The Development and Prospects of Bitcoin

Jingxiao Ma[1, a]

[1]Department of Finance and Economics Huizhou Engineering Vocational College Huizhou, Guangdong Province, China.

[a]monica.ma@connect.umac.mo

Abstract

Today, some people think that Bitcoin is one of the currencies, but some people disagree with it. In my perspective, Bitcoin is a kind of virtual speculative assets rather than currency. But Bitcoin is also the revolution of currency. In this paper, I will focus on four three aspect of Bitcoin, principle and characteristic, the development, existing problems and prospect.

Keywords

Bitcoin, Digital currency, Blockchain.

1. Principle and Characteristic

1.1. Bitcoin Principle

1.1.1. Basic Principle

Bitcoin generates through the encryption algorithm, it has not got physical properties, it is a series of code in reality, therefore the price of Bitcoin will be determined by market requirement directly. Once the Bitcoin being attacked by hackers or suffered by the negative social opinions influence, it will be crashed easily. Bitcoin is a kind of P2P digital currency, it saves all the transaction history in block chain. Once the new block added into the block chain, it will not be removed. Actually, the blockchain principle like distributed database.

The Bitcoin system will create a new block every ten minutes, the block includes all of the Bitcoin transactions in the ten minutes. Each block has the previous block's ID, therefore, each block can find its previous node. One by one, it can track back to the first block. Since the Bitcoin born, the system generates only one main block chain. It records all of the Bitcoin transactions. Once the main block chain adds to a new node, it will be announced to the system, and each joined Bitcoin transactions' computer will get a copy version. It means that, the Bitcoin transaction history is saved in every joined computer in the world. Even if there is only one installed Bitcoin software computer in the world can be used, the main block chain can be read. Therefore, it is almost impossible to lose the transaction information.

Bitcoin has limited total amount, 21 million. Nowadays, the smallest unit is 0. 00000001BTC. When the total amount is certain, more miners will cause higher mining difficulty. The mining difficulty of Bitcoin is related to the miners' average operational capability.

1.1.2. Transaction Principle

There is not have central bank or some other similar organization to control Bitcoin. Bitcoin uses P2P network node's distributed database to record the transactions. After installed Bitcoin client-side, the client-side will send a private key and a public key to the user. The private key is the user's identity certification, the public key can verify the private key, the address can be generated from public key through Message Digest Hash Algorithm. In transactions, sender use the recipient's public key to encrypt the payment, only the corresponding private key can decrypt it and receive the money.

Users should back-up their e-wallet which contains the private key, to make sure that their asset will not loss. However, if you format the hard disk, or the hackers stolen the private key, your Bitcoin will lose.

1.2. Bitoin Characteristics

1.2.1. Decentration

Bitcoin is the first distributed virtual money in the world, the whole network of the Bitcoin is consisted by the users, there is no central bank to control it.

1.2.2. No Circulation Restrictions

People can manage the Bitcoin in any connected network computer, after download the Bitcoin software, we can mine, purchase or sell the Bitcoin in anywhere.

1.2.3. Exclusive

Using private key to control Bitcoin is very important. The private key can be separated saved in any storage medium, others will difficult to obtain it. The private key is also the user's identity certification in transaction.

1.2.4. Anonymous

Through the random changes of accept payment address, both of sellers and buyers can hide their true identity. Bitcoin not only dependents on traditional virtual money account system, but also depends on public key technology. Each transaction can regenerate a pair of public and private key. It means that one transaction has one encryption and decryption. This method can make the anonymous transaction come true.

1.2.5. Fixed total amount

Cause of limited by the algorithm, the Bitcoin has a fixed total amount, 21 million. This avoids the inflation caused by human disturbance or central bank's some bad policy.

1.2.6. Open Source

The Bitcoin software is open-source. Merchants, service providers, customers and investors are able to create abundant services and financial system around the Bitcoin open source systems.

1.2.7. Great Fluctuation of Price

Actually, Bitcoin is a series of code in essence. The cost and essence value of Bitcoin is the digging cost (electricity cost, corresponding software development cost and so on), but it is far less than Bitcoin price in reality. The Bitcoin price is almost totally decided by market demand (and it has been hyped), so the Bitcoin market is very sensitive and the price will have a great fluctuation.

