Application Prospects of Blockchain in Government Data Opening

Mei Kuang(✉)

Koguan School of Law, Shanghai Jiao Tong University, Shanghai, China
kuangmei@sjtu.edu.cn

Abstract. The government data opening which relies on central platform has the problem of excessive centralization. The blockchain technology with four-layer mechanisms such as communication, storage, security, and consensus has the characteristics of decentralization, which is in contradiction with the inherent characteristics of government data opening. However, this technology has great application prospects in solving the problem of government data opening. Specifically, blockchain technology can connect data between multiple nodes, ensure data circulation, overcome central platform's single point of failure and the limitations of bureaucracy, prompt government to transform its functions and provide opportunities for different entities to participate in data opening.

Keywords: Government Data Opening · Blockchain · Four-Layer Mechanisms

1 Introduction

Nowadays, with the rapid development of intelligent technology, data has become an important resource. The government has collected and stored a large amount of data when performing public functions, which makes it the main data holder of human society. However, most of the government data are still shelved. Therefore, in order to release the value of government data, opening government data has become an urgent issue for governments of all countries. In recent years, many countries in the world have successively applied blockchain technology to E-government, especially the government data opening. But, the opening of government data is inseparable from the central platform, which is in sharp contrast to the distributed blockchain technology. To better apply blockchain technology to government data opening, the purpose of this article is to explore how does blockchain work? Compared with the existing open model of government data, what are blockchain's advantages when applied to open government data?

2 The Technical Architecture and Characteristics of Blockchain

The concept of Bitcoin was first introduced by Satoshi Nakamoto's paper Bitcoin: A Peer-to-Peer Electronic Cash System. Although he does not explicitly mention the term

S. Kadry et al. (Eds.): BDEIM 2022, AEBMR 233, pp. 334–339, 2023.
https://doi.org/10.2991/978-94-6463-124-1_40

Table 1. The Technical Architecture of Blockchain [Drawn by the author]

<table>
<tr><th>Layers</th><th colspan="4">Main Technologies</th></tr>
<tr><td>Consensus Mechanism</td><td>Proof of Work (PoW)</td><td colspan="2">Proof of Stake (PoS)</td><td>Delegated Proof of Stake (DPoS)</td></tr>
<tr><td>Security Mechanism</td><td colspan="2">Asymmetric Encryption Algorithm</td><td colspan="2">Hashing Algorithm</td></tr>
<tr><td>Storage Mechanism</td><td colspan="4">Block-Chain Data Structure</td></tr>
<tr><td>Communication Mechanism</td><td colspan="4">P2P</td></tr>
</table>

blockchain in his paper, the way in which Bitcoin uses a series of time-stamped data blocks chained together can be perceived as the source of blockchain. [1] As the core technology of Bitcoin, blockchain was created to cope with the global financial crisis in 2008. [2] The reason is that blockchain can create trusted services in an untrustworthy environment.

In order to fully understand the application prospects of blockchain in government data opening, we must analyse the technical architecture and characteristics of blockchain. Blockchain combines the advantages of different technologies and is a comprehensive information technology. From a broad perspective, blockchain is the integration of computer technologies such as point-to-point transmission, distributed data storage, encryption algorithms, and consensus algorithms. In particular, the main technical architecture of blockchain shown in Table 1 includes four layers of mechanisms such as communication, storage, security, and consensus.

At the first layer of blockchain is the "communication mechanism". The P2P (Peer-to-Peer) network shown in Fig. 1 is the infrastructure of blockchain. In a P2P network, each node can implement routing, discover new nodes, verify and disseminate data through multicast (that is, point-to-multipoint communication). Each node in blockchain plays the role of server and client at the same time, and finally forms a distributed system that does not depend on central server. Based on such a distributed system, blockchain can build decentralized services that can achieve the same goals as trusted central services.

At the second layer of blockchain is the "storage mechanism". Data propagating via the P2P network is stored on the blockchain in a block-chain data structure. The so-called block-chain data structure means that the data in blockchain is stored in blocks, and then connected into a "chain" in time series. A block usually consists of a block header and a block body. Among them, the block body can store the verified transaction data generated in the block creation; the block header is responsible for connecting with the previous block, and maintaining the integrity of historical data with timestamps. Accordingly, the data recorded by each node is shared with the whole blockchain, and all nodes can obtain a complete copy of data.

