Trust, Currency, and Science: The Rise of the Fintech and Token Economy

Linqi Han[1]

[1]Department of Computer Science, Hangzhou Dianzi University, Hangzhou, Zhejiang

Abstract—This paper primarily focused on the concept and correlation between the trust mechanism and currency system iterations from the early civilization age till nowadays. Structured as starting from diving into the history and evolution of the "format of the money", by illustrating the changes associated with "TRUST" and "CONVENIENCE" as a timeline, and finally research into the ultimate of the current money - bitcoin and cryptocurrency.

1 INTRODUCTION

During the historical process of the development of the global economy, the currency is playing an important role in the global economy. At a certain level, we are able to recognize world economy iteration history and even world civilization iterations by understanding the evolution of the currency. With the development of the global economy and technology, the existence form of currency is constantly being iterated and taking revolutionary transformations.

2 HISTORY OF CURRENCY

2.1 Barter System and Commodity Currency

A barter system is an ancient method of exchange. The history of barter could be traced back to 6000BC. Barter is the exchange of goods and services without money [1]. Both parties should identify the value of commodities from the other party at first and then barter with each other. Due to swapping by human's subjective standard, humans gradually adopted fixed commodities (e.g., shell, salt, tea) as the role of currency. According to the statistic, at least 2000 commodities had played this role. Later on, gold and silver became the standard for value measurement of money and human beings rely on it to build the further gold standard. While after a long time of using gold as a currency, humans realized that it was very inconvenient to carry large amounts of gold and it was unnecessary for trading to exchange the gold in goldsmith. Hence, humans gradually traded in certificates of metal deposits. The first explicit evidence of representative money dates back to the ancient Chinese empire in which commodity warehouses issued certificates of deposit, guaranteeing the holder has the equivalent portion of the goods stored in the warehouse [2]. Since representative money circulation still depends on the quantity of gold, its endorsement is also in gold. Representative money in itself doesn't have intrinsic value, but it is a certificate of value and wealth.

2.2 Modern Currency

Modern currencies mainly consist of fiat. Fiat money is different from commodity money and representative money. Fiat takes national sovereign credit as currency and no longer relies on the gold standard and issued by the central bank according to the variation in the financial market. Since fiat is not a scarce or fixed resource as gold, central banks have much greater control over its supply, which provides governments the power to manage economic variables such as credit supply, liquidity, interest rates, and money velocity [3].

2.3 Digital Currency

In January 2009, the bitcoin was launched - a new form of peer-to-peer currency had emerged -- Digital Money. Digital money is a series of numbers as physical attributes. In the transaction, it flows online between the traders. There are two main forms of digital currency, the most common form is the cryptocurrency, including Bitcoin, Ethereum, Litecoin, and Ripple, and the other one is the digital currency issued by the central bank.

From barter to commodity money, from representative Money that depended on the gold standard to Fiat Money backed by national credit. In the Internet era, we develop digital currency backed by mathematical algorithms [4]. Money emerged from a simple exchange. Its form and endorsement have been evolving with the development of trade and technology. However, the essence of currency has never changed. That is to build trust between people. When trust between people can be fully established through money, then we can build a truly shared and trust society.

hanlinqi@hdu.edu.cn

3 RISE OF TRUST AND CRYPTOGRAPHY

3.1 Traditional Trading System Drawback

Banks are the main credit intermediaries, and clearinghouses are the credit basics between merchants and consumers. The existence of central clearinghouses can eliminate risks in transactions and enable market participants to conduct better transactions and enhance market liquidity. However, the traditional clearing system has several disadvantages:

3.1.1 The remittance speed is slow. A cross-border business needs to go through at least two Banks and one transfer bank to reach the designated account. But each bank has its settlement and clearing system, so the settlement time will be prolonged.

3.1.2 The remittance fee is high. Since the cross-border transfer involves the transferring bank, which will charge certain fees and procedures.

3.1.3 Low transparency. As each bank has its independent core system, customers are unable to check information in time, which leads to the inconvenience of payment information communication.

3.1.4 Poor privacy. Since the customer's information needs to be completely handed over to all banks in the remittance path, it is easy to lead to the disclosure of the user's information.

