Operation Mechanism for G2B System Based on Blockchain

Yonggui FU, Jianming ZHU

Abstract: The characteristics of blockchain as decentralization, transparency, business activity undeniable proof mechanism etc. have achieved extensive attention from the academic circles and industrial circles. In view of the current deficiency of poor data sharing in G2B system, data authenticity, data security, and transaction subject identity's confidentiality cannot be effectively guaranteed, and the lack of authentication for government management departments (organization institutions) providing service or implementing management to enterprise businesses, this paper proposed to construct G2B system based on blockchain. Based on maintaining the architecture of traditional G2B system and the serviced or managed characteristics of enterprise businesses, was constructed respective G2B system based on blockchain for each section of enterprise business process. Each G2B system was based on blockchain correlated by the virtual links of enterprises and serviced or managed data for enterprises' business, and constituted blockchain interconnection network. The protocol was designed and the characteristics of G2B system analyzed based on blockchain. Application mode for G2B system was designed based on blockchain. A case based on blockchain was designed, including business operation principle, consensus mechanism, and supervision to government (organization).

Keywords: blockchain; G2B; interconnection network; operation mechanism

1 INTRODUCTION

With the technology development of Internet of things [1], cloud computing [2], big data [3], and mobile Internet etc., as a new government management system, "Smart Government" [4] has been gradually getting the attention from government management departments (organization institutions) and information field's research experts. "Smart Government" is the advanced stage of e-government development, and is the inevitable choice for government realizing high efficient and intelligent office, intelligent supervision, intelligent service, and intelligent decision. Through the "intelligence", "Smart Government" can provide service, implement management, and record business operation data for enterprises, find the bad behaviors of enterprise violating normal production engineering, business process, laws and regulations, and find the bad behavior of enterprise tampering business operation records etc., can form macro decisions and guidelines by the statistics and analysis results of enterprise business operation data. Therefore, "Smart Government" is the inevitable choice for government management departments (organization institutions) providing service or implementing management to enterprise businesses.

At present, in the whole world the construction of "Smart Government" is still at the exploratory stage[5], some reasons mainly rooted in the popularization and application level of information and network technology, the restriction from social and government system, the public recognition and acceptance extent to information products, etc., and the other reasons mainly rooted in the requirement to the identity confidentiality of the serviced or managed objects, and the requirement to the business data security and authenticity of the serviced or managed objects, etc.

G2B is one kind of e-government, G2B is one kind of electronic network system in which government management departments (or government authorized organization institutions) provide services or implement management to enterprise businesses. In G2B system, the main business contents include network bidding and purchasing, network taxation, management business electronic handling, and information consultation service, etc.

One enterprise's businesses will obtain service or management from a series of management departments, these management departments include government management departments, some organization institutions that are authorized by the governments and have the authority of servicing or managing enterprise businesses. These departments or institutions have different degrees of knowing right, servicing right, supervision right, and managing right to enterprise businesses in different sections of enterprise business process. At present, the government management departments (organization institutions) in China have constructed many electronic systems to provide service or implement management to enterprise businesses such as Chinese bidding and purchasing network (http://www.gc-zb.com), that was constructed for cooperating Chinese government to implement "People's Republic of China, Tendering and Bidding Law" and standardizing the public purchasing market; such as the network taxation systems that were constructed by Chinese state taxation bureau and local taxation bureau for the corresponding specific regional enterprises etc. taxation objects; such as the electronic systems that were constructed by Chinese industry and commerce management departments for applying, auditing and granting the corresponding specific regional enterprise business license, etc; such as the e-government systems that were constructed by Chinese land management departments, environmental certification departments etc. departments for the corresponding specific regional enterprises etc. objects, and so on. Although at present some Chinese G2B network systems have not completely realized the informatization and no-artificial management for providing service or implementing management to enterprise businesses, but still have provided great conveniences for the service and management between the government management departments (organization institutions) and enterprises.

In the specific system operation process of G2B, Chinese each level governments have also published the corresponding management measures, such as "Electronic Tendering and Bidding Measure" that was published by Development and Reform Commission, P. R. China on February 4, 2013, "Shandong Province State Taxation Bureau Electronic Declaration Tax Management Measure (Trail)" that was published by the state taxation bureau,

Shandong Province, China on August 17, 2010, "Shanghai City Electronic Business License Registration Management Measure" that was published by administrative bureau for industry and commerce, Shanghai City, China on December 28, 2015, and so on. In addition, in China, the other each level government management departments (organization institutions) have also charted the corresponding management measures for using electronic network system to provide service or implement management to enterprise businesses, and in the operation process the corresponding electronic network systems have also got the restriction from the corresponding law and regulation.

Similarly, the world's other countries' government management departments (organization institutions) have also constructed the corresponding electronic network systems and published the corresponding management measures for providing service or implementing management to enterprise businesses.

Although at present most of Chinese government management departments (organization institutions) have constructed the specific G2B systems for providing service or implementing management to enterprise businesses, but in the actual operation process, these G2B systems camp respectively, in its own "information island", and because of the deficiency of supervision mechanism from the third party to these G2B systems, the phenomena of government management departments (organization institutions) "embezzle" or "conspire" with enterprises to cheat society and consumers also are the indisputable facts. So, at present, G2B system is not only facing the problems of system data isolation and poor data sharing, but also facing the problems of data authenticity and security, business subject identity confidentiality, while also facing the requirements of strengthening and improving the supervision to G2B system operation. In actual operation procedure, the management measures, systems that were formulated by each level government management departments (organization institutions) more are operation and management norms for G2B system, punishment afterwards measures for bad behaviors, these are unable to completely solve the problems of G2B system data's security and authenticity, and subject identity's confidentiality.

Blockchain [6-8] was proposed by Satoshi Nakamoto on November 2008, which is a decentered, open, and transparent transaction ledger. All the authorized nodes in the whole blockchain system share the whole blockchain, using hash algorithm [9] and time stamping technology [10] to construct business data management system, making the businesses based on blockchain have the characteristic of non-repudiation, and the business data have the characteristics of higher security and authenticity.

Based on the development and application situation of G2B system in the whole world, this paper makes Chinese G2B system structure as a research instance object, proposes to construct the corresponding blockchain system in light of the characteristics of each section of enterprise business process, introduces enterprises and the corresponding government management departments (organization institutions) (the government management departments (organization institutions) provide service or implement management to some section of enterprise business process, and the blockchain is constructed for the section) to the corresponding blockchain system. We call the blockchain system "G2B system based on blockchain", the research will promote the development of G2B system to "Smart Government". At present, because the mode is similar for different countries' government management departments (organization institutions) providing services or implementing management to enterprise businesses, this paper's research results have equivalent guidance significance for the construction research of other countries' G2B system based on blockchain, and for the stride of other countries' G2B system to "Smart Government".

In each G2B system based on blockchain (one G2B system based on blockchain is constructed for one section of enterprise business process), by the government management departments (organization institutions) which come from different geographical areas and provide service or implement management to the businesses of enterprises in the section, composing "multi-authentication center" to certify the authenticity of enterprise business service or management data, effectively solved current no supervision problem of G2B system subjects' service or management businesses, ensured the security and authenticity of the service or management data.

