Charles University

Faculty of Social Sciences

Institute of Economic Studies

MASTER'S THESIS

The Principle and Economic Analysis of Bitcoin

Author: **MA. Jiang jinggang**

Supervisor: **doc. Mgr. Tomáš Holub, Ph.D.**

Academic Year: **2021**

Declaration

1. I hereby declare that I have compiled this thesis independently, using only the listed resources and literature.

2. I hereby declare that all the sources and literature used have been properly cited.

3. I hereby declares that the thesis has not been used to obtain a different or the same degree.

In Prague 27.04.2021 Jiang Jinggang

Acknowledgments

My deepest gratitude goes first and foremost to my supervisor Doc. Mgr. Tomáš Holub, Ph.D.who promised me to be my supervisor when I first emailed him. Related knowledge, methods, research content, and even English grammar errors, he is always very enthusiastic to give me advice and help me modify the thesis. Whenever I send an email to him, he can reply in time and provide useful information in the email, which makes me feel very warm. I am so lucky and happy to have Doc. Mgr. Tomáš Holub, Ph.D. to be my supervisor.

Throughout the writing of the paper, I would like to express my gratitude to Doc. PhDr. Tomáš Havránek, Ph.D. He gave me many suggestions about my paper and other useful information to help me complete my paper. Meanwhile, I would like to express my gratitude to all professors who helped me and encouraged me during my all study in Prague.

Abstract

The development of Internet technology has promoted the progress of all aspects of society. Under the background of Internet finance, the traditional financial model is changing, such as currency payment. With the deepening of Internet technology, the virtualization of money is deepening, and the market entry, trading and payment methods are also subverting the tradition. Bitcoin as a new means of payment began to appear in the public eye. It is a challenge to the traditional way of trading supported by Internet technology. Despite the constant controversy since its inception, Bitcoin still occupies a place with its unique advantages - Asymmetric encryption, decentralization,transparency of transaction records and so on. In the eyes of opponents, Bitcoin is more of a highly speculative asset, and as it becomes progressively more difficult to mine, the cost of mining is increasing. However, in the eyes of supporters, it is a reliable means of payment, not subject to government supervision, nor will it produce a virtual transaction record. From the regulator's point of view, it is more like a shelter for unscrupulous people to evade regulation and commit money laundering and crime.

It is undeniable that in just a few years, Bitcoin has developed to a certain scale,has a certain industrial chain structure and market, and even has become a financial tool for some investors. However, judging from the records of bitcoin transactions, whether the huge price fluctuations will be a bubble, so far, bitcoin prices have experienced four sharp rise and fall, many countries even began to prohibit the operation of its trading platform. With the development of Bitcoin, more and more voices begin to gather here. As a highly innovative and controversial "invention" in the 21st century, this paper will discuss the supply and demand equilibrium of Bitcoin price and its influencing factors on the basis of monetary economics, and discuss the correlation between the price of Bitcoin against US dollar and macroeconomic data by using VAR model. The transaction and speculation properties of Bitcoin are described.

From the perspective of economics, finance and Internet technology, this paper will analyze the influencing factors of Bitcoin price, describe the historical transaction records, discuss its price formation mechanism from the theoretical model of supply and demand in economics, and focus on the analysis of the impact of government regulation and Internet search on Bitcoin price.

Key Words： Bitcoin; Monetary Attribute; Price

Contents

1 Introduction

1.1 Background and significance of the study

1.1.1 Background of the study

With the continuous development of Internet technology, the Internet economy began to emerge, and a large number of Internet financial products and their derivatives began to appear in the public eye. While capital began to seek investment opportunities, more and more people began to seek information and transparency in transactions. Libertarians' concern about government power and the emergence of traditional banking crisis made investors believe that the government controlled the number of money issued through administrative means to create a certain amount of inflation to squeeze people's wealth, and investors could not grasp the information about the overall macro transaction volume well and were prone to the problem of information asymmetry. In his 1970s monograph The Denationalization of Money, the Nobel Prize-winning economist Hayek made a radical proposal - to abolish the central banking system, issue money privately and compete freely to produce a better type of money, rather than retaining the state's "monopoly" on money. It was the combination of monetary and economic theory and information technology that led to the creation of Bitcoin on November 1, 2008, as a "currency" that was not regulated by central banks or any financial institutions, and experienced its first frenzy upon emergence, with a wave of digital currencies sweeping the world.

Digital currencies① are divided into two main categories according to their definitions One is "stablecoins" - whose underlying asset is not just gold, but also something else (e.g. an official currency or its basket),while the other is cryptocurrencies, - such as Bitcoin, Litby and other cryptographically implemented using asymmetric cryptographic algorithms network currencies. By far, Bitcoin is the most representative and globally recognized cryptocurrency. By its very nature, Bitcoin is a bunch of complex algorithms with special solutions. Initially, Bitcoin was only spread among geeks who were proficient in network cryptography, and after a period of time, its mechanism gradually became sound, and the venues providing trading services started to appear. First appearing in the media in 2011, the price of Bitcoin has seen explosive growth, with the total market cap peaking at $10

billion.After a brief rise, the price quickly fell back to a low point. In early 2013, the outbreak of the European debt crisis began to worry investors, and Cyprus announced that it was freezing people's bank deposits. The decline in confidence in fiat currency caused a new round of rapid rise in bitcoin, peaking at $266 on April 10, but then quickly falling to $100. In October 2013, however, it climbed rapidly again On December 5, 2013, the People's Bank of China and other ministries jointly issued a "Notice on Preventing Bitcoin Risks On December 5, 2013, defining Bitcoin as an "illegal currency", and more and more national regulators began to block it.

①Bitcoin is categorized in foreign literature as Cryptocurrency, a term synthesized from the cryptographic Crypto and currency Currency, including gold currency (Digital gold currency) and cryptocurrency (Cryptocurrency). This paper refers to cryptocurrency specifically as Bitcoin-like cryptocurrency.

It's undeniable that investors' enthusiasm for this new currency has not waned. Behind the huge price fluctuations is a huge investment opportunity and speculative demand, and due to Bitcoin's secure encryption and high level of privacy,more and more investors are looking to trade Bitcoin, and in 2014 "Bit China" became the world's number one Bitcoin trading platform. As with other online investment vehicles, in March 2014, hackers attacked MT.GOX's back office and looted $467 million worth of bitcoin, causing the platform to file for bankruptcy protection. Bitcoin, a new product of history, still has many problems, but it is beginning to provoke thoughts about the evolution and development of the monetary form. "Money is not a product of the state," wrote Menger(1892), the founder of the Austrian school, "it is not a product of legal provisions, and its existence does not even require the approval of political authorities. In his work, Mises wrote that in the course of its development, money has been challenged by other commodities all the time. From the beginning of primitive society, when people bartered for goods, to the emergence of precious metals, to the current paper money and electronic money, people not only consume goods, but also trade with money. In his book The Denationalization of Money, Hayek supports the idea of private creation of money, and this idea of liberalization provides the theoretical support for the emergence of Bitcoin.

Currently, Bitcoin is attracting the attention of investors, cyber hackers, programmers and governments alike. As investors are paying more attention to the price of bitcoin, focusing on studying its price fluctuations and its intrinsic value, some financial institutions are starting to develop derivatives of bitcoin to hedge against its huge price fluctuations. And as programmers and hackers active on the web, they are starting to teach each other about information security. The government, as

the regulator, has to prevent bitcoin from becoming a place of lawlessness and a tool for criminals to launder money, and study whether it will have an impact on the existing economic structure in a controlled manner. From the perspective of academic research, how to explain the formation and influence of prices from economic theory, how to regulate and how to treat this new medium of exchange is very important for the improvement and development of the entire financial system. The scale of Bitcoin trading is currently dwarfed by the macro economy, but if the price breaks down it will inevitably cause concern among global investors. In addition, cryptocurrencies such as Bitcoin, although not perfect, are useful for future monetary development. In this thesis, we analyze the price formation mechanism of Bitcoin precisely by the principles of basic economics, focusing on the influence of transactional demand, speculative demand and government policies on the price of Bitcoin, and reacting to the correlation between the former three and the price of Bitcoin by the trend of macroeconomic data.

1.1.2 Significance of the study

The use of Bitcoin as a new payment method will not only enrich the current payment methods, but also provide a tradable platform for global trade, which not only enriches the financial product market, but also is a great progress for human society. In today's society, with the gradual deepening of global trade, traditional cross-border payment means cannot meet the increasingly large transaction scale, especially in terms of price. Banks not only charge up to 2.5% for B2B transactions and up to 5% for C2C transactions based on the transaction amount and destination, etc., but will also charge payment fees and may pass these fees on to customers(lianlianpay official website), while bitcoin as the representative of the emergence of digital currency has provided a new and more efficient and convenient option for all kinds of cross-border transactions. In less than a decade since its inception, Bitcoin's price has fluctuated dramatically, making it difficult for investors to "navigate", and due to the lack of a sound theoretical framework, Bitcoin has not yet become a good investment tool. Most of the research on bitcoin has been influenced by government policies and has focused on the legal regulation, concepts and technical principles of bitcoin, but there is a lack of quantitative analysis of bitcoin prices. The link between the virtual economy represented by Bitcoin and the real economy has not yet been established, and the literature on the impact on the capital market and the real economy is scarce. In this thesis, we analyze the formation

and influencing factors of bitcoin price, and provide reasonable suggestions to investors based on the domestic and international literature, and provide ideas for domestic financial institutions to develop derivative products of bitcoin.

Bitcoin was first talked about in a cryptography group and gradually attracted the attention of the elite outside of cryptography, including economics, programming and math enthusiasts, and eventually gained widespread worldwide attention through media ferment along with the big ups and downs of the bitcoin price. Of course many economists scoffed at Bitcoin and were unimpressed, believing it could not succeed. Robert Shiller spoke at the World Economic Forum in Davos, Switzerland in 2014, where he specifically sang the praises of Bitcoin, declaring it a bubble. Paul Krugman, the proverbial "Keynesian economist," said the currency was designed with a libertarian bent to undermine the authority of the established financial system established by governments.But Bitcoin as an experiment of monetary freedom , due to its decentralized idea and constant total amount, provides a lot of reference meaning to the reality of traditional fiat money, and it is possible to transform traditional fiat money with the framework of Bitcoin, naturally there are a lot of meaning that we should study and explore, and also more people can really recognize the emerging thing of Bitcoin.

The significance and purpose of the Bitcoin selection is analyzed from four perspectives as follows.

(1) Monetary Economics. Bitcoin, as a virtual cryptocurrency, has the characteristics of a traditional currency, such as medium of exchange, unit of account, and store of value. Even today, with such huge price fluctuations, it can still have good storage value in the long run because of its constant volume (if it can continue to circulate "basically indefinitely"),but at the same time, the limited quantity also affects its function as a currency. Although it is difficult to see at the moment, to break the dollar-centered monetary system, Bitcoin is a good reference. It does not require the credit of a central bank or the intervention of the state, and it flows around the world entirely by virtue of internet technology.

(2) Decentralization. The gold standard, which is tied to the U.S. dollar, is somewhat more decentralized than the traditional monetary system, but does not completely remove government control over the currency. Bitcoin is fully supported by Internet technology, with open source code and an open ledger that allows every investor to view the history of transactions and the creation of each bitcoin. The government only needs to regulate the entire transaction environment and not the

currency itself. Although there are still many issues such as mining costs and transaction approvals, the decentralized nature of Bitcoin is the first time that private property has been secured purely through technical means and is a major change in the history of money.

(3) Complement and development of Internet finance. At present, Internet finance is developing steadily, and the contribution of the Internet economy to the economy is gradually increasing in proportion. However, Internet finance is still not free from the traditional means of payment, and is still based on the Traditional Currency. Bitcoin, as a "currency" born and raised on the Internet, is developing slowly, but it is undeniable that this new means of payment is a new development idea for traditional currency payments.

(4) Data mining and analysis. In the era of big data, there is a simple mathematical logic behind any complex economic behavior, and through analysis and mining, more valuable behaviors can often be created. Bitcoin is anonymous for any one transaction due to its decentralized nature, but the transaction records are public. All transaction records are stored in a distributed ledger. Once the number of transactions reaches a certain size, analysts and investors can often uncover the size of the economy in different regions, for example. From a regulatory perspective, although there is no record of the purpose of each transaction in Bitcoin, the combination of Bitcoin destination, address, and history information can often determine whether an investor is engaging in illegal transactions and other criminal behavior. Therefore, it is unrealistic to simply dismiss Bitcoin as a side scam and deny its future growth prospects.

1.2 Research framework and ideas

The framework of this paper is divided into two main sections: the main conclusion of this section is the basis for classifying Bitcoin's monetary properties, i.e., Bitcoin can be classified as a cryptocurrency, unlike the current online currencies, point certificates, etc., which are mainly classified as virtual currencies and owned through the purchase of physical assets. The latter is a special commodity generated using Internet technology - based on asymmetric encryption algorithms - and is not tied to a physical asset, so this paper categorizes Bitcoin as a cryptocurrency. A one-by-one comparison of Bitcoin's properties reveals that Bitcoin is consistent with Hayek's(White, L. 1999) theoretical model of money. Specifically,the quantity of

bitcoins is approaching a ceiling (21 million), satisfying the characteristic of scarcity, secondly, although bitcoins have no intrinsic value, they can be viewed as having some use value by reducing transaction costs, and finally, although Bitcoin is not a fiat currency, it introduced the mechanism of monetary competition due to its decentralized nature. It is based on Bitcoin's monetary properties that this paper explains the reasons for its dramatic price fluctuations from the perspectives of supply and demand. Specifically, the development of Bitcoin can be divided into three phases: the startup phase, the speculative phase, and the free exchange of fiat currency phase.In each phase, the development environment, Bitcoin's own technical regulation, and the government's attitude differ in their respective supply and demand characteristics, and therefore correspond to the equilibrium prices in each period.

