The Influences of Blockchain Technology Application on Stock Market Operation System

Fangyuan Sheng

School of Foreign Studies

Central University of Finance and Economics

Dr. Wu

June 25, 2017

Acknowledgments

I would like to express my sincere thanks to all those who offer help and valuable advice in the course of making this thesis a reality.

First of all, my greatest gratitude goes to Professor Yusong Chen, my academic adviser, who guided me throughout my writing of the thesis. She carefully read every draft of my thesis, corrected many mistakes I made and offered illuminating instruction as well as precious criticism. Her standards of academic excellence have greatly enriched my thesis.

I also owe a special debt of gratitude to all the professors in the School of Foreign Studies, from whose devoted teaching I have learned a lot of practical skills and academically prepared for the thesis.

Last but not least, I would also like to thank my friends and beloved family. It is their encouragement and support that help me go through frustration and depression.

ABSTRACT

As the underlying technology of Bitcoin, blockchain technology works in a form of open books. It records all transactions on the chain, i.e., a system composed of inter-linked blocks. This unique recording method, along with the contention among nodes for bookkeeping right - another special design within the system, endows blockchain technology such properties as decentralization, unforgeable information, confirmation of ownership, and high transparency. These characteristics make blockchain technology stand out among its counterparts and can help solve the credit problem, agency problem, information asymmetry problem, and etc. It is predictable that the combination of blockchain technology and the financial industry will bring about a remarkable transformation on capital market operation mode and its organizational structure.

This paper focuses on the influences of blockchain technology application on stock market operation system. To start with, the paper introduces the principles and operation mode of blockchain technology, and analyzes its characteristics. In doing so, it is made clear that blockchain technology helps to improve settlement speed, cut transaction cost, facilitate equity investment, and tackle information asymmetry and distrust. It is also pointed out that blockchain technology poses a potential threat to some traditional financial services like the third-party depository system, securities brokerage business, listing process, and equity investment. Then, this paper demonstrates that the anonymity of blockchain system leads to certain dependence on existing intermediary organizations. At last, policy recommendations are given at the end of the paper. All in all, the blockchain technology is a revolutionary force in the IT era. Despite incomparable advantages, blockchain technology has its disadvantages. In the future, the application of blockchain technology to the stock market will become a top priority in the world, but it takes time.

KEY WORDS：blockchain　bitcoin　decentralization　stock market

Contents

The Influences of Blockchain Technology Application on Stock Market Operation System

In the year of 2008, Nakamoto[1] published his paper "Bitcoin: A Peer-to-Peer Electronic Cash System", in which a new currency system and its sophisticated trading model were provided. At an astonishing speed, Bitcoin, as a new type of electronic currency, attracted the attention of the world. However, very few have realized the importance of blockchain technology – the cornerstone of this "Bitcoin frenzy" – even until now. This new technology is characterized by decentralization, unforgeability, confirmation of ownership, and transparency. Achieved by a unique record mode and the competition between nodes for right of bookkeeping, these technological features of the blockchain help solve many problems in the traditional trading system such as intermediary problems and information asymmetry. It is expected that the application of blockchain technology to the financial industry will trigger a dramatic change, bringing the capital market a tremendous transition in its trading and operation system.

Introduction

Since the commencement of the financial market, countries around the world have made great efforts to improve the efficiency of the stock market and shorten its trading time. Obviously, efficient operations and accurate recordings are the right way to go in that they will greatly enhance the sensitivity of the financial market and achieve rational allocation of the resources. In 2008, Nakamoto published his paper

[1] Nakamoto, S. (2016, March 23). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Retrieved from https://www.bitcoin.com/bitcoin.pdf.

"Bitcoin: A Peer-to-Peer Electronic Cash System", creating the first Bitcoin in the world and its supporting technology—blockchain.

Blockchain technology requires all nodes within the system to fight for bookkeeping rights through calculation, which endows it characteristics of decentralization, unforgeable information, confirmation of ownership and high degree of transparency. Blockchain technology can help the traditional security market to overcome its credit problems, intermediary problems and information asymmetry.

The technology is able to exert great impact on the capital market operations and stimulate market transformation. Therefore, it is predictable that the application of blockchain technology to the financial industry has a promising future. However, on the other hand, blockchain technology is tied tightly with electronic money by design. And the defect of electronic money increases the risk of money laundering and the possibility of smuggling, affects the central bank's money supply and the effectiveness of the monetary policy. Hence, how to take full advantage of blockchain technology and minimize its disadvantages should be the focus of research in the future.

An intensive study on blockchain technology and Bitcoin started in 2008. The two are often linked with each other and studied together. By now, scholars' researches have covered the introduction of blockchain technology and its technical details, as well as the exploration of the value, reliability and application prospect of Bitcoin.

Nakamoto (2008)[①], founder of Bitcoin, is the pioneer in this area who combines the blockchain technology with Bitcoin perfectly. Using workload proofs and hash algorithms, Nakamoto safeguards the authenticity of the transaction within the Bitcoin system. Furthermore, his usage of Poisson distribution model confirms the security of the application of the 6-time sub-block inspection method, which opens a new chapter

[①] Nakamoto, S. (2016, March 23). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Retrieved from https://www.bitcoin.com/bitcoin.pdf.

of the Bitcoin system. Since then, the blockchain technology's application in finance has become the focus of the study. Scholars like Carlo R. W. de Meijer[①] recognize the advantages of blockchain and want to develop it in a balanced way. Also, It is noteworthy that Chinese scholars like Cai (2016) [②]point out that blockchain technology can play a role in digital currency, digital bills, payment and settlement, the proof of interests, and etc. Accordingly, they recommend that Chinese government not only keep a close eye on the progress of the world and seize opportunities, but also be aware of the risk of money laundering.

In addition, with the development of blockchain technology, many scholars tend to believe that the blockchain technology is able to breed a real "direct finance", i.e., a "self-finance"(Cao[③], 2016) without any financial intermediaries. In the "self-finance" system, blockchain technology will solve the problems of information symmetry, symmetry of financial technology, and information authenticity, leading to a dramatic change in both financial regulatory institutions and traditional financial institutions. Besides, Cao (2016) identifies two models of the blockchain technology concerning its development and application in the future: blockchain start-up companies invested by the investment company and blockchian application developed by banks and other financial institutions. Then he analyzes the advantages of blockchain technology on effective private transaction, rollback transaction, reduced transaction cost, privacy protection, and so on.