In G2B system based on blockchain, the government management departments (organization institutions) respectively store each business' service or management data with uniform format, what provides a convenience for data analysis and management. In G2B system based on blockchain, by constructing the corresponding virtual link chains for businesses' service or management data, analyzing the businesses' service or managing big data produced in system operation, can provide evidences for evaluating enterprise's operation efficiency and legacy, can realize the authentication and promote mutual supervision for government management departments (organization institutions) providing service or implementing management to enterprise businesses, also can provide data guarantee for the statistics and analysis of some industry, ensuring the high value density, format consistency, and retrieval convenience of the data.

In this paper following discussion, G2B businesses infer "government management departments (organization institutions) providing service or implementing management to enterprise businesses", are different from enterprise businesses. For expressing expediently, making "government management department (organization institution)" abbreviate as "government (organization)", making "government management departments (organization institutions)" abbreviate as "governments (organizations)", and making "government management department (organization institution) provide service or implement management to enterprise businesses" abbreviate as "service or management".

2 BLOCKCHAIN

Due to the characteristic as non-repudiation of behavior authentication, blockchain's application range is wide. Bitcoin system is the first successful application of blockchain technology, and bitcoin system is constructed in view of the requirement of non-repudiation authentication of transaction behavior [11]. In fact, blockchain technology has many application spaces in the aspects of crowdfunding, market forecasts, smart contracts, sampling, health record management, etc.

2.1 Application Research Status

Since its generation, blockchain has been groping forward, and got a rapid development in 2015, therefore, people define 2015 as the first year of blockchain technology [12]. In the application, the comparatively representative blockchain project results of the foreign countries (the countries other than China) mainly include Ripple, Counterparty, Ethereum, BitShares, etc., and the comparatively representative blockchain project results of China mainly include Bubi, Litecoin, CerChain, DAI Bond, etc. At present, UK, China, the United States, Japan, South Korea, Russia etc. are the countries which are more concerned about blockchain, and these countries are embarking the test and application research on blockchain. Due to the technology characteristics of blockchain, at present, the key areas for blockchain's application research are the business fields as financial field, including banking, securities, insurance, etc. Other fields such as insurance, futures, Internet of things, accounting, auditing, education, medical care, communications, intellectual property etc. are also beginning to embark blockchain product's exploitation. At present, the application researches of blockchain technology have already divorced from the initial digital currency, and have obtained the breakthrough progress in intelligent contract. In future the blockchain technology will be hope to achieve large-scale applications in various fields and industries.

In the aspect of academic research, the current Chinese and other countries' blockchain research results can be divided into two parts, one part mainly focuses on blockchain principle analysis, blockchain value analysis and discussion, and the analysis and discussion of blockchain bringing influences to people life, etc., the other part mainly focuses on blockchain algorithm improvement, model construction and product development, etc.

In the aspect of principle analysis, value and influence analysis and discussion, the research results are still in the primary stage of cognition on blockchain. These researches focus on analyzing blockchain's application environment and its characteristics, and the research value is to improve the understanding of people to blockchain, promote blockchain's development. For example, Kavanagh et al. [6] analyzed the value and social significance of bitcoin and blockchain. Kosba et al. [13] proposed a blockchain system -Hawk, realized the transaction's privacy protection, and introduced system operation principle. Meredith [14] explained and proved blockchain linear proof mechanism's significance with some model methods. Garay et al. [15] formally analyzed bitcoin protocol's principle and application. Kiviat [16] integrated in the thoughts from outstanding computer scientists and cryptographers of current research field to promote the development of blockchain in legislation field, explained blockchain's value in the field of digital currency to promote assets transfer, blockchain's value in the field of legislation area is ascription authentication, ownership transfer, and smart contracts. Birch et al. [17] constructed a simple sharing ledger classification and layered structure to facilitate communication for the related personnel in financial service field.

In the aspect of blockchain algorithm improvement, model construction and product development, basing on the technology principle of bitcoin blockchain and Ethereum blockchain, the researchers analyzed and improved the technology principle, formatted blockchain technology protocol of the concrete field, realized the concrete product's improvement and the product technology characteristics' analysis. For example, Zhu et al. [18] analyzed blockchain's characteristics, technology principle, aimed at B2C supply chain process to construct B2C supply chain's multi-center collaborative authentication model based on blockchain, and carried out case analysis. Zhao et al. [19] proposed a sensor data authenticity guarantee method based on blockchain technology, and applied the method in microbe sampling robot system. Xiang et al. [20] proposed a robust blockchain based on tabu search algorithm, applied the algorithm to dynamic product return and remanufacturing batch problem, and analyzed with demonstration. Fromknecht et al. [21, 22] proposed a decentralization system-Certcoin. Kuo et al. [23] aimed at the requirement of health nursing's privacy protection, proposed a model based on blockchain-ModelChain, and described the model's structure and operating algorithm mechanism.

By integrating current research results we can find, the research on blockchain technology is still in the exploration and discussion stage, the corresponding products are still in the test stage, has not yet found the protocol research results on blockchain application in government (organization) providing service or implementing management to enterprise businesses, and also has not found the valuable research results on blockchain data's index and important data's confidentiality management. Based on the existing research results from experts and scholars, this paper constructed operation mechanism for G2B system based on blockchain, so it has a certain practical significance, and has a certain promotion function to blockchain application in government intelligent field and blockchain development.

2.2 Core Technologies

The blockchain's core technologies include hash function pointer, digital signature technology [24], and binomial tree structure. Using consensus mechanism (such as Pow, Pos, DPos, etc.) to realize businesses' decentralization authentication and supervision, to realize business subject behaviors' and contents' non-repudiation proof. At the same time in block header adding time stamping, ensuring block data's traceability in time.
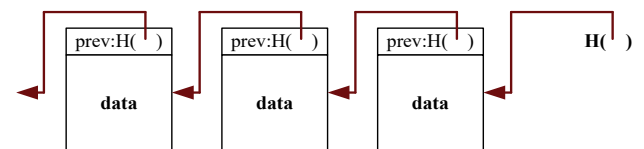

Figure 1 The structure of hash function pointer for blockchain

(1) Hash function pointer
The function pointer is used to help find data storage location; hash function pointer is not only demanded to find data storage location, but also to confirm data authenticity. The main function of blockchain is recording business content, its structure is linked list and hash function pointer. The structure of hash function pointer for blockchain is shown in Fig. 1.

(2) Digital signature technology

For the business based on blockchain, some business subject first makes business related data hash to achieve hash function value (digital abstract 1), next signs the hash function value with its private key to achieve digital signature, the signature information are attached business related data, together with the business subject's public key broadcast in the whole blockchain network. Once the blockchain system's authentication subjects (including business activity subjects and other subjects) achieve the business subject broadcasted data information, the authentication subjects will make the business related data hash to achieve hash function value (digital abstract 2), and use the business subject's public key decrypt digital signature to achieve the hash function value before signing (digital abstract 1), by comparing both (digital abstract 1 and digital abstract 2) to confirm the authenticity of the business data. The digital signature principle for business related data of blockchain system is shown in Fig. 2.
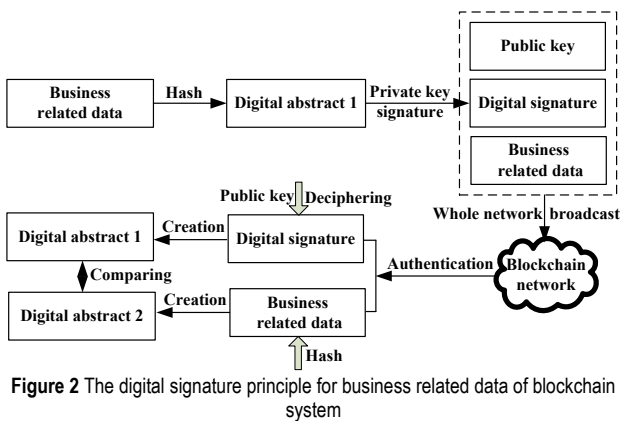

