we all know, money is created by the central banks of various countries printing and issuing paper money. How does Bitcoin make money? We must introduce the word "digging". What is "digging"? In plain English, mining is a way to make money out of thin air. The characteristic of Bitcoin is that it combines bookkeeping and making money out of thin air, which is the essence of mining. First, we will talk about bookkeeping. All virtual currencies, including Bitcoin, are known to be decentralized. In other words, there is no central authority like a bank to record and guarantee every transaction. Thus, how do we keep our trading books? Who will keep it? Furthermore, how to supervise? In the face of such a situation, Satoshi Nakamoto stipulated that every ten minutes to pack the book, the book contains all the transaction records within ten minutes. In addition, anyone can pack a ledger and become a bookkeeper. Meanwhile, bookkeepers record bitcoin transactions in public ledgers that become official records for everyone to consider. We call the ledger package that travels every ten minutes a block, and all transaction records formed by linking all blocks together are called blockchains. In this process, all balances can be determined on the blockchain. To encourage everyone to participate in bookkeeping, the first transaction in a block, according to Satoshi Nakamoto, is a special transaction that creates a new coin held by the block's originator. This provides an incentive for nodes to maintain the network, as well as a mechanism to get currencies into circulation at first. The continual creation of a fixed number of new coins is akin to gold miners devoting resources to increase the amount of gold in circulation [3]. Therefore, the act of bookkeeping is called mining, which is the production of bitcoins out of thin air. The bookkeepers are called miners.

4 Characteristics of Bitcoin

The first feature is decentralization. Bitcoin is not regulated by any institution such as a central bank. The second feature is the limited amount. When Bitcoin was first used, miners were rewarded with 50 bitcoins per block, according to an algorithm developed by Satoshi Nakamoto. For every 210,000 blocks mined (approximately every 4 years), the block reward is halved and will continue to be halved until the reward per block becomes 0. Finally, the final output of Bitcoin in 2140 is 21 million [4]. The third feature is that the address is anonymous. In the world of Bitcoin, everyone's address is random. The computer automatically generates a 256-bit binary private key and computes the respective addresses through operations. The fourth feature is global circulation. The Bitcoin network is a global network, and transactions can take place anywhere there is a network.

5 Bitcoin's Future

5.1 Bitcoin Becomes an Asset to Invest

The possibility of bitcoin as an asset investment will remain. After the war between Russia and Ukraine, we saw the European Union, the United States, and the United Kingdom start sanctions against the Russian oligarchic elites at the fastest speed. Western countries have frozen the assets of Russia's central bank to prevent it from using its $630bn (£470bn) dollar reserves, according to the BBC. In addition, the United States has blocked $600 million in debt repayments to Russian banks in the United States, making it more difficult for Russia to fulfill its foreign debts [5]. However, buying and investing in Bitcoin can avoid this risk. Bitcoin, gold and the U.S. dollar have similar patterns, according to Dyhrberg. Bitcoin can be used alongside other financial assets to protect investors. [6]. The decentralized nature of Bitcoin makes it unregulated by any bank in any country. Therefore, no country can confiscate other people's bitcoins. Meanwhile, there are many costs associated with holding assets, such as maintenance costs, transfer costs, and time costs. For example, if someone buys gold bars but has no place to store them, he can rent a safe at the bank to manage them. The fee charged by the bank is the maintenance fee. Another example is someone who wants to sell their fixed assets and turn their house into a liquid asset. At this time, transfer costs and time costs will be incurred. Selling a house requires various brokerage fees, handling fees, and too much time. In contrast, bitcoin costs zero to transfer and maintain, and can be deposited and transferred at any time as long as there is a network. Thus, Bitcoin can be used as a good store of value and safe haven.

5.2 Bitcoin Becomes a Payment Method Accepted by More People

Because of the institution's monitoring, traditional payment methods can result in transfers that are more costly, less efficient, and last longer. The process of overseas remittance is that the counterparty sends the money to the bank, and the bank submits the money to UnionPay, which then sends the money abroad. The bank will charge a certain fee for this process. At the same time, the process is very cumbersome, and it takes a long time to transfer money to the other party's account. According to reports, the global average transfer charge is 6.04 percent of the remittance amount [7]. On the contrary, bitcoin's remittance cost is relatively low because it can be transferred at any time without any intermediary supervision. Besides, because of the decentralization of Bitcoin, transfers are very efficient. According to Goldman Sachs, transaction costs for foreign remittances utilizing Bitcoin were about 1%, while the transaction cost of traditional remittances is 8–9%, which means cost savings [1].

Second, in recent years, credit card theft, fraud and other problems emerge in endlessly. Fraudsters use Trojan software and other methods to copy the cardholder's CVV, card number, and expiration date. Fraudsters use this information to steal and swipe cards at will. In addition, scammers also obtain other people's information through illegal means and falsely claim credit cards for overdraft consumption, which is a huge loss to enterprises, cardholders, and banks. However, because of the Bitcoin's encryption algorithm and anonymity, this problem can be properly solved. In the world of Bitcoin, everyone automatically generates a unique 256-bit binary private key through a computer. The computer then uses the private key to calculate the address that belongs to them. Because these algorithms are encrypted, scammers cannot steal other people's Bitcoin information.

