Advances in Economics, Business and Management Research, volume 203
Proceedings of the 2021 3rd International Conference on Economic Management and Cultural Industry (ICEMCI 2021)

Analysis of Bitcoin Development and Investment Value

Tianyu Li[1,*,†] Wanying Li[2,†] Siyi Li[3,†]

[1] *Hengshui NO.1 High School Hengshui City China International Department*
[2] *Chengdu Shishi High School Chengdu City China Cambridge International Department*
[3]*Anqing NO.2 High School Anqing City China*
[*] *Email: guanghua.ren@gecacademy.cn*
[†]*These authors contributed equally.*

ABSTRACT
Bitcoin started out as a cryptology group, and gradually gained the attention of an elite group of economists, programmers, and math enthusiasts outside of cryptography, eventually rising and falling as the price of Bitcoin skyrocketed, after the fermentation of the media has received widespread attention around the world. Therefore, this paper wants to conduct an overview about Bitcoin. Stages of mining, begins with an initial profit that was small and easy to come by, after decades of development, to a mine that cost more than $50,000 a piece and required a specific CPU, huge profits drove people to go crazy. In 2020, Bitcoin has increased by 300%, and as more and more economic entities accept Bitcoin as a means of payment in the future, the role and value of the virtual currency will increase, and the long-term upward trend in Bitcoin can be expected. However, the value of Bitcoin can not be determined. The value depends entirely on the trust of the market, while the vast majority of Bitcoin is in the hands of a very small number of people. And because of its scarcity, its value is extremely volatile. Moreover, Bitcoin regulation varies from country to country, from optimism to caution. China and some countries have banned the exchange of digital currency, especially legal tender and digital currency, the future of Bitcoin remains problematic.

Keywords: *Bitcoin, Mining, Bubble, Investment, Regulation*

1. INTRODUCTION

In November 2008, a paper by Satoshi Nakamoto was published online under the title "Bitcoin: A P2P Electronic Cash System."The paper details how peer-to-peer networks can be used to create an "electronic trading system that does not rely on trust". In January 2009, the Bitcoin network went online and launched the first open-source Bitcoin client software. Satoshi Nakamoto used the software to "mine" the first Bitcoin "block" and obtained the first batch of 50 Bitcoins. On August 6, 2010, a major flaw in the Bitcoin protocol was discovered, in which transactions were not fully authenticated before being logged into the record or the "block chain", allowing users to bypass the economic limits set by Bitcoin and create an unlimited Bitcoin. As of February 2014, this is the only major security breach in Bitcoin's history that has been discovered and exploited. That single transfer generated 184 million Bitcoins. On April 10, 2021, Bitcoin crossed the $60,000 mark. In a filing with the Securities and Exchange Commission, Tesla claimed to have purchased $1.5 billion worth of Bitcoin. Mr. Musk said the Bitcoin purchases were meant to "provide greater flexibility to further diversify and maximise our cash return". In addition to this purchase, Tesla will also start accepting Bitcoin payments in exchange for its products, the company's official spokesman said. That would make Tesla the first major automaker to accept Bitcoin as payment. After Tesla's announcement, the price of Bitcoin soared to a new high, reaching at least $43,200. Tesla shares rose more than 2 percent in premarket trading. Therefore, through all these phenomena, we have reason to think that the future market and market of Bitcoin is very good, and it may become a form of payment or even a mainstream currency. Therefore, in general it is very necessary and valuable for us to study the future development and current situation of Bitcoin.

2. LITERATURE REVIEW

2.1. Bitcoin Transactions

Moser do a researche about Bitcoin Transactions during his university period. He has already been studies

showing the possibility to deanonymize Bitcoin users based on the transaction graph and publicly available data. Then he evaluates three of these services-Bitcoin Fog, Bit Laundry, and the Send Shared functionality of the Block chain.info-by analyzing the transaction graph. Finally, he concludes that both Bitcoin Fog and Block chain.info make it hard for an attacker to relate input and output transaction., What's more, he also mentioned that Bit Laundry cannot be considered to reliably increase anonymity [1].