2. Development of Bitcoin

2.1. Global Development

The first transaction of Bitcoin was happened on May 22, 2010. A Florida programmer, Laszlo Hanyecz, has used 10000 bitcoins to buy a pizza which worth 25 U.S dollar. Since then, Bitcoin is gradually being accepted by people.

From figure 1, the development of Bitcoin has reached a peak in 2013, the top price in this year even up to 1151 U.S dollar, 2000 times higher than three years ago. However, the market is very sensitive, and the Bitcoin price always fluctuate, even some hearsay may also have a huge impact on Bitcoin price.

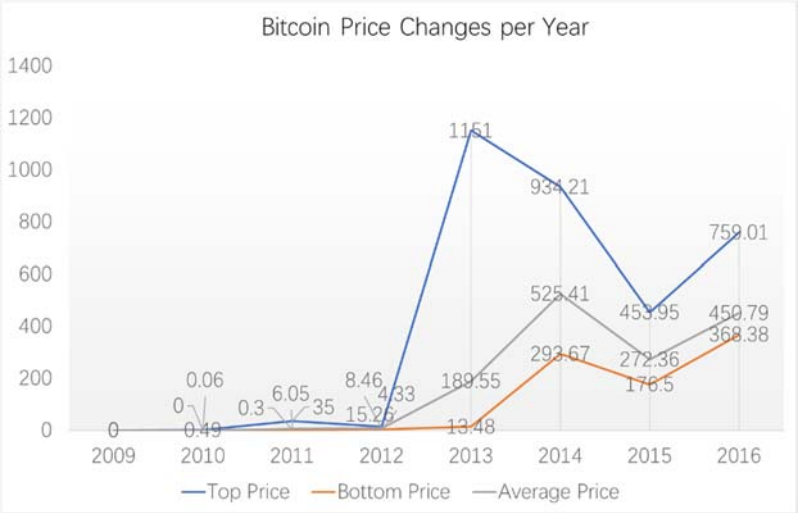

Figure 1. Bitcoin Price Changes per Year

In 2013, Bitcoin developed rapidly than ever before. The total value of Bitcoin is reached to 1 billion U.S dollar. More and more people accept it, Bitcoin occupied the digital currency market rapidly. However, cause of the big fluctuation of price, many people still stay conservative to Bitcoin. The rapidly development of Bitcoin is an opportunity and also a challenge for each country. The corresponding policy and regulatory of each government are still improving gradually. Nowadays, many countries have issued the laws and regulations of Bitcoin and digital currency. However, cause of the characteristics of decentration, account anonymous and no circulation restrictions, there are still some supervision loopholes on Bitcoin.

According to 2014-2016 Global Bitcoin Report, with the digging of Bitcoin, there are more than 15.6 million Bitcoins into the circulation, the Bitcoin price also changes dynamic between supply and demand (figure.2).