3.2 Cryptographic Algorithm

In order to effectively protect the privacy of information, mathematical algorithms have gradually become the foundation of human being's trust and gradually developed into cryptography. Like ancient Egypt, Ancient Rome, ancient Greece and other ancient civilizations began to use cryptographic technology to protect the confidentiality of information. About 4,000 years later, modern cryptography was gradually established, introducing a more rigorous mathematical definition of asymmetry. At the end of the 20th century, with the popularization of the Internet, a large amount of sensitive data was transmitted on the network. There is a growing need to protect data, and cryptography technology also develops rapidly. There are three types of mainstream encryption algorithms [5].

The first algorithm is symmetric encryption, which uses a single key for both encryption and decryption. Symmetric Ciphers are divided into Stream and Block Ciphers. Stream Ciphers encrypts a single bit of plain text at a time. Block Ciphers takes several bits and encrypts them as a single unit. Primarily used for privacy and confidentiality. The second algorithm is asymmetrical encryption, which uses one key for encryption and another for decryption. The encryption key is public information and the decryption key will be kept as secret. And the last is the Hash Function, which uses a mathematical transformation to irreversibly "encrypt" information, providing a digital fingerprint. Primarily used for message integrity.

The reason why cryptography can make people trust and protect users' privacy is based on the theory of computational difficulty. In the privacy protection scenario, the computing difficulty theory is that for the same private data subject, the degree of difficulty for getting the same result by different computing has asymmetry. In asymmetry, relatively easy computing is used to construct authorized data access, while difficult computing is used to avoid unauthorized data leakage.

Due to the unique advantages of cryptography, it appeared in many application scenarios around us. The most typical application is the Instant Message (IM). For encrypted IM applications, the most important is security. Nowadays, the RSA encryption and Advanced Encryption Standard (AES) of crypto methods are the most popular and safe. Telegram and Signal both use end-to-end encryption. RSA and AES encryption methods are also used. And Signal also uses the Transport Layer Security (TLS) encryption during transmission. It means that a layer of encryption is added at the transport end. Even if someone cracks the encryption of the ciphertext, they just get the messy code that was previously encrypted by RSA and AES. Besides, Crait is also mainly designed for secure encrypted chatting. It uses the TLS encryption during transmission and for the client, RSA and AES were used for double encryption.

4 CONSENSUS IN BLOCKCHAIN

The consensus mechanism is the voting of special nodes in the blockchain, which can complete the verification and confirmation of transactions in a short time. If several nodes with unrelated interests can agree on a deal, we can assume that the whole network can also agree on it. The consensus algorithm is essentially a rule that each node uses this rule to validate its data.

4.1 Proof of Work

The Proof of Work (PoW) is probably one of the most common consensus algorithms. Essentially, PoW requires members of a community to solve challenging puzzles. This work builds on previous puzzle solutions. As a result, PoW is a way of verifying current and past transactions. Additionally, the work that goes into solving the puzzle generates rewards for whoever solves it. In the world of cryptocurrency, that's basically what "mining" is. And there are some advantages to PoW. As it's very hard to do the work, PoW reduces the risk of a 51% attack. At the same time, each solution is easy for the community to verify. This makes it easy to check all transactions for trustworthiness.

4.2 Proof of Stake

And the other consensus is Proof of Stake (PoS). The proof of stake was created as an alternative to the proof of work. PoS is that a person can mine or validate block transactions according to how many coins he or she holds. This means

that the more bitcoin or altcoin owned by a miner, the more mining power he has. Proof of Stake is seen as less risky in terms of the potential for miners to attack the network, as it structures compensation in a way that makes an attack less advantageous for the miner.

All transactions in the bitcoin's network were clearly recorded on the blockchain. Although it was stated as anonymity, this is not completely anonymous. It belongs to the Anonymous Public, which means that all the currency transaction details are opened and can be consulted. But this "public anonymous" does not guarantee full privacy, which is also one of bitcoin's main drawbacks.

4.3 Zero-Knowledge

In order to solve this problem, we have to mention the breakthrough of Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARKs). Zero-Knowledge means that a certifier is able to convince the verifier that an assertion is true without providing any useful information to the verifier [6]. Non-Interactive means that after the certifier submits the proof, the verifier will not reveal what the wrong information is. Argument means that certifiers who possess enough computational power can create proofs/arguments about wrong statements to cheat the verifiers.