In the second part of this thesis, we survey the current empirical research on Bitcoin. By comparing some macro data, we find that Bitcoin currently has a large price bubble, is more investment-oriented, and lacks a financial derivative that can effectively mitigate the risk of price fluctuations, so it does not function as a general unit of account in the short term. In addition, due to its inherent characteristics, there are still many countries in the world that are against it, including China. In this part, we look at the different policies and attitudes towards bitcoin in Germany, the United States and China and explore the impact of policy factors on the price of bitcoin.For example, Germany has fully agreed to include bitcoin in the scope of personal income tax regulation, while other countries have done the opposite. In the empirical part, we analyze the correlation between macroeconomic indicators and bitcoin price fluctuations over the same period, and use the ADF unit root test to confirm whether the time series is smooth. Finally, the impulse response and variance decomposition are used to determine the interaction relationship between variables and the degree of influence. Finally, the current development status of Bitcoin is analyzed for the future development trend, and whether Bitcoin can stabilize its price is discussed.

1.3 Research Methodology

(1) Combining literature research and interdisciplinary research: Bitcoin is generated through specific Internet technologies, and is simply a special solution generated by a complex algorithm that neither possesses a physical form nor is tied to any financial asset. Therefore, the study of such "cryptocurrencies" requires a combination of Internet technology, computer principles, and economics and finance, as well as access to a wide range of literature from different disciplines. It is important

to analyze how the virtual economy is linked to the real economy in the context of Internet technology, whether its evolution has changed in the face of technological constraints, and the impact of macroeconomic policies. By reviewing and analyzing some of the literature on the technical principles of Bitcoin, it is concluded that the essence of Bitcoin is to generate a public key and a private key using asymmetric cryptography by mining the computing power of the address generated by solving a specific algorithm, with the public key being broadcast across the network and the private key being kept by itself to be matched during transactions.

(2) A combination of statistical analysis and quantitative research:introduces an analysis of the Silk Road black market trading platform and the attitudes of countries such as the US, Germany and China towards Bitcoin, and highlights the problems that the introduction of Bitcoin may cause in terms of illegal trading, policy failures and taxation. The empirical section begins with a statistical analysis of the historical price of bitcoin and macroeconomic indicators over the same period to determine a preliminary correlation between the two. Secondly, a VAR model is constructed by combining the bitcoin price (BPI) with the S&P 500 (SPX), the New York Futures Exchange gold futures price (GP), the Shanghai Stock Composite Index (EQ), and the USD/CNH exchange rate (EX), using Granger causality tests to determine whether the prior period information of one indicator affects the current period information of the other variable, and discussing the interrelationship and degree of influence of the variables through impulse response and variance decomposition. The interrelationship between the variables and the degree of influence are discussed by impulse response and variance decomposition.

1.4 Focus, Difficulties and Shortcomings of the Study

The focus of this thesis is first to distinguish the monetary properties of Bitcoin, and to define the conditions under which Bitcoin is distinguished as a commodity and a currency. Secondly, we study the technical principles of Bitcoin, and dig into the economic principles behind Bitcoin through a deep technical study of Bitcoin. We focus on describing Hayek's theory of free money, elaborating on its central idea of the denationalization of money, combining the monetary properties of Bitcoin with the corresponding theoretical foundations, and analyzing Bitcoin from the supply and demand perspectives by analogy with the supply and demand equilibrium model of fiat money prices in macroeconomics. The reasons for the huge price volatility at this stage are analyzed from both supply and demand perspectives. The policy factor and

public attention are the two most important factors to be studied to analyze the correlation with the price.

The difficulty of this paper is that Bitcoin, as a cryptocurrency, is supported by computer technology, which is complex and requires a certain level of computer knowledge. Second, Bitcoin, as a financial innovation product, has only been developed for more than a decade since its creation, and has a short history related to the development of cryptocurrency. The direct research literature is scarce and focuses mainly on legal issues and regulation regarding Bitcoin, making it difficult to accurately study the correlation factors of price. Finally the market related to Bitcoin is also a difficult market to explore and is not well developed and lacks a relevant regulatory mechanism.

The shortcoming of this thesis is that there is less analysis of the factors influencing the price of Bitcoin, and a complete mathematical model is lacking for the analysis of Bitcoin, especially the price formation mechanism of Bitcoin. Due to the limitations of the literature and data, it can only be analyzed from an specific perspective. In particular, it is difficult to conduct accurate quantitative and qualitative analysis on the endogenous factors of bitcoin prices - such as transaction fees, circulation speed, and mining revenue - due to the lack of authoritative data, which can only be correlated by placing bitcoin in a macroeconomic context. Second, Bitcoin's history is so short that all analysis can only be done with the help of historical trading records, although in the long run Bitcoin has good investment properties. However, in the short term, it is difficult to judge the price direction, and it will take time to see if there is even a large speculative bubble in Bitcoin. The research in this thesis focuses on the technical principles behind Bitcoin and provides a general economic analysis of Bitcoin's price fluctuations from a Keynesian equilibrium of money supply and demand. In any case, unlike state-issued credit currencies, Bitcoin is no less a practitioner in achieving monetary liberalization.

2 Literature Review

2.1 Analysis of the monetary properties of Bitcoin

There is no international definition of what constitutes a bitcoin, but as noted above, most scholars would classify it as a cryptocurrency. This description is consistent with the technical principle that Bitcoin is generated by an asymmetric

cryptographic algorithm, and that it is "mined" through a competition of network algorithms, with computers with higher computing power being more likely to obtain Bitcoin, which in the eyes of its proponents is the monetary equivalent of money and can be used to purchase goods and services. For most lawmakers, however, the bitcoins earned through mining are more likely to be a form of payment for services rendered.

In 2013, the German government defined bitcoin as "another form of currency", and the associated transactions would be taxable, but at the same time the German government granted tax exemptions to individuals holding bitcoin. Chowdhury and Mendelson (2014) argue that for Bitcoin to become a real currency it must realize its intrinsic value, and they also believe that it is only a matter of time before the virtual currency represented by Bitcoin becomes a real currency. From a network economics perspective, the intrinsic value of bitcoin can be measured by the number of users. Surda (2012) argues that the mutual trust between participants in the network environment constitutes the value system of bitcoin, and that bitcoin itself does not have any monetary function. The stronger the confidence of investors in bitcoin, the higher the market value. This credit maintained by investors is often fragile and will not be backed by any authoritative financial institution, which then in turn is a blow to investors, and no other factor including the constant supply factor of bitcoin itself can really change the price of bitcoin. In other words, contrary to some proponents, he believes that the bitcoin economy is a bubble, with huge price fluctuations causing speculation by investors, and that once the collapse spreads, the foundation of the trust-based bitcoin economy will completely collapse, arguably making bitcoin more of a commodity.

Philipp Guring and Ian Grigg (2011) also take a negative view, arguing that with the current network-wide computing power saturation, the cost of mining is already severely impacting revenue, and that once super-users emerge, the low cost of mining will drive most regular users out of the bitcoin market, leaving more and more bitcoins in the hands of a few institutions who could even determine its price and become the new price manipulators. Yermack (2014) argues that bitcoin is a speculative instrument and that the price of bitcoin is not correlated with the exchange rate of the US dollar and the exchange rate of the US dollar against other fiat currencies, making it difficult for investors to rationally measure and hedge their risk. The relevant market cannot develop financial instruments to hedge risk, cannot be denominated in loan contracts, and cannot be incorporated into a deposit-guaranteed banking system.

2.2 Hayek's idea of free money

In the 1970s, Hayek completed his work "The Denationalization of Money", which confirmed the free market economic view from the point of view of philosophy and cognitive science. The traditional Keynesian school seemed unable to explain the coexistence of high inflation and high unemployment in a period of "stagflation" in the West. The monetarist school pointed out that inflation is essentially a monetary phenomenon. Monetary theory focuses on the effect of the quantity of money on prices, ignoring the effect of the "threshold" for the input and withdrawal of money on prices. Hayek differed from Friedman, the representative of the monetarist school, in that Friedman always thought about economics in terms of statistics, quantities and price levels, while Hayek saw that inflation was caused by distortions in the relative price structure that led to unemployment. Massive unemployment is bound to come as a result of long-term inflation under the government's long-term monopoly on money issuance, which leads to a distorted price structure. (Based on the Phillips curve, when governments tackle unemployment, they tend to do so by issuing more money, but there will be limits to this approach and it is going in the wrong direction.) ② Hayek's central idea of monetary theory is to allow private issuance of money, in the book he presented the following conclusions：

（②Source: https://www.jianshu.eom/p/ddfeal45c4a9）

(1) The government's monopoly on issuing money does more harm than good. It is not the function of the government to control the issuance of money, and the current situation is nothing more than regulating the economy from a macro perspective, as this approach has proven to be the most efficient. But when the government is in a credibility crisis and the monetary mechanism fails, it tends to produce greater damage, such as high inflation and high unemployment. If money is issued freely and competes freely, it is unlikely to produce inflation and deflation, because every time the value of the currency rises, the pressure on liabilities increases, and when the value of the currency falls, assets depreciate. Each currency issuer will stabilize the quantity of money by constant regulation to bring the value of the currency to equilibrium for a certain period of time.

(2) Private issuance of money will create a high quality currency. It is easier to increase competition before a currency is issued by the same entity than by the same institution. The market will test different currencies, decide and choose which currency to use. If the price of a currency is stable, there will be a stable demand for it,

and for an open market, the inferior currencies will be eliminated, and through this process of constant creation and elimination, those that remain will be of high quality, and the currency will be able to maintain its purchasing power even when the credibility of the country decreases.

(3) The public should change its behavior in accordance with the performance of money, not by regulating it. Denationalization of money would eliminate the need for a central bank to regulate economic behavior, and money would no longer be a policy tool to regulate phenomena in order to achieve a desired outcome. On the contrary, the free competition of money would put it into "autopilot mode", where individuals would constantly regulate their behavior based on the information they receive, thus avoiding the construction of a faulty monetary system.

2.3 Comparison of Free Money Ideas and Bitcoin

According to Marx's (1867) theory of money, money is a fixed commodity that acts as a general equivalent. The exchange between commodities is essentially an exchange of socially necessary labor time. Generally speaking, the functions of money include: "medium of exchange, measure of value, and store value, etc." The Austrian school, represented by Hayek(1976), believes that the most important property of money is its circulating value as a medium of exchange. In order to become money, it must first be able to purchase goods and services, and secondly, it must have a certain storage value. Third, it acts as a unit of value, and fourth, it is a contract for deferred payment. A combination of these four characteristics is used to select and consider money.

Another important attribute is scarcity. One of the reasons that precious metals have been able to become fiat currency for some time is because of their scarcity. If this scarcity is accepted by the vast majority of people, and they believe that the value built on it will continue to increase, then they are more likely to accept the commodity as money. In terms of the definition and properties of money, any good can become a currency, and it is a combination of factors that makes it a currency. In terms of the development process of money, a commodity eventually becomes a fiat currency is often determined by factors such as scarcity, interchangeability, security, etc. However, since ancient times, it has rarely been due to the needs of the economic system or the need to preserve the interests of the ruling class that commodities have been defined as money, that is to say, political considerations have rarely been taken

into account.

Bitcoin can be used as a representative of Hayek's idea of free money mainly in the following ways：

(1) Since bitcoins are not issued by a specific monetary institution, they are a special solution generated by a large number of calculations based on a specific algorithm. Therefore, when Bitcoin was created, it was created in a ultimate of about 21 million, which satisfies the scarcity characteristic of the currency.

(2) Bitcoin has no intrinsic value, but it has value. In traditional Internet financial transactions, there is a "secondary purchase" problem③. When buying or selling goods offline, the seller does not have to worry about receiving fake money (unless he doesn't know how to identify it), and the buyer does not have to worry about purchasing other goods before paying for them. But if it is a "digital currency", the situation is completely different, the digital information can be easily copied, the buyer's account may not actually receive the payment but the buyer shows that it has been paid, or the buyer actually pays and then withdraws the payment request after the seller confirms the information, For example, bank transfers in China can currently be requested to be revoked within 24 hours. Financial intermediaries are needed to act as third parties to achieve a fair transaction, and to solve such problems, financial institutions charge a fee. However, Bitcoin can fulfill the role of an intermediary as well as solve the problem of "secondary purchases". Bitcoin uses blockchain technology to store all transactions in a single block, and all networks are discrete, eliminating the need for financial institutions and making all records public to Bitcoin users. If someone tries to change this block, then all users will find out and vote it down. In short, you need to have more computing power than all the other users on the entire Bitcoin network combined in order to hack into the system to pay a bitcoin over and over again, which is clearly a problem where the costs outweigh the benefits. So according to the Austrian school, the reduction in transaction costs in the Bitcoin network is seen as the basis for the value of Bitcoin, which, despite having no intrinsic value, has use value as well as being a medium of exchange.