Figure 2 The digital signature principle for business related data of blockchain system

(3) Merkel tree

In the structure of each block, because the upper layer data is achieved by hashing the next layer data, if the hacker tampered the underlying data, that would lead to the inconsistency between the tampered data's function pointer and its upper layer function pointer, if the hacker tried to tamper all the function pointers, he need tamper all the way to the root, while so long as the blockchain's other nodes remember the value of the root function pointer, the nodes will find the hacker's tamper behaviors. In fact, in the blockchain's each block, data are preserved as a binomial tree structure named Merkel tree. In this structure, business related data are hashed respectively, then the initial hash values as the leaves of the tree first two pair, then point to the upper layer by pointers, the upper layer pointers again two pairs and point to the more upper layer, and ultimately reach the tree root. The structure of the Merkel tree for blocks is shown in Fig. 3.
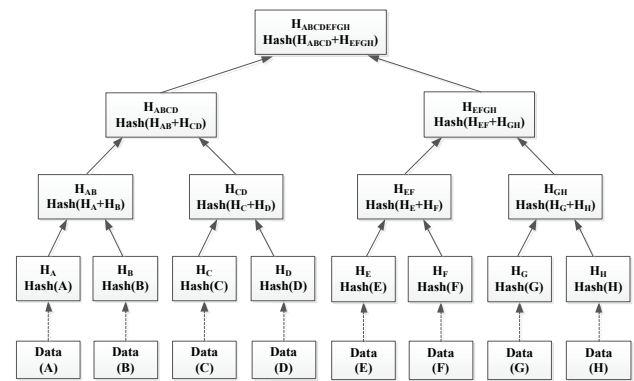

Figure 3 The structure of the Merkel tree for block

In Fig. 3, business related data can be stored in blockchain with Merkel tree hash value structure, also can only be constructed mapping relation with Merkel tree's leaf nodes and stored in different database apart from blockchain. In this paper's following research, we suppose business related data are stored in block body together with Merkel tree hash value structure.
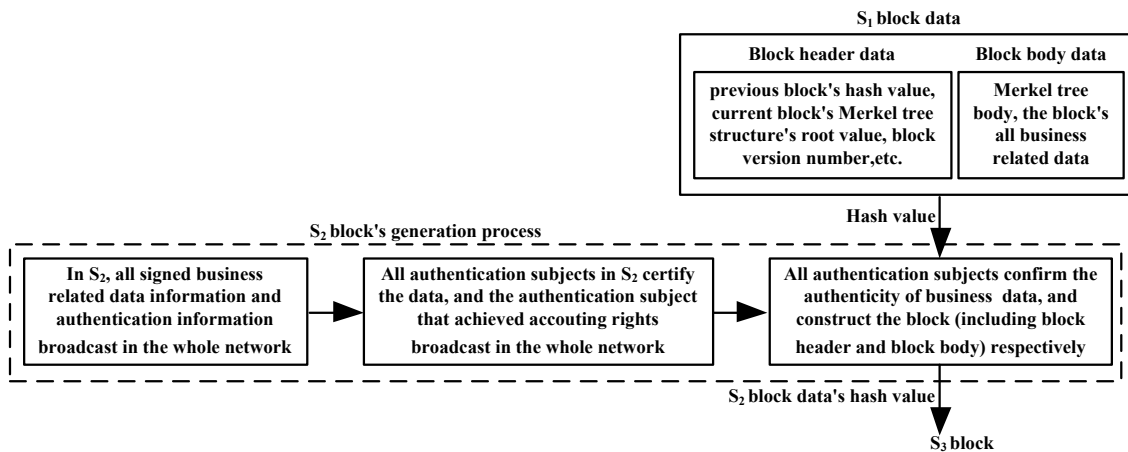

Figure 4 The work principle of blockchain

(4) The work principle of blockchain

Because the work principle of blockchain has not a fixed mode, so, here is only introduced the blockchain's classical work principle. In blockchain, all the authentication subjects participate in block's each business related data's (business sorted by time sequence) authenticity proof; if some authentication subject has achieved a block's accounting rights, it will broadcast the authentication results of the business related data (the block time period's all business related data), all the other authentication subjects confirm the results and introduce the business related data to its own block and account, these business related data constitute block body with Merkel tree hash value structure (block body does not include Merkel tree structure's root value), and collect the previous block's hash value (actually, the hash value is for

the previous block's header), this block Merkel tree structure's root value, time stamping information, this block version number, block generation mechanism etc. data or information to form this block's data header, the block is comprised by block body and block header. So, in a block, not only including its own block's business related data and information, but also including all previous blocks' business related data's information. In the blockchain, different business data are linked according to time sequence, through the corresponding business subjects' public key information (public key hash value, representing business data's address.) to confirm the link objects. The next block is linked with the previous block by the sequence of digital time stamping, in the structure of blockchain, the next block is linked with the previous block through block header. As this is carrying on, the blockchain is formed. The work principle of blockchain is shown in Fig. 4.

(5) Consensus mechanism

The distinct characteristic of the decentralization authentication system of blockchain business related data is mainly reflected in blockchain using consensus mechanism. Under consensus mechanism, all the nodes (including business subjects and other subjects) that affiliate the blockchain are authorized to participate in the real existence proof of business related data in blockchain system, the proof way is finding the hash value of business related data and by consensus algorithm to get the priority of accounting, once some node gets the priority of proving the authenticity of all the business related data in block, it will broadcast to the other nodes in the blockchain network system, the other authorized nodes confirm and introduce all the business related data to its own block. Furthermore, in consensus authentication stage, intelligent contract can also be operated and the operation results can also be authenticated by the authentication nodes. For improving the enthusiasm of node accounting, the blockchain system need set up the concrete incentive measures for the nodes that participate in consensus mechanism.

3 THE PROTOCOL AND CHARACTERISTICS FOR G2B SYSTEM BASED ON BLOCKCHAIN

As a social entity, enterprise businesses need governments' (organizations') service or management, at the same time the serviced or managed enterprises own its right of privacy, furthermore, the constructed G2B system based on blockchain need improve its service or management efficiency on the basis of maintaining the original system's service or management structure. Therefore, this paper proposed governments (organizations) construct their own G2B system based on blockchain by its business characteristic (the business characteristic is coherent with enterprise business process' some section's service or management requirement), and different type of businesses' G2B systems based on blockchain correlated through the enterprises that affiliated the systems and the service or management data of enterprises' businesses, to form blockchain interconnection network.

3.1 The Protocol for G2B System Based on Blockchain

The subjects in some G2B system based on the blockchain are composed of the enterprises and the governments (organizations) that correspond to the system.

Different type of enterprises' business process is different, and the corresponding governments (organizations) are also different, so different type of enterprise's whole business process' each section affiliated G2B system based on the blockchain is also different (in this paper research, only considering the G2B business of enterprise's whole business process, so, in here, the business process is also the G2B businesses which are linked according to the time sequence, and is different from the actual enterprise's business process.). At present, the service or management authorities of governments (organizations) to enterprise businesses are usually divided by geographical areas, and in the belonging geographical area, governments' (organizations') service or management activities are sorted by the time sequence.