2.2. Bitcoin block chain

Crosby et al. do deep research about a Bitcoin block chain. They think that the main hypothesis is that the blockchain establishes a system of creating a distributed consensus in the digital online world. This allows participating entities to know for certain that a digital event happened by creating an irrefutable record in a public ledger. As a result, they make a conclusion that BlockChain is Bitcoin's backbone technology. The distributed ledger functionality coupled with the security of BlockChain makes it a very attractive technology to solve the current financial as well as non-financial industry problems [2].

3. BITCOIN MINING

Bitcoin's mining mechanism is a clever economic and mathematical design. The mining mechanism for Bitcoin is a kind of digital currency issuance mechanism. Mining refers to the process of issuing Bitcoin. Miners were rewarded with an initial reward of 50 Bitcoins, halved every four years to 25 Bitcoins, and now 12.5 Bitcoins. The world's reserves of Bitcoins are fixed, and miners will work to release Bitcoins into human society.

The specific mining is divided into three steps. The first step is to package the deal into new blocks. Then it is the hash encryption machine calculation. Finally, new mines are identified as full nodes. In fact, only the second part is being mined, because it requires relatively little computation. In general, the core idea of mining is to use computers to do things instead of humans. So in this respect, the core part is a calculation, miners need to have strong calculation power, in order to obtain the corresponding rewards. In addition, the idea of being rewarded for success cleverly exploits the human reward mentality. Thus, in my opinion, Bitcoin is really a superb technological and economic product.

The development of the Bitcoin mining mechanism is also worth exploring. The mining began in 2009 when Satoshi Nakamoto used a PC's central processing unit (CPU) chip to mine the first batch of 50 Bitcoins. At this time, in the early days of Bitcoin, mining was easy. Miners needed only the CPUs of their personal computers. Miners in those days generally made more money than they cost, and they dug so many mines that they could dig hundreds a week. By 2010, as mining became more difficult, PC CPUs were no longer capable of performing the high-speed calculations needed. So, around this time, a piece of software called GPU came out. This software has extremely high computing power and efficiency. As a result, most people are starting to use GPUs for mining. With more and more people began to mine, FPGA and ASIC professional mining machine was born. However, due to the high-power consumption of FPGA, it was not long before the obsolete. But ASIC Mining has survived the ups and downs of Bitcoin. In 2010, the first Bitcoin mining Pool, Slush Pool, appeared. From then on, the advantage of the low-computing miner is getting smaller and smaller. The pool has a significantly higher chance of success than a single miner, and the pool participants have a greater share of the proceeds.

In general, the Bitcoin mining mechanism is developing continuously, and there may be more new mining methods such as cloud mining and quantum computer in the future. But there is no denying that the emergence of Bitcoin provides people with a new way to distribute money. However, the popularity of Bitcoin has also led to some problems, such as hackers illegally stealing other people's resources to mine. A common method is to attack miners' computers with web pages, which, once infected, will become sluggish, consume a lot of power and damage their hardware badly. The most important thing about this problem is that miners should be vigilant. Miners can protect themselves by using a browser like Opera, which has more features than Chrome. And miners need to protect mobile phones, which are more vulnerable to these malicious scripts than computers. To fundamentally solve this problem, we need a sound law. The law can raise people's awareness and vigilance, and its enforceability will solve the problem more completely.

4. INVESTMENT VALUE

The practical value of Bitcoin is to act as a general equivalent. As long as it can satisfy the functional characteristics of currency (all five functions of a currency: value scale, circulation means, storage means, payment means, and world currency), and accepted by the public (including the state), Bitcoin can be used as currency, similar to the shell of ancient currency, which has no value in itself, but can be used for the exchange of things[3].

The most important thing is to be accepted by the public. Since the total issue of Bitcoin is 2100W, and the block chain technology is guaranteed, it is deflation in the long term and will not be like endless printing on the dollar, so Bitcoin is gradually pushed to the top of the wave. If all countries intervene in control, it is worthless.