However, not all scholars are optimistic about this technology. Ling (2014)[④], based on the paper by Nakamoto, gives a detailed analysis of the technical principles of Bitcoin transactions, with which blockchain technology ties. Statistically and empirically, he proves that the address of Bitcoin and the actual user are not fully correspondent. He then uses ADF unit root test and Granger causality test to show

[①] Carlo R. W. de Meijer (2015). The UK and Blockchain Technology: A Balanced Approach. Journal of Payments Strategy & Systems, (4)：220.

[②] 蔡钊(2016),区块链技术及其在金融行业的应用初探[J],《中国金融电脑》,(2):30-34.

[③] 曹磊(2015),区块链,金融的另一种可能[J],《首席财务官》,(24): 12-13.

[④] 凌清(2014),比特币的技术原理与经济学分析[D]。硕士学位论文。上海：复旦大学，5-10.

that Bitcoin has a strong speculative trend. Zhang[①] (2013) focuses on the impact of Bitcoin on the economy and the financial system. He believes that Bitcoin greatly promotes the financial innovation, making virtual wallet to be a representative of the new market and profit model; but at the same time, Bitcoin also increases the risk of money laundering and smuggling. With characteristics of "black market" currency, Bitcoin might affect the transmission of money supply and monetary policy, weaken the prominent position of the central bank, threaten sovereign currency, and affect the country's seigniorage revenues and the regulation of the financial system.

Similarly, Wu, Fang and Zhang[②] (2013) question the reliability and investment value of Bitcoin while analyzing the problem of Bitcoin. According to them, the most serious problem is that Bitcoin is an unstable currency and tends to have deflationary bias. Meanwhile, the existing law for virtual currency is still imperfect and information security still faces a great danger.

Apparently, although blockchain technology has been recognized by the research community, for now its application effects and risk control mechanism still remain problems to be addressed. Besides, the existing studies on the influences of blockchain technology are not only insufficient but also overly general and macroscopical. Much research interest has gone to the formality of electronic money, the value of Bitcoin, i.e., whether it can replace the existing system, and blockchain technology’s impact on the intermediaries. However, the direct impact of the blockchain technology is neglected by many. In other words, scholars’ researches on the impact of the blockchain technology are mainly based on the macro-background, instead of focusing on a specific market. In addition, with scholars concentrating their research on the formality of electronic money and the possibility for Bitcoin to replace the existing currency system, an overwhelming body of the literature is

[①] 张超(2013),新型虚拟货币比特币的发展现状及其对现实经济和金融影响的研究[J],《时代金融》,2013(05):291-293

[②] 吴洪,方引青,张莹(2013), 疯狂的数字化货币——比特币的性质与启示[J],《北京邮电大学学报(社会科学版)》,(3):46-50.

devoted to the study of Bitcoin's impact on various intermediaries as well as on the payment and settlement system. And this has left scant research attention paid to the impact of the blockchain technology application on the stock market, which this paper is going to direct at.

Hence, this paper aims to fill the void by demonstrating various influences on the stock market brought up by blockchain technology in detail and elaborating its impacts on the stock market operation system specifically. Hopefully, this paper can help to boost the development of the blockchain technology application in the stock market. However, there are still some problems concerning this paper. The paper discusses the structure and principle of the blockchain technology theoretically. Since the blockchain technology is still a brand new or nascent technology, it is very difficult to collect complete and ideal sample data and associate the result caused by the implementation of the blockchain technology with other related factors. Therefore, the empirical analysis is not carried out perfectly and further study needs to be done.

I. Introduction of Blockchain Technology

1.1 Definition

Technically, blockchain is a distributed database that maintains an ever-growing list of ordered records called blocks. Blocks are connected with each other by cryptography method. And every block contains a timestamp and a Hash value which links it to the previous block. Once recorded by a random node (user in the system), the data in a block cannot be altered retroactively.

1.2 Terminology

1.2.1 Hash Algorithm

Hash algorithm is a one-way function, through which the encryption of a piece of information can be achieved. And this algorithm is irreversible, namely, Y can be obtained from the X through mapping, but X can not be obtained from Y in return. SHA-256 is a typical Hash algorithm. When a user inputs a piece of information of arbitrary length into SHA-256 function, he or she will get a hash output of a fixed length; if the user changes the input number slightly, the computer will show a totally different output. Because of its characteristic of irreversibility, Hash algorithm is often regarded as a perfect method to check the integrity of information and data.

1.2.2 Digital Signature

The essence of digital signature is a process of cryptographic transformation. It is used to verify the integrity of the original data. Public key and the private key is an integral concept of digital signature. The public key is similar to an E-mail address, which goes public, while the private key, like a code, is owned by the owner only. In the process of transaction, the sender will sign on the information package with private key, and the receiver verifies information with the sender's public key. The two are complementary to each other to ensure the authenticity of transaction.

1.2.3 Proof of Work

The proof of work is the extra work done by blockchain users, in order to prove the authenticity of the information they send. It seems to be a waste of computing power, but it actually reflects "the handicap principle", that is, when all users in a system are equal in status and lacking in confidence in each other, they have to do extra work to express their "good intentions". Therefore, proof of work is the method for all nodes to show their authenticity.

1.3 Technology

1.3.1 Transaction Order Generation

In a typical Bitcoin transaction, here we get two problems when owner 1 wants to transfer 500 dollars to payee 2. Firstly, the owner 1 wants to check the safety of money flows, that is, whether his money goes to payee 2 safely or not. Secondly, the payee 2 wants to know the source of the money, that is, whether the owner1 is the lawful owner of the money. So how does blockchain technology solve this kind of trust problem?

First of all, referring to figure A1, the transaction initiator (owner 1) needs to input Hash value H0, the amount of money and the public key of payee 2 into the system. The Hash value of the last transaction (H0) shows the source of the money, by which the public key of owner 1 can be obtained. Meanwhile, the public key of payee 2 tells the address of the beneficiary of this transaction. Then, owner 1 needs to input this information package into the SHA-256 function so as to generate another Hash value, and encrypts it by his private key.