The protocol for G2B system based on blockchain is shown as the following:
1) Constructing different G2B systems based on blockchain according to enterprise business process' different sections (or according to different governments'(organizations') business characteristics), by registration of the formal enterprises and governments (organizations) that corresponding some a business section affiliate the corresponding business section's G2B system based on blockchain.
2) For some section of an enterprise business process, by geographical area to determine the corresponding governments (organizations) of this section business for the enterprise.
3) Different business section's enterprises as the subjects sign its serviced or managed data.
4) In some enterprise business process' section, only by this section business corresponding governments (organizations) as authentication centers to authenticate the service or management data, and any enterprise has not the authority of authenticating other enterprise businesses' service or management data. Therefore, only corresponding business section's governments (organizations) preserve the business section enterprises' business service or management data, and any enterprise has the authority of downloading the corresponding blockchain's other enterprise businesses' service or management data.

The topology structure of G2B systems based on blockchain is shown in Fig. 5.
5) Business service or management. For some business section's G2B system based on blockchain, if some enterprise needs the corresponding government's (organization's) service or management, the enterprise will first propose business service or management "application" towards the corresponding geographical area's government (organization), next "sniffing" to the system (subsystem corresponding to the geographical area). If the corresponding geographical area's government (organization) is servicing or managing another enterprise businesses, set system status as "busy", and set the enterprise status as "wait". If the corresponding geographical area's government (organization) is not servicing or managing the other enterprises' businesses, then set system status as "idle". The different enterprises of the same geographical area are sorted by the time sequence of proposing business service or management "application" to "line up and

wait" the corresponding government's (organization's) service or management. If some enterprise has achieved the right of acceptance of business service or management from the corresponding geographical area's government (organization), the enterprise meanwhile has achieved the business service or management acceptance "token", and set system status as "busy", to accept the service or management for its businesses, till the business service or management finished, the enterprise hand over the business service or management acceptance "token", and set system status as "idle", entering into the business process' next section's G2B system based on blockchain and accepting the corresponding government's (organization's) service or management.
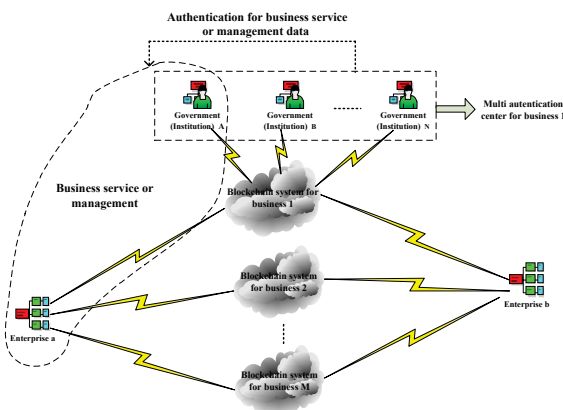

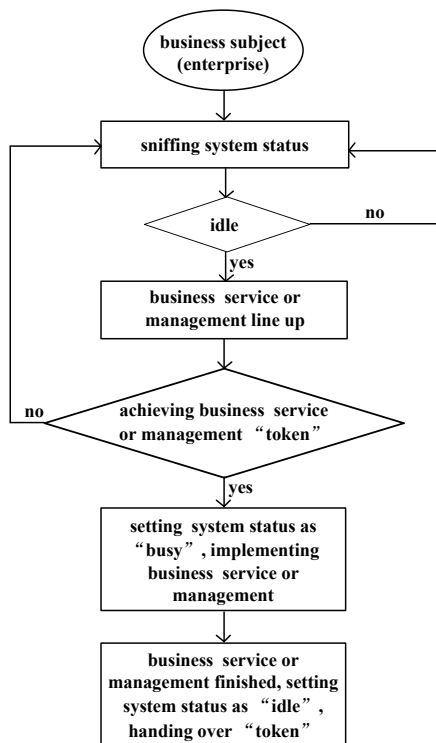**Figure 5** The topology structure of G2B systems based on blockchain

Figure 6 The serviced or managed procedure protocol of enterprise business for G2B system based on blockchain

The serviced or managed procedure protocol of enterprise business for G2B system based on blockchain is shown in Fig. 6.

6) Authentication on service or management data. For enterprise business process' some section's service or management data in a specified time period, by the "idle" governments (organizations) that in the section's G2B system are based on blockchain comprising "multi-authentication center" to authenticate the service or management data, to authenticate the service's or management's authenticity, and form a block.

7) After an enterprise's some section businesses' service or management being finished, it will enter the next business section, and the enterprise will accept the corresponding government's (organization's) service or management and other corresponding governments' (organizations') authentication on the service or management data according to the steps of 4)-5).

3.2 Characteristics Analysis on G2B System Based on Blockchain

1) For a different business, the corresponding G2B system based on blockchain is different, and the different blockchain systems do not affect each other. By the enterprises and governments (organizations) of the same type businesses constituting a system, not only convenient to service or manage enterprise businesses uniformly and coordinately, can realize enterprise business service or management dispersedly, but can improve the efficiency of servicing or managing, efficiently ensuring the security, traceability, and authenticity of data for enterprise business servicing or managing.

2) The G2B system based on blockchain is coincident to the original G2B system in the structure of business service or management. Although the different enterprises are induced to the same blockchain system basing on the uniformity of business servicing or managing, but an enterprise businesses' service or management only provided or implemented by its belonging geographical area's government (organization), and the authentication for enterprise business service or management data only implemented by the belonging business section's governments (organizations), observing enterprise business' original service or management system's structure.

3) Although each geographical area corresponding governments (organizations) have joined the corresponding businesses' blockchain system, in a specified time period (a time period for block generating), only by the "idle" (having authentication authority and can accede the authentication) governments (organizations) implementing authentication for the service or management data, so in this paper constructed G2B system based on blockchain, different block's authentication subjects are dynamically varied.

4) For the same enterprise, in the interconnection network for blockchain, we can by each G2B system based on blockchain's last block (inferring the last block of all containing enterprise businesses' blocks) comprising virtual chain achieve the enterprise's all business service or management data's record authentication.

4 APPLICATION MODE FOR G2B SYSTEM BASED ON BLOCKCHAIN

4.1 Interconnection Network

For meeting the general demands of research, this paper supposes a serviced or managed enterprise as "δ". Supposing δ business process' each section's service or management involved governments (organizations) as "$A = \{A_1, A_2,..., A_x\}$", "$B = \{B_1, B_2,..., B_y\}$", "$C = \{C_1, C_2,..., C_z\}$",... , "$N = \{N_1, N_2,..., N_w\}$". Supposing the governments (organizations) that provide service or implement management to δ business process' each section as "A_1", "B_1", "C_1",…, "N_1". The interconnection network's structure of enterprise business process' each section's G2B system based on blockchain is shown as Fig. 7 (for an enterprise, its G2B business process' structure maybe dynamic varies with time and the requirement for enterprise business service or management, so this paper research focus is on some enterprise's G2B service's or management's business chain process that is formed as time sequence, and the process structure of different time period can be different).
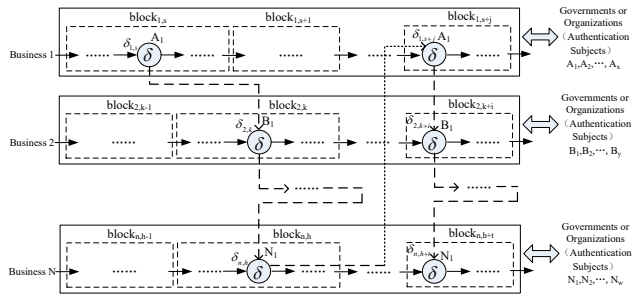