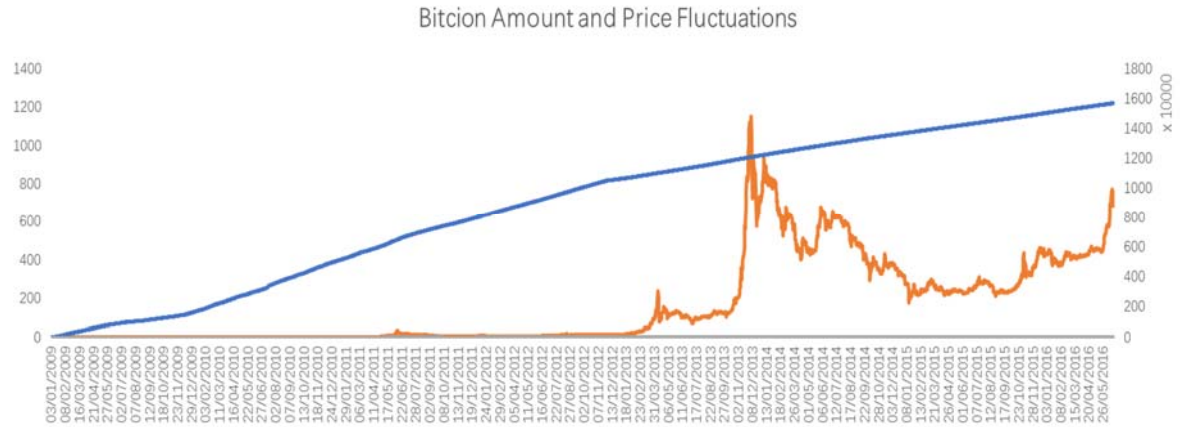

Figure 2. Bitcoin Amount and Price Fluctuations

The rapidly development of Bitcoin also make hackers find the chance to earn money. In February 2014, the global largest Bitcoin transaction platform Mt.gox collapse, 850000 Bitcoins have been stolen by hackers, panic spread to the Bitcoin market, the Bitcoin price even went into free fall at that time. Actually, many Bitcoin transaction platforms have been attacked by hackers, the platform secure problem is still the reason why some potential consumers cannot become the real consumers.

Though the Bitcoin price has a big fluctuation, the active address (the number of transaction address) are still increasing(figure.3). It means that people are still have great enthusiasm and

speculative mentality on Bitcoin. According to the Bitcoin sampling investigation report, 80.77% Bitcoin investment users transact for gain short-term profit. It is also the reason of the phenomenon.

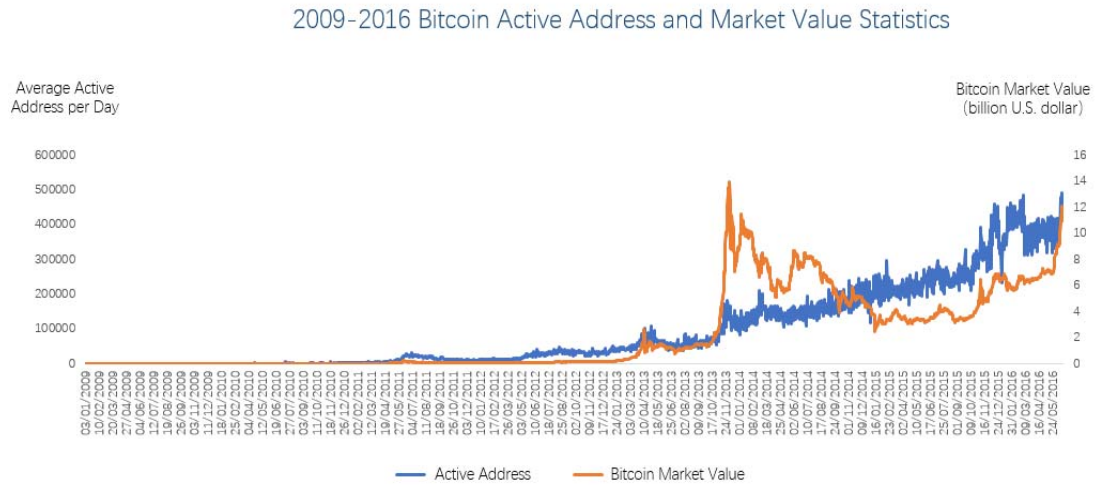

Figure 3. 2009-2016 Bitcoin Active Address and Market Value Statistics

In these years, with more and more people interested on Bitcoins, the Bitcoin's internal ecosystem has been changed gradually. Since 2017, the pace of the Bitcoin forward stumbled, but it still in the value of four digits stable. Many parts of the Bitcoin system are showed a trend of rising, such as Bitcoin wallet, Bitcoin transaction volume, Bitcoin unit value and so on. It means that the Bitcoin market is still full of vitality.

2.2. Development in China

On December 5, 2013, The People's Bank of China has announced The Notice on Preventing the Risks of Bitcoin. The file clear that:

① Bitcoin is not the currency, it is the virtual product. Bitcoin cannot be used as currency.

② In the condition of fully warning the risk, people can join in Bitcoin market and take the risk by themselves.

③ Financial organizations and payment organizations cannot do the business related to Bitcoin.

④ Strengthen supervision on Bitcoin transaction platform. Bitcoin transaction platforms should undertake anti-money laundering obligations.

From the file, we can see that the government is still conservative on Bitcoin, one of the important reasons is that government cannot control it. However, Bitcoin is still hot in China. There are 80 percent of Bitcoin transactions are coming from China until 2016, other 20 percent are mainly from United States and Europe (figure.4).