(③Zhao, Z. , Lan, Y. and Wu, X. (2016) The Impact of Electronic Banking on the Credit Risk of Commercial Banks)

(3) Bitcoin is not a fiat currency and is not enforced by the state for its circulation and trading, and the related regulation is still in a grey area. Bitcoin trading is still a personal activity of some investors, which satisfies the Hayekian definition of private money. Does a commodity need to be recognized by the government to

become a fiat currency? From the initial evolution of money, it is clear that it does not. It simply acts as a medium of exchange on the basis of use value.

However, the Austrian school was the sharpest critic of the value scale. Hayek used to guarantee the purchase and sale of commodities with gold as collateral, but once the demand for gold rises sharply, its price also rises rapidly. In this case, it is difficult for merchants to accept this scale of value for gold, because their debts will keep changing with the market environment and tend to prefer currencies that remain stable. Bitcoin's price is currently so volatile that it hardly functions as a scale of value, and an investor who is completely unable to accept the returns themselves from its risk would have a hard time hedging its risk even in a mature capital market.

As discussed above, Dirk Baur and Adrian D. Lee and Kihoon Hong (2017) also mention that Bitcoin is not a currency at the moment, but only a medium of exchange, and that this medium of exchange is still only used by a small number of people However, according to cybereconomics theory, as the number of users of bitcoin increases, its function as a medium of exchange may be amplified. However, in terms of value metrics, Bitcoin currently has difficulty achieving a stable price, which is a significant barrier to its development as a currency.

2.4 Empirical studies related to Bitcoin

Empirical research on Bitcoin has focused on three main areas:

(1) On the motivation of users to hold bitcoin

Ron (2013) analyzes the three years of Bitcoin's existence (approximately 180,000 blocks) and finds that most Bitcoins are owned by a small number of players, especially in the early years of its existence, when the network-wide algorithm was low and 20% of Bitcoin players held approximately 70% of the quantity, and these Bitcoins were rarely traded. This raises the question of whether their true purpose for holding bitcoin is to create a "bubble" on purpose. Gandal and Halabruda (2014) find that there is room for arbitrage between different virtual currencies by looking at the exchange rates between them, and that by manipulating the data more frequently, they are often able to profit from a small arbitrage space.

(2) About the risks of holding bitcoin

Moore and Christin (2013) studied the risks of Bitcoin exchanges and according to their Proportional hazards model, it is easy to see that the larger the trading volume

the less risky the exchange itself is to operate, but the external risks increase. For example, they are more vulnerable to hackers. They also found that users often do not focus on the risk of the exchange itself when choosing an exchange, but are too concerned about their own earnings.

Davey and Felten (2013) develop a miner decision model for mining systems, where investors with strong computing power tend not to launch attacks, but they still face attacks from hackers. The Bitcoin network will only work well if all investors agree to abide by the relevant trading rules, which may vary from country to country depending on the level of regulation and the scope of regulation. Therefore, the author calls on all countries to agree on the regulation of bitcoin and to adopt a common strategy.

(3) About Bitcoin's transaction fees

Houy (2014) modeled and calculated some transaction fees in the post-mint era and found that they mining benefits tend to outweigh mining costs, and one of the premises of the existence of this deficit is that they tend to act in obedience to the government and do not themselves initiate such unprofitable actions. In blockchain technology, transaction fees tend to be low, but too low a transaction fee may or may not lead to disinvestment in mining and lower defenses.

3 Analysis of the derivation and operation principle of Bitcoin

3.1Derivation of Bitcoin

First proposed by Satoshi Nakamoto(2008), Bitcoin is a product of a P2P network built on open source software, which means that this peer-to-peer approach is decentralized. Unlike traditional currencies that are issued by central banks, Bitcoins are generated through a large number of calculations based on a certain algorithm. A bitcoin can therefore be seen as a special solution to an algorithm, which is unique and therefore produces only one bitcoin. The decentralized nature of P2P and the algorithm itself ensure that the value of the currency cannot be artificially manipulated through mass production of bitcoins. The cryptography-based design allows bitcoins to be transferred or paid only by the real owner. This also ensures the anonymity of the currency's ownership and circulation transactions. The biggest

difference between Bitcoin and other virtual currencies is that the total number of Bitcoins is very limited and extremely scarce. The cryptocurrency system had no more than 10.5 million for four years, after which the total number will be permanently limited to 21 million. In general Bitcoin has the following concepts：

(1) Decentralized peer-to-peer network (Bitcoin protocol)

(2) A public ledger of transactions (blockchain)

(3) Decentralized mathematical and deterministic currency issuance (distributed mining)

(4) Decentralized transaction validation system (transaction scripts)

In 2009 the Bitcoin system completed the first transaction in its history, priced at $1 = 1309.03 bitcoin, and its value was calculated by：

$$1\text{bitcoin}=\frac{\text{CPU high load operation one year electricity 1331.5kW*h x previous year average cost of electricity 0.1136\$}}{\text{12 x}\Delta\text{Number of new bitcoins added in the last 30 days}}$$

In order to maintain a constant rate of bitcoin mining, the algorithm has become progressively more difficult to solve. Over the course of nearly a decade, bitcoin price fluctuations have been impossible to accurately predict or control, which further increases the investment nature of bitcoin. Bitcoin network security remains a concern as network services continue to be upgraded. But the digital currency represented by Bitcoin is growing wildly, and the different policies of various countries also make the future of Bitcoin's development with great uncertainty.

3.2 Analysis of Bitcoin Technical Principles

3.2.1 Asymmetric cryptography

In today's world where information is transmitted so frequently, how to achieve absolute security of information transactions is the first thing to consider. From ancient times to the present, any information leakage may bring devastating disasters. In order to prevent information from being intercepted by them, we have created many encryption algorithms, such as Caesar's cipher, Morse code, Enigma encryption machine used by the German army during World War II, DES (Data Encryption Standard) in the last century 70, AES (Advanced Encryption Standard) in the 21st century in line with the new generation of security, etc. All these traditional cryptographic encryption methods have a common feature, when decryption is

actually the inverse of encryption, after the information publisher encrypts the file, the receiver only needs to decrypt it according to the way agreed with the publisher. Then it can be seen from this that once this private agreement is accessed by others, both sides of the transaction may still be unaware of it and a large number of transaction records will be tampered with. One of the characteristics of traditional symmetric encryption is that the same key is used by both encrypting and decrypting parties.

In order to solve the insecurity of key passing in symmetric encryption algorithms, cryptographers Whitfield Diffie and Martin Hellman(1976) proposed the concept of two sets of ciphers in their paper, which means that the public key encryption can only be decrypted by the private key, and the private key encryption can only be decrypted by the public key . There is no connection between the public key and the private key, and one cannot infer the other cipher by one cipher. In simple terms, the process of asymmetric encryption is as follows, A gets two keys through certain algorithm before the transaction, called public key and private key, the public key is open to the public, all users on the bitcoin network can get it, when a user gets the public key, the information that needs to be transmitted with its encryption and send it to A, A can decrypt it through his own private key after getting the encrypted information, symmetric encryption algorithm and The comparison of symmetric and asymmetric encryption algorithms is shown in Figure 3-1.

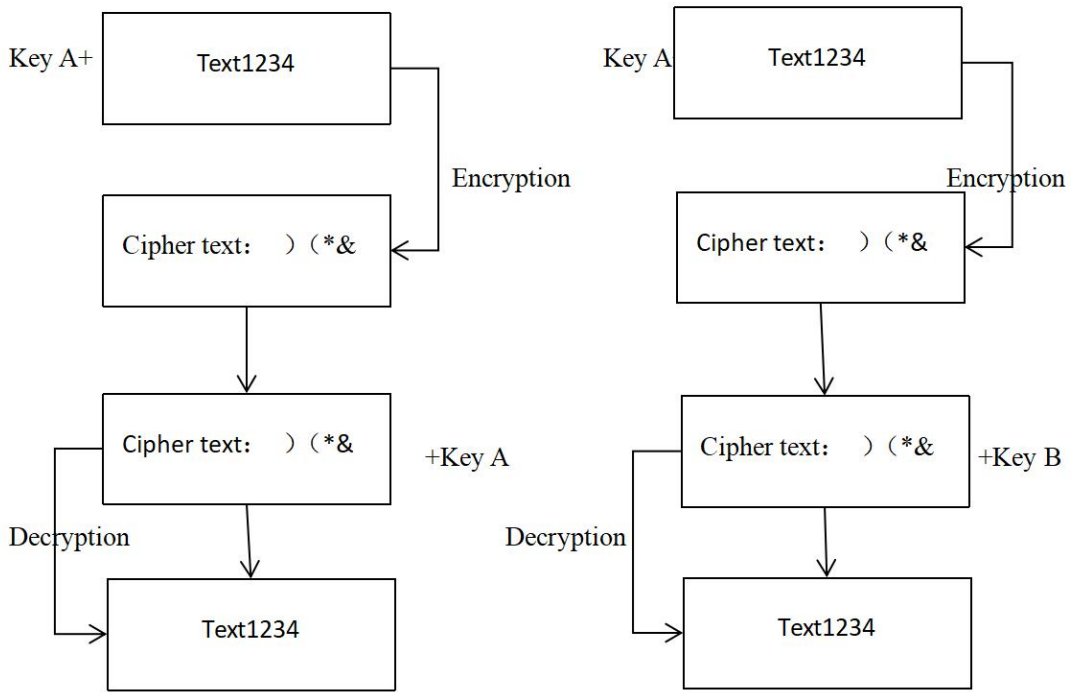

Figure 3-1 Comparison of symmetric and asymmetric encryption

In 1977, three mathematicians, Rivest, Shamir, and Adleman, devised an algorithm that would enable asymmetric encryption. This algorithm, named after the three of them, is called the RSA algorithm. Since then, RSA has been the most widely used "asymmetric encryption algorithm" until now. It is no exaggeration to say that wherever there is a computer network, there is an RSA algorithm. This algorithm is so reliable that the longer the key, the more difficult it is to crack. According to the disclosed literature, the longest RSA key that has been cracked is 768 binary bits. In other words, keys longer than 768 bits are unbreakable (at least no one has publicly announced it). Therefore, it is safe to assume that 1024-bit RSA keys are fundamentally secure and 2048-bit keys are extremely secure. Bitcoin, on the other hand, uses the elliptic curve algorithm (ECC), which is more secure than the RSA algorithm, such as 160-bit ECC can reach the strength level of 1024-bit RSA, DSA, and secondly, due to the small amount of computation, it is faster in decryption and signature, and has advantages such as small storage space and low bandwidth.

3.2.2 Hash (hash) algorithm application

The algorithm that maps a binary of arbitrary length to a fixed length binary becomes a hash algorithm, and the resulting binary becomes a hash value (256 bits). A hash is a unique and extremely compact numerical representation of a piece of data. If you hash a piece of plaintext and change even just one letter of the paragraph, subsequent hashes will produce a different value. It is computationally impossible to find two different inputs with the same hash value, so the hash of the data can be used to check the integrity of the data. It is generally used in fast lookup and encryption algorithms. It is important to note that the bitcoin hash algorithm uses a double sha256 algorithm, which increases the security of the generated key. Each bit is a 0 or 1, and 256 bits is a string of 256 0 or 1 binary digits, expressed as 64 bits in hexadecimal numbers. This length of key is very difficult to crack in today's advanced information technology. It can be said that the current hash algorithm used by Bitcoin, SHA-256, is an extremely secure algorithm, and any attempt to crack the computer wastes computing power that is absolutely worth the revenue from mining.

Due to the characteristics of the hash algorithm itself, some of the original data will be lost and it is difficult to achieve lossless transmission, but it still has important use value in the following three aspects (1) file checksum, the commonly used checksum algorithms are parity and CRC checksum, but these two checksums cannot

prevent the data from being tampered with and cannot avoid malicious damage to the data. The Hash algorithm outputs a different hash value for any modification of the original input, thus avoiding malicious tampering, which is important for file transfer overP2P networks.(2)Authentication protocol, also known as challenge-authentication mode, where the authenticated party sends a message to the challenger, and the challenger uploads the random message he received and the previously agreed password to the P2P network for hashing, and the resulting hash value is passed to the authenticated party, and then compared with his own authentication password for consistency, which is one of the simple ways that others can access but cannot be modified (3) Digital signatures, which can only be generated by the transferring party in a Bitcoin transaction, are simply forgery-proof strings. By verifying this digital string, it proves on the one hand that the transaction was initiated by the transferring party himself, and on the other hand that the transaction information was not altered during transmission. The digital signature consists of a digital digest and an asymmetric encryption technique. The transaction information is first shortened into a fixed-length string by the digital digest technique, and then the digest is encrypted with one's private key to form a digital signature. After completion, the complete transaction information together with the digital signature needs to be broadcast to the miner, who verifies it with A's public key. If the verification is successful, it means that the transaction was indeed sent by A and the information has not been altered..

3.2.3 Analysis of the logic of solving the secondary purchase and 51% attack

Consumers have a "secondary purchase" problem, meaning that when transaction A occurs, the consumer can generate another transaction that redirects BTC to a new address owned by the consumer, or pay for another transaction again with the same address, while the buyer has not yet received the BTC. Adding a block is required to generate more than 5 subsequent blocks before it can exist, so it takes a while for the Bitcoin network to acknowledge the transaction. In other words, a transaction is not immediately recognized by the entire network; at intervals of about one block every 10 minutes, a transaction takes about one hour to be recognized.

