The Feasibility of Issuing Central Bank Digital Currency

By

Jinwen Shi

A Dissertation

Submitted to the National College of Ireland, August 2022

Abstract

Central banks all around the world are now concentrating heavily on Central Bank Digital Currency (CBDC) in recent years. CBDC is often characterized as a digital representation of a nation's sovereign currency that is issued by a central bank and supported by central-government credit. Many countries and regions' central banks and monetary authorities constantly monitor fintech advances and investigate the digital form of fiat money, which is moving from theory to reality. But implementing it is complicated by several legal, technological, and political issues. It is hoped that through this article, people can have a more accurate understanding of the current development of the central bank’s digital currency. It also has a specific reference significance for selecting the operation mode of the digital currency.

Keywords: Electronic Payments Security Central Bank

Submission of Thesis and Dissertation

National College of Ireland

Research Students Declaration Form

(Thesis/Author Declaration Form)

Name: Jinwen Shi
Student Number: 21118507
Degree for which thesis is submitted: Master of Science in Finance

Material submitted for award

(a) I declare that the work has been composed by myself.

(b) I declare that all verbatim extracts contained in the thesis have been distinguished by quotation marks and the sources of information specifically acknowledged.

(c) My thesis will be included in electronic format in the College Institutional Repository NORMA (thesis reports and projects).

(d) ***Either*** *I declare that no material contained in the thesis has been used in any other submission for an academic award.

Or *I declare that the following material contained in the thesis formed part of a submission for the award of

---

(State the award and the awarding body and list the material below)

Signature of research student: Jinwen Shi

Date: 24/08/2022

Acknowledgements

I have had a lot of help and assistance as I wrote this dissertation. I'd want to express my gratitude to my supervisor, Joe Naughton, for his advice during this project. I also want to express my gratitude to my parents for their support. They are always there for me.

1 Introduction

This paper examines digital currencies, focusing on the definition of digital currencies, the meaning of digital currencies, and the digital currency framework, using bitcoin as a prototype. In addition, this paper has also studied the blockchain, the technology behind digital currencies, focusing on the implications of meaning and improvements.

1.1 Background

Human society is constantly moving forward, and money has developed from nothing. From physical capital to credit money, the form of money with the development of productive forces continually changes.

As early as 4,000 years ago in Mesopotamia, people began to use clay blocks to deal with some economic affairs (Snell, 1982), and now they use central bank-issued credit currency for economic activities. (Blinder and Stiglitz, 1983). With the change in people's living habits and the advancement of science and technology, the form of currency has also undergone tremendous changes today. Primitive people first used livestock for exchange and later used shells, and agricultural tools, then minted coins, gold coins, silver coins, gold, and silver tokens, etc. Then gradually developed into paper money supported by the credit of the state and central bank, etc., that is, through the development stages of physical money, metal money, minted coins, credit money, etc. We are now at the stage of credit currency, where money is decoupled from the precious metals of traditional money and is not convertible. The backing behind credit money is essentially the credit of the state and the central bank.

Although the concept of digital currency was proposed by Chaum(1983), Bitcoin must be brought up whenever digital currency, especially cryptocurrencies, is mentioned. The idea of Bitcoin was first proposed by Satoshi Nakamoto (2008); it uses Bitcoin as a currency that is free from authority intervention and has no central bank support.

With the great success of Bitcoin since 2009, it has received extensive media attention, the interest of people and institutional investors has supported the notion of a fiat currency alternative, and the belief that blockchain offers the best platform has emerged(Cunha, Melo and Sebastião, 2021). As cryptocurrencies are issued by unofficial institutions such as Bitcoin, their value has been controversial and their price unstable due to the weak credit of the issuer. People believe more in the technology behind this than in Bitcoin itself. The Cyprus incident in 2013 drove up the price of Bitcoin and made people realise that Bitcoin is a safe-haven investment property (Farrell, 2013). Bitcoin was introduced with blockchain technology at its core, creating a way to store value and transfer funds not based on a bank deposit account. It is a

decentralized, trustworthy, and distributed bookkeeping technology (Yaga et al., 2018).

Recently, with the further research and application of blockchain and innovative contract technologies, the functions of digital currencies have been further expanded and "second-generation digital currencies" have emerged (Miller et al., 2015). The second generation of digital currencies has been equipped with new functions such as issuing digital asset certificates and medium financing.

At the same time, its function as a payment instrument has also been improved and enhanced along with the rapid development of digital currencies, especially private digital currencies, and the research and issuance of central bank digital. With the rapid growth of digital currencies, especially private digital currencies, the study and launch a central bank digital currency (fait digital currency) has become an essential issue for the financial authorities of significant countries. According to the Atlantic Council (Atlantic Council), as of July 2022, 105 countries, representing over 95% of global GDP, are exploring a CBDC. Digital currencies have been fully rolled out in 10 countries, and China's pilot program will be expanded by 2023. Euro central bank (2021) has also published a report on the e-euro and announced that it would launch the investigation phase of the 24-month-long digital euro project.

1.2 Research purpose

Digital currency is a new form of currency. The market confidence in the current private digital currencies, such as Bitcoin, is not as stable as fiat currency due to the credit of private digital currencies issuer is not substantial. In this context, central banks of various countries have shown interest in digital currency. Gradually research digital currency and try to launch its fiat digital currency. In this research, through the research on the principle and essential support of fiat digital currency, the operation mechanism of digital currency, such as the issuance mechanism, circulation mechanism, and supervision mechanism, will be carried out some summaries and some forward-looking designs. It is hoped that through this article, people can have a more accurate understanding of the current development of the central bank’s digital currency. It also has a specific reference significance for selecting the operation mode of the digital currency.

This paper examines digital currencies, focusing on the definition of digital currencies, the meaning of digital currencies, and the digital currency framework, using bitcoin as a prototype. In addition, this paper has also studied the blockchain, the technology behind digital currencies, focusing on the implications of meaning and improvements.

2 Literature review

Academicians have focused much of their research on the meaning of digital currencies and the design of their operational framework. Scholars' views on the definition of digital currency have changed over time, with the more obvious The focus varies, with a more apparent trend in the literature toward a more comprehensive definition of digital currency and a broader definition of the feasibility and operational framework of a fiat digital currency has been studied in terms of the design of the operational framework of a digital currency, both monolithic and binary in terms of issuance and circulation, and duration of the regulatory mechanism, scholars have different emphases. And given the many academic definitions, more investigation is required of digital currencies, operational mechanisms, and other vital issues.

2.1 Digital currency

The concept of digital currency emerged in the early 1980s and has been studied for almost 40 years of research. Chaum (1983) proposed constructing an electronic money system with anonymity and untraceable. This was one of the first theories of digital currency. His development of the E-Cash currency sparked the industry's interest in digital currencies, and in today's terms, Chaum's model is still the traditional three-way "bank-person-merchant" model. The subsequent research on group-blind signatures, fair trading, offline transactions, and the divisibility of currencies all built on this foundation.

In a widely accepted term, digital currency is a collection of virtual currencies and cryptocurrencies (Central Bank of Ireland, 2014). In other words, a cash-like object that is kept or exchanged in digital form over the Internet is referred to as a "digital currency." These types of currencies can be exchanged for real-world or digital products and services (European Central Bank, 2015). Still, certain digital currencies are restricted to specific trading environments, such as in-game currencies in online games.

Al-Laham, et al. (2009) make the fact that electronic cash, as a network good, may develop into an effective form of money in the future. These changes will impact how well the monetary policy is implemented and is thriving. Suppose the rising use of electronic money significantly reduces the demand for central bank reserves. Under this circumstance, monetary and fiscal policies need to be coordinated more closely, and operational objectives for central banks need to be adjusted.

Venter (2016) emphasizes that It is essential to distinguish between digital currency and electronic cash held in a retail bank account. Alternatively, he believed that digital currency is a digitization of money—a method of transaction that solely exists digitally

and is unrelated to any physical currency. The most well-known example of digital currency, of course, is Bitcoin.

2.2 Central bank digital currency (CBDC)

Tobin (1987) may have been the first to put up the notion of creating central bank currencies in digital form with the concept of "deposited currency" or " a medium that combines the simplicity of deposits with the security of money" to enforce payments enhancement and reduce dependency on deposit insurance.

The collection of academic literature on central bank digital currency research is small but has grown rapidly in recent years. The most important reason for this is that central banks around the world have gradually taken up and begun to develop research on CBDC (Auer et al., 2021).

In order to evaluate the case for CBDC adoption from the perspectives of users and central banks, a conceptual framework is proposed by Mancini Griffoli et al. (2018). Bilotta(2021) explained CBDC as a central bank liability which is often defined as a digital version of a country's sovereign currency issued by a central bank and backed by central-government credit. He stated that central banks create virtual money rather than producing currency, which is a digital version of coins and banknotes.

Chaum, Grothoff and Moser (2021) explained how institutions should issue central bank digital currency under the technical aspects. A hardware-dependent token-based CBDC and an account-based (or account-based) CBDC are two potential architectures that have been considered in the literature.

According to Keister and Sanches (2019), Barrdear and Kumhof (2016) were the first researchers to analyse the effects of CBDC. They included central banks' digital currencies in a quantitative dynamic stochastic general equilibrium (DSGE) model to examine their effects on GDP and evaluate various monetary policy regulations. They referred to a central bank digital currency providing ubiquitous, electronic, 24-hour access to its balance sheet that is also interest-bearing. According to their approach, when a new digital currency is launched, the asset side balance sheet of the central bank—rather than the digital currency itself—has a big impact. In contrast, in the version of Keister and Sanches‘s (2019) model, liabilities held by the central bank influence the liquidity premium, which modifies the equilibrium interest rate and affects investment.