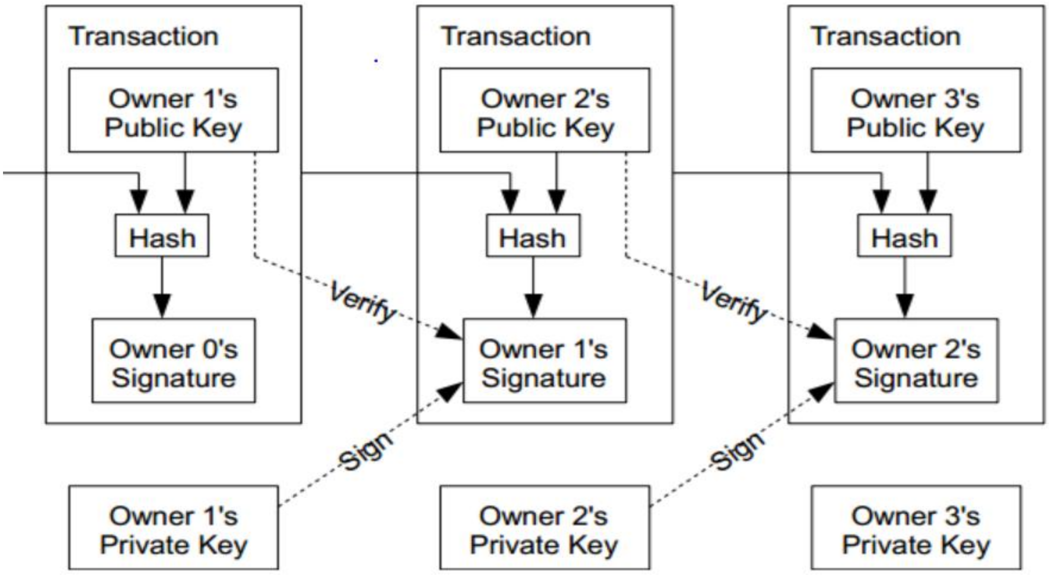


Figure A1[①]

In this case, the encrypted Hash value is the digital signature of owner 1, which verifies the authenticity of the identity of him.So far, the owner 1 has owned an information package as well as their digital signature. And what he should do next is to input them into SHA-256 function to generate the second Hash value (H1) and then transmit it to the whole system. After that, all nodes will help to confirm the deal. For payee 2, he will receive the transaction information and the Hash value H1 of the transaction the moment the owner 1 broadcasts it in the system. Then he has several things to do. Firstly, he is supposed to use his private key to decrypt the public key in the information package. Secondly, he should find the public key of owner 1 through

[①] 凌清(2014),比特币的技术原理与经济学分析[D]。硕士学位论文。上海：复旦大学，5-10.

the Hash value. After completing these two steps, now, payee 2 has all the original content of information package. Thirdly, the payee 2 needs to put the package into the SHA-256 function again to get Hash value H2. Similarly, he will get a Hash value H3 with the owner 1's public key. As long as H3 equals to H1, the credibility of the information is proved, which is determined by the one way mapping nature of the SHA-256 function.

1.3.2 Transaction Record

The moment the transaction is generated, it needs to be recorded accurately. Once a single transaction is broadcast to the whole network, blockchain technology ensures that all nodes are equal and have the ability to record it. And this is an important step of the system to achieve the decentralization. Therefore, a mechanism is needed to motivate every node to record the transaction and help to select a final recorder of this transaction. This mechanism is called "Mining". Through Mining, nodes compete with each other in a mathematical game to win the right of recording and rewarding. In the game, the first node who finds a certain random number set by the system needs to broadcast it to the whole network for verification. So the Mining process (mathematical competition) encourages all nodes to involve themselves in accounting, making the transaction trustworthy.

II. Positive Impacts of Blockchain Technology Application on Stock Market Operation System

2.1 Primary Market: Self-verification and Confirmation of Stock Rights

2.1.1 Public Offering

No matter what kind of listing system (approval system or registration system) a market applies, the priority of listing is to ensure that listed entities provide real financial information to the market so that investors can make right investment decisions. False information will disturb the market order, damp down investment enthusiasm and harm the interests of investors. Therefore, nowadays, in the process of listing, companies are not only required to have a counselor for listing, most commonly investment bank, but also to provide financial statements from an accounting firm and a legal verification from a law firm so as to prove the legitimacy of their business activities.

In contrast, blockchain, an open distributed book without the third party, not only ensures a "real and reliable" market, but also allows investors to obtain information of a company's capital flow. To some extent, blockchain technology covers the business of the law firms, accounting offices, and investment banks.

Thus, theoretically, the blockchain technology can completely replace financial intermediaries mentioned above, shorten the time cost, reduce the listing procedures, and promote the development of the securities market.

2.1.2 Private Offering

In the traditional de-centralized network model, the "Byzantine General" problem remains an unsolved puzzle. Just as Byzantine generals who were faced with the problems of distrust during the war thousands of years ago, the nodes in the blockchain system are also distrustful of each other. But now, a mechanism called workload proof might provide a perfect solution to it by increasing the time-cost significantly once someone wants to pass false information. In the blockchain system, each transaction initiator must provide their digital signature. In order to get it, transaction initiator should encrypt SHA-256 output with their own public key.

For a real transaction, time costs in the process relative to their authenticity proof are quite low. However, it is a totally different picture for counterparts who want to convey false information. Their time to produce digital signatures will exceed the counterfeiting activity itself. In this way, the blockchian technology can inhibit fraud activity efficiently. Therefore, in this way, blockchian technology can be used to confirm the ownership of the stock market and exert a direct impact on equity investment, especially for private equity.

By definition, private equity is the stock not open to the public, and its registration is particularly important. The application of blockchian technology can reduce the uncertainty of equity registration, stimulate the private equity investment and investment normativity.

In 2015, George Osborne, British Chancellor of the Exchequer, announced that the United Kingdom would increase its investment in electronic money and blockchain technology, showing a promising future of this technology. Several years ago, company Chain.Com successfully issued shares to private investors through blockchain trading system. In January 2016, after Deloitte & Touche applied Rubix software into audition and information registration, PricewaterhouseCoopers began to set up technical team to speed up the integration and application of blockchain technology in the accounting industry.

2.1.3 Stock Pricing

In accordance with the current system for IPO, two stages witness the completion of a lawful inquiry: preliminary inquiry and bookbuilding. For preliminary inquiry, it is the issuer and its sponsor that determine the price range and price-earnings ratio range after at least 20 inquiries are made; afterwards, the final issue price will be set in the bookbuilding phase.