So how does the Bitcoin network solve this problem? First, bitcoin addresses generated based on asymmetric encryption and hash functions are basically impossible to forge, and hackers who want to attack the bitcoin network to obtain a

user's private key must have more computing power than the entire network. Second, according to the Bitcoin payment principle, it is impossible to pay more than the balance in one address, i.e., overdraft transactions, because of the Bitcoin network's unique "change" mechanism. However, it is possible to pay for two transactions at the same address, for example, if there is 40 BTC at address 1 and the user pays both A and B at the same time. This situation exists in a network of central nodes, where banks, for example, determine that the first transaction is valid by the order in which it occurs, and the second transaction is invalid if the account balance is low. But the Bitcoin network is peer-to-peer, and there is no central node. Obviously when a super user has more computing power than the entire network, they can create a block first and then add their transactions to that block. Of course, this is only theoretically possible, because most of the computing power of the entire Bitcoin network is concentrated in the hands of miners, and it is impossible for a single computer to exceed the computing power of the entire network.

The Bitcoin network is actually about block generation, which is a vote of arithmetic power. After each block is generated, all miners mine behind the block, forming a short chain of blocks called a "subchain", and multiple "subchains" have to be successfully added to the "main chain "The Bitcoin network is based on the principle of "length first, time first". Blocks that are eliminated from the competition do not contain transaction list information, but are re-traversed by the Bitcoin network to store the valid transaction records in the mining pool, which will be included in the legitimate blocks when new blocks are created.

In his paper, Satoshi Nakamoto(2008) devised a Poisson race model in which when an attacker with 51% of the network's computing power tries to create a node faster (note that the 51% attack can modify its own transaction records but not others, and can prevent valid blocks from being generated and confirmed, but cannot generate bitcoins out of thin air), the contest between the attack chain and the honest chain can be described by a binomial tree random walk, because the number of nodes is increased by the real transaction record, and the actual number of nodes is decreased by the fraudulent transaction by modifying the record itself to achieve the secondary payment, then the attacker needs to catch up with the real number of nodes in order to launch the 51% attack, based on the Gambler's Ruin problem. In his paper, Satoshi Nakamoto found by comparing the success rate of 51% attack with different probabilities that by using the workload mechanism to record the public information of transactions, it is difficult for a single attacker to tamper with the transaction records because the majority of CPUs are occupied by honest nodes. The probability

of success of such an attack is extremely low or even negligible.④

(④The appendix section shows the Poisson distribution of Bitcoin)

3.3 Bitcoin Network Construction and Messaging

It is on the basis of information technology that the Bitcoin network operates. Unlike the traditional server-client architecture, the P2P network uses distributed nodes to exchange information without uploading all information to a central server, which avoids the huge risk of being hacked and also makes the whole network run more smoothly. A node can both provide resources to the outside and allow other starting points to read the data. All bitcoin transactions have a corresponding bitcoin address. The blockchain of the bitcoin protocol is actually the maintenance of transactions rather than accounts, and the transaction data itself does not require a private key, so the encapsulation of the public key, also known as the address, is extraordinarily important, requiring a balance of security, efficiency, and scalability.From the public key to the bitcoin address is shown in Figure 3-2.

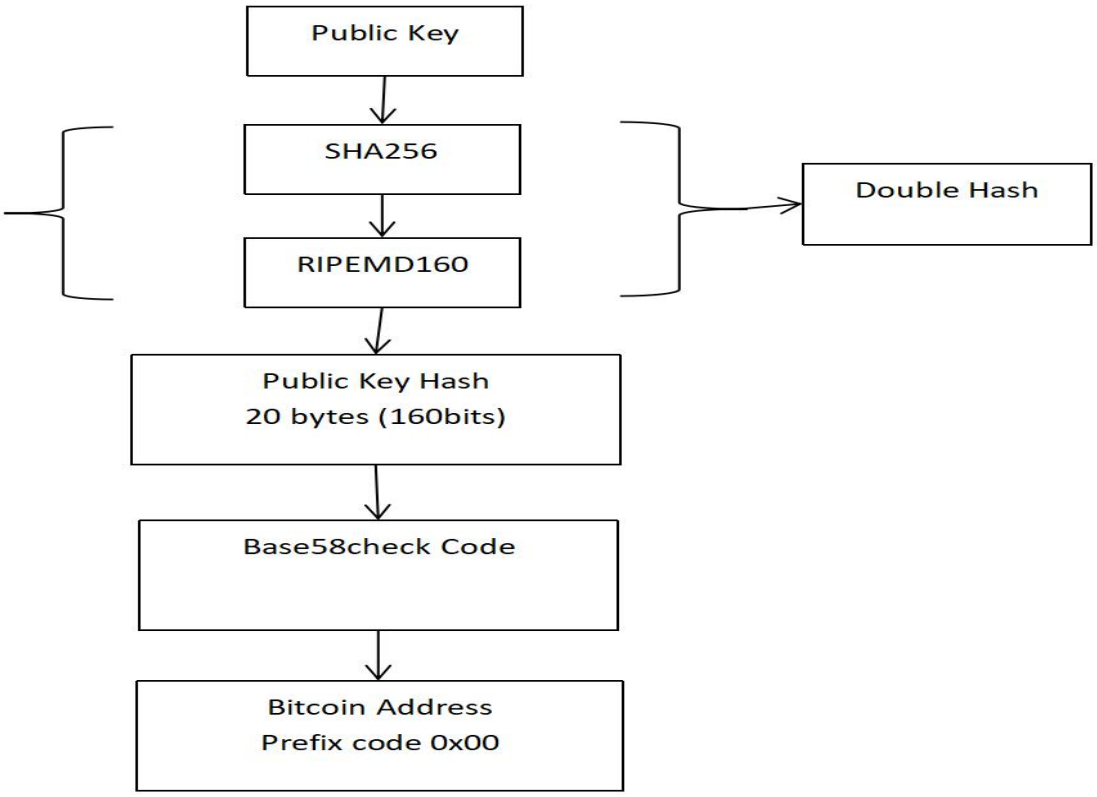

Figure 3-2 Public Key to Bitcoin Address

3.3.1 Analysis of Bitcoin's transaction process

The Bitcoin network is a peer-to-peer distributed network, which means that there is no need for intermediary financial institutions to be involved, and one party to a transaction can pay the other party directly. The bitcoin transaction process is essentially a peer-to-peer communication process. A centralized system of transaction nodes is characterized by the fact that all transactions need to be completed through a central node and uses its own credit to complete transactions between two strangers, solving the problem of large traffic volumes. Bitcoin, on the other hand, is implemented between nodes through a correlation script that contains a locking script and an unlocking script, where the former is the output condition for future transactions and contains a public key, while the latter sets the conditions that need to be met to satisfy that transaction. The process of solving the "change" problem in the Bitcoin payment network is analyzed as follows - the basic requirement of the transaction is that the payer sends money to the payee. The technical challenge is cryptography, which aims to prevent third parties from intercepting or even tampering with the remittance amount. The mechanism of the transaction from OwnerO to Ownerl and the subsequent remittance is shown in Figure 3-3.

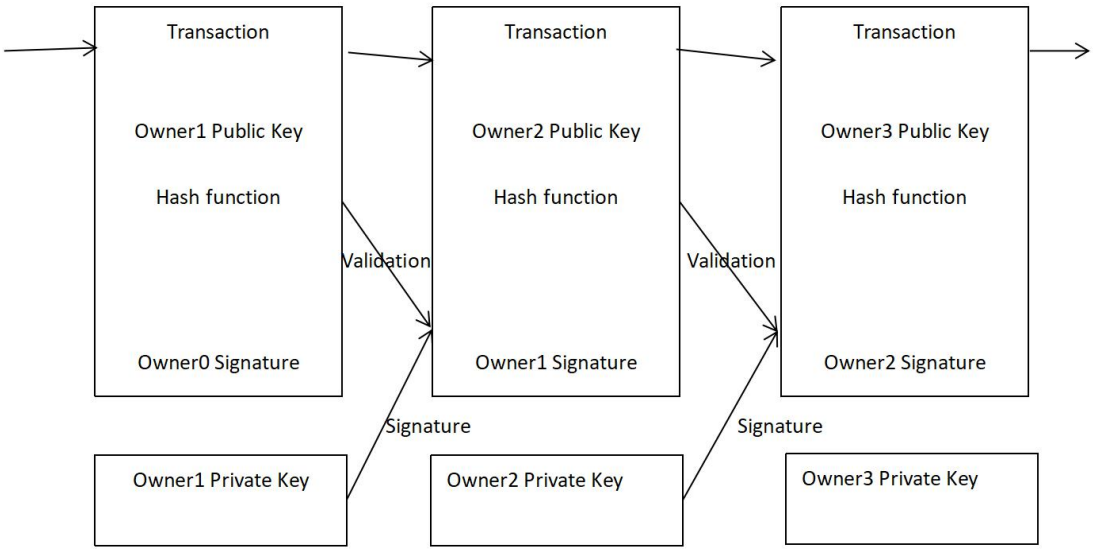

Figure 3-3 Bitcoin Trading Chart⑤

⑤Satoshi Nakamoto (2008)Bitcoin: A Peer-to-Peer Electronic Cash System

(1) OwnerO first checks the public key of Ownerl. The remittance details are encrypted with Ownerl's public key. In this way, only Ownerl himself can open the encrypted remittance details with his own private key.

(2) In order to facilitate Owner1 to verify that the remittance comes from Owner0 and not from someone else, Owner0 sends a remittance slip with the encrypted remittance details and Owner0's digital signature (Signature). Owner0's public key can be used to verify the digital signature of Owner0 in the remittance slip.

(3) When Owner0 sends the money order, the money order is not only delivered to Owner1, but is also widely distributed so that anyone who wants to participate in the BitCoin audit can receive all money orders sent by everyone in the world.

(4) Following the principles of (1), (2), and (3), Owner1 sends remittances to Owner2, and then Owner2 sends remittances to Owner3. BitCoin connects all remittance transactions involving the same BitCoin in a chain through the Hash mechanism, with the purpose of tracking down fraudulent.

However, one of the problems with actual bitcoin transactions is that for the same transaction, there can be multiple payment addresses, and the change for a transaction can be assigned to multiple addresses. This change mechanism can also be implemented in the network. If A and B have addresses a and b, and if A pays 40 BTC for a product, then there are several scenarios for this transaction:

(1) A has 40 BTC in his Bitcoin account, so A transfers them directly, encrypting A's Bitcoin address, which is the ID value and payment amount generated by the previous transaction, and the payee address b after recording it in the transaction slip, which B decrypts according to his public key. After a successful transaction, A's account balance is zero.

(2) A's bitcoin account balance is greater than 40 BTC, then the bitcoin network will generate a new address c, record the receiving address b, c in the transaction sheet, the source of funds for the last transaction ID value, after the transaction, address b gets 40 BTC, while address c gets the remaining bitcoins, the original address is cleared.

(3) A's bitcoin account balance is greater than 40BTC, such as 60BTC, respectively, for transaction 1 to get 30BTC, transaction 2 to get 20BTC, transaction 3 to get 10BTC, transaction when the recorded source of funds for the transaction if the transaction for transaction 1 and transaction 3, then this case transaction 1 and transaction 3 address clear, save transaction 2 to store bitcoin address can be used for the next transaction. If the recorded source of funds for the transaction is transaction 1 and transaction 2, then again a new address will be generated to store the remaining 10BTC from transaction 2, and the original transaction 1 and transaction 2 addresses

will be zeroed out.

As you can see from the above, the Bitcoin network addresses the change problem by generating a new address to store the balance, rather than directly modifying the amount of the user's account in the Bitcoin address. The newly generated address still belongs to the original counterparty, and if there are too many addresses to manage the transaction, the user can still transfer the account balance from the new address to the original account through another transfer operation, or generate a new account address by re-hashing the two account balances. Therefore one of the best features of the Bitcoin network is that it does not record every user's account, but only all transactions. All transactions are stored in a block, and when the block reaches its maximum value, another block is generated, and the blocks are still mapped to each other via hash addresses to form a blockchain.

3.3.2 Blocks and Blockchains

A block is a distributed cryptographic ledger. There is no central server in the Bitcoin network, so there is no uniform bookkeeping period, but UTC is used to coordinate the consistency of the Bitcoin network, but the problem remains that peer-to-peer communication can be inconsistent depending on the number of nodes. This means that each transaction does not take effect immediately after it is created, but is temporarily set aside in a discrete manner, and then stored in a block after a certain interval. As a result, each block records inconsistent transactions, and in the early days of inactive transactions, a block may store one to a few records, while up to the current maximum of January 2018, a block reaches 485 MB. the current time interval is about 10 minutes to generate a block, which basically covers the time inconsistency problem.

The Bitcoin network uses a TimeStamp to concatenate the ID values of this block and the previous block. The resulting sequence is difficult to tamper with and easy to verify. Each transaction record and each block is formed into a chain by hash values, so that the records between each node can be independent of the system time, and a block is broadcasted across the network after it is successfully created, and can be linked to the whole chain only after it is recognized by the network. Obviously, the attempt to modify such a transaction record is achieved based on exceeding the network-wide arithmetic power, which is obviously unrealistic, and the blockchain is schematically shown in Figure 3-4.