Auer and Boehme (2020) evaluate the usefulness of central bank digital currencies and how to combine customer desires for digital currencies that resemble cash with the convenience of payment systems for intermediaries. It investigates whether CBDCs are direct or indirect requirements for central banks and payment

intermediaries. Consumers also want payment security similar to that of cash, which means that the central bank's payment system must prevent the insolvency or technological failure of intermediaries and the central bank's failure. the research mentioned that if a national system is built on digital tokens, international residents will have access by default. It may be beneficial to have more hands-on experience with specific design choices once you've established a framework for decision-making. Auer and Boehme also suggest that sharing the findings of these trials across borders will provide a clearer picture of which technological options are good for community development centres in general, as well as how the best designs are determined by the characteristics of each jurisdiction. As a result, the argument over whether and how to issue community bonds becomes more informed.

Andolfatto(2018) developed a balancing framework and used the model to assess the economic impact of central bank digital currencies. The preceding study implies that, rather than in a competitive environment, where banks utilize their market power to hold down deposit rates, the principal advantages of CBDCs will flow to depositors. Although the quantitative extent of this impact may depend on project parameters and the degree of financial development available, the model predicts that CBDCs will increase financial inclusion and reduce cash use. It also implies that if the central bank respects interest rate policy norms, CBDCs do not necessarily have a detrimental influence on bank lending operations. Finally, based on theory and evidence, I conclude that a well-designed CBDC is unlikely to jeopardize financial stability.

The decrease in demand for central bank monetary liabilities has been occurring for some time now, and the move away from physical money is just the most recent manifestation of this trend. This is due to how advanced technology has made it feasible for retail customers and financial institutions to conduct financial transactions without using central bank money (2021 Kovanen). In his study, Kovanen noted that while a decline in the demand for central bank monetary liabilities would not affect the effectiveness of their policies, it would have other effects, such as a decrease in their revenues, which could undermine their independence and policies' effectiveness and make them dependent on government funding. Although many people consider the creation of a CBDC to be the ultimate answer to the issues that cryptocurrencies have brought about, it has its own set of risks and the potential for unexpected effects. Based on the discussion of China's national conditions at this stage, Yao(2018) has different views on the central bank's digital currency. Yao proposes the concepts of account-based digital currency and wallet-based digital currency, as well as a design for the coexistence of bank accounts and DFC wallets at various levels, incorporating DFCs into the traditional "central bank-commercial bank" binary system to reuse existing mature financial infrastructure and avoid the consequences of narrow banking. In terms of coinage, a legal digital currency is a credit-based currency, a cryptocurrency in terms of technology, an algorithm-based currency in terms of implementation, and an intelligent currency in terms of application scenarios, according to this research.

All current private payment instruments should be of greater quality than a Chinese DFC or CBDC. It is evident that implementing a legal digital currency cannot be accomplished quickly and that such a lofty aim must be accomplished incrementally.

Many questions remain, as with any new shape of literature. Which fundamental qualities of CBDC—as a medium of exchange and a store of value—are vital for families' portfolio selections over which assets to use, in my opinion, is the most crucial question. Indeed, empirical research on consumer payment preferences, such as that by Koulayev et al (2016), demonstrates that people's preferences for different payment methods are varied and not entirely explained by demographic factors like income and age. Understanding consumer payment choices is crucial because a CBDC will, first and foremost, increase the range of payment and saving options available to households. This understanding is necessary to fully comprehend the macroeconomic and microeconomic effects of introducing a CBDC in a theoretical framework.

2.3 Blockchain

The operational structure and technological components of conventional banks have been altered by blockchain technology (Chang et al., 2020). Firstly, it lowers expenses and value transmission. Additionally, it makes risk management more efficient. And last, it looks for novel methods to turn a profit. The poly centricity, public autonomy, and immutability of blockchain fundamentally alter the business model of centralised banking systems, optimise banks' back offices and infrastructure, increase service effectiveness, enhance user experience, and provide institutions options for transformation. From the conventional financial sector to the online financial industry. Commercial banks may reduce labour and technology expenses by using blockchain technology to prevent money laundering and improve client knowledge.

Bitcoin has been the subject of numerous blockchain-related studies and projects. Although it can be used in many different contexts, Bitcoin is merely a small portion of the blockchain. For a greater impact, blockchain can be used with other technologies. (Leible et al., 2019). Blockchain, according to Nguyen (2016), has enormous potential and will become more important to the growth finance industry and the actual economy. Consumers, the present financial system, and society at large are anticipated to gain significantly from the new technology.

Morganti, Schiavone and Bondavalli (2018) against the backdrop of the blockchain boom, the risks of blockchain technology are assessed and presented in detail, and people are reminded of the need to be more aware of the risks and make plans for future work to prevent risks and reduce related losses.

3 Research Methodology

There are presently no authentic national, or regional public offers in central bank digital currencies as there are no set quantitative conditions. Therefore, this article picking a qualitative study is not only necessary but also appropriate. The main objective of the research described in this article is to carry out a theoretical investigation supported by the principles of a legitimate digital currency. It also aims to provide some summaries and make some predictions about the operational mechanisms, such as the creation, transfer, and regulation of central bank digital currencies.

By reading the relevant literature, the theoretical explanation of digital currency and the technical basis of digital currency are sorted out and summarized. Then the practice of digital currency (taking Bitcoin as an example) is introduced. Finally, combined with the literature, the framework design of central bank digital currency is sorted out and put forward its design.

3.1 Research Methods

3.1.1 Literature research method

The research method is to analyze the study's object and read a large amount of literature to explain the theory of digital currency, the technical basis of digital currency, and the operation mechanism of digital currency.

The researcher will conduct an in-depth study on the theoretical explanation of digital currency, the technical basis of digital currency, and the operation mechanism of digital currency, and then put forward his own views.

3.1.2 Qualitative Analysis Method

This is a qualitative analysis of the definition of digital currencies and the operational framework of digital currencies.

3.1.3 Comparative Analysis Method

A comparative analysis of legal digital currency and existing paper money, a comparative study of legal digital currency and private digital currency
A comparative analysis is conducted to analyse the advantages of legal digital currency over existing paper money and private digital currency.

3.2 Possible Innovations and Shortcomings

3.2.1 Points of innovation

Digital currency is a new form of money, and although Bitcoin has been around for a long time, it has not been in the limelight not long ago; the emergence of Bitcoin has inspired many scholars to research private digital currencies, for This paper adopts the binary issuance mechanism and binary circulation mechanism of digital currencies. This paper adopts the binary issuance mechanism and binary circulation mechanism of digital currencies and selects online and offline transactions of digital currencies for innovative design.

3.2.2 Shortcomings

The final framework for the issuance, circulation and regulation of legal digital currency given in this paper is based on the published literature. It does not have a deep understanding of the operating environment of legal digital currency, and the operational framework of legal digital currency is not well designed. The framework is not well designed.

These chapter below provides a simple but thorough introduction to digital currencies, central bank digital currencies, the blockchain idea, etc., and more details on the significance of the central bank issue of digital currency. In conclusion, the ideas addressed in this chapter should give the reader the expertise needed to pursue this study issue and broaden the necessary knowledge base.

4 A Theoretical Explanation of Digital Currency

4.1 Digital currency definition and classification

In terms of confusing concepts among the coins that have emerged so far, electronic money, cryptocurrency, virtual money, digital money, etc. are easily confused, in addition to tokens. In terms of the definition of various currencies, combining the published papers of several scholars and the public literature on the Internet and the actual situation in China, virtual currencies are non-physical currencies, including digital currencies, cryptocurrencies, electronic currencies, tokens (including game coins and various kinds of coupons with limited applicability after the exchange with fiat currencies), etc.; electronic currencies are the digital form of RMB that we are using now; cryptocurrencies are a kind of cryptographic principle to ensure the security of transactions. In the concept of cryptocurrency, the security of transactions can be ensured by using cryptographic principles; and tokens are currency-exchange equivalents that have a limited scope of application and no currency effect, such as QQ coins and game coins. Not all items with the word "coin" in them are currencies. Some virtual coins can only perform the function of an equivalent within a certain time and space frame and can therefore only be called tokens, not currencies. Digital money is a new form of money. Digital currency, which has no physical form, exists only on a storage medium, is secured by computer technology and is transferred via the internet.

4.1.1 Definition of digital currencies

The function of money has not changed from paper money to digital money, but the form of money has. Digital money is cheaper to circulate than paper money because it not only reduces unnecessary wear and tear on the currency in circulation but is also more secure and portable. The offline transaction mechanism of digital currencies is designed so that offline transactions through digital currencies do not require the participation of a third party and can simulate the offline transaction mechanism of paper currencies, making payments more convenient and faster. It can make up for the shortcomings of offline transactions in electronic payments. Compared to paper money, digital currencies are more virtual and have a smaller value. In terms of credibility, people's confidence in a credit currency is more about the promise that the

issuer will not issue money indiscriminately. The credibility of a digital currency is naturally higher than that of a paper currency.

In terms of technology, the reliance on technology for credit money is more about paper, printing and anti-counterfeiting. In contrast, the reliance on technology for digital money will be much more robust, as it is an inherent property that is stored on a storage device without a physical body. We can develop and innovate on the technology used in Bitcoin to design a more suitable solution that is central and critical to the operation of digital currencies.

Many scholars define some online virtual coins as digital currencies, such as point coupons. Traditional digital currencies cannot be strictly called currencies. They cannot be used as general equivalents and therefore do not have monetary properties. With the development of Bitcoin, a new type of digital currency has emerged, which differs from traditional digital currencies in that it relies more on technologies such as cryptography and blockchain. With the emergence of Bitcoin, the concept of digital currency has begun to change, and as research has been conducted, so to have the views on digital currency.

