

Bitcoin Present Situation and Its Applied Research

Zhao Rong

School of Economic and Management
Shengyang Aerospace University
Shengyang, China
Zhaorong@sau.edu.cn

Abstract—The development and orientation of bit-coin is the forefront of currency issue for it is directly related to the currency position of bit-coin and affects the progress direction of the world economy. At present, there are serious differences in people's discussion about the orientation of bit-coin, the typical representation of which is that they do not have a thorough understanding of the basic properties of bit-coin, neither is there a legal orientation for it, and especially that is a lack of the basis of methodology of various research. All these have been hindering the application and progress of bit-coin. By discussion the current classification and future development of bit-coin, we believe that the generation of bit-coin is a reflection of the Internet economy.

Keywords- *bit-coin; virtual currency; security application; Internet finance*

I. BACKGROUND AND SIGNIFICANCE OF BIT-COIN RESEARCH

Since this year, the currency of the fastest appreciation is not the sovereign currency of any country, but a virtual currency called "bit-coin". On January 2, 2013, the value of 1 bit-coin was \$ 13.16, on February 28, its trading price was over \$ 32; on March 29, \$ 92; on April 1, over \$ 100; and on April 10, the trading price of bit-coin reached a record high of \$ 266, and then plunged 60% and fell to \$ 105 hours later, since then it has rebounded to \$ 175 and then remains stable. In the subsequent days, the oscillation of bit-coin continued until April 16 and the trading price fell to \$ 76; on April 25, bit-coin was traded publicly for the first time with the trading price of \$ 0.03 per bit-coin. Taking the highest trading price of \$ 266 as the benchmark at that time, the exchange price of bit-coin to dollars in the three years has increased nearly 8900 times. Currently, there are nearly 11 million bit-coins in circulation, and calculated according to the highest trading price of bit-coin the total value of bit-coins in circulation at present has once reached \$ 2.9 billion after they have been converted into dollars. It is foreseeable that bit-coins represent the development direction of new currency system in the future. We must further understand the influence of the rise of new virtual currency to the field of economy and finance and explore the corresponding countermeasures.

II. SUGGESTIONS TO IMPROVE THE BIT-COIN DEVELOPMENT

There are many risks to the maturation of bit-coins. Virtual currency like the bit-coin has been emerging one after another, including Litecoin, Peercoin, and Primecoin, etc. All these new currency will compete with bit-coin.

The biggest risk to the development of bit-coin is regulatory uncertainty. And most countries have claimed that they are highly alert to illegal activities of using bit-coin for money laundering and terrorist financing, etc.

There is still a long way to go for bit-coins and other virtual currencies to have become mature. The following measures should be taken to continuously track the research on the basis of strengthening the regulation of bit-coins.

First, legal status of bit-coins should not be recognized for a long time. Currency is the trust relationship for general equivalents. A recent American official survey has shown that currently the legal status of bit-coin has not been recognized in any country. It should meet the minimum technical requirements for a new form of currency to become mature. And it is also necessary to have a good mechanism design, market cultivation and development, the corresponding policies and systems and the improvement of legal system and tax system.

Second, bit-coin supervision and consumer protection should be strengthened. The anonymity of bit-coin makes it easy to be used for illegal activities, so we can strengthen the bit-coin exchange regulation, and force the implementation of the anti-money laundering provisions. The circulation of bi-coin on the Internet makes it easy for cross-border transaction. Therefore, it is necessary to strengthen regulations all over the world. At the same time, due to highly concentrated distribution, the bi-coins are easy to be hyped, so research into relevant laws of bi-coin as special virtual goods must be speeded so as to safeguard consumer rights and interests.

Third, research of Internet currency should be increased. Internet currency, represented by online community currency and bi-coins, should be paid attention to. Currency evolution matches economic development. The Internet economy has created a new economic model, thus a new form of money is bound to be born. In our opinions, Internet currency will be widely used in network economic activities, and human society will return to the situation in which legal currency of the Central Bank coexists with private currency.

Four, regulation of bit-coin should be improved. As a new Internet product, bit-coin is in the blank of regulation in each country. And as the price of bit-coin gets higher and higher, more and more people have been joining the transaction of bit-coin. Therefore, the government should carry out timely regulation and supervision over bit-coin transactions to ensure the legitimate rights and interests of traders. Meanwhile, more and more virtual currency are been developed and traded, so the sooner to improve regulation and supervision over bit-coins, the better can we ensure the country's financial stability and security.