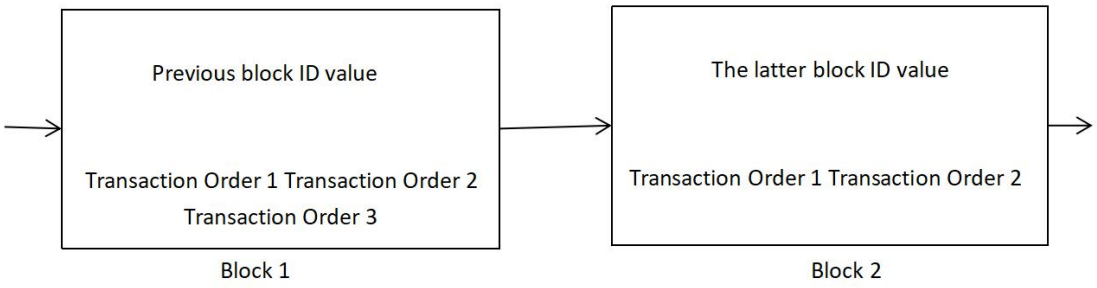

Figure 3-4 Blockchain diagram⑥

⑥Satoshi Nakamoto (2008)Bitcoin: A Peer-to-Peer Electronic Cash System

3.3.3 Mining Competition

In the Bitcoin network, block creation is essentially achieved through a competitive mechanism, where a number is needed when a new block is created, which must be obtained by the SHA256 algorithm and it's length is under a set threshold. There is no fixed formula for this number, it can only be calculated continuously by the computer, i.e. a trial and error mechanism. As mentioned before, the generated hash is actually a 64-bit string, and by constantly adjusting the threshold (which is done about once after the 2016 blocks are created), the difficulty to get such a number is constantly rising, and from 2009 to 2016, the difficulty of mining Bitcoin rose 1600 times to 800PH/sec-2.5EH/sec. Such a mechanism ensures that only one block is created every ten minute interval. After several years of development, Bitcoin exchanges have launched a number of miners, which users can access for a fee to mine bitcoins with these arithmetic miners.

The process of finding this number can be called mining, and the specific steps are as follows (1) The last transaction record of the previous block is used as the input value, and a hash is obtained by a hash function. (2) Perform a screening and query on all transaction records of the whole network, and exclude some transaction orders with zero balance and those that have been used. (3) Set a number and calculate this number as a new input along with the original hash value previously obtained and all valid transaction records to get a hash value. (4) Test whether this new hash value already exists, if it does, repeat step 3, if not, it indicates that the mining is successful and needs to be broadcasted across the network with some reward. If during the mining process, a new block number is obtained by a user first, then repeat step 1,

adding the new block number to the end of the previous block, and so on from step (1) to (4). According to the Bitcoin system, anyone who participates in the bill-keeping contest can add a special transaction to their bill-keeping, with the payer being the Bitcoin system and the payee being themselves, in an amount limited by the system, e.g. 12.5 BTC in 2018, halved every four years.

3.4 A brief summary based on technical principles

As mentioned above, Bitcoin, which is encrypted through asymmetric encryption as well as layers of hashing algorithm technology, has a fairly high level of security, making it acceptable to investors. At the same time, its peer-to-peer network distribution and the fact that the transaction process does not require the participation of financial institutions makes it not only faster and more liquid than traditional currencies, but also reduces transaction costs. And its unique blockchain bookkeeping means that it has the privacy that other traditional currencies can hardly offer, which is favored by many investors in today's highly developed information era. All in all, Bitcoin is a wonderful combination of computer technology, cryptography, and liberal economics, and has a place in the world's monetary system with its unique technical features that are different from traditional currencies.

4 General Economic Analysis of Bitcoin

4.1 Bitcoin supply and demand analysis

The price of money is the result of a game between money supply and demand. The central bank issues a certain amount of money according to the macroeconomic performance, while the demand for money mainly includes transactional demand, speculative demand and precautionary demand. For a more market-oriented economy, the price of the currency is influenced by the international economic fluctuations and its relevant changes are mainly expressed through the exchange rate and, conversely, through the interest rate. The basis for defining a new type of digital currency such as Bitcoin as a currency has already been discussed in the previous section, so this chapter will provide a general analysis of its price in terms of economics based on its status as a currency. Bitcoin, as a digital currency in a computer network, not only has its own value but also can be used as a medium of exchange. Bitcoin is created by

mining the computing power of computer networks, which consumes a large amount of resources (mainly electricity costs), and has a certain value especially in the context of a certain total amount and gradually increasing costs. Its value in use is mainly in the medium of exchange, and from the establishment of Bitcoin exchanges to the creation of Bitcoin futures, more and more entities are beginning to use it as an important financial asset. With fewer and fewer additional incremental quantities, the price of bitcoin has risen thousands of times from when it was created, and the creation of speculation has led more and more users to value its storage value, even as a means to combat inflation. In addition, the distributed ledger nature of Bitcoin shows how transparent transactions can be.

The premise of product pricing in financial markets is to satisfy the utility maximization, and when the market reaches equilibrium there is no arbitrage and the supply curve is characterized by exhibiting a relatively flat form. In contrast, the virtual bitcoin supply curve is close to vertical in the long run, and price and demand are negatively correlated, Q_d=f（P）(which P is the price of bitcoin in terms of USD). At the time of Bitcoin's creation, there was little public recognition of it, especially for the security of Bitcoin savings, and users involved in Bitcoin transactions were not yet active, and the price of Bitcoin was low at this time, with Bitcoin's price being only a few dollars in 2010. As the mechanism for bitcoin continues to improve, exchanges and the issuance of financial derivative futures such as bitcoin futures are driving demand growth, so in the short term demand for bitcoin will feed back positively on the price. However, in the long term the growth in bitcoin prices will allow substitution to emerge and investors may seek out gold, futures and other transactions, exhibiting a downward sloping demand curve. On the other hand, with bitcoin exchanges being attacked by cyber hackers and more and more countries taking a stance against it, especially after China, the largest trading platform, was banned, the price of bitcoin suffered a precipitous decline, and the sluggish demand led to a rapid price decline can be concluded that the price of bitcoin is more elastic in the short term. But similarly, when the value scale of bitcoin gradually stabilizes, the demand is no longer sensitive to price changes and gradually shows inelasticity. The short- and long-term characteristics of the supply and demand curves for bitcoin are shown in Figure 4-1.

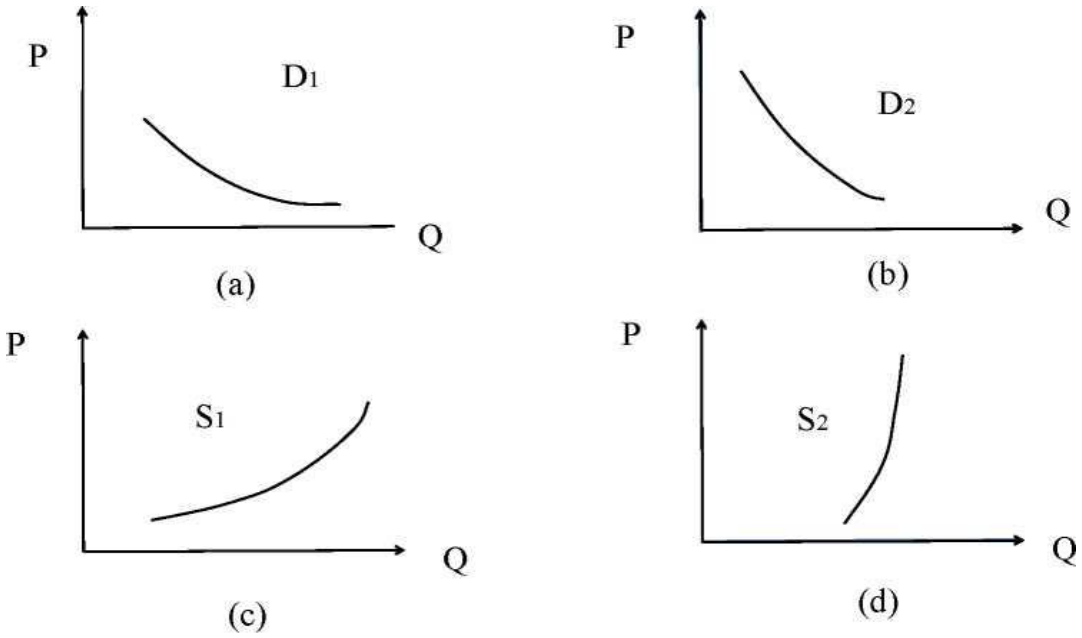

Figure 4-1 Bitcoin Short-Term and Long-Term Supply and Demand Curve Characteristics⑦

⑦The formal origin of the figure:Joan Violet Robinson(1982)

Where D1 represents the short-term demand curve, D2 represents the long-term demand curve, S1 represents the short-term supply curve, and S2 represents the long-term supply curve. The main constraints on bitcoin supply include network-wide computing power, mining difficulty factor, and mining revenue. As bitcoin is a digital currency, the level of computer computing power determines how fast or slow it is in generating hashes, usually reflected in the computer graphics card and CPU. currently, the network-wide bitcoin computing power is far more difficult than that of a personal computer, and individual investors who want to generate bitcoin can only get it by renting a server on the official website, i.e. renting a "mining machine ". As the difficulty and cost of mining increases, the supply curve for bitcoin will shift to the left(which Q is the number of new bitcoins obtained by mining). Factors that limit the demand for bitcoin include the level of activity in trading, the integrity of the market system, expected returns, and government regulatory policies. At present, the future of bitcoin is unclear, the legal status of bitcoin varies widely among different countries, and the financial tools for defusing and preventing the corresponding risks are not yet sound. However, based on this paper's positive outlook on Bitcoin, the following reasonable assumptions are made.

(1) Bitcoin can get good growth and some rich people who hold bitcoin are willing to trade.

(2)The value of bitcoin currency returns to stability and can be exchanged to some extent with fiat currency, gold, etc.

(3) The price protection mechanism of bitcoin is formed, and the bitcoin futures market is sound.

(4) There are no countries that regard bitcoin trading as illegal

Based on the above assumptions, the demand curve for Bitcoin will shift to the right in the long run. The price fluctuations based on supply and demand are analyzed below through the reasonable expectations of Bitcoin's development stage.

(1) Startup Phase

In the initial stages of Bitcoin's creation, due to the low level of public awareness, Bitcoin was only circulated on a small scale, mainly by web development programmers. The demand was low but the supply was high, and the supply was much higher than the demand, resulting in a price that was essentially zero compared to today. So this is a good explanation for the fact that in the startup phase, although demand has a positive feedback on price, the demand curve is still downward sloping in the long run. At this point, bitcoin does not have value or use value, so the supply and demand for bitcoin reaches a short-term local equilibrium at this stage. This state is only an early equilibrium at this stage, and as the interest in bitcoin increases and more investors enter the market, the demand for bitcoin increases further. It is important to note that the demand at this point must be higher than the demand at the previous stage, and similarly, the supply increases significantly due to the lower difficulty of mining in the early stages. The total demand and supply for bitcoin is low during the startup phase, and the short-term equilibrium price is low, as shown in Figure 4-2.

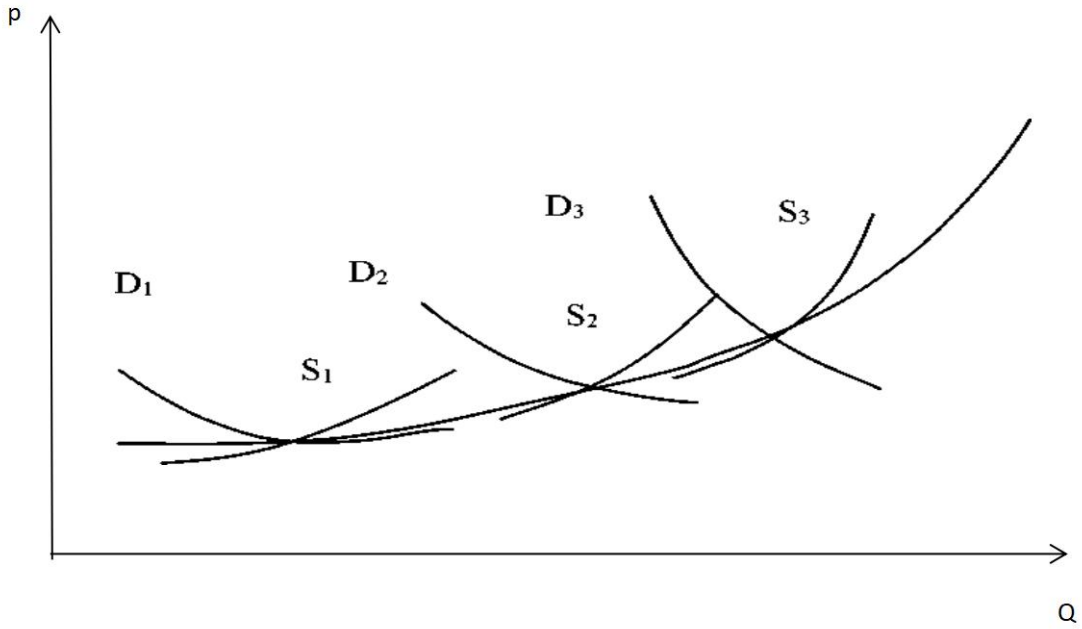

Figure 4-2 Short-term supply and demand equilibrium diagram for Bitcoin

(2) The speculative phase of bitcoin to fiat currency exchange

The main features of this phase include the peak of the number of people involved in bitcoin trading, the principles and mechanisms of bitcoin generation, risks and precautions, and the emergence of "mining" agents, compared to the initial period. Some speculators began to sell bitcoin while government regulation was not yet in place. At this point in time, demand has increased considerably as Bitcoin is still in its early stages, and the supply side is constrained by the cost of mining, so there is an oversupply. As shown in Figure 4-3, the supply and demand curves are represented by S1 and D1 respectively in the startup phase, and an equilibrium point is represented by E1. As bitcoin is gradually understood by the public and some potential investment value is magnified, the demand for bitcoin grows rapidly, and the demand dashed line moves from D1 to D2. Driven by demand, the supply of bitcoin grows further (manifested by the supply curve moving to the right), but at this time, due to the lack of mature agents, professional mining services are not yet available, the supply curve moves to the right to S2, but the magnitude is less than the magnitude of the demand curve movement, at this time S2 and D2 form a new equilibrium point price E2, E2>E1, appears in the upper part of the image. After a short period of equilibrium, some large platforms and wealthy individuals start to sell their bitcoin holdings due to the regulatory loopholes and the negative attitude of some countries, especially after the platforms are hacked and stolen. At this point the demand curve moves to the left to D3, the supply curve is also affected to the left to S3, the magnitude of the

movement is still less than the magnitude of the demand curve movement, the equilibrium price formed at this time is E3, E3 is less than E2 but large E1 (E1 < E3 < E2), that is, the price of bitcoin is more volatile, but did not fall below the price of the initial stage. Therefore, in the phase of bitcoin to fiat currency exchange, the price of bitcoin fluctuates significantly and the value gradually increases. Although the public is still unclear about the future of bitcoin, it is worth affirming that bitcoin as a new payment method can well prevent monetary inflation, and from the public and transparent transaction records, bitcoin still has a certain investment value.