At the third layer of blockchain is the "security mechanism". The encryption algorithms of blockchain can be used to protect data to prevent malicious tampering or

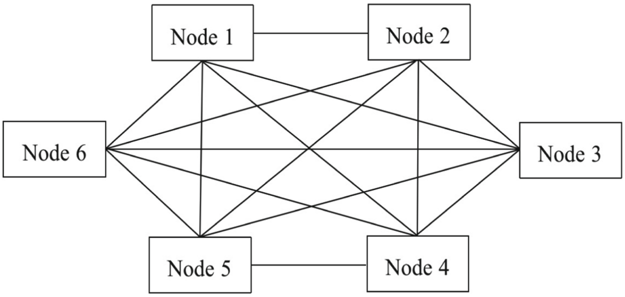

Fig. 1. P2P Structure [Drawn by the author]

theft of data. Commonly used encryption algorithms in blockchain include asymmetric encryption algorithm and hashing algorithm. The asymmetric encryption algorithm encrypts and decrypts data through keys consisting of public keys and private keys. In the operation of asymmetric encryption algorithm, the public key is published to the outside and encrypts the data to be sent, and the private key is used to decrypt the received encrypted data. Moreover, the asymmetric encryption algorithm can guarantee that the private key cannot be deduced from the public key. The hash algorithm is responsible for converting the input data into a fixed-length binary value (also known as hash value). In the operation of this kind of algorithm, the hash value of each data packet on the chain is unique, according to which the authenticity of the data packet can be verified.

The fourth layer of blockchain is the "consensus mechanism". In blockchain, distributed nodes function as if there is only one central node. It is inseparable from the guarantee of consensus mechanism among nodes to reach agreement on various rules. Consensus mechanism is the basis and premise for blockchain to achieve distributed autonomy. In details, consensus mechanism mainly includes Proof of Work, Proof of Stake, and Delegated Proof of Stake. The consensus mechanism proposed by Satoshi Nakamoto is Proof of Work. Its essence is that computing power determines management power, and the node that pays the most computing power will gain the management power to create the next block. In addition, the consensus of each node in blockchain also relies on programmable smart contracts, which can be automatically executed when conditions are met. [3].

3 Four Advantages of Blockchain for Opening Government Data

In the 1950s, the movement of governments' information disclosure rose, with its focus on the publicity of government information and the protection of the public's right to know. The vigorous development of intelligent technology has promoted human society from the information era to the data era. In this process, data plays a role in carrying information. As a manager of social affairs, the government has accumulated a lot of data. Data is a valuable resource that can be used, but only through free circulation can it produce value. In this context, government data opening has become an important support for building a smart government and promoting sustainable economic development, which is also a new development of governments' information disclosure. Previously, blockchain was mainly used in the field of finance. Nowadays, governments are also starting to use blockchain technology in areas such as voting, healthcare, education, and smart city construction. Especially in solving the centralization dilemma of opening government data, blockchain technology presents the following four application prospects.

First, connect data between multiple nodes. The premise of government data opening is data sharing and data collection. However, relying on the central platform to open government data is powerless in the face of massive, scattered and circulating data. The application of blockchain helps to aggregate and link data in decentralized and diverse nodes. Based on P2P structure, blockchain builds an algorithmic trust that is negotiated and maintained by multiple nodes, giving multiple nodes the same power without distinction between master and slave. Based on open source code, the standards and protocols on which the blockchain is based are non proprietary and can be used non competitively and non exclusively. This kind of flat structure not only helps to connect data between governments and the public, but also helps to achieve data sharing within the government, reduce the risk of individual opportunism.

Second, overcome the central system's single point of failure. In the government data opening relying on the central platform, data is distributed from the central node to the multiple nodes via "server-client". In such a centralized system, there is a risk that the failure of central server endangers the entire data opening system through the clients. Blockchain technology can overcome the single point of failure by setting up independent nodes, ensuring multiple backups, and intercepting attacks from less than 51% of nodes. Firstly, since the data on the blockchain is stored in a distributed fashion, there is no need to rely on a central server, and all nodes are independent. By setting up independent nodes, the blockchain can avoid external full-scale attacks on the system of government data opening. Additionally, the block-chain data structure of the blockchain helps to ensure that the data is backed up multiple times. Because each node on the blockchain holds a copy of blockchain, and a single node cannot modify the data on the blockchain alone, it needs to complete this operation according to collectively agreed rules. Therefore, even if a single node on the blockchain is attacked, the intact copies of the blockchain held by other nodes will continue to exist. Only when more than half of the nodes change, the data of the entire blockchain will change. However, the current technology is still difficult to control more than 51% of blockchain's nodes at the same time.