By using Zero-Knowledge Succinct Non-Interactive Argument of Knowledge, it solves the disadvantage of "public anonymity". Besides, the most important advantage of zero-knowledge proof is that the security of zero-knowledge proof is derived from unsolved mathematical problems (e.g., discrete logarithm, large integer factorization, square root), so the security which based on mathematical problems will not be reduced. Secondly, it has complete secrecy, and it is not necessary to let the verifier know sensitive information in the verification process. Therefore, in the point-to-point cash system, zero-knowledge proof makes complete protection come true. It can automatically conceal the address of the transfer sender and receiver, and even the amount which can only be seen by people with specific permissions. Zero-knowledge proof brings complete anonymity to cryptocurrency and reduces risks in the transactions. Thus, it has a great development prospect in the future. Through the combination of blockchain, it provides secure super-platform protection for everyone.

In order to make consensus more efficient in blockchain distributed systems and make blockchain operate normally, the consensus mechanism plays a decisive role in it. As the core element of blockchain technology, the design of the consensus mechanism determines the degree of scalability, security, and decentralization of the system. And if we have a better consensus mechanism, the system can bear more complex applications and adapt to a wider range of applications

5 Trigger of the Fintech Revolution

Fintech, the abbreviation for financial technology, is a broad category that refers to the innovative use of technology in the design and delivery of financial services and products [7].

In recent years, with the continuous improvement of science and technology, the function and influence of technology on financial innovation has been paid high attention and widely concerned by society. From the definition of the Financial Council in 2016, it can be shown that fintech has been given a new definition. The technology brings about financial innovation and also generates new business models, applications, processes, and products produced. Fintech has a significant impact on the financial market, financial institutions, and the way in which financial services are provided. Fintech has several typical characteristics:

Technological foundation. Technology is the key to promoting the development of fintech. There are some technologies in the past, such as databases and networks. However, in the past, technological iterations were very slow. After decades of innovation and development, the speed of technological iteration has become faster and stronger. At the same time, new technologies are emerging one after another.

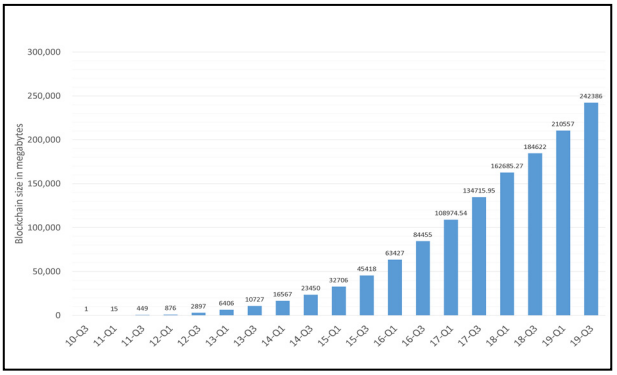

Figure 1. Size of the Bitcoin blockchain

New technologies such as artificial intelligence, blockchain, cloud computing, and big data have further promoted the development of fintech. In the fig1, we can find that from 2010 to 2019, the scale of blockchain was getting larger and larger.

Diversification of subjects participating. Except for financial institutions, internet companies, third-party payment companies, and even big data and credit investment companies can all participate in the fintech revolution.

Large-scale service targets. In the past, finance mainly services customer groups with a certain amount of assets, and the number of services was limited, but in pushing ahead with technology, financial companies can extend the scope of services and effectively expand the service radius to cover more customer groups.

Fintech involves all aspects of society and people's lives, including alternative lending, capital market, consumer finance, digital assets, financial services IT, insurtech, payment, money transfer, regtech, wealth-tech, and other relevant industries. For example, Neo-banking emerged about 5 years ago, namely in the UK through FinTech players such as Monzo and Atom Bank, which is a new type of digital bank that exists without any branches. Neo Banks are reinventing the practices and processes associated with traditional banking [8].

6 THE VALUE, BENEFITS AND ESSENTIALNESS OF DIGITAL CURRENCY

With the development of financial technology, the form of currency is constantly changing. In the modern banking system, electronic currency is the main body of currency circulation, and the bank is a centralized institution to provide credit. It is currently based on the dual system of central banks and commercial banks. The cost of payment and clearing is very high. With the distributed network technology becoming mature gradually and the cryptography theory gradually perfect, the digital currency has emerged. Digital currency and electronic currency are essentially different. Digital currency is endorsed by algorithms as credit and doesn't depend on central institutions. In addition, the digital currency can solve the problem of credibility and double cost and make value transfer come true by point-to-point.