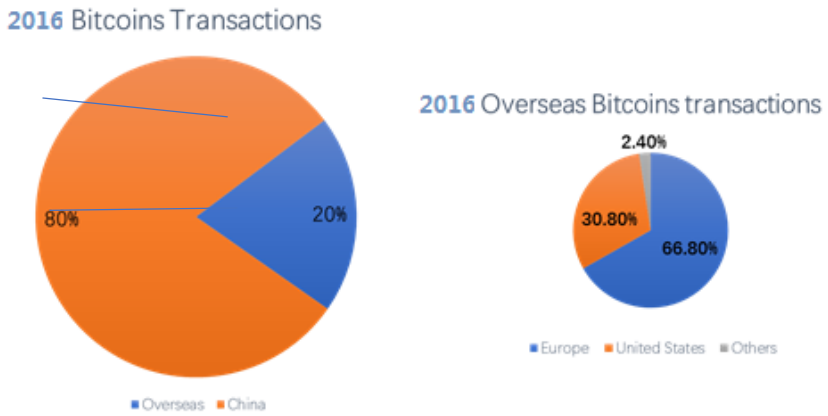

Figure 4. 2016 Bitcoin Transactions

Why the Bitcoin transaction volume is such large in China? Because,

① There are no transaction fees in Chinese Bitcoin transaction platforms until 2017.

② In China, personal investment demand is rising in recent years.

③ Low labor costs, mass produce the Bitcoin mining hardware.

④ There are 50 percent of mining coming from China, especially in cheap electricity area.

Since 2017, the government has paid more effort on supervise Bitcoin. Central bank has interviewed and investigated the Bitcoin transaction platforms. Since then, the Bitcoin transaction volume in China has fallen dramatically, the price of Bitcoin also suffered negative influence. Figure 5 is the transaction volume of OKcoin, one of the three famous Bitcoin transaction platforms, from October 2016 to April 2017. We can see that, since 2017, the Bitcoin transaction volume have fallen sharply, other two platforms, Huobi and BTCC have suffered the same situation.

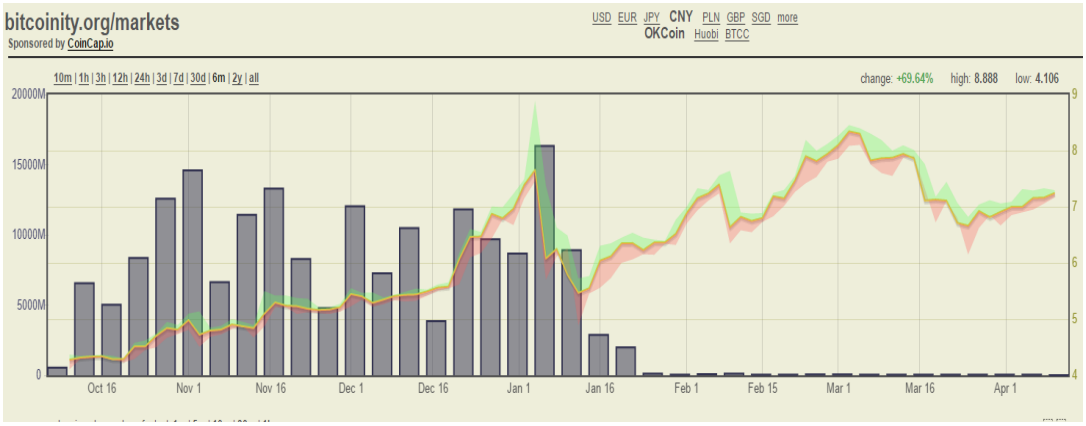

Figure 5. 2016.10.16-2017.4.1 Bitcoin Transactions in OKcoin (CNY)

Actually, some transactions have transferred to other platforms, like LocalBitcoins platform. Before 2017, there are less CNY transactions in LocalBitcoins. But now, the platform have many Chinese customers, from the figure 6 we can see that, since February 2017, CNY transaction volume is increasing rapidly, and maintain high performance. And now, CNY become the top three transaction currency in LocalBitcoins.