Third, break the shackles of bureaucracy. Influenced by bureaucracy, the government relies on central platform when opening data. However, the quality, efficiency and security of data cannot be fully guaranteed in this way. When the blockchain is applied to government data opening, the mutual supervision and recognition of multiple nodes in blockchain makes the writing and reading of data inseparable from the consensus of all nodes, thus ensuring the authenticity of data. In addition, the operation of blockchain is based on self-executing smart contracts. The content of smart contracts to be executed can be programmed in advance, and then the automatic operation of blockchain can be realized, so that there is no need to bear additional supervision or execution costs. [4] What's more, blockchain is a self-organizing network that does not rely on the supervision center which can save the cost of collecting, publishing and monitoring data, and reduce the time consumption of centralized decision-making. Considering data security, data in blockchain is constrained by private keys and public keys through asymmetric encryption algorithm. [5] Each private key is only used to decrypt the data encrypted by corresponding public key, which can protect data from being illegally read. Through hash algorithm, any change of data in the previous block will result in a different hash value. Such a chain of hashes ensures that no one can manipulate the contents of blocks or reverse the order of chain. Also, the data converted to binary cannot be directly linked to an individual's identity, which guarantees the anonymity of data. Through timestamps, the data flow on the blockchain has a time stamp that can be traced back.

Fourth, promote public participation. Relying on the central platform to open government data forms a closed single-center system, which hinders the public from downloading, evaluating, requesting and sharing data. Blockchain can guarantee interaction between governments and the public in government data opening from the following two aspects. On the one hand, blockchain can facilitate the transformation of government functions. Blockchain is a distributed consensus network without trusted parties, in which all transactions are to be announced to the public. The platform of government data opening based on blockchain is no longer at the center, but on an equal footing with other nodes. The application of blockchain technology encourages governments to no longer require users to adapt to unified standards, but to provide personalized services according to users' needs. On the other hand, blockchain technology can empower multiple subjects to participate in data opening. Blockchain is an open source code which maximizes the transparency of data opening process and ensures the accessibility of public data. The underlying general protocol and algorithm model of blockchain can be freely used by all nodes, and each node can read and download data in the system through an open interface. Thus, all subjects can actively participate in data opening, rather than passive bystanders or recipients, and the demands of each subject can get timely feedback in point-to-point transmission.

4 Conclusions

Under the existing open mode of government data, it is difficult to avoid the problem of excessive concentration and ensure the overall effect of data distribution. To get past this problem, blockchain has four-layer mechanisms of storage, security, consensus and communication, which provides reliable technical support for government data opening from the following four aspects: connecting data between multiple nodes, overcoming the central platform's single point of failure, breaking the limitations of bureaucracy, and promoting public participation. Therefore, the blockchain can be introduced into the government data opening as a technical tool to jump out of the current single regulatory model. However, technology cannot replace supervision. The adoption of a single blockchain technology in the government data opening poses risks of circumventing regulation, solidifying errors, decrypting algorithms, and re-centralizing. In the face of problems that cannot be solved by technology, the government should strengthen guidance.

References

1. VAN PELT R, JANSEN S, BAARS D, et al. Defining Blockchain Governance: a Framework for Analysis and Comparison[J]. Information Systems Management, 2021, 38 (1): 21-41.
2. DE FILIPPI P, MANNAN M, REIJERS W. Blockchain as a Confidence Machine: The Problem of Trust & Challenges of Governance[J]. Technology in Society, 2020, 62: 101284.
3. TSHERING G, GAO S. Understanding Security in the Government’ s Use of Blockchain Technology with Value Focused Thinking Approach[J]. Journal of Enterprise Information Management, 2020, 33 (3): 519-540.
4. KIVIAT T I. Beyond Bitcoin: Issues in Regulating Blockchain Transactions[J]. Duke law journal, 2015, 65 (3): 569-608.
5. KSHETRI N. Blockchain’ s Roles in Strengthening Cybersecurity and Protecting Privacy[J]. Telecommunications Policy, 2017, 41 (10): 1027-1038.