Therefore, Bitcoin has some unique investment value in the following aspects: 1) Limit: only 21million Bitcoin, the more scarce, the more valuable; 2)No regime or organization control: Bitcoin is not controlled by anyone. There is a set of fixed algorithms, which cannot be changed even by the people who created it which means it is very stable and reliable; 3) Confidentiality and convenient transaction: because of its confidentiality design, Bitcoin is sold anonymously and cannot be traced. In addition, the transaction cost of Bitcoin is low, and tax is not required, so it can allow foreign exchange supervision and so on. Bitcoin is a decentralized global cryptocurrency, which can be freely circulated in the world. It is an investment asset for global investors to fight inflation. The uniqueness of Bitcoin promotes its price to rise continuously.

However, Bitcoin is not based on basic technology, but on speculative market rules and unregulated exchanges in fake trading volume. People buy cryptocurrency not because of their technology and ideas, but because they want to get quick and easy profits. At that time, digital money did not have many use cases, and the price was high, because (fear of error) made new people start buying enthusiastically. Another argument is that Bitcoin has no real value. Fiat currencies have some stability because they are supported by governments and banks. But cryptocurrency is not supported, owned, or controlled by anyone[4].

We believe that Bitcoin is the bubble, but not it is not worth anything. First of all, at the beginning of the user is a Silk Road Dark Web. This web includes lots of illegal things. Because when you use the Bitcoin to change, it is hard to trace. So, if without this web, the value of Bitcoin can’ t show it all. It has some characteristics of the bubble: nearly all the government reject using Bitcoin, so it can’ t buy anything. Given how much money is in cryptocurrency, it’ s not surprising that people are alarmed by the unknown impact of the first ever space-impacting regulation. People don’ t like volatility, and inexperienced investors are more likely to sell their currencies in mass panic, which affects market prices. More reason: 1) It has the smallest current purpose; 2) it is hard to determine its true value as a digital asset[5].

Reasons about the recent Bitcoin plummets: (1) When Bitcoin prices stay low for a long, long time. By the time society had forgotten it, the dealers had amassed enough chips to hold a large amount of Bitcoin or other digital currency in circulation, and they were able to manipulate market prices. At this time, the dealer began to move, slowly raising the price. Then that part of the retail currency is still speculation on the Bank of the free ride, slowly began to make money, the hands of the currency is also higher and higher. Then these retail investors will tell the friends around, said he made money in currency speculation. These friends may not be very interested in the beginning, is not very willing to enter the market, the market is the law, no one will accept a small profit because of the new investment. And then, the price will go up, and those early investors will make more and more money, and their friends will be tempted to start investing in Bitcoins. Borrow the power of the network, in the money market money, money-making news will explode-type spread, coupled with the good news of the market, thousands of retail investors will follow the wind, large into the money speculation army. At this time, the price has been pulled by the market high, these thousands of retail investors became a take-over. Then the next is the dealer’ s shipment, in the high cross-selling, or pull up the shipment. When the shipment is almost, there is a certain chip in hand, then the dealer will not trade horizontally and pull up, bringing the plate. Prices plummeted, trapping numerous retail investors in the peak, a long period of no return. (2) There’ s been a lot of talk lately that digital money may come under more pressure from regulators. Countries are looking more closely at the risks associated with digital money, and it seems to me that the concern is that criminals are using Bitcoin to launder money, it is good for crime[6].

Moreover, we think Bitcoin is not worth anything: 1) Some economists argue that bubbles are essential to the proper functioning of economics and can trigger a flood of investment. 2)A decrease in supply is often referred to as a halving of Bitcoin-an an event in which mining remuneration is reduced by a factor of two. The next halving is expected to be completed by May 2020, and the miners will receive 6.25 Bitcoins each, instead of the current 12.5 Bitcoins. Currently, about 1,800 Bitcoins are mined every day, so halving the supply would reduce it to 900 Bitcoins per day; 3) The price of Bitcoin goes up every time the incentive is reduced. But past behaviour does not determine future prices, so the expected boom may not happen.