Proposer	Year	Focus	Viewpoint
European Central Bank	2012	Regulation	Virtual currencies are distinguished from regulated electronic currencies and business bank deposits by being described as unregulated digital currencies.
Fung and Halaburda	2016	Issuer	Fiat digital currency refers to a digital format currency issued by a central bank.
FATF	2014	Form	Digital currencies include electronic currencies that are fiat currencies and virtual currencies that are not legally regulated currencies
Bank of England		Form	New types of systemic digital money might be offered publicly or privately, much as traditional forms of payment. An electronic version of central bank money offered for retail usage is known as a central bank digital currency (CBDC).

IMF		Form	Digital currency is digital expression of money

It can be seen that the views of institutions or individuals on the definition of digital currency are relatively different, stemming from different emphases. This article believes that the concept of digital currency should be explained from the two aspects of "numbers" and "money". First, from the perspective of "numbers", "numbers" are virtualization. Compared with the physical characteristics of the current credit currency, it has no independent entity but relies on computer technology and is stored in the intermediate in the form of binary and so on; The second is money, which is a generic equivalent, which can act as a scale of value and a medium of exchange within a certain range. Therefore, the definition of digital currency in this article is a generic equivalent of computer technology to ensure storage and security.

The fiat digital currency issued by the state as the issuer has not yet appeared, stemming from several points. First, the change in the form of the currency has a significant impact on the economic development of a country, and hastily changing the current form before it is clearly studied may lead to market confidence instability; Second, the monetary system for the operation of fiat digital currencies has not yet been designed and sound; Third, the technology required behind fiat digital currency cannot be simply modified directly on the private digital currency operation technology, and it needs to be carefully designed. However, the research work on digital currencies at the national level is closely advancing, and legal tender, as a national legal tender, must have the nature of legal tender and have unlimited legal compensation attributes. This article believes that the fiat digital currency should be issued by the central bank, using cryptographic encryption of the non-physical form of the virtual fiat currency to replace the existing fiat currency, from the perspective of issuance, because it is issued by the central bank of the legal tender, with unlimited solvency, so it is a legal tender, from the form of the use of computer storage technology for storage and trading, there is no physical form, so it is a digital currency, so it is a fiat digital currency.

4.1.2 Classification of digital currencies

Digital currencies can be divided into private digital currencies and fiat digital currencies, depending on the issuing entity. A fiat digital currency is one that is issued by a nation's central bank and has the state's credit support in addition to having the characteristics of a fiat currency. Private digital currencies are those that are created by private institutions. The boom in private digital currencies began with the stimulation of Bitcoin, and with the development of digital currencies came other private digital currencies such as Ether, Litecoin, Ripple, Dogcoin and Futurecoin. Many of the private digital currencies that followed Bitcoin were designed with reference to the Bitcoin source code, with some improvements to Bitcoin, such as Litecoin.

Private digital currencies such as Bitcoin are now accepted for payment by many companies around the world, such as major IT companies like Microsoft and Dell, department stores like Overstock, food and beverage companies like Starbucks, etc. However, their value fluctuates and can cause some revenue volatility for companies, so Microsoft suspended the Bitcoin payment option for a time and then reintroduced Bitcoin payment channels. The value of private digital currencies has been less stable in recent years because they are new and inevitably fragile and are influenced by laws and regulations, and because the issuer is private and less credible than the state, there is a lack of trust in private digital currencies. The legal digital currency is a legal tender and the state's coercive power ensures that it becomes a fiat currency, so it has the attributes of a currency from the day it is born.

4.2 The inevitability of digital money

4.2.1 Classical monetary theory

According to the classical explanation of the origin of money given by Karl Menger, commodities have different degrees of marketability depending on their "marketability" (Ikeda, 2008). Menger's (1892) first emphasis is on the mystery of why each person would exchange his wealth for something that is merely symbolic; according to Menger's theory, money is simply a tool that people use to satisfy their needs, for example, to obtain the goods they want. Friedman, on the other hand, argues that money is a representation of wealth, but that money itself is not wealth and has limited value. In the mid-19th century British 'currency debate', the 'currency school' argued that only metal money and banknotes were money. In contrast, the 'banking school' argued that credit such as demand deposits was money. "In the 19th century British 'currency debate', the 'currency school' argued that only metal money and banknotes were money. In contrast, the 'banking school' argued that credit media such as demand deposits should also be included in the category of money because they also functioned as a medium of exchange. Marx held the view that money was primarily a specific good fixed as a universal equal (Graziani and Vale, 1997). This theory is based on metal money. According to Menger's theory, before the state had a monopoly on the issue of money, money was more often a medium of exchange for a few highly marketable commodities selected by the market to exchange with other commodities. Money is, therefore, a spontaneous creation. In other words, money is a measure of value and a medium of exchange. Many academics have provided separate definitions of money, each with a different focus. However, most economists now consider money to be generally accepted in the exchange of goods, the payment of debts or the provision of services.

There are different views on the origin of money, a genius invention, natural exchange, intermediary, etc. Since the invention of genius theory and the natural exchange theory are so outrageous, we now explain the origin of money more, starting with the

intermediary theory. This assumes that if there are n goods in the market, then there are (n $*$ (n - 1))/2 ways of exchange forms of exchange, the high cost of exchange in the market, when examining the emergence of money, only n forms of exchange were needed, for market efficiency gains and exchange costs can be reduced with significant effect. However, for the intermediary theory, there is no clear information on why and how the money economy replaced the primitive economy. There is no clear information on why and how the monetary economy replaced the primitive economy, so the origins of money are generally logical deduction and comparative analysis.

From the perspective of the development of currency form. With the development of productivity and technological advances, the form of money has evolved considerably, from the initial use of commodities as money to the casting of metal coins and now to paper money. Money has changed in terms of shape, security, and security, all of which have improved.

In terms of the main body issuing the currency, it was not uncommon to allow private minting, but the state eventually withdrew the right to mint money, on the one hand allowing the state to control the minting tax, and on the other hand allowing the state to guarantee the domestic circulation of the currency through administrative regulations. For instance, throughout the Warring States and Spring and Autumn Epochs, the demand for money increased, but if iron smelting technology had not been widely used at the time, iron for coinage would not have been available, and the widespread use of copper coins would not have been possible. The evolution from minted money to paper money, for example, was the result of the contradiction between the needs of the people and the realities of the world, which led to the creative use of deposit certificates in commerce and the emergence of paper money. The development of money has gone through four stages: commodity money, metal coinage, substitute money and credit money. We are now in the credit stage, where money is separated from commodities and becomes legal tender, secured by the credit of the state, and the generic equivalent of commodities in circulation. In the era of commodity money, the demand for commodity exchange had not yet reached the point where money was necessary to meet the demand for exchange; later, as technology progressed and people became more practical, it was found that metals with a practical or decorative function could meet people's needs in terms of portability and divisibility, hence the emergence of metal coins. Later, with the advent of paper, people began to use tokens to start their economic activities. In historical practice, the shift to non-convertible money in a country generally began when the central government gave a single institution the legal privilege of having a monopoly on issuing money.The portability of credit money has changed little in comparison to tokens, although it has cut off convertibility with metal money and has a slightly lower value than tokens. The confidence that the issuer will not issue money indiscriminately.

In terms of the function of money. In recent years, electronic payments have become widely accepted by the public, and we only need to show our payment device when we pay. The payment is still made during our transaction in credit money, but through a tripartite institution and not face to face. Money is a general equivalent, which exists as a medium of exchange for commodities, but when the demand for exchange is low, there is no need for money and people do not need to spend time and effort on research and design of the monetary system, so the development of money is limited by the level of productivity. With the development of productivity, people were able to produce more and more commodities and entered the era of the commodity economy, when the purpose of production was not only to meet their own needs but also to meet market exchange. As productivity increased, the variety of commodities became more diverse and the demand for money became stronger. The need for generic equivalents in human society led to the emergence of money, the form of which changed as human productivity increased, eventually developing into the RMB, USD, GBP, EUR, JPY, etc.

4.2.2 The inevitable trend in the evolution of money

The evolution of money is the history of its advancement. The evolution of money is a matter of form, divisibility, value stabilization and security. In terms of value stability, the initial currency had value, but as the currency evolved, the value of the currency became smaller and smaller, almost negligible, eventually, people's trust in the currency changed from trust in the value of the currency to trust in the issuer. When inflation is severe, people lose confidence in the issuer and turn to fiat currency for investment or to the stable value of other countries' fiat currencies. In terms of security, advances in science and technology have forced the improvement of the currency's anti-counterfeiting features.

In terms of the form of money, from the beginning to the end, from physical money to credit money, the form of money has developed towards portability, and portability has gradually become an important leading mechanism in the development of money. Firstly, as productivity increases and the exchange of goods becomes more frequent, the requirements of exchange agents for the portability of money gradually increase. Secondly, the advances in science and technology have ensured the emergence of digital money, as each generation of money has been subject to technological constraints. In the days before iron smelting technology, even though people realized that copper had many advantages over physical money, they were unable to use and promote it. When did it occur to people that money could be turned into tokens, even before the advent of paper? Now that technology has made it possible to virtualize money, why can't virtual money become the next generation of money? Thirdly, people's payment habits have made a legal digital currency a necessity. With the development of e-commerce, people are becoming more and more accustomed to electronic payments and are gradually moving away from their reliance on physical currency. The emergence and use of digital currency is not unacceptable compared to

the payment habits people have developed, but rather a logical step in the right direction. Fourthly, digital currency is not a reversal of the current monetary system, but rather an improvement. It does not challenge the state's right to mint money, but rather allows the state to retain the right to mint money and mint taxes by guaranteeing the issuance of money, while allowing the state to play its role as a service provider for the issuance, circulation, and regulation of legal tender. There are already some legalized digital currencies that are pegged to the US dollar to increase their investment value and expand the global market for the dollar, but these are not backed by the US dollar and are not issued by the Federal Reserve, but rather attempt to add value to both using a correlation system, and therefore are not particularly stable in value.