5.3 Bitcoin Cannot Be the World Currency

Yermack argues that bitcoin does not function as a currency since it does not fulfill the three fundamental textbook functions of money [8]. In microeconomics, Marx pointed out the nature of the general equivalent of money. Money is commodity money and a contract for the exchange rights between owners. Value scale, means of circulation, means of storage, means of payment, and world currency are the five basic attributes of money [9]. Firstly, as far as the medium of exchange is concerned, while many companies now accept Bitcoin as one of the payment methods, some countries such as China do not. In this case, Bitcoin cannot be used as an accepted currency and circulated around the world. Second, money needs stability, and bitcoin is a measure of value, so it doesn't provide that. There is inflation and deflation in the currency, which are determined by its supply and demand. If Bitcoin gradually develops into a currency, the growing demand and limited supply of 2100W will lead to a shortage of Bitcoin. Thus, the price of bitcoin skyrockets, and the increase in price makes more people want to hold bitcoin. Currently, the growth rate of Bitcoin's demand continues to rise, while its supply growth rate is decreasing. In this process, if Bitcoin becomes a currency, its value will continue to rise predictably. At the same time, bitcoin will also face persistent deflation, prompting it to withdraw from circulation, lose its function as a payment tool and become a collection. What does a good currency look like? The answer should be moderate inflation. While relatively stable, its supply is proportional to the economy. The economy is in an upward spiral. In the early stage of the outbreak, countries appropriately issued currencies to provide monetary support for economic development. When an economic bubble occurs, the currency is tightened by reducing issuance and other means to bring the currency back to its true value. However, bitcoin has always been deflationary. As the economy develops, the value of Bitcoin keeps rising because of the fixed output. People can get more growth interest if they hold the currency. Eventually, borrowers no longer have an incentive to borrow, making markets less liquid. Meanwhile, the companies have nowhere to lend to develop their businesses, so the economy cannot develop.

6 Conclusion

This paper draws out the reasons for the emergence of Bitcoin from the historical background and then introduces the principle, operating mechanism, and characteristics of Bitcoin. Combined with its characteristics and reality, analysis of its possible future route, finally draw a conclusion. The results suggest that no matter how bitcoin develops, it is unlikely to become a global currency in the future. However, because of the decentralization and anonymity of Bitcoin, it can become a good store of value and may even become a mainstream payment method. I believe that blockchain technology will become more and more mature in the long run, and more and more countries will recognize Bitcoin and use Bitcoin.

7 Limitations of This Paper and Expectations for the Future

There are some deficiencies here. The article mentions that the supply of Bitcoin is certain. This question will have a big impact on the future development of Bitcoin. But this paper does not study how to solve the problem of a certain supply of Bitcoin. It is hoped that in the future, the shortcomings of Bitcoin will be overcome from the technical level and from the level of equal replacement.

References

1. C. Smith and A. Kumar, “CRYPTO-CURRENCIES - AN INTRODUCTION TO NOT-SO-FUNNY MONEYS”, *Journal of Economic Surveys*, vol. 32, no. 5, pp. 1531–1559, 2018. Available: https://doi.org/10.1111/joes.12289.
2. G. Shrivastava, D. Le and K. Sharma, *Cryptocurrencies and blockchain technology applications.*
3. Bitcoin.org, 2022. [Online]. Available: https://bitcoin.org/bitcoin.pdf. [Accessed: 26- May-2022].
4. "Bitcoin Block Reward Halving Countdown”, *Bitcoinblockhalf.com*, 2022. [Online]. Available: https://www.bitcoinblockhalf.com/. [Accessed: 17- May- 2022].
5. "What sanctions are being imposed on Russia over Ukraine invasion?”, *BBC News*, 2022. [Online]. Available: https://www.bbc.com/news/world-europe-60125659. [Accessed: 17- May- 2022].
6. A. Dyhrberg, “Bitcoin, gold and the dollar – A GARCH volatility analysis”, Finance Research Letters, vol. 16, pp. 85–92, 2016. Available: https://doi.org/10.1016/j.frl.2015.10.008.
7. "Remittance Prices Worldwide | MAKING MARKETS MORE TRANSPARENT”, *Remittanceprices.worldbank.org*, 2022. [Online]. Available: https://remittanceprices.worldbank.org/en. [Accessed: 17- May- 2022].
8. D. Yermack, “Is Bitcoin a Real Currency?”, SSRN Electronic Journal, 2013. Available: https://doi.org/10.2139/ssrn.2361599.
9. 10. N. Capaldi and G. Lloyd, The Two Narratives of Political Economy. Somerset: Wiley, 2011.