Potential Technical Risks of Widely Applying Block Chain and Its Impact

Juanye Shang

Technical College, Xi'an International University, Xi'an, 710077, China

Keywords: Block chain, Application, Potential technical risks, Influence

Abstract: Block chain is the basic technology of bITcoin and the core of bitcoin. Now it has been widely concerned by IT industry and finance. The block chain has now been rated as the "leader" in controlling the future technology. Its technology can far surpass cloud computer technology, Internet of Things technology, Internet technology, big data computing, artificial intelligence technology, etc. Blockchain technology originates from bitcoin, and digital currency is also considered as the first generation application of blockchain technology.

1. Introduction

In the current era, block chain technology has been widely used in many industries. For example, in the practical application of intelligent pipeline management system, advanced information means and supply can be used to realize digitalization of resources in all aspects, thus forming a digitalized space for the overall pipeline management system. This paper analyzes the potential technical risks and impacts of the wide application of blockchain, discusses the blockchain technology, and puts forward the future prospects for the practical application of blockchain technology, so as to promote the sustainable development of modern technology in China.

2. Overview of Block Chain Technology

Block chain technology uses consensus mechanism and cryptographic algorithm to realize the distribution and circulation payment of decentralized digital cash. Block chain technology refers to a distributed system, which can realize the combined application of currency digital storage, sharing mechanism and cryptographic algorithm. It is a distributed book technology and can fully embody the digital value. Block chain technology in a narrow sense means that block chain is a data structure, that is, data appears in the form of blocks and is connected by chains. Blockchain technology can effectively improve the relevance between data, and cannot tamper with the sequence of a certain block in practical application. Through data analysis, it can be seen that the essence of blockchain technology is a decentralized large database, which is a new database at present. For example, effective application can make the data set more centralized.

For example, the blockchain technology refinement can be divided into three types, and the functions of various blockchains are different. For example, the public chain belongs to the sharing area, the private chain belongs to the individual independent open area, and the alliance chain is the authorization area. The decentralization of blockchain technology makes it impossible to tamper with in practical application, so the source of data can be traced in practical application, and the traced data is accurate. De-centralization of block chain technology can be programmed with chains, which lays a good foundation for the formulation of intelligent contracts [1]. At the same time, the block chain technology is composed of a plurality of blocks, and each area has a fixed connection but is relatively independent, so the characteristics of the block chain technology improve the safety of the system. It can be seen from this that the wide application of block chain technology can realize effective data sharing and can be applied to platform system construction, such as block chain data storage platform system, block chain electronic currency system, block chain application development platform, block chain deployment structure platform, block chain intelligent contract platform, digital asset (value) management, value transfer, etc.

As far as the current situation is concerned, block chain technology can be widely applied in the

  DOI: 10.25236/ictmic.2020.026

fields of finance, securities, insurance, virtual currency, auditing, network system management, money tracing, supply chain management and other application scenarios. Effective application will get twice the result with half the effort.

3. Application of Block Chain Technology in Current Market

The block chain technology basically appears as a distributed accounting structure. In practical application, the distributed accounting structure can be managed independently, thus realizing the complete decentralization of the technology. For example, all transactions need to be completed through a centralized place to promote capital flows such as inter-bank markets and foreign exchange markets. The advantages of the decentralized mode are obvious. For example, the traditional bookkeeping mode is changed to make the overall operation efficiency higher, and the central exchange and centralized clearing are no longer required for transactions through the block chain technology. This method can effectively reduce the transaction and management costs, thus improving the overall work efficiency. In addition, blockchain can effectively improve the security and identification of transactions in the current actual market transactions, and reduce some transaction costs.

(1)Application of Block Chain in Credit Investigation

Under the traditional accounting system, if the system breaks down during the transaction, the backup system will have the same problem. Therefore, theoretically, if the system breaks down and other failures occur during trading, the security of trading data will be threatened. In addition, the traditional accounting system may make mistakes in trading. However, the distributed bookkeeping of the block chain is tamper-proof, and can realize simultaneous archiving of multi-person data to avoid data loss. If you want to change the archiving in the transaction process, you need everyone to archive together. This method enables each step of the virtual transaction to accurately trace the source [2]. In the market of the current era, most Internet transactions and virtual transactions are completed in a contract mode, and contracts can be registered by using the characteristic of block chain distributed bookkeeping, thus reducing the risk aggregation of central counterparties and increasing the reliability of contracts.