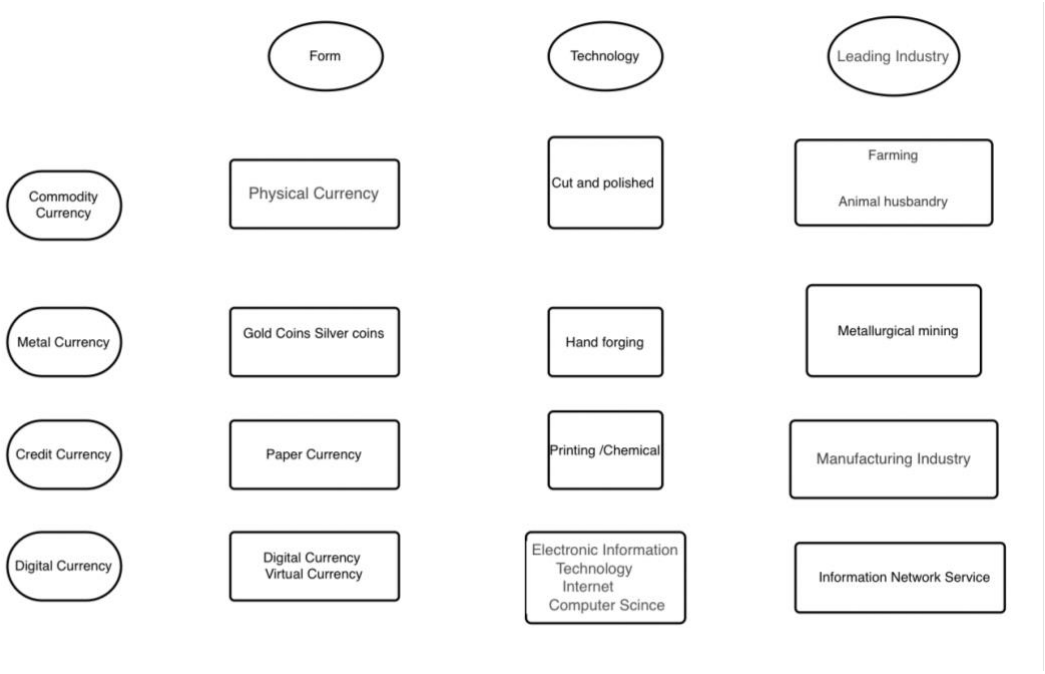

Figure 1: Evolution of monetary forms and technological progress

The progress of money is the sum of all aspects with the characteristics of the times that have gradually manifested with the development of the times and the progress of science and technology, and the progress of money-related technologies, monetary systems, and other aspects is the basis for ensuring the efficient and stable operation of new monetary forms.

To be able to qualify as currency, an item must meet several requirements with regard to its nature. First, the value must be stable and cannot change too much. Otherwise, as a medium of exchange in the transaction process, it is necessary to adjust the value of various goods from time to time. The price is quite troublesome; second, it is easy to save. If the medium of exchange as a currency is easily damaged, on the one hand, it will increase the cost of people’s preservation of it, on the other hand, it will affect people’s acceptance of it. It will bring additional transaction costs when both parties deliver; third, easy to divide, easy to divide is another feature that currency as a

medium of exchange should have, otherwise it will also cause a series of inconveniences in the transaction process.

The first reason for the popularity of metal coinage was the mastery of iron smelting technology, which led to a massive expansion in the forging of copper coins. It was only as people developed the habit of trading that the new currencies became more popular. With the development of Bitcoin, people began to be exposed to new digital currency prototypes, and digital currencies began to enter the research horizon of scholars, and central banks gradually began to research digital currencies. The study of private digital currencies (such as Bitcoin) has been operating steadily for ten years with the support of blockchain technology, which shows the stability of blockchain technology. Digital currencies are not the same as Bitcoin, nor is digital currency technology the same as blockchain. Blockchain is a new technology, and no other technology has yet emerged to support the operation of digital currencies, so the technology currently used to study digital currencies is generally blockchain. In the next chapter, we examine the technological foundations of digital currencies.

4.2.3 Demand, habit and technology make digital money inevitable

The evolution of money forms has been driven by demand, habit, and technology. After more than 70 years of development since the founding of New China in 1949, China's GDP has changed dramatically, from $ 59.72 billion in 1960 to $ 14.72 trillion in 2020. The growth in GDP and increased demand for transactions has increased the need for the portability of money.

In terms of payment habits, the rapid spread of Alipay, WeChat and UnionPay has also helped people to adapt to a cashless society, with people gradually adapting to electronic means of payment, which has laid the groundwork for digital money to be accepted once it is released. In terms of the way money is settled, there has been a shift from the use of silver and goods to the use of credit cards and mobile payments, making payments more convenient and efficient. Apart from remote areas, mobile payments are now a popular way of paying for money daily in most areas.

For historical reasons, China missed out on the first industrial revolution and the second technological revolution, which led to a modern China that was already impoverished and weak compared to the Western countries at the time of the founding of the country. In 2009, in Beijing, you still had to carry some cash when you went out, but now, even in some third and fourth-tier cities and rural areas in China, not paying with cash does not affect your daily settlement and does not affect your work and life. The rapid development of mobile payments is not the result of a single factor, but of several factors that have contributed to the development of mobile payments and led to a dramatic change in people's perception of payments. Secondly,

the popularity of IOS, ANDROID and other touch screen smart devices and the development of related applications have made payments more convenient and the experience better; thirdly, the development of computer technology has ensured payment security; fourthly, Taobao and JingDong e-commerce platforms have developed rapidly since their emergence, providing guaranteed transactions and safe transactions, and at the same time providing financial services. Fourth, the e-commerce platforms of Taobao and JingDong have grown rapidly since their emergence, offering secured transactions, safe transactions, and financial services, enabling consumers to experience the benefits of mobile payments, and occasionally offering payment incentives to attract consumers, develop their habits and increase their stickiness. This has deepened the habits people have developed on e-commerce platforms.

Of course, the continuous improvement of relevant policies (regulation of e-commerce transactions) and supporting facilities, as well as the continuous improvement of the industry (courier industry, etc.), have also provided particular convenience to the development of mobile payment. In terms of people's payment habits and perceptions, as people's financial experience increases, their understanding and use of finance become more accurate, and most of their daily transactions are no longer in direct contact with cash (except for some possible illegal activities and less convenient places).

The circulation of credit money in the real economy has also changed over a long period of time, as the original transfer of money between enterprises was generally carried out by bank transfer, while individual users would generally take out some banknotes for daily settlement services in addition to their accounts at banks. According to the China Union 2021 report, residents in Tier 1 cities spend over RMB 5,000 on mobile payments on a monthly average, making up more than 80% of their average monthly consumption. Residents of Tier 5 cities spend more than RMB3,000 per month on mobile payments, which makes up 90% of monthly consumption on average. People were used to using wallets with paper money for transactions, but now people's habits have changed, and they are more used to using their mobile phones for payments.

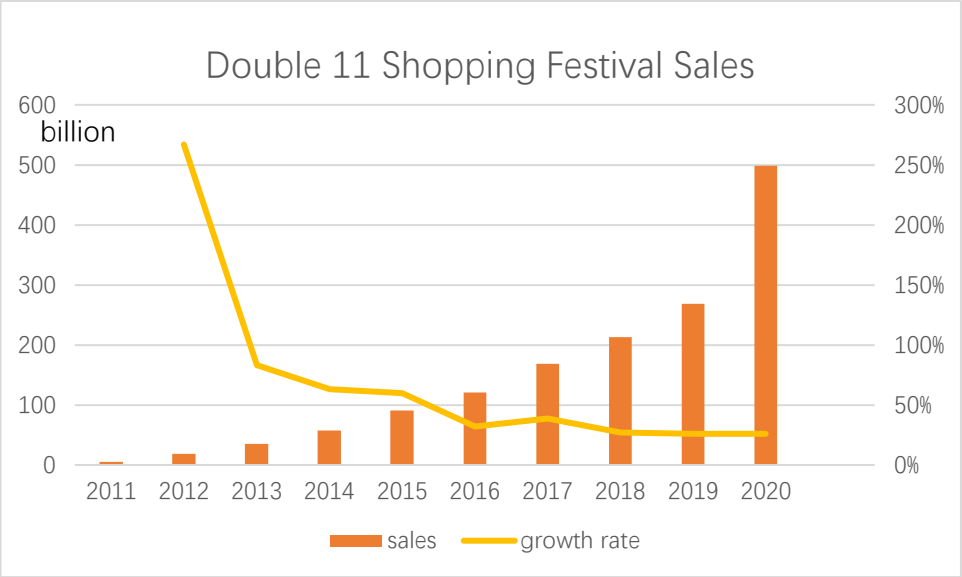

Figure2 Alibaba's Double 11 Shopping Festival Sales

The graph above shows Alibaba's sales figures on the day of the Double Eleven from 2011-2020, which grew rapidly from 5.2 billion yuan in 2011 to 498 billion yuan in 2021. The development of e-commerce is far from being dependent on the electronic means of payment, which is rapidly gaining acceptance among the population and has led to a certain change in people's habits. When electronic payments were not widely accepted, there was a currency omission rate in the money multiplier, but when electronic payments became widespread, the money multiplier for legal tender notes would change. Fortunately, there is ongoing research into the impact of electronic payments on the money multiplier, and although digital currencies will impact current monetary theory, we believe that as academics pay more attention to them, theory will catch up with practice and eventually be used to guide it.

The emergence of blockchain technology has led directly to the emergence of private digital currencies such as Bitcoin. The stable operation of Bitcoin is proof of the stability of blockchain technology. Just because Bitcoin is anonymous and decentralized does not mean that the blockchain is anonymous and decentralized, so the operation of legal digital currencies can also be supported by blockchain technology.