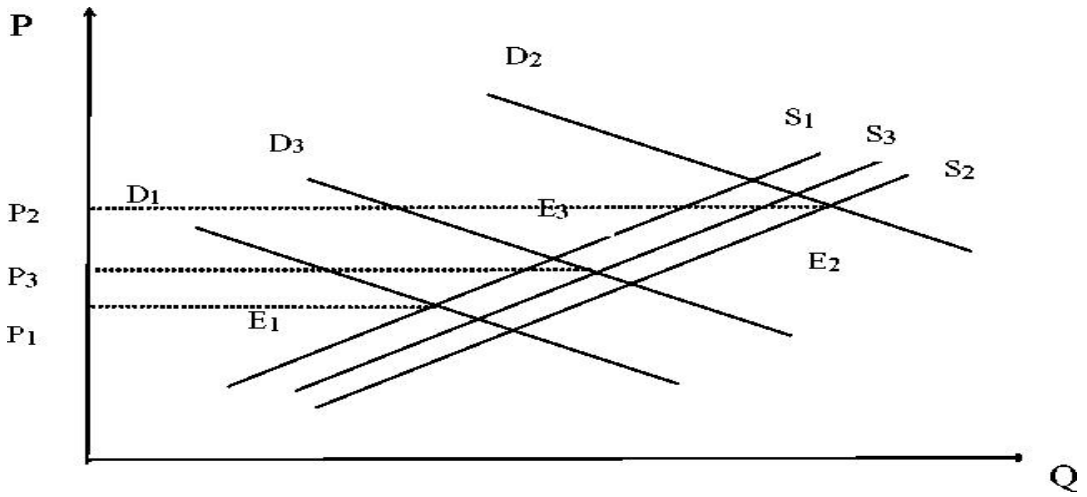

Figure 4-3 Bitcoin to Fiat Currency Phase Demand and Supply Changes

(3) Bitcoin investment trading stage

After experiencing a roller coaster of price fluctuations in 2017, bitcoin's market sentiment gradually stabilized in 2018, which is closely related to the gradual improvement of the bitcoin ecosystem and the gradual popularity of blockchain technology. However, compared to other financial products, its price increases and decreases still exceed public expectations. The root cause of this is that the relevant risk prevention mechanisms are not fully established, and the Bitcoin futures market is small and not able to provide good protection against price fluctuations. The bitcoin investment and trading phase is a period when risks are well controlled and public investors are able to use bitcoin for investment and finance. Worldwide, Bitcoin gains a degree of open regulation and gradually develops into a more mature financial product. The main characteristic of this phase is that the price fluctuates within a controlled range and the public demand for bitcoin is dominated by precautionary and transactional demand. The demand and supply curves are still represented by D1 and S1, and the equilibrium price is still E1. As Bitcoin enters the mass consumption phase, the change in transactional and investment demand shifts the demand curve to

the right to D2, and the supply curve is shifted to the right to S2 by the increasing number of miners. When bitcoin is affected by government macro policy or a series of hot events, the demand curve D2 and supply curve S2 move to the left to D3 and S3, and an equilibrium price of E3 is formed. Due to the existence of price protection mechanisms or the risk hedging of other financial derivatives, the demand and supply do not fluctuate much, and the vertical intercept between the equilibrium prices P1, P3, and P2 is significantly smaller than the speculative phase of bitcoin to fiat currency. Therefore, the volatility of bitcoin price will be significantly reduced after the public consumption phase of bitcoin, and a mature market is backed by a series of strict regulatory measures and a perfect market environment. Bitcoin is volatile at the moment, but due to the "deflation" caused by the limited amount of bitcoin and the transparency of transactions and decentralized nodes, bitcoin has some investment prospects in the long run.

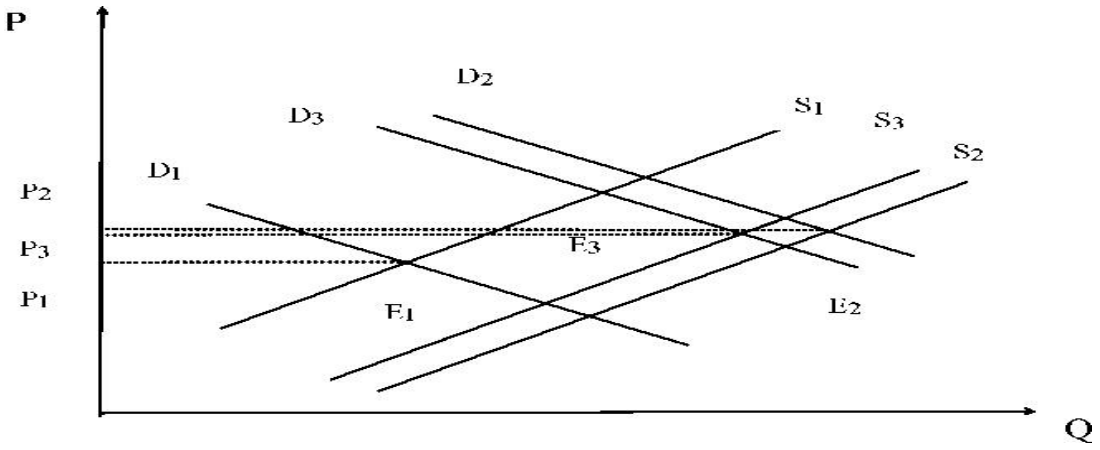

Figure 4-4 Changes in Bitcoin Demand and Supply during Mass Consumption Phase

4.2 Marginal Costs and Network Effects of Bitcoin

Anna Nagurney (2002) introduced the concept of network economics in her article and pointed out that with the development of Internet technology and information industry, network economics with network effects as the core is emerging. Traditional economic behavior should nowadays consider network effects, and this is especially true for Bitcoin. At a narrow level, network economics mainly refers to the information technology industry group with computer networks as the core, but in a broader sense, network economics also includes the industry group consisting of telecommunications, electricity, energy, transportation, and other net-running industries.

In traditional economics, it is believed that when the rest of the conditions remain the same, increasing the input of a factor of production does not lead to progressively higher returns, but rather there is a general law of diminishing marginal efficiency. The marginal cost of bitcoin, as a commodity developed by Internet technology, increases as the CPU power increases and the algorithm is optimized. The marginal cost of bitcoin, like the cost of traditional commodities, decreases within a certain range with the expansion of production, but beyond a certain range, the marginal cost will increase, showing a clear "U" shape characteristic.

The computational difficulty of Bitcoin is shown in Figure 4-5.

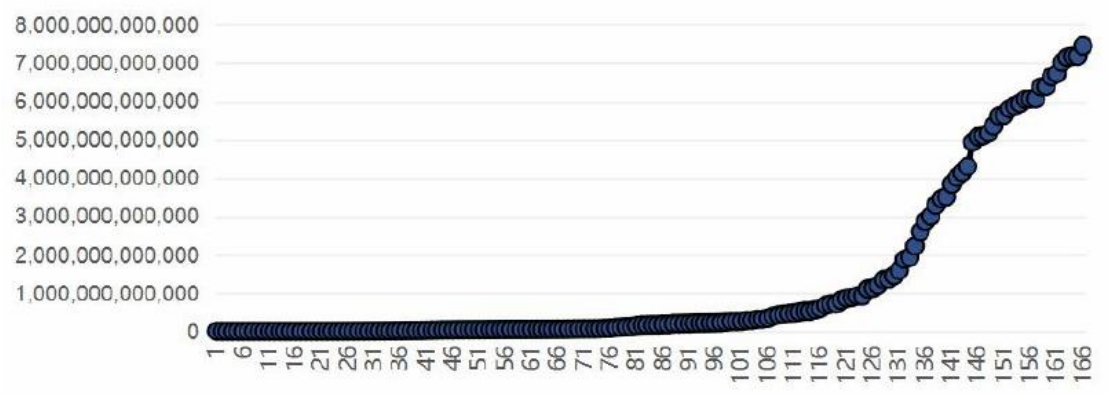

Figure 4-5 Computational Difficulty of Bitcoin®

⑧source:mining-cryptocurrency.ru

The graph above shows that the computational difficulty of Bitcoin has been increasing, especially in the last three years, and the difficulty level has been much higher than when it was first created. Other things being equal, such as electricity costs and asset investment, the CPU load will continue to increase and the cost will gradually increase. As the number of bitcoins approaches the theoretical value, the marginal cost goes up. On the other hand, there is a network effect on economic behavior under network conditions, and when the number of Bitcoin users increases, the value of the Bitcoin network increases further. Likewise when hackers invade exchanges, government regulation, or changes in the investment environment will have the opposite effect, in other words, the network economy has a positive feedback effect on the price of bitcoin. The law of diminishing marginal cost of bitcoin and the positive feedback effect of the network are shown in Figure 4-6.

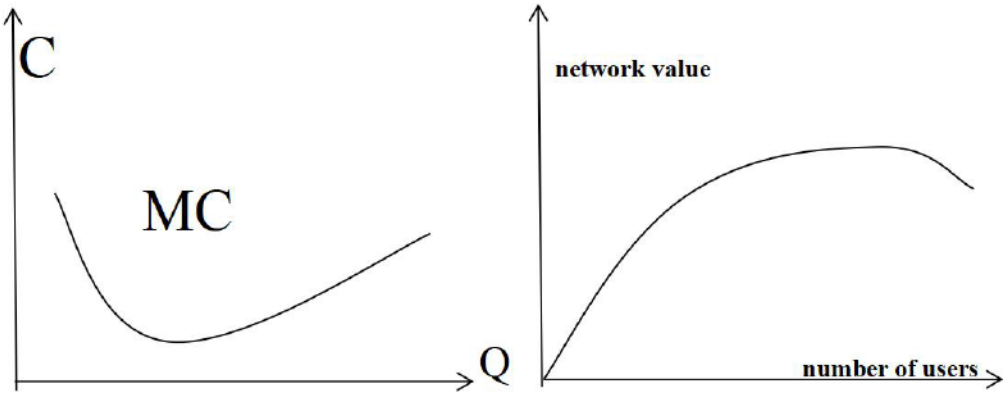

Figure 4-6 Decreasing marginal cost and network positive feedback curve

5 An empirical study of the correlation between bitcoin prices and macroeconomics

5.1 Bitcoin Price Volatility and Macroeconomic Linkages

5.1.1 Indicator selection and data sources

Among the currencies exchanged, the price of bitcoin against the U.S. dollar accounts for a large and dominant factor, so the U.S. dollar price index of bitcoin is selected as the explained variable (BPI), while in terms of macroeconomics, in order to analyze the correlation between bitcoin and macroeconomics, the top two economies in the world are taken as sample references in this paper, and the COMEX gold futures price of the New York Mercantile Exchange (GP), the Standard & Poor's 500 Index (SPX), the spot exchange rate of the U.S. dollar against the Chinese yuan (EX) and the Shanghai Stock Composite Index (EQ) are selected as explanatory variables,all of which are available for direct download at http://hk.investing.com. Due to the large historical price movements of Bitcoin, which may be a non-stationary time series, some treatment is applied to the variables. Using April 1, 2013 prices as the base period data, and adjusting the data by the formula (the Percentage change (%)$=\frac{\text{Variable}_{t+1}-\text{Variable}_{t}}{\text{Variable}_{t}}$).Due to the small size of bitcoin before 2013, the price is too low compared to the current, the time span of the data is the weekly data from April 1, 2013 to November 22, 2018 (5-day-week), except in the case of

missing sample data, the closing price of the previous trading day is taken as the price of the current trading day, the actual effective sample size of a single variable is 1473.