III. IDEAS AND METHODS FOR FURTHER DEVELOPMENT OF BIT-COINS

A. *Main Restrictions to Long-term Development of Bit-Coin*

The background of currency emergence is the development of barter against the background of social division, and the background of bit-coin emergence is the global economic integration and globalization of the Internet. Bit-coins are born with the characteristics of globalization and decentralization, which is adapted to the development of the Internet economy. However, the use of bit-coin has a strong reliance on systems and network externality, therefore, if a new currency is to replace the traditional currency, it must have an obvious advantage in some respects, and is also not significantly weaker than the existing currency in other aspects. From this perspective, the long-term development of bit-coin is significantly subject to the following defects:

1) *Security Risks*

As mentioned before, a set of strict cryptographic system is used in bit-coins, and unless there are major breakthroughs in relevant field of mathematics, otherwise the security of bit-coin itself is worth trusting. However, as the market price of bit-coin increases continuously, incidents like that some relevant transaction websites are attacked and the accounts are stolen away have occurred from time to time. Why these security accidents frequently happen to bit-coin which is theoretically safe?

Because the bit-coin account is just an account, and the only evidence of ownership of the account owner is the private key, therefore, hackers have neither the ability nor the necessity to attack the bit-coin system itself, instead, they just have to steal the user's private key and then they will get the bit-coin. So far, there are the following ways for hackers to steal bit-coins: first, to steal the private key files stored in the user's computer through Trojan program and then send to the hacker; second, to intercept relevant information through the vulnerabilities of software and operating system and then analyze them to get the complete private key. Generally, the spread of private-key-related information on the Internet should be random and strictly encrypted, but there are loopholes in the design of some programs and they always use the fixed encryption or the encryption level is not enough, so that hackers can calculate the entire contents of the private key after they have intercepted relevant information and then they will steal the bit-coin. Third, to attack network wallet server by using DDOS (distributed denial of service, which is an attack way by using a large amount of false network requests to occupy and attack targeted computing and

network resources so as to make it able to handle user's normal requests) to paralyze the server. When staff is diagnosing and repairing the server, hackers use the temporary system vulnerability to steal the private key. Fourth, as there are loopholes in the certification of some network wallet websites, once the hacker has invaded into user's e-mail account and get the relevant information, they can reset the certification information of network wallet to avoid certification, thereby enter the user's account and steal the private key. In fact, the above threats faced by bit-coin can also be met in the existing online banking system. However, due to the anonymity of bit-coin, even if the police have found the stole bit-coin, it is also difficult for them to determine the criminals. More importantly, because there is no corresponding arbitration institution, the victim has no way to appeal. And even if he can appeal, because the criminals have mastered the private key, leading the victim has no other way to prove his ownership of this account, so it is difficult to get evidence and make arbitration. Strangely, the security defects of bit-coin is caused by the typical characteristics of anonymity and decentralization, which shows that at the same time of innovation, bit-coin has also left troubles for its own development.

2) *Policy Risk*

So far, faced with the new thing of bit-coin, different governments take a different attitude. Some of the countries represented by the United States and Germany give the full affirmation to bit-coin, and they are working to revise some relevant laws and regulations in order to adapt to the changes bit-coin may bring. India and some other countries have always taken a wait-and-see attitude, they neither clearly support nor oppose the development of bit-coin-related industries, but wait to take corresponding measures until the time is ripe. China, Thailand, South Korea and other countries are opponents to bit-coins, and they all have made public opposition as well as requiring domestic financial institutions to stop bit-coin-related services.

3) *Social Acceptance*

Compared with the traditional currency, the convenient use of bit-coin is also faced with the following problems: first, as mentioned before, each of the bit-coin transactions can only be confirmed after the several subsequent blocks have been added in the main block, which is very time-consuming. The minimum time of a bit-coin transaction is 5 minutes while the maximum is nearly 20 minutes, which has posed a stark contrast to the current traditional bank transactions, which only need a few seconds. Second, fluctuations of bit-coin's market value also limit its use. Few people would be willing to accept a currency of a move of more than 50% within a day, for it has gone beyond most people's risk tolerance. Just as Yermack (2013) put it, the alteration scale and volatility of bit-coin's exchange rate have exceeded more than other common currencies, destroying the effectiveness of bit-coin as a valuation unit and storage means. Third, in the design philosophy of bit-coin, there is the hidden idea that you bear your own risks, for example, there is no central node, central regulation and arbitration mechanism, and in addition to the private key, there is no other identity verification mechanism and the transaction verification only includes validation but not legitimacy, etc. Therefore,

once there is a problem, it can hardly provide any guarantee to users. However, at present most people are used to be protected when they are using money, and in order to get this protection, they can even sacrifice part of privacy. This is an inherent thinking formed in the long evolution of society and cannot be changed substantively in a short period.