4.3 Functions of legal tender and its implementation

4.3.1 Analysis of the functions of digital currency

Different scholars believe that the function of money is different, the common function of money is said to have two functions, three functions are said to be four functions and five functions are said to be, etc. The two functions of money are recognized as the value scale and circulation means, and the two functions can be separated, when a country's legal tender is unstable, gold can be used as a value scale, and the means of circulation are exercised through legal tender. There is a three functions' theory believe that the scale of value, the means of circulation and the means of storage are the three functions of currency, the function of means of storage is added based on the other two functions of money. There are five interpretations of the role of money in Marx's political economy: the scale of value, the medium of exchange, the functions of storage, the means of payment, and the global reserve currency. The function of money itself is also a process of gradual development and perfection, initially the production of money is only to meet the needs of instant exchange, the need to be able to measure the value of commodities, in addition to acting as a general equivalent in exchange, and with the exchange, money gradually began to act as a means of storage, means of payment, world currency and other functions. Therefore, this article believes that the analysis of the currency function should be carried out from the five functions.

As a medium of exchange, the central bank's digital currency is similar to traditional legal tender and can be used for commodity trading. The purpose of a commodity economy is for exchange rather than self-sufficiency. As a measure of value, it can be used as a general equivalent to determine the value of various commodities, like the existing traditional legal tender, which is backed by the state. They may not be kept because of their nature, but by transforming them into money they can fulfil the function of a store of value and therefore become a means of storage. Paper money can be held by individuals, but it is more likely to be kept in banks through demand or time deposits and may be invested through securities companies. In its function as a approach of payment, it is not very different from a traditional fiat currency and can also be used as a means of settling other services etc. World currency: as a means of payment, a fiat digital currency can move around the world to carry out payment activities.

4.3.2 Functional realization of digital currencies

At present, fiat currency has a set of institutions to ensure its functionality, while the legal digital currency, as a virtual currency, is different from physical currency such as paper money. And therefore, its issuance, circulation and regulation must be redesigned to meet the functions of a legal tender and its operation. Several scholars around the world have studied this issue, and this paper will then summaries and present their views on it.

5 Technical Foundations of Digital Currency

5.1 Blockchain Background and Operating Principles

The blockchain was proposed by Satoshi Nakamoto (real name unknown) in 2008 and has since become the key technology supporting the operation of Bitcoin. The blockchain behind Bitcoin was designed as a public chain to ensure openness for users, and later, as research progressed, permission chains such as federated chains and private chains emerged.

Currently, there is no standard academic definition of blockchain. Generally, blockchain was considered as a technology which can verify and store data by using the blockchain data structure, generate and update data with distributed nodes, ensure information security by cryptography, and generate smart contracts with automated scripting code. By linking the blockchains one by one into a single chain, the whole chain reaches consensus, which greatly enhances the security of the data stored.

5.2 Blockchain core technology and features

Consensus mechanism (node agreement), why do we need a consensus mechanism? Because everyone is equal in a blockchain and there are too many of them, so when making certain choices or voting, there needs to be a unified rule to regulate and manage the behavior. Some the problem can be solved in a distributed scenario by the consensus mechanism of blockchains' consistency. The consensus of Bitcoin consists of four separate processes for all nodes: first, the nodes verify the transaction; second, the nodes pass the verification, and the transaction record is recorded in a new block; third, the nodes verify that the new zone is fast and linked into the blockchain; and fourth, the nodes choose the longest chain according to an algorithm.

The consensus mechanism used in the blockchain in Bitcoin is POW, there are more than one consensus mechanism, there are also POS, DPOS, etc. POW is called proof of work. The POW is called proof of work, which means proof of work is mining, because it is difficult to calculate new blocks, so it is necessary to exhaust the nonce to calculate the hash of new blocks. The proof of work used in POW consensus technology will lead to the centralization of arithmetic power, and the risk of individual miners mining is greater, which may lead to miners joining together to form a pool with huge arithmetic

power. These pools will then be able to easily gain mining revenue and transaction fees, which will lead to the gradual marginalization of nodes with less arithmetic power, and eventually the blockchain with POW consensus will become a competition for arithmetic power, which will eventually lead to a competitive threshold, which is clearly unhealthy in terms of the decentralized design of currencies such as Bitcoin. The most important concept in POS consensus is the age of the coin, and the disadvantage of POS is that it encourages people to hold on to coins, which is not conducive to the circulation of coins. The disadvantage of DPOS is that to obtain voting rights, users must first obtain coins, but the way to obtain coins, such as recording blocks or transaction fees, is to have voting rights to be elected as a trusted node, resulting in a relatively high barrier to entry.

In everyday use, credit cards often require a signature on the bill to confirm the transaction, or in corporate business, sometimes a stamp is applied, and each party keeps a copy of the document after it has been separated, for verification and security purposes, but it is not practical to sign or stamp a stamp in online transactions. Because there are so many users, the private key is randomly generated by the digital wallet, while the public key is obtained by converting the private key to an elliptic curve, and the Bitcoin address is obtained by a series of hashing algorithms from the public key.

The technical core of the blockchain gives it its own characteristics. At present, the characteristics of the blockchain are, firstly, decentralized. In the blockchain network, each node has equal power, and each event needs to be confirmed by the whole network, therefore, the loss of some nodes' data or leaving the network will not affect the accuracy of the event. Second, the database is reliable. Blockchain uses a distributed ledger where each node has a full ledger of transaction events, and theoretically, a hacker would need to control at least 51% of the nodes to attack the ledger, but it is much harder to hack 51% of the nodes than it is to hack a single node. Thirdly, anonymity. In Bitcoin's blockchain technology, participants are anonymous and do not need to be authenticated, but this feature poses some regulatory challenges.

Just because Bitcoin is decentralized does not mean that the blockchain is necessarily decentralized and de-regulated. Central banks can also use it to launch their own 'centralized' digital currencies, which are protected by national sovereignty.

5.3 Blockchain classification and application

In 2018, blockchain is a hot spot in China's capital market and has become a money-spinning gimmick for many projects. Some unscrupulous elements have fooled investors under the banner of decentralization, and the central bank and relevant regulatory authorities have issued a series of policies and opinions to regulate the

development of some projects based on this technology, which has led to some prejudice against blockchain and digital currency.

According to the openness of blockchain participation, blockchain can be divided into public and licensed chains, and licensed chains can be divided into federated and private chains. Public chains allow any organization or individual to read and send a consensus blockchain that can confirm transactions and obtain valid confirmation. Consortium chains are managed by multiple institutions, each of which operates one or more nodes, and only those institutions that have agreed to enter the chain are allowed to read and write data, send transaction information, store transaction data, etc. The consensus process is controlled by pre-selected nodes. Coalition chains are partially decentralized and can achieve data sharing and low cost. Private chains are managed by a company or institution, and the requirements for joining nodes are very rigorous. In addition, because private chains also use P2P network technology, they are also very good at protecting the integrity of information, etc.

At present, blockchain technology has been applied in ABS and supply chain fields. Many companies and organizations have started the process of exploring the application of blockchain technology. Internet companies generally do Baas (Blockchain as a Service), which is generally an enterprise-level blockchain platform based on cloud servers that can be quickly deployed and accessed, and can support public chains, alliance chains and private chains. There are now many enterprise-level BaaS, such as Ping An Group's "One Account Chain baas". In addition to financial application scenarios, Ping An Group's Financial One Account Chain also has multiple application scenarios such as medical, automotive, real estate and smart city. Tencent TBaaS (Tecent blockchain as a Service) uses a federated chain mechanism with Hyperledger Fabric and FISCO BCOS as the underlying layer. The BaaS platform developed by IBM: IBM Blockchain Platform, supports Walmart's food safety and food traceability in the supply chain food procurement.

6 Digital currency in practice: the example of Bitcoin

6.1 Bitcoin's Launch

In 2008, against the backdrop of the global financial crisis, Satoshi Nakamoto, under the pseudonym Satoshi Nakamoto, published a paper entitled Bitcoin: A Peer-to-Peer Electronic Cash System, describing the emergence of Bitcoin and its algorithm. Following the 2009 launch of the Bitcoin software, Bitcoin was sought after by many internet users for its blockchain characteristics, which allowed for peer-to-peer transfers (decentralized, no central bank), worldwide circulation (internet-based), exclusive ownership (private key), limited quantity (scarcity), low transaction fees, no hidden costs, and cross-platform mining.

The core technology behind Bitcoin is the use of the blockchain, a virtual form of currency that can be transferred peer-to-peer from a third party and is based on a voting mechanism, due to its It is a virtual currency based on a voting mechanism, which is highly secure (due to the voting mechanism), anonymous, globally mobile and free from regulation (the market was not perfect at the time of the emergence of the new thing). Bitcoins are tokens and can be exchanged for bitcoins using credit currencies for trading purposes. Confidence in Bitcoin is also driven by its scarcity and global liquidity.

Bitcoins are issued through "mining", where miners calculate a target hash through a computer and are rewarded with the right to keep track of it. Bitcoins are issued on a one-dollar basis, with a privately designed algorithm being used to issue the currency over the internet and directly to users.

Bitcoin is issued in a monolithic manner, which is more efficient and transparent, but as a national fiat currency it has drawbacks and requires an independent issuer and storage institution to serve the financial system.

6.2 The Operation of Bitcoin

Bitcoin operates in a decentralized manner, with users transferring bitcoins anonymously through peer-to-peer network technology, but the relationship with the issuer is not monolithic or binary, as the issuer only designs the algorithm for the

currency and does not provide savings or other functions, so there is a need for specialized institutions or nodes to provide services to other users.