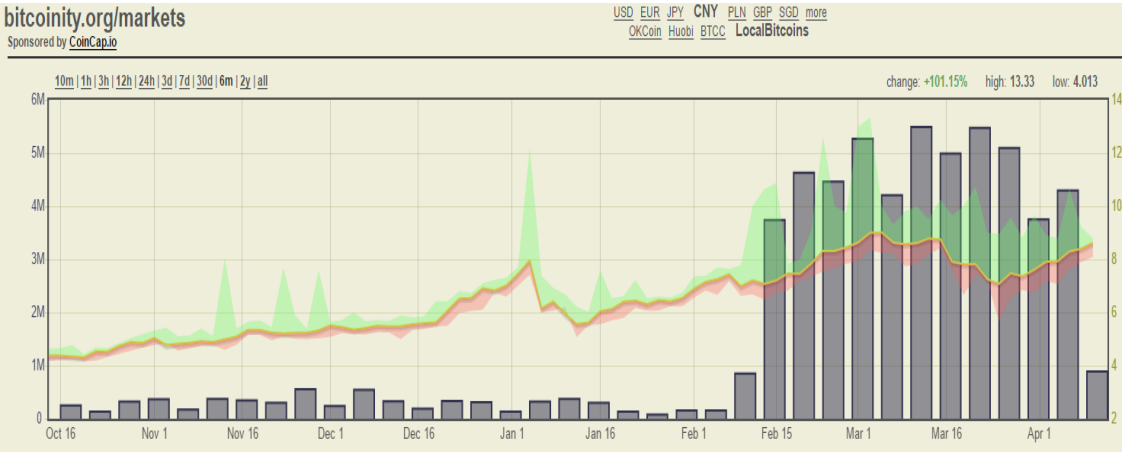

Figure 6. 2016.10.16-2017.4.1 Bitcoin Transactions in LocalBitcoins (CNY)

Though the tranaction volume have fallen sharply in China, CNY transactions are still hot. It means that Chinese market is still occupy an important position in Bitcoin transaction, many people are still have a great passion on Bitcoin in China. Our government realize the vitality of digital currency from Bitcoin. At the end of 2016, the central bank have released the digital currency researcher recruitment information in order to research and develop digital currency.

3. Existing Problems

3.1. Bubble Risk

Classic finance theory has indicated that, the market price cannot deviate from its intrinsic value significantly for a long time, otherwise, the asset price bubbles will be occurred.

As a kind of virtual money, Bitcoin's own value is not high(just s serious of code). Bitcoin was mined easily at the beginning, at that time, the price is only $0.03, the labor time and machine equipment cost are also low. But nowadays, with more and more Bitcoins have been dug out, more and more people join in Bitcoin mining, mining Bitcoin become more difficult than ever before, it will spend much labor time, machine equipment cost, electricity cost and some other costs. So the Bitcoin value is also increasing. However, the price of Bitcoin does not fluctuate around its intrinsic value, the price far more than its intrinsic value.

People may not know how much the Bitcoin's real value is, but they believe it can bring profits for them. Even if the present price is artificially high, but many people still believe that it will higher then, therefore, the Bitcoin price will increase, and the bubble occurred.

3.2. Laws and Regulations

With the development of Bitcoin, many countries have issued corresponding laws and regulations. Different country has different attitude on Bitcoin. Cause of the characteristic of Bitcoin, it is difficult to supervise, and there are still many Bitcoin criminals in the world.

3.2.1. Bitcoin in international trade

There is no third party as a guarantee in Bitcoin published and circulation environment, therefore, once the seller or the buyer do not keep their promise, it is difficult to safeguard their rights, especially in cross-border transactions.

In cross-border transactions, buyer and seller are far away from each other, they are in the different jurisdictions, if the buyer use Bitcoin to pay for the bill, the seller cannot make sure that the buyer will really pay them after the delivery, on the other hand, the buyer also cannot make sure that the seller will deliver the goods after the payment. This way of transaction looks like avoid the middle exploitation of bank, but actually, it exists huge risk. The international trade should not be restricted by credit only.

3.2.2. Bitcoin Laws and Regulations Standard

Once the Bitcoin criminals occurred, it is difficult to confirm the criminal happened location. For example, In Bitcoin stolen cases, the theft may steal the Bitcoins through transaction platforms, or hacked personal computer. So, how to confirm the case happened location? hacker's location, victim's location, or some other locations?

