Research on Digital Currency Supervision Model Based on Blockchain Technology

Jie Li¹, Yansheng Chen¹*, Huitong Song²

¹Guangdong Industry Polytechnic, Guangzhou, China, 510300
²Macau University of Science and Technology School of Business, Macau, China, 999078

*Corresponding author e-mail: yansheng@must.edu.mo

Abstract. With the rapid iterative development of computer information technology, financial technology is also constantly innovating. In this context, the digital currency which should be used in blockchain technology has been developed and popularized rapidly. However, effective supervision of digital currency has become a big problem in the rapid development of blockchain and digital currency. Based on this, this paper first studies the blockchain technology and application, analyzes the technology principle and application of blockchain, secondly, analyzes the digital currency supervision model based on blockchain technology, and studies the necessity of the construction of the supervision system and the strategy of supervision.

Keywords: Digital Currency Supervision, Blockchain Technology, Computer

1. Introduction

With the rapid iterative development of social economy and the continuous change of financial technology, digital currency has become the focus and hot spot of domestic and foreign financial institutions and central banks[1]. The development of digital currency is related to several factors as shown in Figure 1 below, and is affected by the policy supervision system.

![Figure 1](image-url)  

Figure 1. The development factors of digital currency.

Based on the current theoretical and technical basis of digital currency and the existing regulatory model, risk analysis of digital currency is of great value for ensuring the financial stability of digital
currency and analyzing the impact of monitoring model on monetary policy. On the other hand, the anonymity and decentralization characteristics of blockchain technology make it have a wide range of application potential and development prospects. With the continuous iteration of consensus mechanism algorithm, a large number of digital tokens have been produced, which greatly expands the transaction scale and selectivity of token market.

In addition, with the development of blockchain technology and the deepening of its application scenarios, the role of its functional voucher is also widely used, and based on the different application scenarios, the meaning and function of digital token are also significantly different. Under the condition of network globalization, the globalization of virtual currency has been significantly enhanced. With the deepening of digital currency circulation, countries have generally strengthened the supervision of digital currency, so as to reduce its harmfulness as far as possible. Therefore, the research of digital currency supervision model based on blockchain technology has important practical value.

2. Research on blockchain technology and application

2.1. Background of blockchain technology

The current monetary credit needs to be established and maintained through a center. For example, money is based on the central bank\[2\]. However, there are some typical problems and deficiencies in currency centralization, which are embodied in the following aspects. First of all, once the center of the centralized credit system goes wrong, the credit system will collapse completely and it is difficult to save it. Secondly, the centralized credit system is opaque and lack of supervision. In addition, the centralized credit system also has the problem of high cost. All transactions between people should be based on the credit of the other party to complete various transaction processes. In this context, bitcoin, which is not controlled by the central bank and any financial institutions, was born, and its underlying layer adopted blockchain technology. Blockchain technology has several typical characteristics as shown in Figure 2.

![Figure 2](image_url)

**Figure 2.** Typical characteristics of blockchain technology.

2.2. Working principle of blockchain technology

Blockchain is based on a kind of cryptographic calculation, which allows nodes in the whole network to compete for bookkeeping right randomly, and the nodes competing for the accounting right will be rewarded with bitcoin, and the account book after recording will be released to all nodes of the whole network for saving\[3\]. The important elements in the blockchain mainly include several aspects as shown in Table 1 below. It can be seen that the essence of blockchain technology is to establish a completely distributed database independent of any center through cryptography.

In addition, the distributed accounting of blockchain technology makes the accounting responsibility decentralized. The distributed transmission makes every exchange spread to all nodes in the network, and its distributed storage makes the data information highly fault-tolerant.
Table 1. The important elements in the blockchain.

| Elements             | Contents                                                                 |
|----------------------|--------------------------------------------------------------------------|
| Public key           | Each node has a public key                                               |
| Private key          | Identification of public key                                             |
| Transaction          | Payment between nodes                                                   |
| Block                | The transaction is packaged into a block                                 |
| Blockchain           | All data is tamperable                                                   |
| Bookkeeping right    | Package and time stamp the deal                                          |
| Consensus mechanism  | Algorithm to generate and update data                                   |

2.3. Network architecture of blockchain
For the public blockchain, the nodes in the network can access at will, the data read and write permissions in the network are not restricted, anyone can participate in the consensus process, and digital currency is a typical public chain\(^4\). For private blockchain, consensus mechanism, verification, reading and other behaviors are limited to a scope, controlled by an entity, and only open to the internal entity. The alliance blockchain is between the public chain and the private chain, which is more in line with most industry scenarios. It is moderately open to the outside world and is highly praised by more fields.

2.4. Advantages of blockchain
Blockchain has the following typical advantages. First of all, it is fully distributed, any node downtime will not lead to network crash. Secondly, it can accept the transaction of the other party. In addition, it also reduces transaction costs to a great extent, and improves the reliability and unforgeability of transactions. In addition, it also has the typical characteristics of privacy. It can obtain the encryption of the transaction and guarantee the privacy of the transaction without the other party's credit. Blockchain is a general term for a series of technologies, and it was born with digital currency. As a revolutionary technology of the Internet, its influence is far greater than digital currency itself.