In the first stage, in order to get a reasonable issue price range, the assessment of stock value is of great importance. In general, the intrinsic value of the stock is the present value of dividend income in the coming years: $V = \sum_{t=1}^{\infty} \frac{D_t}{(1+i)^t}$

Where V is the intrinsic value of the stock, Dt is the dividend income in year t, and i is the discount rate. Modern stock pricing methods such as portfolio theory, capital asset pricing model (CAPM) and arbitrage pricing theory (APT) are all based on this idea.

In these models, the historical data of issuer's operating conditions, financial situation and the future development determine the theoretical value of Dt. Therefore, a reasonable pricing model requires the authenticity and accuracy of historical data. In the view of this, since blockchian technology can ensure the credibility of the data, it would be easier for the market to reflect the true value of the enterprise if this new technology is applied.

In the second stage, a stage of bidding to set the final issue price, issuance costs and subscription costs are always taken into consideration. Bidders will bid on different prices according to their own conditions. As a result, the deviation from the true value is inevitable if issuance costs, distribution costs and subscription costs exist. But this is not an issue to worry about for blockchain system. The blockchain technology reduces the intermediaries and various costs through direct communication and quick accounting. Thus, blockchain technology can help to get reasonable stock prices and narrow the price difference between the primary and secondary market.

2.2 Secondary Market: Decentralization and Reduction in Intermediaries

Decentralization is the biggest and the most distinguish advantage of blockchain technology. Because of distrust problem among market participants, in the traditional information interaction, the third party, security companies for example, is regarded as an information collection and distribution center to promote the transactions.

In the blockchain system, a peer-to-peer network is established in which all nodes are equal and all information is disclosed. Various participants compete for a specific transaction accounting right through mathematical games. If this happens, intermediaries that help to promote the transactions turn out to be unnecessary. Thus, blockchain shows the benefit and possibility of reducing the intermediaries:

2.2.1 To Increase Settlement Speed

Blockchain technology can complete the confirmation and accounting of a transaction every 10 minutes after information broadcasting and 6 times' node verification. And this time interval is controllable through adjustment of target number by programmer, a number to control "mining" difficulty degree and adjust the accounting speed.

Consequently, settlement speed can become faster and faster if the target number in the blockchain system is set properly. At present, stocks are traded two days after transaction (T + 2) in the US, one day after transaction (T +1) in Shanghai Stock Exchange. But this situation can be changed totally if blockchain technology is applied, making a instant trade possible and improving the effectiveness of the market.

2.2.2 To Impact Brokerage Business and Third-Party Depository System

As mentioned above, the blockchain technology shows its advantage in reducing the financial markets' dependence on the third-party intermediaries. By far, brokerage business and the third-party depository system have played an essentially role in intermediating. Brokerage business is the business of a securities company who is committed to help investors to trade and settle stocks in exchange for commission. In contrast, blockchain technology allows investors to sell and buy securities themselves and trade with their counterparts directly, which exerts a huge impact on brokerage business.

Third-party depository system is the agreement among investors, securities companies and asset depository banks. The appointed bank, acting as an asset depositor, will open an account for the investor during the transaction to ensure the security of the assets in the account. However, the need for this system is weakened by blockchain technology too, for it requires a specific Hash value for each transaction. Therefore, just like carrying a stamp, any node of the assets can be queried and retrospected.

2.2.3 To Save Transaction Costs

Reduced transaction costs are always associated with the reduction in intermediaries. And it is quite easy to realize blockchain technology's benefit in this area. Once the brokerage business and third-party depository system are weakened, a lot of manpower and resources can be saved and freed. Investors do not need to pay for the commission and asset management fees anymore. In addition, the financial market can reallocate resources saved into other parts to further improve the marginal efficiency.

2.3 Settlement: Collective Maintenance and Insurance of Real Information

The task of all miners in the blockchain system is to find a random number N, which is used to generate a 64-bit hexadecimal number that meets requirements of SHA-256 function for a particular transaction. The difficulty of this task can be adjusted by the target number set by programmers.

At present, blockchain system requires that the hexadecimal number found by miners should be small enough. It usually starts with 17 zeros, so that transactions can be recorded every 10 minutes. Once the number is confirmed by other nodes for more than 6 times, the first node who finds it will get certain financial reward from the system. And each successful transaction will be broadcast to the whole system to ensure that all nodes are informed of new information.

Apparently, this is exactly a realization of information equality. Meanwhile, various confirmations also guarantee the authenticity of information. If an intruder wants to alter a piece of information or falsify it, only a computing power that defeats the other nodes in the whole system can help him and make it possible. And this possibility is so small that it can be neglected.

This collective maintenance mechanism of blockchain technology takes advantage of the power of the group, making it impossible for a single individual to challenge the system so as to solve the problem of information asymmetry. And this problem is particularly serious in the Chinese stock market, where a sharp difference between ordinary investors and institutional investors leads to tons of abnormal phenomenon such as "unbeaten new shares" and "white knight".

Therefore, the application of blockchain technology is expected to achieve information equality in the IPO and other segments of the market.

III. Negative Impacts of Blockchain Technology Application on Stock Market Operation System

3.1 Lack of Identity Verification

At present, the traditional stock trading system consists of four segments: account opening, commissioning, transactions matching, and settlement and confirmation. To start with, investors need to open a stock account and a capital account at the brokerage firm and designate a bank as the third-party to ensure the security of funds and stocks. After account opening, brokerage firms will make all transactions on behalf of investors in exchange of commission and transaction fee. Besides, the existing rules require securities companies to revisit at least one percent of their new customers in a month, which also helps to guarantee the account identification.

In the exchange hours, investors give orders to their brokers after making investment decisions based on market information and personal judgment. And brokerage must verify the investors' account first to decide whether to accept the transaction commission or not. Once the order is accepted, it will be sent into exchange system to find a counterpart of the trade on a certain price. Usually, this counterpart is an institutional investor or another similar investor who opens an account and makes investment under the help of his broker.

The setting of the transaction price is divided into periodic auction and continuous auction. All investors need to bid or offer their price to the system in the first place. Under the principle of time priority and price priority, the exchange matches buyers and sellers automatically. Then the transaction will be confirmed by the system after the transaction price is set, namely, settling buyers and sellers' account and the ownership of the stock.

To conclude, although the existing system is relatively more complicated and has many problems, it ensures connection between reality and network, through which investors can trade with a counterpart in reality and facilitate the confirmation of rights and responsibilities.