From data collected by Yahoo Finance on Bitcoin price changes. As shown in the chart, Bitcoin's price fluctuations are influenced by market demand, with the price of Bitcoin showing a general upward trend after 2015, reaching a high point of $20,809 on 17 December 2017, with some exchanges likely to be priced at no more than $20,000. Bitcoin then fluctuated significantly in 2018, with the price falling by 13.37% on 19 November 2018 with the introduction of government regulation and the impact of negative news. The bitcoin price has subsequently remained around $4,000. The COVID-19 pandemic shut down the economy in 2020. The cost of bitcoin skyrocketed once more. At the beginning of the year, bitcoin was worth $6,965.72. Investor worries about the state of the world economy were stoked by the pandemic shutdown and the government initiatives that followed, which hastened bitcoin's growth. Bitcoin once more reached an all-time high of $68,789 in November 2021. Later, as inflationary uncertainty and the advent of a new COVID-19 model, Omicron continued to worry investors, and the price started to vary significantly. The price of bitcoin continued to slowly decline over the first half of 2022, dropping to $28,305 on May 11. The price of the cryptocurrency crashed on June 13. For the first time since December 2020, the price of bitcoin drops below $23,000.

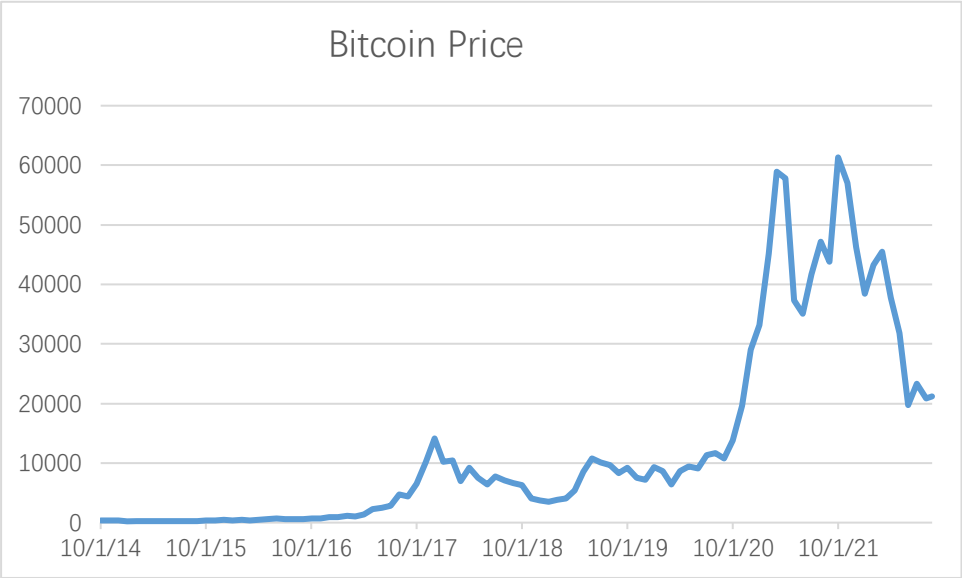

Figure 3: Bitcoin price chart

As can be seen from the operation of Bitcoin, s private digital currency issuance that lacks the backing of state credit has an unstable value stable, and therefore the issuance of digital currencies properly combined with state power can make the operation of digital currencies more stable.

6.3 Regulation of Bitcoin

According to Blockchain.com, 19 million bitcoins have been mined and less than 2 million have yet to be mined. According to the Wall Street Journal (Vigna, 2019), 95 per cent of recorded bitcoin transactions are made on unregulated exchanges and are artificial rather than real, a report that has undermined confidence in bitcoin and revealed that some exchanges have engaged in counterfeiting to make a profit, after trading in CBOE bitcoin futures was suspended because the underlying had shrunk too much, and its value was unstable. Bitcoin price volatility should be a detriment to merchants, but there are many merchants around the world who are willing to take the risk of bitcoin price volatility, and some industry giants accept bitcoin payments, such as Microsoft, Dell, Overstock, and others. Bitcoin payments were first accepted on the internet from around 2011, according to internet sources, initially by VPS and VPN service companies, then in March 2013, name cheap started accepting bitcoin for domain names; in 2013, US retail giant Overstock started accepting bitcoin; in 2014, Microsoft started accepting bitcoin payments, and has since tentatively accepted bitcoin several times due to its unstable value, before restarting bitcoin payments in early 2018; since then there have been businesses joining the bitcoin payment army, and in 2019, Starbucks also began accepting bitcoin payments.

As a private digital currency, it attracts investors under the banner of decentralised, anonymous transactions and circumvents regulation, and is inevitably subject to government sniping, and unsurprisingly, the Chinese government has taken a strong regulatory stance on private digital currencies to protect the interests of investors. In terms of Bitcoin regulation, three countries - China, Ecuador and Bolivia - have adopted a strong regulatory stance towards Bitcoin, while many of the more financially developed regions such as North America, most of South America, Australia and Japan and South Korea are more tolerant of Bitcoin (Schaupp and Festa, 2018). The attitude of some less developed regions such as Africa, Central Asia and Outer Mongolia towards Bitcoin regulation is unknown, and countries such as Russia, Kazakhstan and India have controversial attitudes towards Bitcoin.

At present, the regulation of Bitcoin in various countries is mainly focused on access, circulation and ICOs. We should design the regulatory framework and circulation process from the perspective of the security of the digital currency itself, and at the same time, as the transaction records of the digital currency are more easily readable, we should focus on illegal and criminal acts in conjunction with big data.

6.4 Functional Analysis of Bitcoin

Bitcoin is a special commodity, an organic unity of use value and value. Bitcoin is special because it was designed to be a medium of exchange, i.e. it was designed to be a currency. Bitcoin's monetary function: Money generally has five functions: a

medium of exchange, a measure of value, a means of storage and a means of payment; a medium of exchange: With the development of Bitcoin, although historically the price of Bitcoin has not been stable, there has been a large number of companies accepting Bitcoin payments in areas such as department stores, computers, internet services and restaurants, and more companies are joining the Bitcoin payments are made with reference to the real-time price of bitcoin, and goods are denominated in US dollars, with reference to the real-time US dollar price of bitcoin, and are then paid in bitcoin. Value scales: Bitcoin prices are relatively volatile and it is unrealistic to use Bitcoin for valuation purposes. Storage: As a means of storage for currency, the value of a currency should be relatively stable. Means of payment: It is possible to use bitcoin as a means of payment, and to make bitcoin deliveries with reference to the real-time price of bitcoin. World currency:The technology behind Bitcoin allows it to be a world currency, with global mobility, online P2P transactions, regulatory avoidance, cryptographic encryption for security, and network-wide node justice.

According to the statistic of bitcoin ATM Radar, there are 36,659 Bitcoin ATMs operating in the United States as of April 2022. By 2020, 28% of small companies in America will accept cryptocurrencies as payment. In the United States, there were over 260,000 Bitcoin transactions daily as of May 2022. Over $1 million being spent using Bitcoin every single day in the United States on products and services. As the number of merchants accepting Bitcoin payments increases, Bitcoin's function as a medium of exchange grows. Bitcoin is a special commodity, but because of its unstable value, it is not yet fully accepted as a general equivalent. Although Bitcoin is a currency and can support transactions to a certain extent, there is an insurmountable gap between it and a real currency - legal tender - and without the backing of state credit, Bitcoin is unstable, without state coercion to guarantee circulation, and without the trust of the people.

The value of private digital currencies such as Bitcoin is not as stable as that of commodities such as gold, and not as stable as that of fiat currencies backed by state credit, so they are not suitable as a medium of exchange and can be considered as an investment. It has the same basic value, unlimited legal compensation, and trust, but also the advantages over physical fiat money: reduced costs (circulation costs, settlement costs), increased liquidity, etc.

7 Designing the Operational Framework of a Fait Digital Currency

7.1 Issuing Mechanism of Fait Digital Currency

There are basically two types of issuance mechanisms for digital currencies, one is direct issuance, where the central bank issues directly to public accounts or wallets, which is a monolithic issuance structure (Qiao, Wang and Xie, 2018). The other is indirect issuance, where the central bank issues to public accounts or wallets through commercial banks, which is a binary issuance structure (Yao, 2018). The unilateral issuance structure will change the functions of the central bank and will have a certain impact on the traditional banking structure, as well as on commercial banks. The Central Bank's Institute of Monetary and Digital Studies is currently focusing on the binary issuance structure for digital currencies.

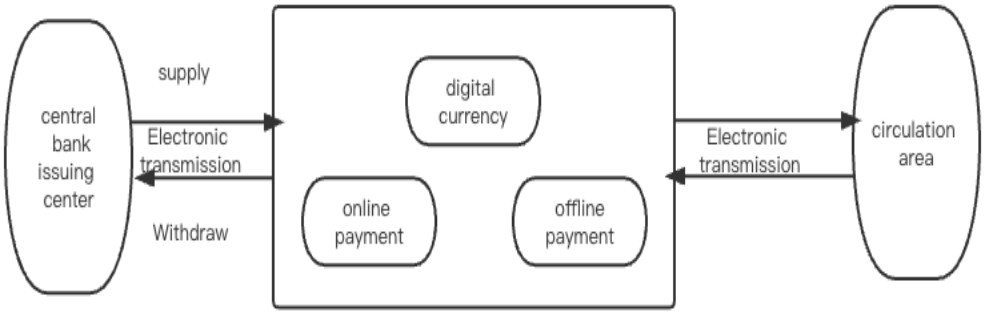

Figure 4: The Design of a monolithic issuance structure for Fait Digital Currency Issuance (Qiao, Wang and Xie, 2018)

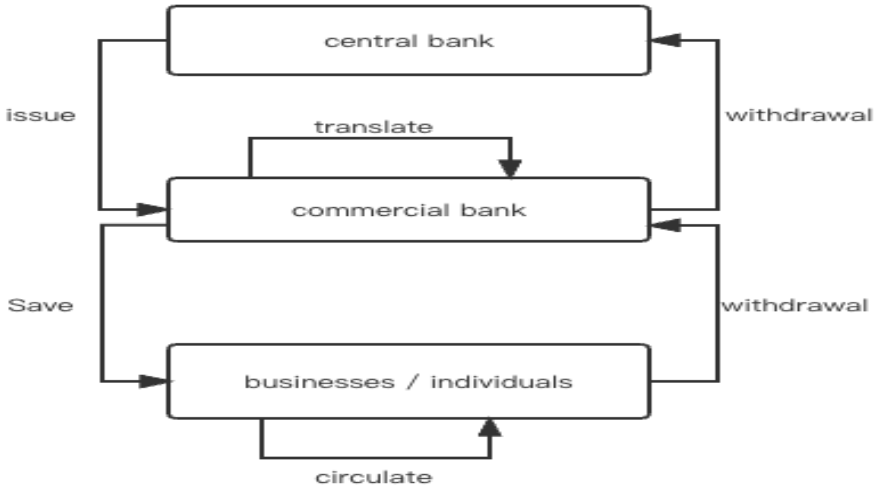

Figure 5 Binary operating system of central bank digital currency (Yao, 2018)

In principle, there are two types of legal digital currency issuance: monolithic and binary, but the monolithic approach ignores the independence of the central bank in the financial system, and if a monolithic credit issuance system is adopted, the position of commercial banks will be weakened and their role in the financial system will become very limited, contrary to the requirements of professionalism.