Except for that, different countries have different laws, regulations and attitude on Bitcoin, and it will lead to different results on the same case. Therefore, it is necessary to make an international standard on Bitcoin cases.

3.2.3. Money Laundering and Fraud

Some illegal organization can use Bitcoin to do some money laundering things. For example, some drug deal or Gambling websites use Bitcoin as medium to do the transactions. They can buy the Bitcoins in one country, and pay the bills which from other countries. Once the receiver received the Bitcoins, they can sell it and gain money. This way will make the central bank's foreign exchange controlling exist in name only.

Except for that, there are also some frauds in Bitcoin transactions. Cause of the anonymity of Bitcoin, once the cheater succeeded, it is very difficult for the victims to provide some useful evidence and safeguard their rights. The governments should put more effort on improving corresponding laws and regulations, and should also intensify supervision.

3.3. Secure Problems

3.3.1. E-wallet Risk

Bitcoin need a storage place, such as e-wallet. People can encrypt it, but if your computer have some viruses or trojans, the hackers may hack your e-wallet, and steal your Bitcoins. Bitcoin stored in computers, it has no physical body. Once the Bitcoins storage has been broken or stolen and if there is no backup copy, you will never be able to find the Bitcoins back forever. Except for that, there is also have another risk that the e-wallet providing company may disappeared, in order to prevent these problems, you should build and maintain an online and an offline backup copy, and this is also a trouble.

3.3.2. Transaction Platforms Risk

This is a big secure problem since the Bitcoin occurred. Many Bitcoin transaction platforms have not got enough protective measures and easy to be hacked. Many Bitcoin platforms have been attacked. Mt.gox, once the largest Bitcoin transaction platform in the world, had been attacked by hackers, all of the Bitcoin had been stolen, the platform closed and bankrupt at last. How to protect the platforms and how to find and punish the hackers are still the big problem.

4. Prospects

4.1. Application of Blockchain Technology

Blockchain technology improve the reliable and authenticity of the Bitcoin transaction information. Each node will save all data of the blockchain, therefore, even if some nodes have been attacked or broken, it will not threaten the whole transaction information, meanwhile, when there is a transaction going on, all of the users in the world can play as a supervisor role. Everybody maintains the blockchain information together.

Blockchain technology not only can be used in digital currency, it is also can be used in economics, finance and society system. For example, data storage, electronic contract, election and voting, financial transactions and so on.

4.2. Strengthen Supervision

Bitcoin has high speculative and risky. Many countries are still research the Bitcoin transactions potential risks. Bitcoin can protect the illegal transactions indirectly, it is difficult for the governments to accept it totally. Bitcoin cannot be controlled by the governments, once it circulates as the legal currency or leaves the governments supervision, it is easy to make some bad influence in domestic financial environment. It is no doubt that the governments will put more effort on supervision in the future, in order to make their domestic financial environment healthy.

4.3. Develop New Digital Currency

With the development of technology, payment method has been changed a lot, digital currency will play an important role in the future. Although the Bitcoin makes the governments upset sometimes, the governments can also learn from Bitcoin and develop new digital currency.

Digital currency belongs to interdiscipline, not only require the computer science technologies but also require the finance theory support. Therefore, when we learn from the Bitcoin technology, we should also make some analysis on circulation environment, corresponding laws and regulations, influence on finance system and so on.

References

[1] Wu Hong, Fang Yin-Qing, Zhang Ying. A Crazy Digital Currency——Nature of Bitcoin and its enlightenment[J]. Journal of Beijing University of Post and Telecommunications (Social Sciences Edition), 2013(7): 46-50.

[2] DORIT, ADI. Quantitative Analysis of the Full Bitcoin Transaction Graph[J]. Department of Computer Science and Applied Mathematics, 2012(7).

[3] Jia Liping. Theory, Practice and Impact of Bitcoin [J]. Monetary Theory & Policy, 2013(12): 14-25.

[4] Su Kai. The Development of Bitcoin and Regulatory Proposal [J]. Pioneering With Science & Technology Monthly, 2015, 28(2): 33-38.