3.2 Expansibility and Dependence

Useless information, accounting costs and the huge number of redundant chains within the system are great flaws in blockchain technology. The accounting ability of blockchain technology is achieved by the effort of miners, from which the cost of accounting derives. Currently, the minimum transaction cost is 0.0001 Bitcoin (approximately $ 0.04). It fluctuates with the change of value of Bitcoin. Miners have the right to receive a mining fee for transaction in which only small amount of money is involved. And this rule causes enormous accounting cost when the system is applied into stock market, where numerous transactions are traded in the primary market and the secondary market. In particular, since the blocks in the system, in order to achieve the authenticity of the information, can no longer be deleted or rewritten even if it contains false information, blockchain will expand uncontrollably and cause great pressure on the system itself.

In addition, blockchain technology and Bitcoin show an interdependent relationship. On the one hand, the blockchain technology can only be applied into the stock market with special carriers like Bitcoin. And Bitcoin itself has become a vehicle of investment in the market. On the other hand, unlike other electronic money, Bitcoin relies on blockchain technology, and its release is entirely determined by computer. This innate virtuality with the addition of investors' skepticism towards blockchain technology can explain the volatility of it. In order to prove the volatility of Bitcoin, this paper carries out the following empirical test.

3.2.1 Data selection

This empirical test is based on data from www.blockchain.info concerning the price of Bitcoin over 60 days in the United States. The test processes the daily return logarithmically to better reflect the volatility of the data:

$$Rt= In\ (Pt)-In\ (Pt-1) \qquad (1)$$

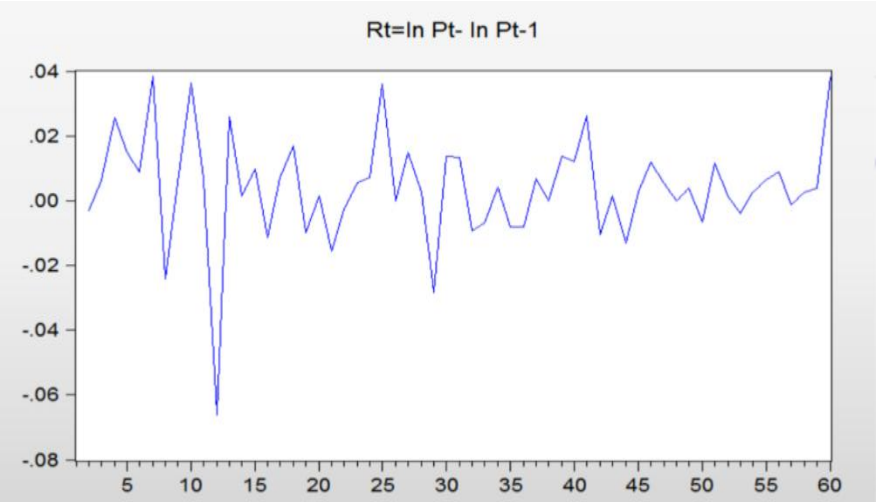


Figure A2: Log Daily Return [1]

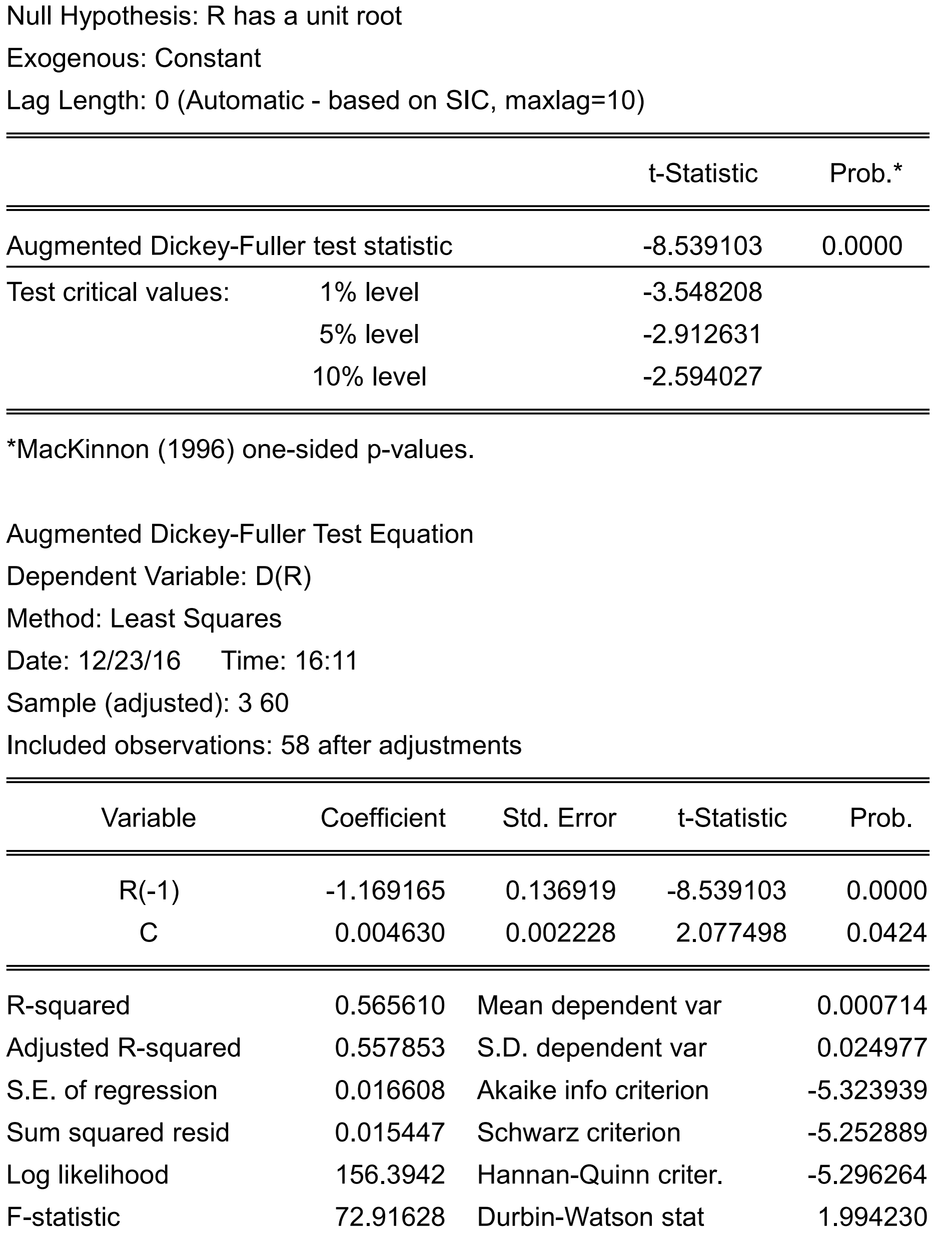
[1] www.blockchain.info

The log daily return shows that the price of the Bitcoin ranges from -6.9% to 3.9% and the greatest fluctuation happens on 11th and 12th. Although the data fluctuates greatly, sample mean is around zero.