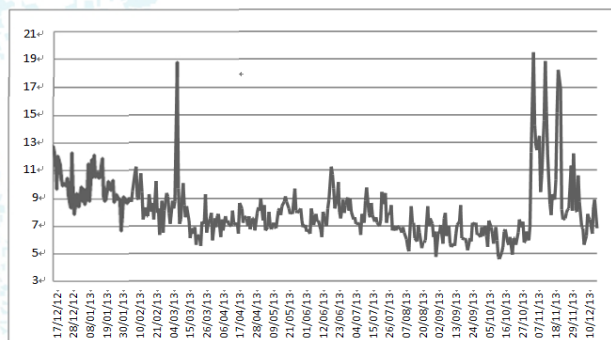


Figure 1. Average Affirmation Time for Trading (Minute)

B. Possible Ways for Future Development of Bit-Coin

For the continuous development and growth of bit-coin, the above restrictive conditions must be overcome. Because bit-coin is the product of the development of cryptography, it must be started from its principles to redesign and improve the bit-coin. However, the in-depth discussion of relevant technologies is beyond the scope of this paper. Therefore, we try to seek some viable development ways for bit-coin from other angles.

1) Innovative Ecosystem based on Bit-Coin

If we do not regard bit-coin as a potential global currency, but regard the bit-coin system as a safe point-to-point trading platform, then the design is rather rigorous. Therefore, we might regard the bit-coin system as a bottom support platform and build more upper applications by using the services it can provide. Just as the five-layer protocol of the Internet, the protocol of each layer is not perfect with its own unique advantages and fatal problems. But with the interactions and complement of protocols at each layer, they form a set of feasible solutions. We can also draw lessons from this idea, that is, the bit-coin itself does not have to be perfect, instead, we see it as an important part of a larger system, and build larger systems by building the upper applications or underlying support that match it. At the several global conferences about bit-coin in 2013, leaders of some bit-coin communities have introduced their active attempts in this aspect. Currently, representative projects include: First, SmartCoins, this is a bit-coin based stock and bonds circulation system providing a more secure and reliable means of circulation for financial products which are not active in floor market trading or simply do not exist on the market. Second, NameCoin, this is a mining system by combining existing currency and bit-coins. Essentially, it uses the advantages of bit-coin to modify the existing currency system, the specific mode of operation of this scheme still remains in discussion. Third, "open trading system", this is a trading system outside the block chains. Currently, we cannot predict how far the above innovative applications can go in the future, but they have indeed provided some more practical and feasible ideas for bit-coin. Bit-coin will not

play as the basic currency in these brand new ecosystems. In a word, it may be a road of development in the future as how to jump out of the fixed thinking frame and then re-examine and re-use the bit-coin system.

2) *Compared with gold and silver, bit-coin is still young and it is still a "guinea pig".*

Although the emergence of bit-coin is determined by market supply and demand, the biggest challenge they are faced with is from the market itself. At present, bit-coin itself also has some defects: first is the credit guarantee problem; second is the system security problem; and the third is the deflation problem. In terms of the generating system of bit-coin, the supply of bit-coin is limited. It is expected that by 2014, the total amount limit of bit-coin is 21 million. Due to the fixed total amount of bit-coin, people tend to hoard rather than circulate bit-coin, thus causing deflation and even economic depression. In a word, if the above defects cannot be overcome, it is difficult to go through the market's "survival test", and bit-coin will eventually be a flash in the pan and go dying. However, with the development of science and technology, especially the innovation of Internet technology, it is not impossible for bit-coin to evolve into the legal currency in the future. Of course, it needs a long time for bit-coin to evolve into the legal currency naturally, just like the gold and silver.

3) *To Draw Lessons from Bit-Coin and Transform Existing Currency*

Over the past few decades, the international financial crisis happened frequently, showing that the current international monetary system is not an optimal system, and it is imperative to reform it. At present, currencies all over the world are faced with various problems, directly or indirectly related to the currency instability. As a medium of exchange, bit-coin is worthy of recognition for its decentralization, security, transparency, traceability, global and convenience, but the defects of fixed total amount and long transaction time are also very prominent. Therefore, we can draw lessons from the invention thoughts of bit-coin, improve its defects and create a new form of currency (we can call it new bit-coin), making it better meet the important characteristics of transaction medium.