Figure 7 The structure of interconnection network for G2B system based on blockchain

With Fig. 7 we can see, for enterprise δ, only in each blockchain contained δ's last block constituted process (shaped like the blocks constituted process $\cdots \to block_{1,s+j} \cdots \to block_{2,k+i} \cdots \to block_{n,h+t} \cdots \to$), includes δ's all historical service or management data's related information. Although each block authentication subjects are dynamically varied, but any authentication subject can download the corresponding blockchain from its belonging blockchain system (such as $A = \{A_1, A_2,..., A_x\}$) can download the blockchain $\cdots \to block_{1,s} \cdots \to block_{1,s+1} \cdots \to block_{1,s+j} \cdots \to$, $B = \{B_1, B_2,..., B_y\}$ can download the blockchain $\cdots \to block_{2,k-1} \cdots \to block_{2,k} \cdots \to block_{1,k+1} \cdots \to$, …, $N = \{N_1, N_2,..., N_w\}$ can download the blockchain $\cdots \to block_{n,h-1} \cdots \to block_{n,h} \cdots \to block_{n,h+1} \cdots \to$, etc.), to update its own existing blockchain, to ensure the consistence of blockchain that is owned by any subject in a G2B system based on blockchain. So, in the same blockchain, each geographical area's government (organization) mutually authenticates, shares data, that can promote the rationality and orderliness of service or management of enterprise businesses, prevent enterprise "bribe" its belonging geographical area's government (organization) to cheat society and consumers.

By analyzing Fig. 8, enterprise δ's business service or management data have the following characteristics:
1) Because business 1 and business 2 are carried on according to time sequence, so data $\delta_{1,s}$ and $\delta_{2,k}$ are correlative.

2) Because data $\delta_{1,s}$ and $\delta_{2,k}$ belong to different business respectively, so both data's contents and characteristics are different.
3) Because data $\delta_{1,s}$ and $\delta_{1,s+j}$ all are the data produced by A_1 servicing or managing δ in business 1, and both of them are contained in blockchain $\cdots \to block_{1,s} \cdots \to block_{1,s+1} \cdots \to block_{1,s+j} \cdots \to$, so both data's characteristics have great similarity, and data $\delta_{1,s+j}$ belonging block $block_{1,s+j}$ contains data $\delta_{1,s}$'s information.
4) Enterprise δ's whole lifecycle's business process' service or management data are constituted by δ's all business service or management data according to its business process with time sequence, reflected in Fig. 8 is virtual chain process contained data set $\{\cdots, \delta_{1,s}, \delta_{2,k}, \cdots, \delta_{n,h}, \cdots, \delta_{1,s+j}, \delta_{2,k+i}, \cdots, \delta_{n,h+t}, \cdots\}$, so we can analyze δ's virtual chain data structure $\cdots \to \delta_{1,s} \to \delta_{2,k}, \to \cdots \delta_{n,h}, \to \cdots \delta_{1,s+j} \to \delta_{2,k+i}, \to \cdots \delta_{n,h+t} \to \cdots$ to grasp the unite service or management on δ's whole business process.

4.2 Data Management

(1) Construction and application of data index

In G2B system, service or management process can produce massive data, with service or management continuously conducting, and time going on, the data capacity can rapidly increase, and will eventually reach big data capacity. Comparing with other data in network, service or management data produced in G2B system based on blockchain have higher value density and business activity specificity, the data format has higher consistency, data storage has higher fixity and stability. By analyzing service or management big data in G2B system based on blockchain can realize the supervision to governments (organizations), and can provide more effective and reliable reference datum for enterprise business analysis, reform, industry service or management, etc.
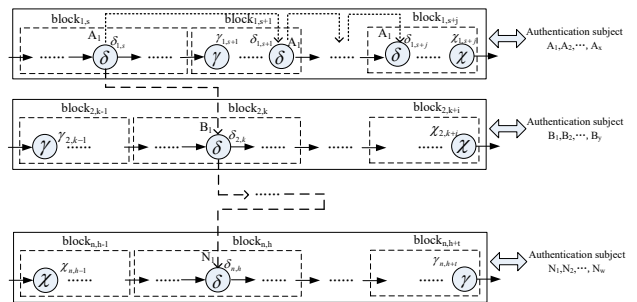

Figure 8 The virtual link network's structure for blockchain big data

Based on the above analysis, constructing big data analysis system for G2B system based on blockchain, by constructing enterprise, industry data related virtual link network to achieve the analysis on enterprise, industry businesses. The virtual link network's structure is shown in Fig. 8.

By using cloud computing technology, data mining technology and the corresponding data analysis model, and constructing data index in service or management data set of blockchain big data's virtual link network can rapidly traverse the required data datum, provide reference for analysis and decision. The data index types that can be constructed in Fig. 9 contain:

1) Transversely, the data index that is constructed in some enterprise's business section's service or management data set (such as $\{\cdots, \delta_{1,s}, \delta_{1,s+1}, \cdots, \delta_{1,s+j}, \cdots\}$).

2) Transversely, the data index that is constructed in some business section's service or management data set (such as $\{\cdots, \delta_{1,s}, \gamma_{1,s+1}, \delta_{1,s+1}, \cdots, \delta_{1,s+j}, \gamma_{1,s+j}, \cdots\}$).

3) Longitudinally, the data index that is constructed in some enterprise's business process' service or management data set (such as $\{\cdots, \delta_{1,s}, \delta_{2,k}, \cdots, \delta_{n,h}, \cdots\}$).

4) In whole, the data index that is constructed in some enterprise's all business process service or management data set (such as $\{\cdots, \delta_{1,s}, \delta_{2,k}, \cdots, \delta_{n,h}, \cdots, \delta_{1,s+1}, \cdots, \delta_{1,s+j}, \cdots\}$).

In the actual application process, we can construct other type data indexes according to the requirements. These data indexes that are constructed in virtual link chain's service or management data set embody the correlation relationship among the service or management big data, and provide convenience for big data analyzing.

By analyzing service or management big data in G2B system based on blockchain, can be constructed enterprise businesses' standardized process, technology's and management's assessment basis, can be formulated the service's or management's improved measures. At the same time, we can by the recorded service or management data assess governments (organizations), further construct the incentive mechanism and constraint mechanism for improving governments' (organizations') work efficiency.

(2) The confidentiality management of identity data

In the G2B system based on blockchain, for managing and using enterprises' serviced or managed data effectively later, it is not suitable for enterprises' identity data using anonymous mode fully (Bitcoin blockchain uses full anonymous data management mode.), so the blockchain data should contain enterprises' real identity data. While because each system's governments (organizations) share the system's blockchain data, if we do not adopt confidential measures for enterprises' identity data, the enterprises would face identity confidentiality problems, because it is usually difficult for accounting for the behavior of some system's government (organization) disclosing the same system's other geographical areas' governments' (organizations') service or management data.

Based on this, in the course of business operation, for some enterprise, first encrypting the identity data by the enterprise business' G2B system based on blockchain corresponding geographical area's government (organization), then together with other service or management data doing signature, broadcast, etc. So, although the service or management data of some blockchain system are held by the blockchain's all authentication nodes, only the corresponding geographical area's government (organization) has the use permission of corresponding enterprises identity data, in this way to realize enterprises' identity data's common preservation and single management. If the belonging geographical area's government (organization) maliciously destroys an enterprise's some identity data, under this government (organization) authorizing, the system's other governments (organizations) can through decrypting achieve the enterprise's true identity data and conduct credit authentication to this government (organization). Certainly,

for other important service or management data, we can also conduct confidentiality management like identity data.