3.2.2 ADF Unit Root Test

The ADF unit root test is performed on the time series of logarithmic returns to confirm its stationarity and prevent spurious regression.

Table B1: ADF Unit Root Test Results



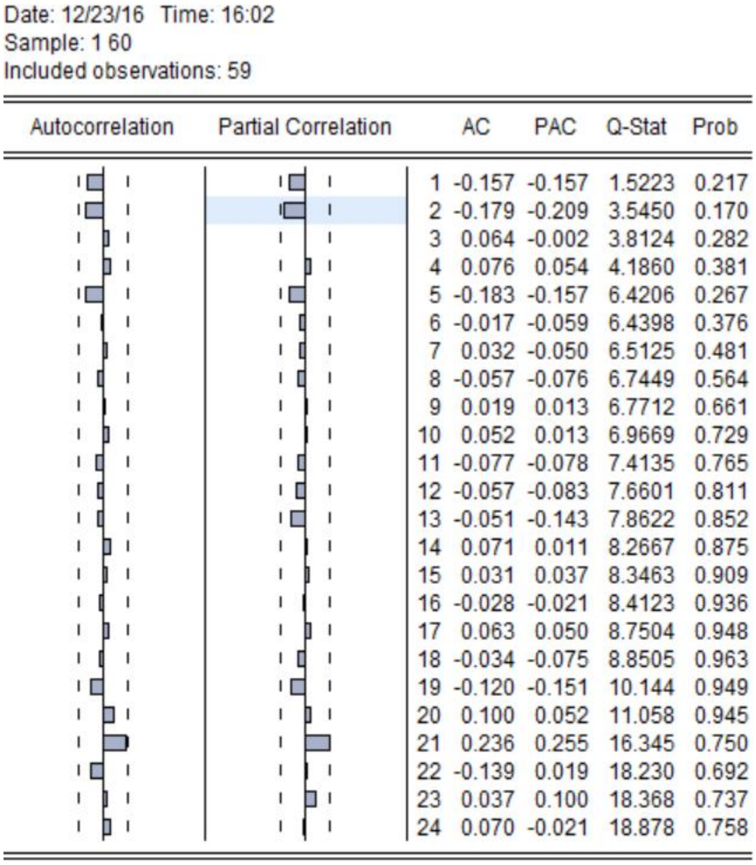
```
Null Hypothesis: R has a unit root
Exogenous: Constant
Lag Length: 0 (Automatic - based on SIC, maxlag=10)
==================================================================
                                              t-Statistic   Prob.*
==================================================================
Augmented Dickey-Fuller test statistic         -8.539103    0.0000
------------------------------------------------------------------
Test critical values:      1% level            -3.548208
                           5% level            -2.912631
                           10% level           -2.594027
==================================================================
*MacKinnon (1996) one-sided p-values.

Augmented Dickey-Fuller Test Equation
Dependent Variable: D(R)
Method: Least Squares
Date: 12/23/16   Time: 16:11
Sample (adjusted): 3 60
Included observations: 58 after adjustments
==================================================================
     Variable      Coefficient   Std. Error   t-Statistic   Prob.
==================================================================
      R(-1)         -1.169165     0.136919     -8.539103    0.0000
        C            0.004630     0.002228      2.077498    0.0424
==================================================================
R-squared             0.565610   Mean dependent var       0.000714
Adjusted R-squared    0.557853   S.D. dependent var       0.024977
S.E. of regression    0.016608   Akaike info criterion   -5.323939
Sum squared resid     0.015447   Schwarz criterion       -5.252889
Log likelihood        156.3942   Hannan-Quinn criter.    -5.296264
F-statistic           72.91628   Durbin-Watson stat       1.994230
```

Prob(F-statistic)	0.000000

The test results in Table 1 show that t values of all coefficient surpass its critical value when the confidence level is set at 95%. Besides, the probability of augmented Dickey-Fuller test equals to 0.0000, which is less than 0.05. Therefore, there is no unit root, and the time series of logarithmic returns is a stationary sequence.

3.2.3 Modeling

The correlation test is performed on the log daily returns basis, and the lag order and model are determined by the test. The correlation results are shown in Figure A3:



Date: 12/23/16 Time: 16:02
Sample: 1 60
Included observations: 59

Autocorrelation	Partial Correlation		AC	PAC	Q-Stat	Prob
		1	-0.157	-0.157	1.5223	0.217
		2	-0.179	-0.209	3.5450	0.170
		3	0.064	-0.002	3.8124	0.282
		4	0.076	0.054	4.1860	0.381
		5	-0.183	-0.157	6.4206	0.267
		6	-0.017	-0.059	6.4398	0.376
		7	0.032	-0.050	6.5125	0.481
		8	-0.057	-0.076	6.7449	0.564
		9	0.019	0.013	6.7712	0.661
		10	0.052	0.013	6.9669	0.729
		11	-0.077	-0.078	7.4135	0.765
		12	-0.057	-0.083	7.6601	0.811
		13	-0.051	-0.143	7.8622	0.852
		14	0.071	0.011	8.2667	0.875
		15	0.031	0.037	8.3463	0.909
		16	-0.028	-0.021	8.4123	0.936
		17	0.063	0.050	8.7504	0.948
		18	-0.034	-0.075	8.8505	0.963
		19	-0.120	-0.151	10.144	0.949
		20	0.100	0.052	11.058	0.945
		21	0.236	0.255	16.345	0.750
		22	-0.139	0.019	18.230	0.692
		23	0.037	0.100	18.368	0.737
		24	0.070	-0.021	18.878	0.758