2.5. Core technology and application of blockchain
The underlying structure of the blockchain is peer-to-peer network, as shown in Figure 3 below. All nodes are treated as leaves of a binary tree\(^5\). The location of each node is uniquely determined by the shortest prefix of its ID value. For any node, the binary tree can be decomposed into a series of continuous trees without its own subtrees. Each node knows at least one node in the subtree. Digital currency transaction records are stored in data blocks, each block generally includes block header and block body. The difficulty value field will be adjusted according to the average generation time of blocks in the previous period to cope with the changing total calculation amount of the whole network. If the total calculation amount increases, the system will increase the difficulty value of mathematical problems, so that the expected completion time of the next block is within a certain time.
2.5.1. Blockchain network
In the same period of time, more than one node in the whole network can calculate the random number, that is, multiple nodes broadcast their own packaged temporary blocks in the network[6]. If a node receives multiple subsequent temporary blocks for the same preceding block, it will establish branches on the local blockchain, and multiple temporary blocks correspond to multiple branches, as shown in Figure 4 below. If the deadlock is broken until the next workload proof is found, and one of the chains is proved to be the longer one, then the nodes working on the other branch chain will switch camps and start working on the longer chain. Other branches will be completely abandoned by the network.

2.5.2. Application of blockchain
The distribution of blockchain industry is shown in Figure 5 below, and its application fields have expanded to finance, supply chain management, new energy mode, intelligent community and other aspects. Among them, in the financial application level, non equity, non debt, unrelated to ownership, only related to the right to use, no income distribution right and residual value recourse[7]. At the level of supply chain management, it should build a perfect supply chain ecological service system, and realize the interconnection of Internet technology at the level of new energy and intelligent community.
3. Research on digital currency supervision model based on blockchain tech

3.1. The necessity of constructing the administrative supervision system of digital currency
First of all, China's domestic digital money market has the typical characteristics of large population base, large number of short-term holders, frequent transactions, and high risk coefficient. The public often falls into the risk of financial fraud, and the property loss is large, which requires a more perfect supervision of the digital money market. Secondly, it is necessary to build a perfect digital currency supervision system in order to deepen the application of multi field scenarios to provide protection. In addition, it is also the need to establish multi-sector supervision and supervision in the field of financial technology, so as to build a digital currency regulatory system and create a universal regulatory model that meets the actual needs.

3.2. Digital currency supervision model based on blockchain tech
The construction of digital currency regulatory system model based on blockchain technology should take into account the characteristics of digital token technology, deal with the impact of digital token on various fields, innovate the supervision concept, supervision method and supervision technology, so as to change all the modes from regulatory objectives to regulatory methods, and incorporate digital currency and its related industries into the supervision based on the framework of regulatory system. Secondly, at the level of industry organization, it is necessary to predict the market information based on the development trend, so as to standardize the industry behavior and order. In addition, in terms of the legal interests of users and trading platforms, the regulation of trading platforms, and the containment of token crimes, these subjects should be included in the supervision, so as to realize the effective development of supervision subjects.

4. Conclusion
In summary, the current theoretical and technical basis of digital currency and the existing regulatory model are summarized, and risk analysis of digital currency is of great value for ensuring the financial stability of digital currency and analyzing the impact of monitoring model on monetary policy. The anonymity and decentralization characteristics of blockchain technology make it have a wide range of application potential and development prospects, and with the continuous iteration of consensus mechanism algorithm, a large number of digital tokens have been produced, which requires the need to prevent crimes and build a perfect digital currency supervision system, so as to deepen the application of multi domain scenarios to provide security. Through the research on blockchain technology and application, this paper analyzes the core technology and application of blockchain. Through the analysis of the digital currency supervision model based on the blockchain technology, this paper studies the necessity of constructing the administrative supervision system of digital currency and its regulatory model.
Acknowledgments
1. GuangDong province in 2018 Provincial Key Platform Scientific Research Foundation, Graph path, circle structure, and its parallelization algorithm (Project #2018GKZDXM004);
2. Guangdong Industry Polytechnic natural Foundation, A smart city hybrid network model based on Argon2 hash function and SDN(Project #X20190132).

References
[1] Gao Ming. Study on the application of symmetric encryption algorithm and asymmetric encryption algorithm [J]. Electronic world, 2015, (15): 59-60.
[2] He Li. Experience of us virtual currency supervision and Its Enlightenment to China [J]. Wuhan finance, 2018 (07): 54-58.
[3] Liu Jia. Bitcoin and mining principles in blockchain [J]. Science and technology, 2020 (15): 213-214.
[4] Lu Yuan. Risk and prevention of "Ponzi scheme" from the perspective of Internet finance [J]. Rural economy and technology, 2019, 30 (16): 51-52.
[5] Qian Yao, Ying-Wei Tang. Some Thoughts on Central Bank-issued Digital Currency[J]. Journal of Financial Research, 2017(07):78-85.
[6] Shan Jianjun. Analysis of foreign regulation of digital currency and Its Enlightenment to China [J]. Financial technology era, 2019 (07): 18-22.
[7] Zhang Chao. A typological study on the legal nature of initial token issuance [J]. Fujian finance, 2018 (08): 62-68.