From the traditional trading mode in our country, if two strangers conduct transactions, there will usually be intermediary intervention. Although both parties to the transaction may be highly guaranteed customers, there will still be problems such as limit authorization and limit. Common three-party intermediary trading platforms, such as Alipay and WeChat payment, etc., also solve the problem of distrust in strangers' transactions. The blockchain does not need any intermediary or third party, which plays a role of three-party credit enhancement in practical application. After the introduction of blockchain technology in the system, it can give full play to the advantage of decentralization to the greatest extent, so as to make transactions between customers safe. Furthermore, it can reduce the dependence on the intermediary or the third-party platform, which has a wide development prospect and application prospect in the current virtual market.

(2)Application of Block Chain Intelligent Contract

The regional block intelligent contract refers to the distributed recording of various clauses in computer language on the basis of distributed bookkeeping. The intelligent contract can realize complete paperless archiving and cannot be easily tampered with after archiving. In this way, the phenomenon of shirking responsibility caused by unexpected conditions of paper filing can be prevented, contract efficiency can be effectively improved, and contract safety can be increased. At present, most financial industries in our country have adopted intelligent contracts to avoid shirking contract responsibility. In addition, transaction margin or risk assessment can also be included in the blockchain system, which plays a role in preventing credit risk for the introduction of non-standard product contracts. The formation of the blockchain intelligent contract is a great change of the current electronic contract. Each contract can even be adjusted according to the actual situation to match the overall parameters with the current customers. The whole process from generation to transaction of the blockchain smart contract will be recorded in the blockchain system, providing effective reference for subsequent services [3].

4. Potential Technical Risks and Impacts

Block chain is a new technology in our country. Its application is not yet fully mature, so it is bound to face risks in practical application. In addition to the traditional risks, the block chain system also needs to identify and analyze the new risks when using the block chain technology.

(1)The essence of decentralized trust

The practical application of decentralization can realize mutual trust between strangers and realize trust materialization through block chain. At present, the most important thing in China's virtual transactions is the materialization of trust, such as machine trust, technology trust and system trust, etc. The de-centralization of the block chain and the non-tampering of the chain naturally form trust rules and formulate a set of mechanisms in practice through algorithms and theories. However, as far as the current data and situation are concerned, the de trust has not been fully successful. For example, the practical application of blockchain will also face the problem of decentralized trust, and the concept of complete trust has not yet been achieved. Therefore, we should fully understand the risks brought by trust and constantly analyze the potential problems of current decentralization [4].

De-centralization of the block chain can also be said to transform relative trust into trust equipment, trust systems, etc. The block chain is composed of various software, programs, etc. However, electronic technology may not achieve 100% trust in practical applications. First of all, the equipment, software or program of the block chain system may still have a back door. Although most of the situations can be controlled, risks still exist in actual application. Among them, the private area chain and the alliance area chain are the most influential, and the two chain structures have greater influence. Secondly, at present, science and technology can't write perfect code. Consensus is reflected in both the blockchain line and the consensus rules. However, there are potential risks in realizing shared maintenance and control in decentralized environment. At this stage, the consensus rules of block technology may change constantly. In order to reach a comprehensive consensus rule, we should fully recognize the possible consensus risks.

(2)Cryptography algorithm and risk of engineering implementation

Cryptographic algorithm is the core technology of block chain. Its location and function are equivalent to the CPU of computer host or human brain, and it is the core factor of the whole block chain. Firstly, the random numbers used by cryptographic algorithms are relatively safe. Secondly, the cryptographic algorithm's key cannot be completely leaked, so cryptographic algorithms support the practical application of block chain technology. However, if there is any problem between secret key and random number, it may cause blockchain collapse, resulting in all kinds of virtual values in a state of no protection.