5.1.2 Descriptive statistics of variables

In order to facilitate comparison between bitcoin prices and other macroeconomic indicators, each variable was first indexed, and then their association was initially determined through descriptive statistical analysis of the variables. The statistical results are shown in Table 5-1(LN stands for natural logarithm).

	LNBPI	LNEQ	LNEX	LNGP	LNGP
Mean	6. 709659	7. 956195	1. 860933	7. 131563	7. 671178
Max	9. 850735	8. 549922	1. 942103	7. 377759	7. 983014
Min	4. 225373	7. 575590	1. 798603	6. 957307	7. 340583
Standard deviation	1. 384832	0. 210713	0. 043194	0. 063248	0. 158248
Skewness	0. 575386	−0. 112594	0. 355421	−0. 120050	0. 172421
Kurtosis	2. 205047	2. 465914	1. 726657	3. 820865	2. 238184
Coefficient of variation	20. 64%	2. 65%	2. 32%	0. 89%	2. 06%

Due to the lack of a unified official data interface for Bitcoin, one of the larger exchanges Investing data was selected. From each statistical indicator, the price of Bitcoin as an explained variable is more volatile than other macroeconomic indicators, indicating that the price protection mechanism has not yet been formed. The coefficient of variation can eliminate the influence of measurement scale and scale while reflecting the degree of dispersion between data. The coefficient of variation for bitcoin is 20.64%, which is 7.78 times higher than the SSE Composite Index, 8.9 times higher than the USD/CNH exchange rate, and 10 times higher than the S&P 500, which is much higher than the price volatility of gold futures. Figure 5-1 provides a more intuitive view of how bitcoin price volatility is linked to other macroeconomic indicators.

Data source:http://hk.investing.com.

The above empirical data shows that the price volatility of bitcoin is much higher than the already existing financial assets trading, and we can initially determine that the development of bitcoin is still in the second stage, which is the speculative stage of bitcoin exchange for fiat currency. It is easy to see that in the stock market and foreign exchange market, earnings consist of two main parts, one is the capital gains from changes in the prices, and the other is the interest or dividends earned during the holding period. Bitcoin does not have an interest rate, and the only way to earn a return on bitcoin is to buy and sell it for the difference in price. Therefore, all else being equal, the price fluctuation of bitcoin includes a time premium for holding the asset.

5.2 Construction of VAR model and correlation test

Vector autoregression (VAR) is a model based on the statistical nature of the data. The VAR model constructs a model for each endogenous variable in the system as a function of the lagged values of all endogenous variables in the system. Its core theory lies in leaving aside economic theory to consider directly the relationship between the time series of economic variables. Thus a VAR model can be constructed

between the variable BPI and other macroeconomic indicators as follows:

$$Y_t = \alpha_0 + \alpha_1 Y_{t-1} + \alpha_2 Y_{t-2} + \cdots + \alpha_k Y_{t-k} + \beta_1 X_{t-1} + \beta_2 X_{t-2} + \cdots + \beta_k X_{t-k} + \varepsilon_t \quad (5.1)$$

where $\alpha_0,\ldots,\alpha_k$, $\beta_1,\ldots\beta_k$ are the parameters to be estimated, ε_t is the random perturbation term, Y is the explanatory variable BPI,X is the explanatory variables GP,SPX,EX,EQ.

Since most of the economic variables are non-stationary time series, in the case of large samples and higher order single integer may lead to the conclusion of a correlation between two uncorrelated variables, the data are first processed in the form of "rate of return" as described in the previous section, and then a unit root test is performed on the processed variables to derive the time series in levels.

Table 5-2 ADF unit root test results

Variables	Differential times	(C,T,K)	DW value	ADF value	5% threshold	1% threshold	Conclusion
BPI	0	(C,n,1)	2.01	-25.39	-1.94	-1.62	***
GP	0	(C,n,1)	2.00	-27.85	-1.94	-2.57	***
SPX	0	(C,I,1)	2.00	-28.88	-2.86	-3.43	***
EX	0	(C,n,1)	1.99	-27.41	-1.94	-2.57	***
EQ	0	(C,n,1)	2.00	-27.25	-1.94	-2.57	***

Note: (C, T, K) indicates whether the ADF test equation contains a constant term, a time trend term, and the number of lags; *** indicates that the variable passes the ADF stationarity test at the 1% level of significance.

The unit root test of each variable after data processing shows that they are all smooth time series and are all integrated of order zero, satisfying the condition of cointegration test. In this paper, we propose to use the JJ test to explore the long-run equilibrium relationship between the variables, as shown in Figure 5-2, where there are five cointegrating equations at the 5% significance level.

Unrestricted Cointegration Rank Test (Trace)

Hypothesized No. of CE(s)	Eigenvalue	Trace Statistic	0.05 Critical Value	Prob.**
None *	0.396937	3039.313	60.06141	1.0000
At most 1 *	0.357517	2311.563	40.17493	0.0000
At most 2 *	0.342266	1674.929	24.27596	1.0000
At most 3 *	0.324756	1072.054	12.32090	1.0000
At most 4 *	0.296943	506.9847	4.129906	0.0001

Trace test indicates 5 cointegrating eqn(s) at the 0.05 level
* denotes rejection of the hypothesis at the 0.05 level
**MacKinnon-Haug-Michelis (1999) p-values

Figure 5-2 Cointegration test results

Whether the long-term equilibrium relationship between variables can constitute a causal relationship and how this causal relationship works need to be further tested. Granger causality test lies in testing the sequence between variables and whether the prior period information of one variable affects the current period information of another variable. The optimal lags are first determined, and according to the AIC and SC criteria given by the formula:

$$AIC = \log\frac{\sum_{t=1}^{T}\hat{u}_t^2}{T} + \frac{2k}{T}$$
$$SC = \log\frac{\sum_{t=1}^{T}\hat{u}_t^2}{T} + \frac{k\log T}{T} \qquad (5.2)$$

The following data results were calculated as shown in Table 5-3.

	One period lag	Two period lag	Three period lag	Four period lag
AIC	-30.45221	-30.45843	-30.47972	-30.47135
SC	-30.34286	-30.25694	-30.18515	-30.08297

Since the data trends of the two criteria are not consistent, the optimal lags need to be determined based on the likelihood ratio test. The optimal lags were determined to be of order 1 by constructing the LR statistic. The obtained VAR model results can be written in the following format:

$$BPI_t = -0.037953BPI_{t-1} + 0.343169SPX_{t-1} - 0.164049EQ_{t-1} + 4.450929EX_{t-1} + 0.485338GP_{t-1}$$
$$Adj.R^2 = 0.004222, F = 2.533688, AIC = -1.609370, SC = -1.591145$$

After obtaining the optimal lags between the variables, a Granger causality test

can be performed, the essence of which is to show whether the lag of the independent variable affects the present value of the dependent variable, and the results obtained using the relevant software are shown in Figure 5-3:

Null Hypothesis:	Obs	F-Statistic	Prob.	Result
GP does not Granger Cause BPI	1439	1.05371	0.3489	Accept original hypothesis
BPI does not Granger Cause GP		1.16332	0.3127	Accept original hypothesis
SPX does not Granger Cause BPI	1471	0.18732	0.8292	Accept original hypothesis
BPI does not Granger Cause SPX		1.68760	0.1853	Accept original hypothesis
EX does not Granger Cause BPI	1471	3.60993	0.0273	Reject original hypothesis
BPI does not Granger Cause EX		0.79280	0.4528	Accept original hypothesis
EQ does not Granger Cause BPI	1439	1.13397	0.3220	Accept original hypothesis
BPI does not Granger Cause EQ		0.07317	0.9294	Accept original hypothesis

Figure 5-3 Granger causality test results

The above statistical results show that only the exchange rate of USD to RMB (EX) is the Granger cause of bitcoin price, the rest of the macroeconomic indicators are accepted as not Granger cause hypothesis. Therefore, the foreign exchange market sentiment affects the bitcoin price to some extent. When the exchange rate rises, more investors are willing to put their money into it to buy foreign currency, and when the exchange rate falls, more investors may shift their money to bitcoin, but when the price of bitcoin falls, investors are not so willing to continue investing. The reason for this may be that holding bitcoin is riskier and does not provide a stable return during the holding period. As for other macroeconomic indicators, the legal status of bitcoin is ambiguous as it is not yet recognized by the majority of countries, and the scale of transactions has not yet reached the point where it is interrelated with other indicators.

6 Bitcoin's development status and future development direction

6.1 Government Policies and Attitudes Towards Bitcoin

Bitcoin has gained a lot of investors' favor at the beginning of its creation with its unique advantages, among which decentralization and de-regulation, anonymity and other features have made the price of Bitcoin soar in a short period of time. However, in the same way, bitcoin became a platform for illegal transactions and was subject to different regulatory attitudes of national (regional) governments. As of now, there are

several gambling sites that accept bitcoin as a means of payment, and there are even a large number of online games that revolve around bitcoin, such as SatoshiDice, bitZino, BitMoose, etc. We find that a variety of gambling methods are moving online, and because bitcoin is not regulated by governments, it is starting to grow wildly, making it difficult for the government to stop users from participating in gambling, and it is also impossible to track the identity of users, which has a serious impact on the government's regulatory function. The government's attitude toward Bitcoin can be illustrated in the following ways.

(1) Facilitating Illegal Trading. In 2011, Anonymous launched an online black market trading platform for Dread Pirate Roberts called "Silk Road". The platform allowed users to purchase many illegal commodities, such as opium and other drugs, as well as precious metals and firearms. Although the FBI soon shut down the trading site and arrested those responsible, and seized 15.1 million worth of BTC , or about 14,400 units. However this government action did not stop these illegal transactions, and in 2013, two years after the shutdown, Silk Road 2.0 came back online, followed by 3.0. it was evident that using Bitcoin as a payment tool could lead to unprecedented disaster and could even fund terrorists. Unlike traditional crime paths, cybercrime is inherently extremely difficult to investigate, and coupled with the unregulated nature of Bitcoin it is difficult to curb the crime.

(2) It may lead to a failure of monetary policy and a reduction in government minting taxes. A mint tax is an economic phenomenon in which countries and organizations that issue money depreciate it after issuing it and absorbing the equivalent of gold and other wealth, reducing the wealth of the currency holder and increasing the wealth of the issuer. For example, if a $100 bill costs $1 to print, the difference of $99 is the minting tax, which is an important financial source for governments. Since the supply of bitcoin is constant, as inflation occurs, the demand for fiat currency gradually increases, interest rates gradually fall, the demand for bitcoin increases, and the price rises. In a way individuals holding bitcoin can circumvent the situation that there is a crowding out effect of bitcoin on fiat currency, making the government's monetary policy dysfunctional and mint tax revenue decrease. Bitcoin breaks the government monopoly on money, although the current number of Bitcoin users is small enough that even if all assets were exchanged for Bitcoin it would not bring about a change in the overall monetary system. However, when demand increases further, the lower government minting tax revenue may well be a valid excuse for the government to ban bitcoin from circulation. Bitcoin could also lead to a failure of monetary policy. According to Friedman's money supply

theory, if bitcoin becomes a substitute for fiat money, when the government adopts an inflationary monetary policy, the increase in the number of bitcoin users and the increase in the number of bitcoin holdings leads to a smaller than expected actual increase in the amount of money in circulation, which makes in the government's monetary policy does not work well. On the other hand, the commodity properties of bitcoin may trigger speculative behavior by investors, and these behaviors will cause bitcoin to be purchased and held in large quantities, all of which will cause the central bank to misjudge the current economic situation, monetary policy will lose its effectiveness, and the country will experience volatility as a result.

(3) Raises tax issues. If Bitcoin is allowed as a means of payment, how it is taxed is also an issue worthy of deeper scrutiny. The German Ministry of Finance, which is supportive of bitcoin, believes that competition should be introduced in the currency, which can be viewed as an alternative financial instrument that is legal to mine, buy trade and sell in Germany, and the Germans have introduced VAT provisions that will not require capital gains tax for bitcoin assets obtained through remittances and mining that are held for more than 12 months. The U.S. Securities and Exchange Commission (SEC) has declared that there are no official laws and regulations for Bitcoin, while other authorities have promptly warned investors of the risks involved and will tax Bitcoin as property rather than currency. In China, according to the State Tax Letter 2008[818], the "Notice on Personal Income Taxation of Income Obtained by Individuals through Network Sales of Virtual Currencies" states that income obtained by individuals through network acquisition of players' virtual currencies and selling them to others at a markup is taxable income for personal income tax purposes and should be calculated in accordance with the "Income from Property Transfer The personal income tax shall be calculated and paid according to the item of "property transfer income". The original value of the property of an individual selling virtual currency is the price paid by him/her for acquiring the network virtual currency and the related taxes. For individuals who cannot provide proof of the original value of the relevant property, the competent tax authorities shall approve the original value of their property. It can be seen from this that the current laws and regulations can use virtual currency, but whether Bitcoin applies requires further clarification, for example, the original value of Bitcoin is difficult to determine, especially when all transactions occur in a network environment.