The enterprises' identity data's confidentiality principle is shown in Fig. 9.
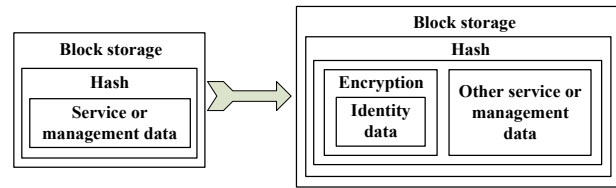

Figure 9 Identity data's confidentiality principle in G2B system based on blockchain

5 CASE DESIGN

The distinction of the governments (organizations) that service or manage different enterprise businesses is great, for example, in China, wood processing enterprises may produce service or management data interaction with industrial and commercial bureau, taxation bureau, quality system authentication center etc., while coal production enterprises will further produce service or management data interaction with quality and technical supervision bureau, safety supervision bureau, environmental protection bureau, coal industry management bureau, geological bureau, land management bureau, environmental protection authentication center etc., and municipal enterprises will further produce service or management data interaction with municipal party committee, municipal government, etc. Basing on these, the service or management interaction relationship of one enterprise with the governments (organizations) in G2B system business process can be summarily described as Fig. 10.
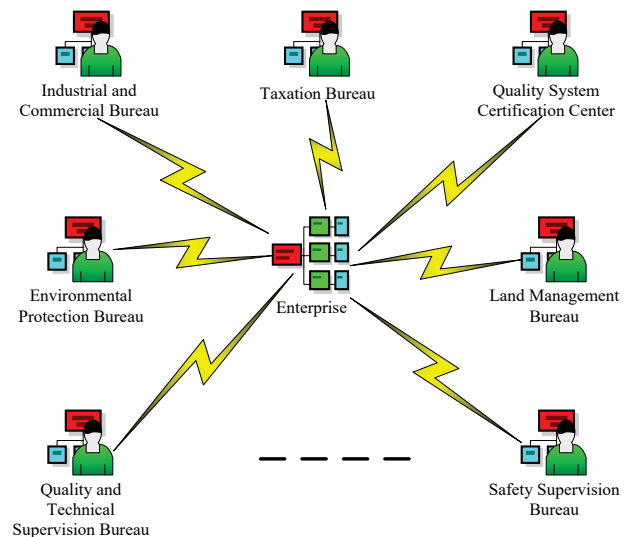

Figure 10 The service or management interaction relationship

The service or management data interaction relationship between these governments (organizations) and enterprises are different respectively, some governments (organizations) and enterprises' electronic data interactions are frequent, while some maybe less. Some electronic data interactions are relatively concentrated in time, while some other may be scattered. Some interactions belong to policies, documents etc. service classification data interactions, and some other interactions belong to management, supervision

etc. management classification data interactions. These governments' (organizations') service or management data interaction procedure penetrates into the enterprises' establishing, purchasing, internal operating, selling, bankrupting etc. whole lifecycle, integrating into enterprise own operation and its communication and coordination procedure with other external entities.

For a long time, the service or management level of governments (organizations) to coal industry is relatively low. With the development of information technology and network technology, the informatization degree of coal industry improves rapidly. At present, most big coal production enterprises have constructed their inner network, and connected to Internet, so it is feasible for constructing

G2B system based on blockchain for big coal production enterprises. Based on this, we make big coal production enterprise as an example to research.

5.1 Operation Principle

Supposing in time T, the sequence of G2B businesses of some big coal production enterprise δ as: the business for safety supervision bureau (A) (business1) $\rightarrow$ the business for environmental protection bureau (B) (business2) $\rightarrow$ the business for coal industry management bureau (C) (business3) $\rightarrow$ the business for geological bureau (D) (business4).
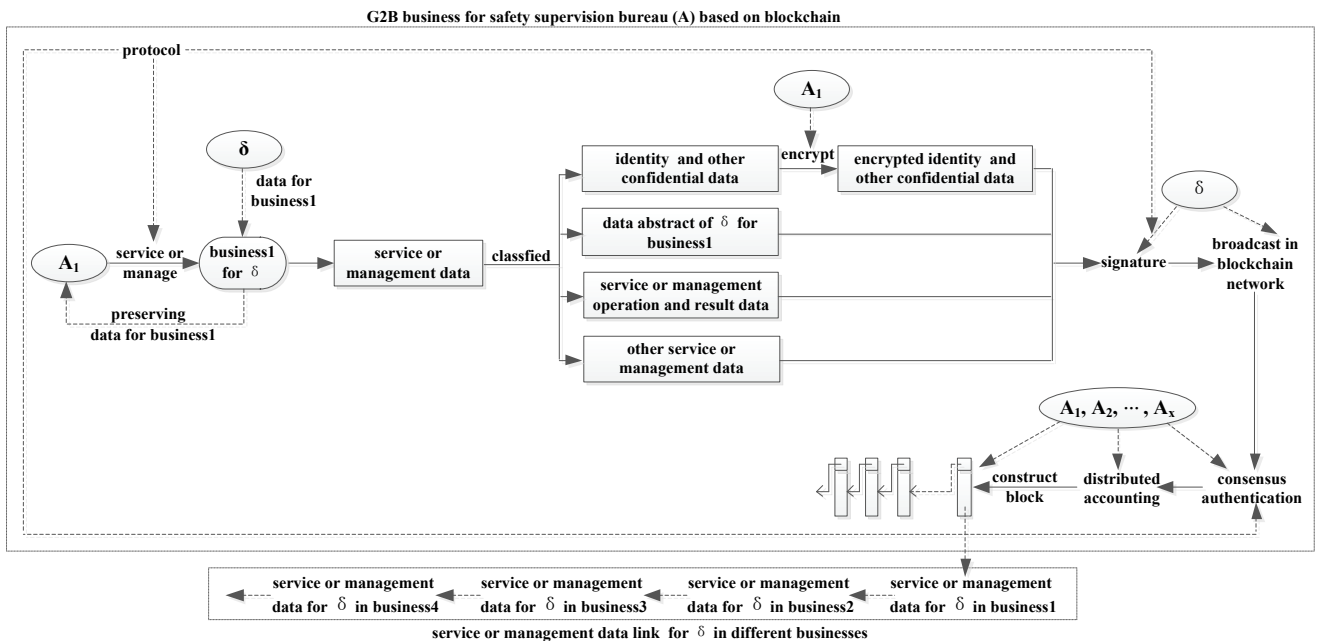

Figure 11 The businesses' operation principle of G2B based on blockchain

Because the G2B businesses of big coal production enterprises are relatively complex, so the G2B system based on blockchain for big coal production enterprises includes internal and external blockchain for service or management. In the G2B system based on blockchain, the data include service or management data, and data that are provided by big coal production enterprises. For the service or management data, that will be classified, signed, broadcast, consensus authenticated, distributed accounted, constructed block, and formed blockchain. For the data that are provided by big coal production enterprise, that are stored by the enterprise and the corresponding government (organization).

The businesses' operation principle of G2B based on blockchain can be described as in Fig. 11.

In the G2B based on blockchain for big coal production enterprises, the big coal production enterprises and the corresponding governments (organizations) join the corresponding blockchain system, the big coal production enterprise businesses' realization process comply with the protocol of "line up and wait", and the protocol of G2B based on blockchain penetrates the whole business process.