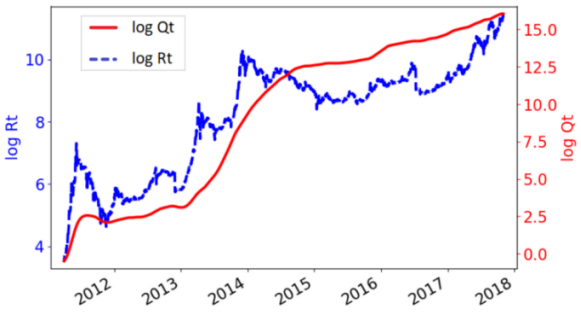

Figure 1 Miners’ Revenues R and Hashrate Q

Figure 2 Bitcoin prices rise and fall [7]

5. REGULATION

Bitcoin is currently a very popular virtual currency in the world, and Bitcoin is a distributed system. Because Bitcoin is a virtual distributed transaction system, it poses difficulties for some legal systems. In particular, how to regulate Bitcoin's distributed network is a very big problem. Nowadays, in the world of rapid development of science and technology, some crimes are often accompanied by the use of high technology. For example, some network hackers and criminals will sell and illegally trade some goods through the dark net. The dark net and Bitcoin are equally hard to regulate. The dark net is very easy to use, and anyone can buy what they want online as well as illegal stuff, like drugs and some pornography. Bitcoin has made trading on the dark net even easier. This is one of the reasons why governments need to come up with regulations and restrictions on the trading of Bitcoin. In addition, there are some other reasons. For example, Bitcoin is currently a disguised financial product, so it also belongs to the assets of a person or an institution. Therefore, when it comes to assets, we should think about how to protect the rights and interests of investors and so on. There are also criminals who use Bitcoin to launder money. And some large international money laundering activities can be carried out, because foreign exchange control can be bypassed, and the risk of money laundering can be bypassed. One of the most common problems is that some people will buy and hoard large numbers of graphics cards for Bitcoin mining. Once they have a certain amount of Bitcoin in their hands, they can further manipulate the Bitcoin trading market, thereby limiting the number of people who can legally and reasonably mine it. In turn, Bitcoin will lose its purpose of existence, its liquidity, and transactionability[8].

About the regulation of Bitcoin, different countries have different attitudes about the regulation of Bitcoin, ranging from optimism to caution. The first thing to understand about the Bitcoin as an asset is that the Bitcoin has no physical connection with the holder and is decentralized. The lack of physical connection means that the transportation and the storage costs are close to zero, so anyone can easily carry Bitcoins from one country to another.easily. Just because the lack of physical connection also means that it's difficult to simply prove whether a person owns some Bitcoins. And the reason is that somebody can't "ferreout" Bitcoins from another person. Decentralization has a bigger impact. Decentralized systems are not controlled by any one or organization, which means that no one person or organization can stop a person from holding or transferring Bitcoins as long as you have access to the Bitcoin network. This is the biggest challenge which facing the regulatory authorities, without doubt, because follow the advent of the electronic age, normal daily life will often come into contact with the physical assets. However, the decentralized assets are something new (it's important to note that digital assets are not innovative, and the assets people interact with on a daily basis are already digital.) According to the CIA and international clearing bank, the world's monetary aggregates for $80 trillion, but only 5 trillion is the currency of the entity, in other words, people almost every day in the use of digital assets, the currency is different from the Bitcoin because it is a decentralized digital asset, the decentralization is the most important thing.

According to Ambcrypto, Anurag Thakur, Minister of State at the Ministry of Finance of India, noted that the government is considering issues related to digital assets as one of its key agendas. The Indian cryptocurrency community has been witnessing tremendous growth, but the lack of regulatory clarity has become a major obstacle. While the Indian government has been concerned about cryptocurrencies, it has recently been talking about keeping an "open mind" and working to promote the development of a national digital statutory authority. The ministers highlighted the fluctuating price of Bitcoin and reiterated that they were on the "technical side" and were considering cryptocurrencies with an "open mind."However, restrictions and regulations on Bitcoin in China are much stricter. According to the Notice on Preventing Bitcoin Risks issued by the People's Bank of China and other five ministries and commissions on December 5, 2013, Bitcoin is a virtual commodity, not a negotiable currency, and cannot be used as a substitute for fiat currency. But as a commodity, ordinary people are free to participate at their own risk. And China has banned digital currency exchanges, especially fiat and digital currency exchanges. The central bank explicitly mentioned that fiat and digital currency exchange services should not be provided, as well as between digital currencies.