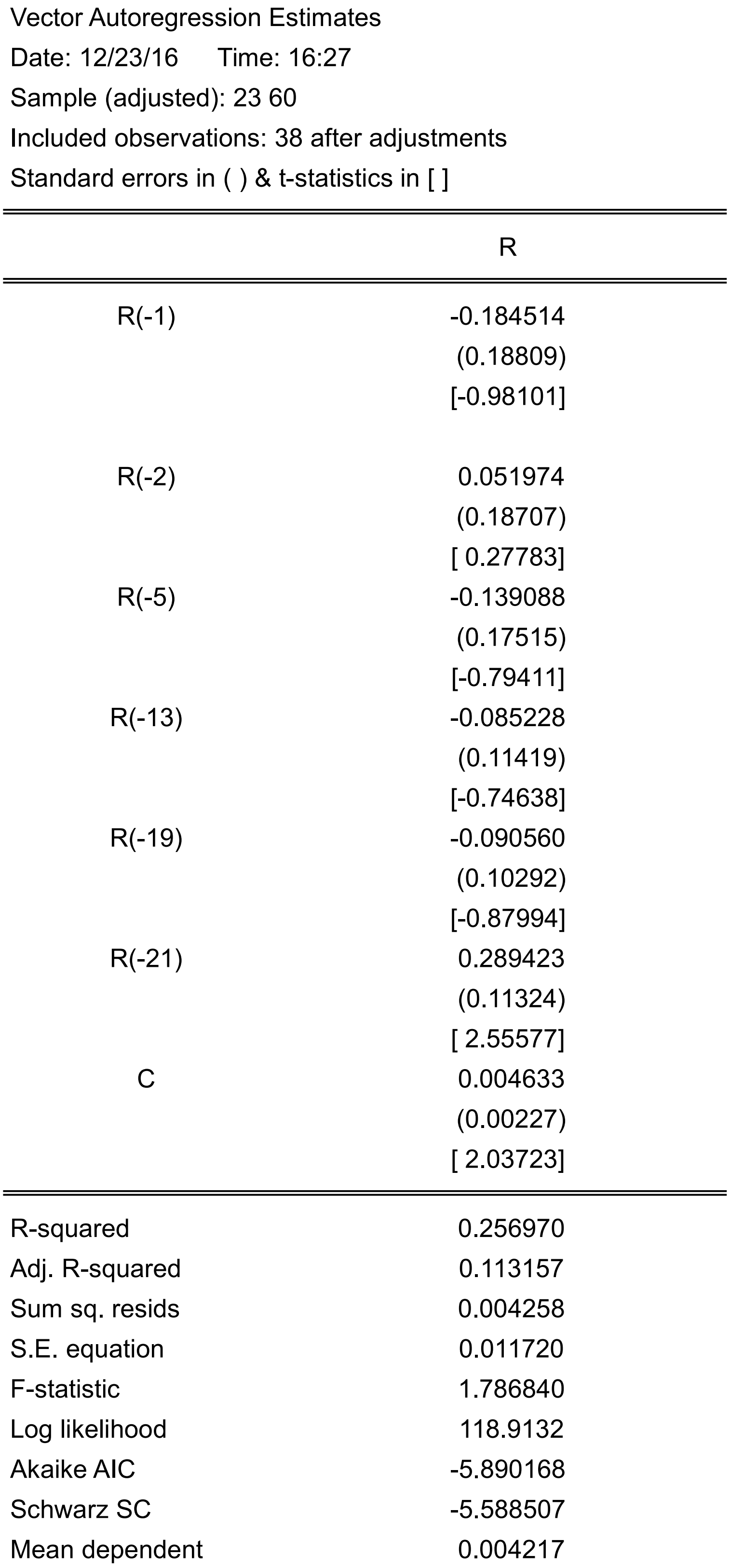
Figure A3: Correlation Test Result

Correlation test result tells that logarithmic returns of Bitcoin has 1, 2, 5, 13, 19, 21th lag orders. Accordingly, the model is set as follows:

$$R_t = c + \alpha R_{t-1} + \beta R_{t-2} + \gamma R_{t-5} + \delta R_{t-13} + \theta R_{t-19} + \omega R_{t-21} + \varepsilon \qquad (2)$$

Afterwards, auto-regression estimation is carried out.

Table B2: Auto-Regression Result



```
Vector Autoregression Estimates
Date: 12/23/16   Time: 16:27
Sample (adjusted): 23 60
Included observations: 38 after adjustments
Standard errors in ( ) & t-statistics in [ ]
==========================================================
                                    R
==========================================================
         R(-1)                  -0.184514
                                 (0.18809)
                                [-0.98101]

         R(-2)                   0.051974
                                 (0.18707)
                                [ 0.27783]
         R(-5)                  -0.139088
                                 (0.17515)
                                [-0.79411]
         R(-13)                 -0.085228
                                 (0.11419)
                                [-0.74638]
         R(-19)                 -0.090560
                                 (0.10292)
                                [-0.87994]
         R(-21)                  0.289423
                                 (0.11324)
                                [ 2.55577]
           C                     0.004633
                                 (0.00227)
                                [ 2.03723]
==========================================================
R-squared                        0.256970
Adj. R-squared                   0.113157
Sum sq. resids                   0.004258
S.E. equation                    0.011720
F-statistic                      1.786840
Log likelihood                   118.9132
Akaike AIC                      -5.890168
Schwarz SC                      -5.588507
Mean dependent                   0.004217
```

S.D. dependent	0.012446

Auto-regression estimation determines the model as:

$$R_t = 0.004633 - 0.184514R_{(t-1)} + 0.051974R_{(t-2)} - 0.139088R_{(t-5)} - 0.085228R_{(t-13)} - 0.090560R_{(t-19)} + 0.289423R_{(t-21)}$$

The model above shows that, although the R-squared (0.25) is relatively low, the volatility and dependence of the Bitcoin is quite obvious. The 21th lag order of the model indicates that the historical information still exerts an important impact on the price of today. Apart from the empirical analysis, in January 2009, Nakamoto dug the first batch of Bitcoin when the value of a Bitcoin was less than $ 0.05. Later, its value reached $ 1 in 2011 but it never exceeded 12 dollars until 2014. However, with the popularization of Bitcoin, its value continues to make new historical record: the value of Bitcoin reached $ 20 at the beginning of 2013 and $ 266 in April; in 2014, a Bitcoin is sold 1240 dollars.