As a product of the combination of financial innovation and technological innovation, the generation and development of digital currency are closely related to the deficiencies of the existing monetary system. In spite of legal digital currency or illegal digital currency, it eventually will produce a reliable, credible and transparent currency system after combining with blockchain technology. Since this new currency system completely adopts digital circulation, it can settle instantly, optimize liquidity, reduce extra fees in complicated settlement processes and counterparty risks. The merchants can make full use of it to achieve specific economic or policy goals. In the fig2, we can find that although there was a brief decline of the bitcoin volume, bitcoin market cap keeps growing in 2020.

In April 2020, the Libra 2.0 white paper was released, Libra is a cryptocurrency created by Facebook, intended to be used as a simple, low-fee medium of exchange to be used around the world. The goal of Libra cryptocurrency is to become a mainstream digital currency that can be used by anyone.

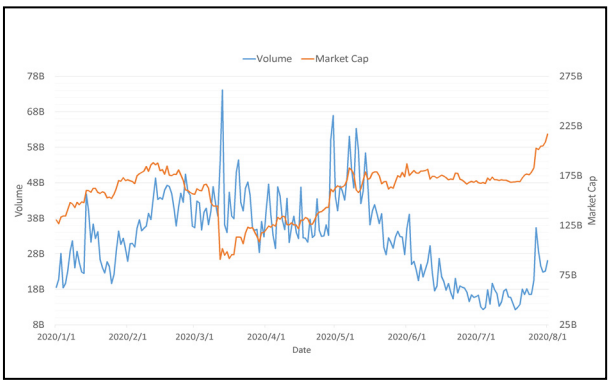

Figure 2. Bitcoin Historical Data

By charging much cheaper fees than other money sending services, utilizing blockchain technology, and holding the value of the currency stable, the Libra initiative wants to provide better, cheaper, and more open access to financial services for all [9].

7 REGULATION AND FIAT ANCHORING STABLE COIN

7.1 The United States

Up to Sep 1, 2020, the US government has taken a positive attitude towards digital currency regulation. On July 9, 2019, the United States Senate approved *Blockchain Promotion Act of 2019*. This Bill was crafted by lawmakers from both parties of the US and it unites a wide range of blockchain stakeholders together. Besides, it also developed the blockchain definition and relevant standards at the federal level in the US to better promote the technology innovation, keep the blockchain's leadership of US in the global technology and industrial development. On July 26, 2020, the federal court in the United States has for the first time define digital currencies such as Bitcoin as "money", which shows a positive attitude to the digital currency. However, America's central bank is still discussing the digital currency policy of issuing, whether it will actually launch remains to be seen.

7.2 England

Up to Sep 1, 2020,, the British government has also taken a positive attitude towards the supervision of digital currency. On January 23, 2019, the UK's Financial Conduct Authority (FCA) published a consultation document on the *Cryptocurrency Asset Guidance*, which outlines a regulatory framework for the cryptocurrency market. Britain's Financial Conduct Authority stressed that tradable tokens would not be regulated for the time being. It is not fiat money under the existing laws of the United Kingdom.

7.3 Singapore

Up to Sep 1, 2020, the Singapore government has also taken a positive attitude towards the supervision of digital currency. On January 14, 2019, *the Payment Services Act* was formally enacted in Singapore, which will directly affect many digital currency exchanges, wallets and OTC platforms in the Singapore market. And it will comprehensively regulate related businesses from the perspectives of risk control and compliance.

Singapore has a positive, comprehensive and transparent view of blockchain and cryptocurrency. Singapore has made clear the regulation of the digital currency business, and it can apply for the corresponding license if it meets relevant regulations. This makes Singapore become one of the few countries with clear supervision of the digital currency business.

7.4 China

Up to Sep 1, 2020, the Chinese government has taken a positive attitude towards the supervision of digital currency. In order to promote the development of the central bank's digital currency, Wang Xin, director of the Research Bureau of the People's Bank of China, said that the central

bank's Digital Currency Research Institute has been set up to develop the system in Shenzhen. The central bank's digital currency, which is defined in China as M0, is an alternative to cash in its way. In 2017, the Institute of Digital Currency of the People's Bank of China was formally established to conduct research on digital currencies. Currently, the China central bank has basically completed the top-level design, standard formulation, functional research, and testing of the legal tender digital currency electronic payment (DCEP). In April 2020, DCEP was first tested in Suzhou, followed by Shenzhen. In the next step, it will steadily promote the introduction and application of the digital form of legal tender.