Therefore, the scholars are more likely to consider a binary credit issuance system, which can make full use of the existing financial architecture. Digital currency accounts are used for large online transactions, while digital currency wallets are used for small online and offline transactions.

7.2 The circulation mechanism of fait digital currency

According to the credit issuance model of digital currency, the circulation mechanism of digital currency can also be divided into monolithic and binary, and both monolithic and binary are divided into "centralized" and "decentralized" models. In the "centralized" circulation model, the digital currency in circulation has a manager, while in the "decentralized" circulation model, central banks and payment institutions only act as the maintainers of the payment system, and the digital currency circulation system uses blockchain technology to automatically transfer money between different individuals. The literature on digital currencies by researchers from the Central Bank's Digital Currency Research Institute (DCRI), including Qian Yao, suggests that the DCRI's design of a legal digital currency is necessarily centralized and binary. This paper argues that a binary centralized structure should be adopted for the circulation of digital currencies.

7.2.1 The circulation mechanism of fait digital currency

Credit currencies are traded online using electronic payment methods, i.e. through bank accounts or third parties such as WeChat or Alipay, and offline using direct transactions such as banknotes, which are carried daily and stored in wallets and other media.

To summarise: online transactions are conducted using third party participation models, offline transactions are conducted using peer-to-peer transmission, and preservation etc. is done through physical media. Digital currencies are different from credit currencies in that they have no physical form and can only be stored on a storage medium, so offline transactions need to be carried out using secure devices.

In addition, due to the development of infrastructure in recent years, public transport in many cities such as buses and subways support NFC devices for payment, so the issuance of digital wallets by the central bank, combined with existing NFC technology, can greatly improve payment efficiency. There are two broad design ideas for how offline transactions can be carried out: one is similar to the current currency in circulation, except that it is stored electronically, and the other is to combine it with other communication technologies (such as satellite communication technology) to build a blockchain for data preservation and monitoring.

7.2.2 The definition of fait digital currency circulation binary credit system

If blockchain is used, the decentralization of blockchain and the distributed ledger make transactions more stable, but there are still several issues to be discussed. If blockchain technology is not adopted, the traditional three-party transaction model is also acceptable because the traditional transaction model is more mature at present. We only need to design some intermediate links of the transaction to make the transaction more intelligent and convenient.

However, because of the strong anonymity of public chains, it is more difficult to supervise and trace back illegal transactions, and it is more appropriate to use coalition chains. The existing commercial banking system, on the one hand, can help the central government maintain the independence of the central bank and make monetary policy more independent. On the other hand, it can form a healthy competition mechanism, which can improve the efficiency of the banking industry. Regardless of whether we adopt blockchain technology as the design of online digital currency transactions or not, the role played by commercial banks in facilitating

transactions must be taken seriously. Commercial banks must be involved in the transaction chain, and there is no clear answer as to what role they play in it. The network latency between different regions will be very high because of the network environment, and because the management of different outlets will affect the settlement of the outlets if they are united, so the broadcast time between the nodes within the network will become very long and affect the settlement efficiency.

The issuance of digital wallets should be authorized by the People's Bank of China(China's central bank) to commercial banks. The People's Bank of China should issue a document regulating the specifications of digital wallets. Digital wallets should not be issued directly by the central bank, as they should not be collected anonymously by entities and individuals. This could lead to unnecessary problems for the relevant authorities in the event of a forensic search. The overall design should be such that digital wallets can be traded online or offline, as offline trading must be unavoidable: the current network coverage in China is not 100%, and there are still some areas with weak signals. There is also no need for online transactions for small transactions, nor is there a need for online operations. However, digital wallets must be real name based, and should be issued with the authorization of commercial banks, who authorise them by binding user information and hardware ids.

Given that the issuance of digital wallets is a fundamental part of the central bank's digital currency, in addition to being a very low-level and security-critical part, the central bank should carry out unified management. The second is that the central government should design and produce the digital wallet system, maintain the security of the digital wallet system and the digital wallet, and maintain the security of user funds. The central bank will design and produce the digital purse system, maintain the security of the digital purse system and the digital purse, and maintain the security of users' funds. The third option is for the central bank to issue a policy on digital currency wallets to regulate the requirements (including stability, security, practicality, etc.), and for commercial banks to customize the hardware and software and submit them to an independent department of the central bank for testing after the development is completed.

Each of these design ideas has its own merits: The first one gives commercial banks sufficient authority, but the strength of commercial banks varies, and there is certainly not enough work done to ensure the security of funds; the second option is for the central bank to take the lead in the design and development of the digital wallet and for commercial banks to customize it. The third option is for the central bank to set up a separate department to interface with commercial banks, which can individually design, develop and personalize the digital wallets but then hand them over to the central bank for system stability and security testing. On the one hand, the central bank only needs to promulgate rules and monitor the results to ensure the safety and reliability of the digital wallet; on the other hand, it gives commercial banks sufficient authority and incentive to innovate in digital wallets. As long as commercial banks are

hardworking and intelligent enough, the digital wallets they design will certainly be more popular with users. Then they will be one step ahead of the competition in the new digital currency era.

7.3 Regulatory mechanisms for fait digital currencies

The current academic debate is on the regulation of private digital currencies, which are different from private digital currencies in that they are sovereign currencies issued by the state and therefore different from private digital currencies in many ways. Therefore, the following points should be noted in the regulation of digital currencies:

Firstly, the security of the digital currency itself is the most basic security. The security of the digital currency itself is the most basic security, and the security and anti-counterfeiting of the digital currency should be reasonably designed to prevent illegal elements from using the counterfeit currency to obtain illegal gains and to protect consumers' rights and interests from being damaged.

Secondly, the regulatory framework of legal digital currency should be improved, the regulatory body should be clear, the regulatory indicators should be selected, and the scale should be adopted in order to combine efficiency and security in the operation of digital currency.

Thirdly, the regulation of anti-money laundering and other illegal acts. The subjects of transactions are anonymous, but the economic activities of anonymous individuals should be able to be analysed when needed, so big data can be used to analyse and focus on unusual transactions.

Fourthly, regulation of global flows. One of the characteristics of digital currencies is that they are prone to global flows, which have an impact on the balance of currencies in the outgoing and incoming countries, thus affecting the stability of the financial system.

8 Conclusions and recommendations

8.1 conclusion

In the history of monetary evolution, each generation of money has been demand-driven and driven by technological progress and habits. The value of private digital currencies is unstable as the issuer is not as creditworthy as the state, and they lack functionality as a medium of exchange. On the basis of private digital currencies, the state, as the issuer of the digital currency, can ensure that the value of the digital currency is stable and that all functions of the currency can be carried out in a stable and orderly manner. From the perspective of monetary development and monetary functions, the development of a legal digital currency is inevitable, and from a technical point of view, blockchain can also be used for certain designs to support the operation of a legal digital currency. In terms of framework, the issuance of digital currency should adopt a binary issuance structure to make full use of the current monetary system, and the circulation should also adopt a binary circulation method.

The emergence of digital currencies has given us an intuitive understanding of them, and academics have been conducting research on them. In addition, research into the framework of a fiat digital currency is underway and, with the support of new technologies, the design of the operational framework of a fiat digital currency will certainly be superior to that of the previous generation of currencies.

8.2 Recommendation on policy

8.2.1 Steadily promoting the integration of the central bank's digital currency system

The foundation for enhancing the capabilities of the central bank's digital currency and allowing its use is the creation of a digital financial system that combines and interacts with financial stability, technical innovation, and application. It is crucial to have an open mind and an impartial posture toward the technology of digital currencies when building the integration system. It is also essential to monitor any dangers and offer pre-determined solutions.

Firstly, the top-level design of the central bank's digital currency should be strengthened, especially the scientific definition of the conceptual scope, payment framework and usage model. The second is to improve the system application for the operation of legal digital currency. Third, based on defining the legal status and

regulatory mechanism of the central bank's digital currency, gradually improve the laws and regulations on the issuance, circulation and other technical aspects of the central bank's digital currency, as well as the laws and regulations on civil and commercial matters.

8.2.2 Maintain innovative research and development of the central bank's digital currency technology

The technology underlying the issuance of the central bank's digital currency is still under constant development and progress, so the application of the central bank's digital currency technology must keep pace with the times while maintaining stability and control. Therefore, for the management of the central bank, it is essential not to pre-determine the technological route, to maintain technological neutrality, to set targets only in terms of technical specifications and indicators, and to encourage technological innovation and full competition among the market participants. In short, the central bank's digital currency should maintain continuous research and innovation in three areas: system architecture, security and stability, and functional extension.