6.2 Bitcoin's Self-Improvement

Bitcoin has rapidly taken the world by storm due to its unique advantages in the course of its development, especially the transparent transactions and decentralized features that are not regulated by the government in the eyes of the public using technological means. In the eyes of its supporters, it represented a benign currency and a challenge to the state monopoly of issuing money. But after the hot spot, we find that Bitcoin itself has many shortcomings, although it seems that Bitcoin investment makes sense in the long run, supported by secure blockchain technology in addition to a constant supply of Bitcoin. But there is still a long way to go to make bitcoin investment transactions possible. Currently, bitcoin prices lack monitoring and rise and fall far beyond what public investors can afford, with huge price bubbles, and the empirical data in this paper shows a lack of significant correlation between them and macroeconomic indicators. Only the exchange rate of bitcoin to fiat currency affects the price unilaterally, while the rest of the indicators are clearly outside the factors of bitcoin's price fluctuation.

On a macro level, it is important to strengthen the regulatory regime of the Bitcoin market. The current trading hours for bitcoin are globally unrestricted, and there is no set amount of ups and downs, allowing the price to fluctuate freely with the market environment. Many of these features are the exact opposite of the stock market, and if the stock market is currently more mature, the bitcoin market undoubtedly still lacks good regulation. In addition, due to the general lack of unified regulations and risk warning mechanisms on bitcoin exchanges, investors trading bitcoins are prone to lose their money in the context of the general market environment, which can lead to a further decline in the trading scale of bitcoin, and more importantly, the smaller market size is not conducive to the circulation and development of bitcoin. In addition to the problems facing Bitcoin itself, the illegal behavior of investors should also be investigated and dealt with by the relevant authorities. The majority of countries around the world are opposed to bitcoin in large part because it is being used by unscrupulous individuals as a tool to transfer illegal assets, launder money, and evade taxes. Therefore it is not only an intrinsic but also an extrinsic need to achieve self-improvement of Bitcoin.

On a meso level, a unified industry association should be established globally to facilitate its unified management. Mature markets often have a professional association or guild, which not only provides a reliable way for investors to defend

their rights, but is also a powerful body for investigating and prosecuting illegal behavior in the bitcoin market. While different countries have different needs, the fundamental point is whether there is a consensus on regulation. Due to the nature of decentralized trading, it is difficult for countries to regulate uniformly from a macro level, which is both an advantage and a disadvantage. The establishment of an industry association is a sure way for Bitcoin to improve itself and develop itself. It is important to take all aspects of bitcoin transaction fees, mining revenue, and fiat currency exchange into account, so that every investor can participate in bitcoin transactions. For some investors who hold a large number of bitcoins with a wide range of addresses, their transaction records should be strictly monitored to ensure that every transaction is compliant. Currently, the scale of online transactions using Bitcoin as a payment medium is not at all on the same order of magnitude as e-commerce transactions on a global scale, or even negligible. This is completely unacceptable for Bitcoin, which is also a digital currency. Bitcoin trading should be promoted (by a possible future industry association) more like other online transaction payment mediums after the price stabilizes, so that more investors can participate and accelerate the circulation of Bitcoin.

On a micro level, Bitcoin lacks a reliable and specialized team, and there is a need to further upgrade the technical means. While Bitcoin is based on asymmetric encryption algorithms, as mentioned above, Bitcoin's own security can be guaranteed, but Bitcoin's trading platform is difficult to do so. The Bitcoin trading platform has a much larger number of Bitcoins, and hackers can often attack the exchange to achieve a "no-win situation". Therefore, it is important to upgrade the hardware and software of the whole industry chain and fix the related technical vulnerabilities. In addition, the distributed ledger of bitcoin transactions can be backed up by keeping the transaction records of each node on two or more servers at the same time, to improve the overall ability to combat external malicious attacks.

6.3 Bitcoin Derivatives Market Construction

Wang Hui, a professor at Central University of Finance and Economics, gave a short introduction to the current bitcoin derivatives market in her lecture on the introduction of global financial derivatives. The video course suggests that Bitcoin has launched futures contracts, but the current market size is still far below expectations.Compared to attitudes on an international scale, the launch of futures contracts on the larger mainland of Bitcoin has been difficult and investors have often

held back. But the futures market is a market that is more likely to burst with trading energy than the spot market. It not only trades on a larger scale, but also assumes the function of value discovery in the process of pricing futures contracts. The futures market tends to gather more information from both the supply and demand sides, and investors are better able to make effective judgments through this information. The bidding process is often close to the true value, and despite the external noise in the market, the public's future expectations for the price of bitcoin as a whole are often embedded in it as they go long and short, which makes up for the lack of revenue during the time investors hold bitcoin in another way. The futures market complements and complements the spot market, and is a "tracker" for spot value discovery. Therefore, at this point in time, Bitcoin should begin to strengthen the derivative market to gradually control the market price of Bitcoin and prevent significant price increases and decreases. We should also incorporate macroeconomic indicators into the price discovery of bitcoin to strengthen the linkage with economic entities and to avoid drastic shocks caused by inconsistent policies.

Conclusion

Bitcoin has been known to the public for nearly a decade, but since the first bitcoin was issued, investor sentiment has followed its price fluctuations, and most people do not understand its nature. In this paper, we analyze the technical principles behind bitcoin, the logic of network communication and combine it with traditional economic conclusions to a certain extent to explain the nature of bitcoin. At the current stage bitcoin is more investment-oriented, and some investors with large holdings are less active in trading, but in the long run bitcoin still has some investment value. This paper concludes with an analysis of the current situation and prospects of Bitcoin's development, and proposes specific development directions and recommendations for the development of a new monetary system structure in conjunction with the empirical data in the previous paper, and the specific conclusions of the analysis can be summarized as follows.

First, although Bitcoin is a digital currency in the Internet, it still has some of the monetary properties of traditional fiat money, mainly in terms of the unity of value and use value, and thus can still be analyzed for price fluctuations using traditional economic principles - from the perspective of supply and demand. In the long run, bitcoin may have deflationary characteristics due to the constant volume. In the short term the demand curve is similarly sensitive to quantity due to Bitcoin's own

decentralized and distributed bookkeeping characteristics, but given the difficulty of mining and transaction costs, Bitcoin's demand may be depressed in the long term. On the cost side, the marginal cost of bitcoin also exhibits a "U" shaped structure, and the positive feedback effect of the network environment makes it more curved.

Second, by combining macroeconomic indicators such as the New York Mercantile Exchange COMEX gold futures price (GP), the Standard & Poor's 500 Index (SPX), the U.S. dollar to RMB spot exchange rate (EX) and the Shanghai Stock Composite Index (EQ), we find that the price of bitcoin is weakly correlated with changes in macroeconomic indicators and that bitcoin has a high degree of investability. Some of the "large" holders of bitcoin have very low trading activity and even lower quantities in actual circulation. Granger's causality test suggests that prior information on the USD-RMB spot exchange rate (EX) affects the current price of bitcoin.

Third, the regulatory attitude of individual countries towards bitcoin can influence its price direction, especially in developed countries and economies. Currently, most countries around the world are neutral or have not taken a position, which makes the future of Bitcoin even more uncertain. To further stabilize price volatility, not only do we need more countries to recognize its legal status, but we also need to accelerate the construction of derivatives markets and improve the policies of each country.

Although the speculative demand for bitcoin is excessive at this stage compared to the transactional demand, the risk of investors taking on the high side is too high. But in the long term, it still holds some investment promise, especially in terms of increased cryptocurrency competition.

Reference

1. Baur, D.G. & Hong, K. & Lee, A. D. (2017), *Bitcoin: Medium of Exchange or Speculative Assets?*

2. Chen Hao. (2015), *Economic analysis of bitcoin [D]*. Zhejiang University.

3. Chowdhury, A. & Mendelson, B. K. (2014), *"Digital Currency and Financial System: The Case of Bitcoin"*. Economics Faculty Research and Publications, pp: 474.

4. Dong Zhonghao. (2018)，*Try to analyze the development prospect of bitcoin and its impact on the financial industry [J*]. National Circulation Economy,pp:101-102.

5. Gandal,N. & Halabruda,H.(2014), *Competition in the Cryptocurrency Market[J].*

6. Hayek, F. A. (1976/1990), *Denationalisation of Money - The Argument Refined. Institute of Economic Affairs* , Hobart Paper Special (3rd edn),pp:70.

7. Houy, N. (2014), *The economics of Bitcoin transaction fees. GATE WP 1407*, Groupe d’Analyse et de Théorie Economique, Lyon.

8. Kroll, J .A.& Davey, I. C.& Felten, E . (2013),*The Econimics of Bitcoin Mining, or Bitcoin i n the Presence of Adversaries[C].*Proceedings of WEIS.

9. Li Xuan.(2019),*Analysis of the current situation and future development of bitcoin [J].* National circulation economy, pp:119-120.

10. Ling Qing.(2014), *Technical Principles and Economic Analysis of Bitcoin [D].* Fudan University.

11. Liu Jingli.(2018), *Literature review of research on the monetary properties of bitcoin [J].* Modern Business,pp:175-176.

12. Marx, K. (1867), *Capital: A critique of political economy. Volume 1, Part 1.* The process of capitalist production. New York..

13. Menger,K.(1892), O*n the Origin of Money.*The Economic Journal, Vol. 2, No. 6 , pp.:239-255.

14. Nagurney,A.& Dong,J. (2002),*Supernetworks: Decision-Making for the Information Age (New Dimensions in Networks series) Hardcover* .

15. Ron,D. & Shamir,A.(2013),*Quantitative analysis of the full bitcoin transaction grap[M].*Finnancial Cryptography and Data Security. Springer Berlin Heidelberg,pp:6-24.

16. Satoshi Nakamoto.(2008), *"bitcoin a-peer-to-peer electronic cash system"* .

17. Sui Bin.(2018),*The birth, development and impact of bitcoin research [J].* Industrial Innovation Research, pp: 97-98.

18. Šurda, P. (2012), *Economics of Bitcoin: is Bitcoin an alternative to fiat currencies and gold?* Ph.D. thesis, Vienna University of Economics and Business.

19. Tang Xiao.(2014), *Teel. Bitcoin issuance and circulation mechanism and its price fluctuation[D].* Shanghai Jiaotong University.

20. Tyler,M. & Christin,N.(2013), *"Beware the middleman: Empirical analysis of Bitcoin—exchange risk."* Financial Cryptography and Data Security. Springe r Berlin Heidelberg, pp:25-33.

21. White, L. (1999), Hayek's *Monetary Theory and Policy: A Critical Reconstruction.* Journal of Money, Credit and Banking, 31(1), pp: 109-120.

22. Whitfield, D. & Hellman, M. (1976), *"Newdirections in cryptography."* IEEE transactions on InformationTheory, pp: 644-654.

23. Wu Jing. (2015), *Research on the price formation mechanism of virtual currency in the context of Internet economy[D].* Ocean University of China.

24. Wu Mengze. (2018), *Analysis of cryptocurrency influence factors and price trend based on supply and demand perspective a bitcoin as an example [J].* Heilongjiang.Finance, pp:55-57.

25. Yang Deng. (2014), *Research on the Generation and Development of Virtual Currency[J].* Talent, pp:277-278.

26. Yermack,D. (2014), *Is bitcoin a real currency? An economic appraisal.* NBER working paper no. 19747, National Bureau of Economic.

27. Yuan Qiumei. (2018), *Is bitcoin a currency or not? An analysis based on the relationship between money and wealth [J].* Southern Finance,pp: 28-32.

28. Zhang Chuanchao. (2018), *A study on the origin, advantages and limitations of bitcoin [J].* Modern Business,pp:67-68.

29. Zhang Zeyu. (2018), *Research on the operation principle and financial attributes of bitcoin [J].* National circulation economy, pp:69-71.

30. Zhao, Z. & Lan, Y. & Wu, X. (2016), *The Impact of Electronic Banking on the Credit Risk of Commercial Banks—An Empirical Study Based on KMV Model.* Journal of Mathematical Finance, 6,pp: 778-791.

Appendix A: Poisson Distribution of Bitcoin

An attacker tries to create alternative blockchains faster than honest nodes can generate chains. Even if it achieves this goal, the entire system is not then completely subject to the attacker's arbitrary will, such as creating value out of thin air or looting currency that does not belong to the attacker. This is because nodes will not accept invalid transactions, and an honest node will never accept a block that contains invalid information. The most an attacker can do is change his own transaction information and try to get back the money he just paid to someone else. The race between the honest chain and the attacker's chain can be described by a Binomial Random Walk (BTRW). The success event is defined as the honest chain being extended by one block, making its lead +1, while the failure event is the attacker's chain being extended by one block, making the gap -1. The probability that the attacker succeeds in filling a given gap can be approximated as the Gambler's Ruin problem. Suppose a gambler has infinite overdraft credit and then starts gambling an infinite number of potential gambles to try to fill his deficit. Then we can calculate the probability that he will fill his deficit, i.e., that the attacker will catch the chain of honesty.

p = probability that an honest node makes the next node.

q = probability of the attacker making the next node.

q = gap for the attacker to catch up to Z blocks behind.

$$q_z = \begin{cases} 1 (p \le q) \\ (\frac{q}{p})^z (p > q) \end{cases}$$

The potential progression of the attacker is a Poisson distribution with an expectation value of:

$$\lambda = z\frac{q}{p}, 则 \sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \begin{cases} (\frac{q}{p})^{(z-k)} (k \le z) \\ 1 (k > z) \end{cases}$$

Further transformation:

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} [1 - (\frac{q}{p})^{(z-k)}] = \sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!}$$