In figure 11, we described the operation process of G2B business for safety supervision bureau (A) based on blockchain, and the businesses' data generation process of enterprise δ interconnection network for G2B system based

on blockchain. In section "5.2 Consensus Authentication Process" and "5.3 Supervision to Government (Organization)" of "5 CASE DESIGN", we also make G2B business for safety supervision bureau (A) based on blockchain the object to research, and the research result has the similar guidance significance to the other type G2B system based on blockchain.

5.2 Consensus Authentication Process

Consensus authentication is a very important content in the operation process of blockchain. Safety supervision bureaus as the authentication subjects authenticate the service or management data of some safety supervision bureau to the corresponding big coal production enterprises, this need be realized by constructing authentication mechanism. Because safety supervision bureau is government department, so the corresponding authentication behaviors can be managed by the higher government institutions. As the authentication subjects, the whole authentication efficiency of safety supervision bureau is an important index to measure the operation efficiency of G2B based on blockchain. So, constructing the consensus authentication mechanism for the service or management data of some safety supervision bureau to the corresponding

big coal production enterprises, not only need embody the concrete characteristics of safety supervision bureau managing, but also need promote to improve the positivity of safety supervision bureaus attending consensus authentication.

Based on this, the authentication mechanism for the service or management data of some safety supervision bureau to the corresponding big coal production enterprises can be described as the following:

1) The authentication algorithm is computing and sorting the security incidences' occurrence time and

corresponding enterprises' anonymous numbers for the last 10 times in time T.

2) The authentication subject that first gets computation result will achieve the accounting right.

3) The authentication subject who achieved the accounting right will receive authentication efficiency award, and the other authentication subjects will receive authentication contribution award.

The consensus authentication process for the service or management data of safety supervision bureau to big coal production enterprises is shown in Fig. 12.
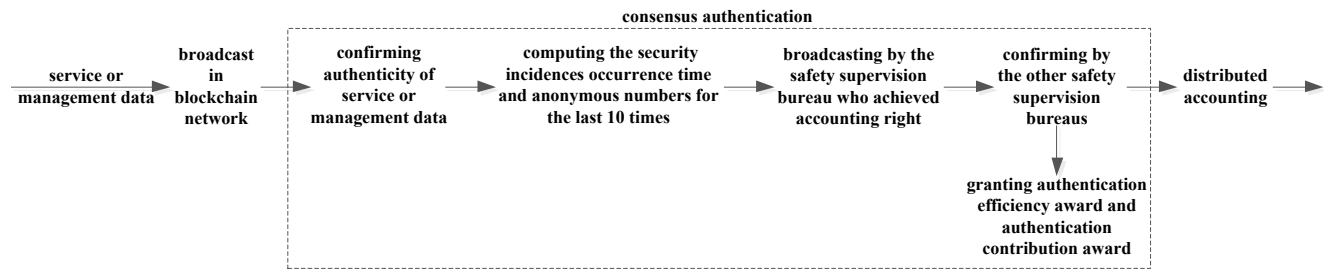

Figure 12 The consensus authentication process for the service or management data

5.3 Supervision to Government (Organization)

An important function of G2B based on blockchain is realizing supervision to governments (organizations), the G2B business should set the rationality provision, and rationality provision is the evaluation system for governments (organizations) and is used to supervise the governments (organizations). The service or management of governments (organizations) to enterprises can be achieved by retrieving service or management big data which are got from blockchain system and are constructing correlation.

For big coal production enterprise, safety is the first place, so it is very important for safety supervision bureau servicing or managing big coal production enterprise. The timeliness, accuracy, and completeness of the service or management of safety supervision bureau to big coal production enterprise embody the implementation level. Because the security problems of big coal production enterprise is complex, so the security service or management to big coal production enterprise also embodies great irregularity. So, for some sudden security incidences, the service or management from safety supervision bureau takes on randomness, so the service or management to big coal production enterprise need be more detailed and targeted. Sometimes the service or management of safety supervision bureau to big coal production enterprise need be conducted according to the policies from the national and local government. Sometimes the service or management of

safety supervision bureau to big coal production enterprise need be conducted according to the enterprise's operation process, etc. Basing on this, the service or management of safety supervision bureau to big coal production enterprise need be conducted according to the job requirement of safety supervision bureau, and combining the security problems' appearance conditions of big coal production enterprise. Therefore, the supervision process to safety supervision bureau need induce and analyze blockchain's external data sources' data to implement.

External data sources' include big coal production enterprise's operation data, national policy data, and the supervision regulations of safety supervision bureau, etc. These external data sources' data are retrieved and analyzed together with service or management data from bolckchain, and the analysis result will be broadcast, consensus authenticated, distributed, accounted, and block constructed.

Because in general the safety supervision bureau is hierarchical, so the higher safety supervision bureau can store the key of lower safety supervision bureau encrypting service or management data, if needing to supervise some safety supervision bureau, other safety supervision bureaus can decrypt the encrypted service or management data under the authorization from higher safety supervision bureau.

The realization process of supervision to safety supervision bureau can be shown as Fig. 13.
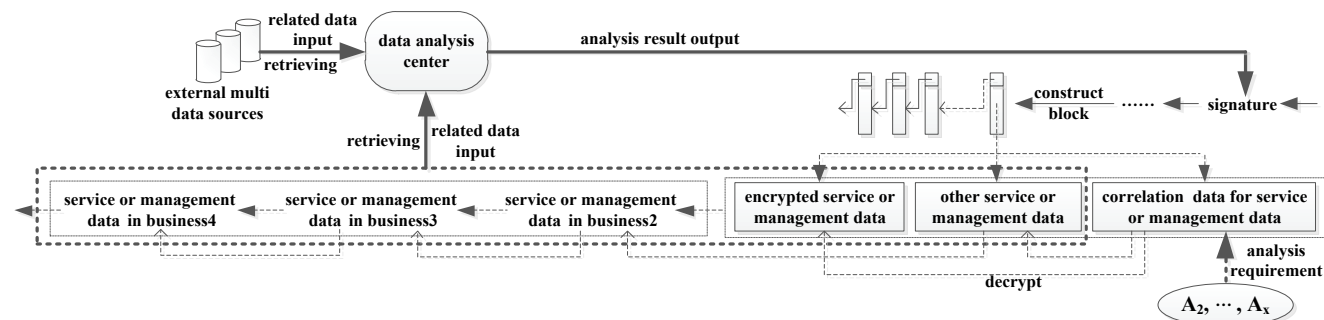

Figure 13 The realization process of supervision to safety supervision bureau

Through constructing G2B system based on blockchain for coal industry, can be improved the service level (or management efficiency) of governments (organizations) to coal industry, and the transparency of service or management of governments (organizations) to coal industry. With blockchain technology, we can duly find the deficiency of coal industry operation, can promote the standardization and intellectualization of coal industry operation, and can improve the market competitiveness of coal industry, which have positive application value.

In this paper we proposed, through analyzing service or management big data, to realize the mutual supervision among governments (organizations). In fact, we can also construct intelligent contract and through the consensus authentication from governments (organizations) realize the mutual supervision among governments (organizations).

6 CONCLUSIONS

At present in the world majority countries' governments (organizations) have constructed their G2B system aiming at enterprise businesses' service or management, while because in the traditional G2B system exist the problems of poor data sharing, authentication difficulty for business service or management data, data security and authenticity, business subject identity confidentiality cannot be effectively guaranteed etc., resulting in the existing G2B system having a great distance compared to "Smart Government".