Meanwhile, its great yield and excellent performance attract more and more investors. The number of investors increases from hundreds at the beginning of the year of 2009 to nearly 10 million people now. At the same time, Bitcoin also gave birth to a lot of Bitcoin related business and increased the number of the participants in the securities market. Nevertheless, when Bitcoin thrived, Mt.Gox, largest Bitcoin trading platform in the world of this kind, bankrupted after 500,000 Bitcoin was stolen in February 2014. This case caused a panic in the market and disagreement on the value of Bitcoin appeared. Accordingly, the Bitcoin price decreased sharply to about $ 400. And on April 7, 2016, the value of Bitcoin remained $ 422.

Hence, both empirical analysis and historical performance of Bitcoin show that the virtuality and dependency are two fatal defects of Bitcoin and they give a blow to the confidence of the market on the blockchain technology.

3.3 Anonymity and Virtuality

Although the blockchain technology can solve distrust problem within the system perfectly, it has two very obvious shortcoming---anonymity and virtuality. blockchain technology functions in a way that public key and private key play an important role instead of the identity verification of each node. It does not require authentic identities when accounts are opened. After uploading necessary information and applying for an account online, all participants can start a trade by a click of mouse. Users have the freedom to trade anonymously and they have no idea about who they are trading with, which increase the risk of black market and money laundering.

As the information on the blocks is interlocked with each other by Hash value, once black money flows in the blockchain system, all participants and blocks that enter the system afterwards, whether informed or not, are connected with the black money. Therefore, it will ask for millions users' identity to be verified in order to find the person who starts money laundering. Hence, the blockchain technology makes the identity verification become more complex and black market and money laundering easier.

Furthermore, in the securities market, it is quite crucial for investors to choose a proper investment vehicle. But anonymity cuts the relation between information and its owners. And many investors will hesitate for a long time before they have deeper understanding of the investment vehicles because they are not sure on which entity they are investing. In addition, many investment vehicles of good performance can hardly get enough investment and attention if they are traded anonymously from the very beginning. Thus, to some extent, anonymity and virtuality also deter transactions.

All in all, as the virtual world is not a perfect substitute for the real life, blockchain technology can not completely replace the traditional intermediary institutions. The market still needs securities companies, exchanges and other institutions to verify the identity of the traders and promote transactions in the real world.

IV. Conclusion (Policy Proposals)

It is undeniable that blockchain technology and Bitcoin system have shown their superiority in their application in the financial market. And how to take full advantage of this new technology is the top priority of the world. At present, the Chinese government holds a cautious attitude to the blockchain technology and Bitcoin system.

At the end of 2013, the government issued and implemented *Notice on the Prevention of Bitcoin Risk*, requiring trading platforms to stop Bitcoin transactions. Although the notice aims to prevent the perturbation caused by Bitcoin market and blockchain technology, it is undeniable that blockchain technology still shows great attractiveness for many countries. It brings both opportunities and challenges to the market. Hence, China should actively seek the initiative in the application of blockchain technology and here are several policy recommendations:

1. Chinese government needs to adhere to the strategy of rejuvenating the country through science and education, and look for ways to overcome the drawbacks of the blockchain technology so as to seize opportunities. It is advisable for the government to increase investment in blockchain technology, train related technical personnel and have in-depth analysis of blockchain technology.

2. On the one hand, Chinese government is supposed to promote the transformation and upgrading of the traditional financial industry. The existing system can no longer meet the need for an open and vigorous financial market. On the other hand, it is important to further improve and perfect financial laws and regulations so as to safeguard the right of investors and stabilize economic situation.

3. Chinese government needs to make efforts in the pilot work of blockchain technology. It is a process asking for patience and gradual improvement. Meanwhile, the government should keep a close eye on the data generated by the pilot work every time and ensure the stability of the promotion of the new technology.

4. It is advisable that Chinese government should always pay attention to the blockchain technological achievements and progress made by foreign countries. Talent exchanges or experience reference between countries would be a wise choice to boost the economy and achieve a "win-win" situation in which the well-being of the whole world can be improved.

Bibliography

Böhme R., Christin R., and Edelman B. (2015). Bitcoin: Economics, Technology, and Governance. *Journal of Economic Perspectives*, (2): 213-238.

Brito, J. (2011). *Online Cash Bitcoin Could Challenge Governments.* Retrieved from: http://techland.time.com/2011/04/16/online-cash-bitcoin-could-challenge-governments/Time Inc.

Carlo R. W. de Meijer (2015). The UK and Blockchain Technology: A Balanced Approach. *Journal of Payments Strategy & Systems*, (4)：220.

Cocco, L., Concas, G., & Marchesi, M. (2015). Using an Artificial Financial Market for Studying a Cryptocurrency Market. *Journal of Economic Interaction and Coordination, (2)*：345–365

Cohen, L., Tyler, R., Contreiras, D., & Pamela, B. (2016, July). Blockchain's Three Capital Markets Innovations Explained. *International Financial Law Review, 35(26)*：36-40

Gronwald, M. (2015). *The Economics of Bitcoins-Market Characteristics and Price Jumps*. Paper presented at CESifo Area Conference, Munich: 2-13.

Nakamoto, S. (2016, March 23). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved from https://www.bitcoin.com/bitcoin.pdf.

曹磊(2015),区块链,金融的另一种可能[J],《首席财务官》,(24): 12-13.

蔡钊(2016),区块链技术及其在金融行业的应用初探[J],《中国金融电脑》,(2):30-34.

黄锐(2016),金融区块链技术的监管研究[J],《学术论坛》,(10): 53-59.

贾丽平(2013),比特币的理论、实践与影响[J],《国际金融研究》,(12):14-24.

凌清(2014),比特币的技术原理与经济学分析[D]。硕士学位论文。上海：复旦大学，5-10.

吴洪,方引青,张莹(2013), 疯狂的数字化货币——比特币的性质与启示[J],《北京邮电大学学报(社会科学版)》,(3):46-50.

杨晓晨,张明(2014), 比特币:运行原理、典型特征与前景展望[J],《金融评论》,(1): 38-53.

袁勇,王飞跃(2016),区块链技术发展现状与展望[J],《自动化学报》,(42):481-493.

张超(2013),新型虚拟货币比特币的发展现状及其对现实经济和金融影响的研究[J],《时代金融》,2013(05):291-293.