At the same time, if the designed cryptographic algorithm has loopholes, it will bring more potential risks to the practical application of blockchain. According to current research data in our country, direct adoption of cryptographic algorithm standards issued by other countries or other organizations will bring huge security risks to practical application security, such as code review, testing and evaluation for core important applications [5].

With the gradual improvement of China's computing power, cryptographic analysis technology is also continuously improving, but such cryptographic algorithms are not absolutely secure. Cryptographic algorithm also exposes many shortcomings and vulnerabilities, such as hash algorithm. Although theoretical collision does exist and collision is an inevitable problem, the probability of collision is low. Secondly, based on the construction of difficult problems in mathematics, most of the current digital signature algorithms are provably secure, and with the advancement of quantum computing research, it is very important to carry out the research or construction of quantum cryptography algorithm.

(3)Secure storage risk of digital assets or values

At present, the protection or management of seemingly semantic private keys can be realized in several ways, such as virtual currency protocol, network value, etc. However, the safe storage of assets or values is completely equivalent to the fact that the secret key has not been lost, destroyed or stolen. The holding right of assets or values is hidden behind the secret key. If the secret key is

lost or forgotten, the virtual assets will not be retrieved, resulting in great harm in the application of block chain. As far as the current situation is concerned, there is no clear solution for the loss of digital assets or value in China. Therefore, in order to apply blockchain technology safely, it is essential to provide a key protection mechanism with security and convenience, and constantly improve the current management system, otherwise it will pose a threat to the security of the key.

Digital assets such as online wallets, cold wallets and hardware storage have their own advantages and disadvantages, which leads to the greatest natural risks of online storage. Such a practice is equivalent to entrusting the secret key to the platform. Such a phenomenon violates the de-centralized idea of block chain technology, but it will be more convenient in practical application. Although the security of hardware storage is relatively high, it is very likely that data will be lost in hardware storage, bringing security risks to storage. Although paper storage in safes can prevent data loss and make storage safer, this method is not conducive to circulation transactions, will prolong the transaction time, and the transaction lacks convenience. Therefore, it is very important to design a secure and convenient key protection mechanism, such as fully considering the risk of key management according to the application requirements of blockchain, so that the secret key mechanism can be continuously improved, and then improve the value of management, so that users can know the details of current assets at any time, and improve the digital asset management through the backup mechanism.

5. Conclusion

Block chain is the only way for China's digital development in the future, so a new network should be built to realize the transformation from networking and informatization to value. As far as the current situation is concerned, the block chain technology depends heavily on the cryptographic algorithm technology, thus it can be seen that the construction based on block chain will be more difficult in the future. The practical application of blockchain technology should fully consider and analyze the application conditions and application requirements, and reserve solutions for potential risks in advance, so as to effectively achieve risk control and reduce the impact of risks.

Acknowledgment

Shaanxi Province Education Science “Thirteenth Five-Year Plan” Project, Study on the Effectiveness of Blended Learning of Computer Courses under the Background of Double First-Class Construction, No. SGH18H538; Research project on school-level teaching reform, PBL-based exploration and practice research on the teaching model of new engineering specialty applied curriculum, No. 2019B16.

References

[1] Li Bin. The Risks, Regulatory Dilemmas and Strategic Paths of China's Blockchain Technology: Enlightenment from the U.S. Regulatory Strategy [J]. Technology Economics and Management Research, 2020 (01): 18-22.

[2] He Shujian. The Status Quo and Suggestion of Blockchain Supervision in China [J]. The Age of Fintech, 2019 (07): 23-25.

[3] Huang Wei. Potential Risks and Model Construction of Blockchain Technology Applied to Derivatives Market [J]. Financial Supervision Research, 2019 (02): 97-111.

[4] Ling Jie. The application prospect of blockchain is broad, and risk control is the key [N]. Wenhui Bao, 2018-07-31 (012).

[5] Xia Shiyuan. Research on Blockchain Financial Risk and Supervision [J]. Modern Management Science, 2018 (07): 90-92.