Blockchain's characteristics of decentralization, publicity, transparency, the real non-repudiation proof mechanism of business activity, data security, etc., provide a certain technology guarantee for the striding of traditional G2B system to "Smart Government".

Based on keeping the characteristics of enterprise's original business process and the architecture of traditional G2B system, this paper aims at enterprise business process of each section to construct G2B system based on blockchain, each section's G2B system based on blockchain correlates by the corresponding enterprises and the service or management data. Designed is the protocol and analyzed the characteristics of G2B system based on blockchain. Designed is application mode for G2B system based on blockchain. Designed is a case based on blockchain, including business operation principle, consensus mechanism, and supervision to government (organization). Blockchain can be divided into public chain, alliance chain, and private chain, and this paper constructed blockchain is alliance chain. G2B system is a huge system, involving many subjects as governments (organizations) and enterprises, these subjects' business volume and scale are also very large, so, "G2B system based on blockchain" is still mainly facing the following difficulties:

1) The barriers for technology identification. Blockchain itself is a technology, database, and protocol, at present majority non-experts are not familiar with blockchain's core principle and application background, so, in the implementation process, G2B system based on blockchain will suffer a certain degree of exclusion from governments' (organizations') and enterprises' different arrangement personnel, even it is also a big problem for persuading the leaders to accept blockchain technology.

2) The difficulties for system construction. G2B system based on blockchain involves many application subjects, on the basis of the original G2B system to use blockchain technology realize system's upgrading and restructuring, and train the original business personnel and information management personnel, will suffer great difficulties, on one hand involving computer network software and hardware system resources' equipment, and on the other hand will bring great technology transform cost to the original staff.

3) The link problems for blockchain systems of different sections for enterprise business process. Because at present blockchain technology is not fully mature, while an enterprise business process' different sections involve different governments (organizations), so, for constructing enterprise business process' different section's blockchain systems' data link interfaces and business interfaces, there still exist a series of technology problems and business subject coordination problems.

At present, blockchain's applications and researches are still in the primary stage, this paper intends to apply the blockchain technology advantage to the original G2B system, promote the striding of G2B to "Smart Government". Although it still needs the test in time and technology for the blockchain technology extensively applying to different application fields, but the application of blockchain technology in G2B system is an inevitable field in the future application of blockchain. In the future, we will continue to research the blockchain technology and its application in G2B system, further to promote the construction and implementation of G2B system based on blockchain.

7 REFERENCES

[1] Zhu, H. B., Yang, L. X., & Yu, Q. (2010). Investigation of technical thought and application strategy for the internet of things. *Journal on Communications, 31*(11), 2-8.

[2] Liu, Z. W., Wen, Z. L., & Zhang, H. T. (2012). Cloud Computing and Cloud Data Management Technology. *Journal of Computer Research and Development*, 49, 26-31.

[3] Meng, X. F. & Ci, X. (2013). Big Data Management: Concepts, Techniques and Challenge. *Journal of Computer Research and Development, 50*(1), 146-169.

[4] Jin, J. J. (2011). Smart Government: the new stage of e-government development. *Informatization Construction*, 16-17.

[5] Zhang, J. G., Zhu, J. M., & Shang, J. (2015). A summary on domestic and foreign research status and development trend of smart government. *E-Government*, 72-79.

[6] Kavanagh, D. & Miscione, G. (2015). Bitcoin and the Blockchain: a coup d'état in Digital Heterotopia? In *CMS conference 2015*, 8-10. https://doi.org/10.2139/ssrn.2624922

[7] IBM. (2019). What is blockchain? https://www.ibm.com/blockchain/what-is-blockchain (04.02.2019).

[8] Wikipedia. Blockchain. https://en.wikipedia.org/wiki/Blockchain (04.02.2019).

[9] Zhang, S. L. (2011). Design and Security Analysis on Several Cryptography Hash Functions. *PhD dissertation*, BUPT, Beijing, China.

[10] Yu, H. (2010). The Technology of Time Stamp Authority in Electronic Evidence Forensics. *MSc thesis*, DMU, Dalian, China.

[11] Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. Available: https://bitcoin.org/bitcoin.pdf (05.12.2016).

[12] 8BTC. Blockchain. http://www.8btc.com/blockchain (10.10.2016)

[13] Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016). Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. Paper presented at *2016 IEEE Symposium on Security and Privacy (SP)*, 839-858. https://doi.org/10.1109/SP.2016.55

[14] Meredith, L. G. (2015). Linear types can change the blockchain Available: http://arxiv.org/pdf/1506.01001v1.pdf (10.11.2015)

[15] Garay J., Kiayias A., & Leonardos N. (2015). The Bitcoin Backbone Protocol: Analysis and Applications. In: Oswald E., Fischlin M. (eds) *Advances in Cryptology - EUROCRYPT 2015. Lecture Notes in Computer Science*, vol. 9057. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-46803-6_10

[16] Kiviat, T. I. (2015). Beyond Bitcoin: Issues in Regulating Blockchain Transactions, *Duke Law Journal*, 65(3), 569-608.

[17] Birch, D., Brown, R. G., & Parulava, S. (2016).Towards ambient accountability in financial services: Shared ledgers, translucent transactions and the technological legacy of the great financial crisis. *Journal of Payments Strategy & Systems, 10*(2), 118-131.

[18] Zhu, J. M. & Fu, Y. G. (2016). Supply Chain Dynamic Multi-Center Coordination Authentication Model Based on Blockchain. *Chinese Journal of Network and Information Security, 2*(1), 27-33.

[19] Zhao, H., Li, X. F., Zhan, L. K., & Wu, Z. C. (2015). Data Integrity Protection Method for Microorganism Sampling Robots Based on Blockchain Technology. *Journal of Huazhong University of Science and Technology* (*Natural Science Edition*), 43, 216-219.

[20] Xiang, Y. L., Baki, F., Tian, P., & Chaouch, B. A. (2014). A robust blockchain based tabu search algorithm for the dynamic lot sizing problem with product returns and remanufacturing. *Omega, 42*(1), 75-87. https://doi.org/10.1016/j.omega.2013.03.003

[21] Fromknecht, C., Velicanu, D., & Yakoubov, S. (2014). A Decentralized Public Key Infrastructure with Identity Retention. https://eprint.iacr.org/2014/803.pdf.(08.06.2015)

[22] Fromknecht, C., Velicanu, D., & Yakoubov, S. (2014). CertCoin: A NameCoin Based Decentralized Authentication System. *MIT, 6.857 Class Project*, 1-19.

[23] Kuo, T. T., Hsu, C. N., et al. (2018). ModelChain: Decentralized Privacy-Preserving Healthcare Predictive Modeling Framework on Private Blockchain Networks. https://www.healthit.gov/sites/default/files/10-30-ucsd-dbmi-onc-blockchain-challenge.pdf (10.08.2017).

[24] Sun, W. G. (2010). Study on the Technology of Digital Signature, *MSc thesis, Xidian University*, Xian, China.

Contact information:

Yonggui FU, Associate Professor
Corresponding author
School of Information,
Shanxi University of Finance and Economics,
108 Jinyang Street, Taiyuan 030031, Shanxi Province, China
E-mail: fygzcd@163.com

Jianming ZHU, Professor
School of Information,
Central University of Finance and Economics,
39 South College Road, Haidian District, Beijing 100081, China