8.2.3 Increase the publicity and education on the security application of the central bank's digital currency

For academic institutions and government agencies, central bank digital currency is a new concept; for the public, it is much more novel.

Therefore, the preconditions for achieving good economic and social effects in the issuance and circulation of the central bank's digital currency in the future are two aspects; on the one hand, it is necessary to ensure the reliability and stability of the central bank's digital currency from the technical and institutional point of view. On the other hand, the central bank's digital currency and the current currency are necessarily to be identified and distinguished to improve the people's own awareness of risk prevention by introducing the differences among the existing means and uses of payments.

First, the campaign's content should emphasized the marriage of sweeping story with figurative language. To put it another way, it's critical to promote both the legal and the usage elements. The use of information technology and Internet thinking for publicity should be our second point of attention. Thirdly, offline promotion needs to be improved. The current bank service locations can be used to set up special publicity

and experience areas, and the public can regularly attend lectures on the knowledge of the central bank's digital money on a variety of subjects. Through publicity, the general public will gradually learn how to use the digital currency of the central bank in their daily lives, create awareness of safety precautions, and significantly improve the public's ability to use the digital currency of the central bank safely.

Reference

Al-Laham, M., Al-Tarwneh, H. and Abdallat, N. (2009). Development of Electronic Money and Its Impact on the Central Bank Role and Monetary Policy. *Issues in Informing Science and Information Technology*, 6, pp.339–349. doi:10.28945/1063.

Andolfatto, D. (2018). Assessing the Impact of Central Bank Digital Currency on Private Banks. *Federal Reserve Bank of St. Louis, Working Papers*, 2018(025). doi:10.20955/wp.2018.025.

Asokan, N., Janson, P., Steiner, M. and Waidner, M. (2000). *State of the art in electronic payment systems*. [online] ScienceDirect. Available at: https://www.sciencedirect.com/science/article/pii/S0065245800800091.

Atlantic Council. (n.d.). *CBDC Tracker*. [online] Available at: https://www.atlanticcouncil.org/cbdctracker/ [Accessed Jul. 2022].

Auer, R. and Boehme, R. (2020). The technology of retail central bank digital currency. *BIS Quarterly Review*. [online] Available at: https://www.bis.org/publ/qtrpdf/r_qt2003j.htm.

Auer, R., Frost, J., Gambacorta, L., Monnet, C., Rice, T. and Shin, H.S. (2021). Central bank digital currencies: motives, economic implications and the research frontier. *SSRN Electronic Journal*. [online] doi:10.2139/ssrn.3922836.

Bank, E.C. (2021). Eurosystem launches digital euro project. *www.ecb.europa.eu*. [online] Available at: https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210714~d99198ea23.en.html.

Barrdear, J. and Kumhof, M. (2016). The Macroeconomics of Central Bank Issued Digital Currencies. *SSRN Electronic Journal*. doi:10.2139/ssrn.2811208.

Bilotta, N. (2021). *CBDCs for Dummies: Everything You Need to Know about Central Bank Digital Currency (And Why You Shouldn't Be Afraid of It)*. [online] Available at: https://www.iai.it/sites/default/files/iaip2124.pdf.

Blinder, A.S. and Stiglitz, J.E. (1983). Money, Credit Constraints, and Economic Activity. *The American Economic Review*, 73(2), pp.297–302.

Blockchain.com. (n.d.). *Blockchain Explorer*. [online] Available at: https://www.blockchain.com/explorer.

Bordo, M. and Levin, A. (2017). *Central bank digital currency and the future of monetary policy*. [online] VoxEU.org. Available at: https://voxeu.org/article/benefits-central-bank-digital-currency.

Central Bank of Ireland. (2014). *What are cryptocurrencies like bitcoin?* [online] Available at: https://www.centralbank.ie/consumer-hub/explainers/what-are-cryptocurrencies-like-bitcoin.

Chang, V., Baudier, P., Zhang, H., Xu, Q., Zhang, J. and Arami, M. (2020). How Blockchain can impact financial services – The overview, challenges and recommendations from expert interviewees. *Technological Forecasting and Social Change*, [online] 158, p.120166. doi:10.1016/j.techfore.2020.120166.

Chaum, D. (1983). Blind Signatures for Untraceable Payments. *Advances in Cryptology*, pp.199–203. doi:10.1007/978-1-4757-0602-4_18.

Chaum, D., Grothoff, C. and Moser, T. (2021). How to issue a central bank digital currency. *SSRN Electronic Journal*. doi:10.2139/ssrn.3965032.

Chen, H. and Siklos, P.L. (2022). Central bank digital currency: A review and some macro-financial implications. *SSRN Electronic Journal*. doi:10.2139/ssrn.4023776.

Cunha, P.R., Melo, P. and Sebastião, H. (2021). From Bitcoin to Central Bank Digital Currencies: Making Sense of the Digital Money Revolution. *Future Internet*, 13(7), p.165. doi:10.3390/fi13070165.

European Central Bank (2015). Virtual currency schemes – a further analysis. [online] doi:10.2866/662172.

Farrell, M. (2013). *Bitcoin prices surges as post-Cyprus bailout*. [online] CNNMoney. Available at: https://money.cnn.com/2013/03/28/investing/bitcoin-cyprus/index.html [Accessed Jul. 2022].

FATF (2014). *Virtual currencies – Key Definitions and Potential AML/CFT Risks*. https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf: FINANCIAL ACTION TASK FORCE.

Fung, B.S.C. and Halaburda, H. (2016). Central Bank Digital Currencies: A Framework for Assessing Why and How. *SSRN Electronic Journal*. doi:10.2139/ssrn.2994052.

Graziani, A. and Vale, M. (1997). The Marxist Theory of Money. *International Journal of Political Economy*, [online] 27(2), pp.26–50. Available at: https://www.jstor.org/stable/40470700.

Ikeda, Y. (2008). Carl Menger's monetary theory: A revisionist view. *The European Journal of the History of Economic Thought*, 15(3), pp.455–473. doi:10.1080/09672560802252347.

Keister, T. and Sanches, D. (2019). Should Central Banks Issue Digital Currency? *Working paper (Federal Reserve Bank of Philadelphia)*. doi:10.21799/frbp.wp.2019.26.

Kovanen, A. (2021). Second Thoughts About Central Bank Digital Currencies. *Applied Economics and Finance*, 9(1), p.1. doi:10.11114/aef.v9i1.5434.

Leible, S., Schlager, S., Schubotz, M. and Gipp, B. (2019). A Review on Blockchain Technology and Blockchain Projects Fostering Open Science. *Frontiers in Blockchain*, [online] 2. doi:10.3389/fbloc.2019.00016.

Mancini Griffoli, T., Martinez Peria, M., Agur, I., Ari, A., Kiff, J., Popescu, A. and Rochon, C. (2018). Casting Light on Central Bank Digital Currencies. *Staff Discussion Notes*, 18(08), p.1. doi:10.5089/9781484384572.006.

Menger, K. (1892). On the Origin of Money. *The Economic Journal*, 2(6), p.239. doi:10.2307/2956146.

Miller, A., Kosba, A., Katz, J. and Shi, E. (2015). Nonoutsourceable Scratch-Off Puzzles to Discourage Bitcoin Mining Coalitions. *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. doi:10.1145/2810103.2813621.

Morganti, G., Schiavone, E. and Bondavalli, A. (2018). Risk Assessment of Blockchain Technology. *2018 Eighth Latin-American Symposium on Dependable Computing (LADC)*. [online] doi:10.1109/ladc.2018.00019.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [online] Bitcoin.org. Available at: https://bitcoin.org/en/bitcoin-paper.

Nguyen, Q.K. (2016). Blockchain - A Financial Technology for Future Sustainable Development. *2016 3rd International Conference on Green Technology and Sustainable Development (GTSD)*. doi:10.1109/gtsd.2016.22.

Qiao, H.S., Wang, P. and Xie, S.S. (2018). Digital Legal Tender: Issue Logic and Substitution Effect. *South China Finance*, pp.73–79.

Schaupp, L.C. and Festa, M. (2018). Cryptocurrency adoption and the road to regulation. *Proceedings of the 19th Annual International Conference on Digital*

Government Research Governance in the Data Age - dgo '18. doi:10.1145/3209281.3209336.

Snell, D.C. (1982). *Ledgers and prices : early Mesopotamian merchant accounts*. New Haven: Yale University Press.

Tobin, J. (1987). A Case for Preserving Regulatory Distinctions. *Challenge*, 30(5), pp.10–17. doi:10.1080/05775132.1987.11471196.

Venter, H. (2016). *Digital currency -A case for standard setting activity. A perspective by the Australian Accounting Standards Board (AASB)*. [online] Available at: https://aasb.gov.au/admin/file/content102/c3/AASB_ASAF_DigitalCurrency.pdf.

Vigna, P. (2019). Most Bitcoin Trading Faked by Unregulated Exchanges, Study Finds. *Wall Street Journal*. [online] 22 Mar. Available at: https://www.wsj.com/articles/most-bitcoin-trading-faked-by-unregulated-exchanges-study-finds-11553259600 [Accessed Aug. 2022].

Yaga, D., Mell, P., Roby, N. and Scarfone, K. (2018). Blockchain technology overview. *National Institute of Standards and Technology*. [online] doi:10.6028/nist.ir.8202.

Yao, Q. (2018). A systematic framework to understand central bank digital currency. *Science China Information Sciences*, 61(3). doi:10.1007/s11432-017-9294-5.

Yao, Q. (2018). Experimental Study on Prototype System of Central Bank Digital Currency. *Journal of Software*. [online] doi:10.13328/j.cnki.jos.005595.