IV. CONCLUSION

In this paper, the author analyzes the typical features of bit-coin through the elaboration of bit-coin's operation principles, and looks forward to the possible prospect of bit-coin. The main conclusions include: firstly, as a major innovation in the history of currency, a series of innovative ideas and methods used in the design of bit-coin is worth learning. It is a positive attempt to solve the currency problems currently faced by the world, therefore, it has received extensive attention. Second, as we are seeking innovative ways to solve the problems of bit-coin, we have also introduced some new incompatible and fatal problems, causing the market to have doubts whether the bit-coin in the existing forms can achieve a long-term development. Third, the development prospects of bit-coin depend on whether the transition is smooth and successful. It is needed to re-examine and re-design it whether we are going to establish other application levels on it or regard it as a component of the global monetary reform. We believe that although there is a long way to go for the development

of bit-coin, if the design is more reasonable, and interests of all parties can be better coordinated in the implementation process, it is still worth looking forward to.

All manuscripts must be in English. These guidelines include complete descriptions of the fonts, spacing, and related information for producing your proceedings manuscripts. Please follow them and if you have any questions, direct them to the production editor in charge of your proceedings at Conference Publishing Services (CPS): Phone +1 (714) 821-8380 or Fax +1 (714) 761-1784.

This template provides authors with most of the formatting specifications needed for preparing electronic versions of their papers. All standard paper components have been specified for three reasons: (1) ease of use when formatting individual papers, (2) automatic compliance to electronic requirements that facilitate the concurrent or later production of electronic products, and (3) conformity of style throughout a conference proceedings. Margins, column widths, line spacing, and type styles are built-in; examples of the type styles are provided throughout this document and are identified in italic type, within parentheses, following the example. PLEASE DO NOT RE-ADJUST THESE MARGINS. Some components, such as multi-leveled equations, graphics, and tables are not prescribed, although the various table text styles are provided. The formatter will need to create these components, incorporating the applicable criteria that follow.

REFERENCES

- [1] Yi Gang, Wu Youchang. Money and Banking [M] . Shanghai: Shanghai People's Publish House, 2013:27.
- [2] Xinhua Net. Gasoline Ticket has Become the New Zimbabwe "Currency" [EB/OL] . (2012-08-10) [2013-06-22] .
- [3] Ma Xiaoyu, Liu Yuxin. Safety Problems and Countermeasures of Electronic Money [J] . Journal of Zhenzhou Economic Management Cadre, 2013, 20(1):91.
- [4] Liu Yanping. Analysis of the Historical Evolution and Consequence of Monetary Distribution in Our Country [J] .The Finance (academic version), 2013(3):33-34.
- [5] Yang Weiguo. Euro and the European Economic Growth [J] .Research of the Europe, 2013(1):1-13.
- [6] Smith Brian, Wilson Ramsey. How best to guide the evolution of electronic currency law [J] . U L REV, 2014 (46) : 1111.
- [7] Guo Yangang. On Centralization and Unification of Currency – Experience from the Debate of Currency Distribution Rights in Ancient China [J] Chinese Currency, 2013(1): 19-23.
- [8] Hayek Friedrich. The denationalization of money [M] . London: Institute of Economic Affairs, 2014: 1-108.
- [9] Friedman Milton. Capitalism and freedom [M] . Chicago: The university of Chicago Press, 2011: 20.
- [10] Grinberg Reuben. Bitcoin: an innovative alternative digital currency [J] . Hastings science & Technology law Journal, 2012, 4 (1) : 170.
- [11] Fei Zhaoqi. Whether Money Growth Causes Inflation – Dynamic Perspective Based on Causality. [J] Research of International Finance, 2012(7): 4-11.
- [12] Lu Zhaofeng, Zhou Zongsen, Wang Daohua. Realization of the Third-Party Payment Platform and Online Payment. [J] Agricultural Network Information, 2012(5): 91-92,36.
- [13] Jia Shaohua, Liang Xiaojing. Research of E-Commerce Tax Collection [J] .Research of Tax and Economy, 2012(3): 1-8.
- [14] Hong Shuning. Challenge of a New Currency to Finance[J].Chinese Credit Card, 2011, (10): 62-63.
- [15] Wang Huili. Analysis of the Cause of Network Virtual Currency and the Trend, 2014.
- [16] Chui Qidong, Zheng Xiaodan. Economics Analysis of the New Currency – Bit-Coin, Modern Economics, 2014 (03) : 11-19.
- [17] Li Cheng. Finance. Science Publishing House, 2013.