The important sentence of the cryptpunk manifesto says that "privacy is essential to building an open society." As a result: how private is Bitcoin? Bitcoin's privacy policy hide and protect the Bitcoin address from the physical identity of the holder. Bitcoin's privacy policies are very different from those of the traditional

financial system or currency. The tenth part of the Bitcoin white paper is devoted to privacy. Satoshi Nakamoto mentioned that the traditional agency's strategy is to bind users' physical identity and their accounts.within the organization, and privacy is reflected in the fact which the public cannot freely access this information. Bitcoin takes the opposite approach and making all transfers available to the public, including the Bitcoin addresses of the sender and reactor, the amount of money transferred and so on. The privacy of Bitcoin is embodied in the fact that there is no binding relationship between the address of Bitcoin and the physical identity of the address holder. The transactions are traceable. Bitcoin is the most transparent payment system in mankind history, and all transaction history will be preserved. This characteristic brings great challenges to the privacy security of Bitcoin. Once exposed, it's hard to become invisible again. In fact, there are many occasions involving the real-name system, which means that the physical identity and people's address are bound, that is, the privacy of the address is exposed. If the original address is exposed, even if people change to a new address and transfer the money from the exposed address to the new address, the correlation between the new address and the old address is very clear, so the new address has no privacy at all. The spread of transactions across the web may also expose privacy. Once Bitcoin transactions are created, they spread from the machines on which they are constructed to many computers on the network in a peer-to-peer protocol, making it difficult to pinpoint the machine from which the transaction originated. The Bitcoin community is also mulling over various improvements. For example, Confidential Transaction and CoinJoin were proposed by the core development team. Later, someone combined these two technologies to propose a new cryptocurrency protocol called Mimblewimble. Mimblewimble has not yet been adopted by the Bitcoin project. But there are two separate blockchain projects that have implemented Mimblewimble: GRIN and Beam.

So after summarizing the regulatory reasons for Bitcoin and the policies of governments and some news reports, in my opinion, the supervision of Bitcoin is very necessary, because there are indeed some loopholes in the current supervision mechanism of Bitcoin, allowing many criminals and speculators to gain illegal profits. There are many governments and local laws that restrict or prohibit the trading of Bitcoin, which is of course, because the production and trading of Bitcoin has no benefit to the development of the real economy under the jurisdiction of the government. Therefore, I think that although the development of Bitcoin is stable for the time being, and it is still growing steadily, in the future, if more and more local laws are issued and Bitcoin trading is prohibited, then the total market volume of Bitcoin will decrease, and they will inevitably drop in price.

6. CONCLUSION

Overall, in this paper, we did some research mainly about three aspects: bitcoin mining, investment value, and regulation. Also, as time goes on, the method of mining is changing and developing. Bitcoin is a good choice for investment as it has uniqueness in limit and the convenience in the transaction. Bitcoin has a characteristic of the bubble due to the unacceptability of government. Besides, it is reasonable of us to consider bitcoin as a worthless currency. Because of the lack of incentives, the appreciation of price won’t lead to the prosperity of the prospect of bitcoin. In addition, we conclude about some reasons of the regulation of bitcoin. It is crucial to have bitcoin regulation. That can forbid some people to earn from mining illegally. Generally speaking, as an up-dated currency, we’re curious about it’s performance in the future.

REFERENCES

[1] Moser, Malte. "Anonymity of Bitcoin transactions." (2013).

[2] Crosby, Michael, et al. "Blockchain technology: Beyond Bitcoin." Applied Innovation 2.6-10 (2016): 71.

[3] Schilling, Linda, and Harald Uhlig. "Some simple Bitcoin economics." Journal of Monetary Economics 106 (2019): 16-26.

[4] Oliver, Capital. ‘Myrmikan Research’ (2017)

[5] Toulet, Gordien. ‘Bitcoin, Currency for a Finite World’ (2017)

[6] Weber, Karl I, et al. ‘Anti-Money Laundering in Bitcoin: Experimenting with Graph Convolutional Networks for Financial Forensics’(2019)

[7] https://www.ouyi.cc/markets/prices/bitcoin-btc

[8] Park, C. Y. , G. Tian , and B. Zhao . "Global Bitcoin Markets and Local Regulations." Social Science Electronic Publishing.