8 Digital Currency Electronic Payment

The Central Bank of China launched the Digital Currency Electronic Payment (DCEP), which is the Digital Currency and Electronic Payment tool. The functional properties of DCEP are the same as those of paper money, but its form is Digital. It can make value transfer without the users' accounts. The issuance of fiat currency is not necessarily based on blockchain issuance, but it should be issued by the traditional centralized account system of central Banks.

According to the characteristics of the digital currency of the Central Bank of China, the design of the digital currency system follows a two-tier operation system. At the top is the digital currency system of the People's Bank of China, which takes charge of the production, issuance and ownership registration of digital currencies; The second layer is the digital currency system of commercial Banks for the deposit and withdrawal of digital currency; Besides, there also is certification center. It is responsible for IBC certification and CA certification. This can not only use the existing resources to mobilize the enthusiasm of commercial Banks, but also improve the acceptance of the digital currency.

Nowadays, electronic payments are so convenient and widespread, so the primary purpose of central banks issuing digital money is to protect the sovereignty of their own currency and the status of issuing currency. Central Banks around the world have been paying attention to the progress of digital money. Once governments start issuing central bank digital money, the competition of central bank digital money will surely stimulate the current monetary pattern.

9 Insight and Conclusion

Currently, worldwide, paper-cash is less likely to be (notes) used, especially during such a COVID-19 pandemic period, human beings finally realized the necessity of digital platforms and digital payments. Fintech and payments companies have been working to remove friction in the process, complaining about the inconvenience of carrying and using cash. In the past few years, the World Central Bank has been paying significant attention to digital currency. Fifty countries are actively exploring this concept, and some countries have launched pilot projects. The central bank of China recently applied for 84 patents related to digital currency. This suggests that digital money is here to stay. The central bank controls price stability, inflation, and employment to ensure economic growth and job creation while controlling inflation.

Acknowledgment

I thank Kaimin Hu (BitMart Exchange Chief Operating Officer) for discussing several research topics together and making suggestions on the manuscripts.

References

1. K. Anderson, "Guide to the Barter Economy & the Barter System History", Mint. [Online]. Available: https://www.mint.com/barter-system-history-the-past-and-present.
2. Tom, "Representative Money: Advantages and Disadvantages", Lumio | Your Money, 2019. [Online]. Available: https://yourmoney.lumio-app.com/representative-money-advantages-and-disadvantages/.
3. J. CHEN, "Fiat Money", Investopedia, 2020. [Online]. Available: https://www.investopedia.com/terms/f/fiatmoney.asp.
4. Z. Bernard, "Everything you need to know about Bitcoin, its mysterious origins, and the many alleged identities of its creator", Business Insider, 2018. [Online]. Available: https://www.businessinsider.com/bitcoin-history-cryptocurrency-satoshi-nakamoto-2017-12.
5. G. Kessler, "An Overview of Cryptography", *Garykessler.net*, 2020. [Online]. Available: https://www.garykessler.net/library/crypto.html.
6. C. Reitwiessner, "zkSNARKs in a nutshell", Blog.ethereum.org, 2016. [Online]. Available: https://blog.ethereum.org/2016/12/05/zksnarks-in-a-nutshell/.
7. M. Blake, P. Vanham and D. Hughes, "5 things you need to know about fintech", World Economic Forum, 2016. [Online]. Available: https://www.weforum.org/agenda/2016/04/5-things-you-need-to-know-about-fintech.
8. CrowdfundUP Team, "What is a Neo Bank and how are they disrupting traditional banking models?", Medium, 2018. [Online]. Available: https://medium.com/crowdfundup/what-is-a-neo-bank-and-how-are-they-disrupting-traditional-banking-models-3c1b2fa5b8e1.
9. "Libra Cryptocurrency - Overvioew, How It Works, Purpose", Corporate Finance Institute. [Online]. Available: https://corporatefinanceinstitute.com/resources/knowledge/finance/libra-cryptocurrency/.