Blockchain Technology for Next Generation ICT

● Jun Kogure ● Ken Kamakura ● Tsunekazu Shima ● Takekiyo Kubo

Blockchain technology, which supports low-cost decentralized distributed data management featuring tamper resistance, high availability, and transparency, is a breakthrough technology that will lead to the next generation of information and communications technology (ICT). Originally devised to support the Bitcoin digital currency, it is expected to be applied to a broad range of financial applications as well as in various other sectors such as distribution and sharing economies. This broader application requires that several technical challenges including data privacy protection and better processing performance be addressed, and Fujitsu Laboratories is working on several relevant R&D projects. This paper introduces blockchain technology and example applications, describes a technology for achieving security in a business context, and examines Fujitsu's efforts in commercializing this technology and an accompanying service as well as the open source software (OSS) project.

1. Introduction

"Blockchain technology" is the name given to the technology supporting the Bitcoin digital currency. Traditional digital currencies are centralized in a certain mechanism to provide value to electronic data and are only distributed in an area under the control of the mechanism. Conversely, Bitcoin data is managed in a decentralized system. This involves the use of a system in which the value of the electronic data is commonly recognized by all individuals while maintaining its consistency. Bitcoin was introduced as the first-ever digital currency to be globally distributed. This innovative system corresponds to blockchain technology. The incident in which Mt. Gox, a Bitcoin exchange, lost coins belonging to customers in February 2014 did not impair the reliability of Bitcoin itself or its technology. This is no different from the case in which currency is stolen from an exchange company and the company goes bankrupt. The value of the currency is not affected.

This paper explains the application of blockchain technology to the Bitcoin system, information sharing, and other fields, the challenges still to be faced, and our efforts to meet these challenges. It also mentions our involvement in the Hyperledger open source collaborative project.

2. Summary of blockchain technology

This paper initially discusses the method by which a blockchain works in the Bitcoin system. A concept equivalent to a bank account in an ordinary financial transaction is termed an "address" in the context of Bitcoin. A Bitcoin transaction consists of an input and an output address and the amount of bitcoin. A digital signature provided by the owner of the input address guarantees that the transaction corresponds to an intentional act of the owner.

To avoid the duplicate payment problem, a transaction is broadcast through a peer to peer (P2P) Bitcoin network, and its validity is checked by all the participants in the network. A set of data with a collection of legitimate transactions that are recorded every 10 minutes is termed a "block," and a "blockchain" corresponds to a multiple number of blocks that are chronologically connected.

New blocks are created and managed by "miners." A miner who constructs a block with a hash value below a certain threshold receives bitcoin as an incentive. The miners "race" to construct blocks. By varying the number assigned to a domain termed a "nonce" randomly, the hash value of a block also varies randomly. The hash value threshold is set so that a race occurs every

10 minutes in average. The hash value is incorporated into the following block, and thus it is not possible to ensure consistency when old data is modified unless all the following blocks are recalculated. Therefore, it is practically impossible to tamper with a blockchain (as shown in **Figure 1**). Furthermore, all the nodes that join the P2P Bitcoin network share a unique blockchain, thereby simultaneously realizing high availability.

Although Bitcoin transactions are managed individually, they are integrated into a unique and consistent blockchain to realize a shared system of tamper-resistant and highly available information (ledger).

3. Application of blockchain technology to information sharing

The Bitcoin blockchain deals only with Bitcoin transactions as data. However, it can handle various other types of data in principle. Next, a case study is introduced in which a blockchain is applied to a business operation as an information sharing system. This was done in a joint verification experiment with Mizuho Bank regarding cross-border securities trading.

A typical cross-border securities trade takes three days from execution to settlement due to the complicated process involved. This is because a long time period is required to confirm settlement instructions and the content of execution in each process. It is extremely important to reduce this time to avoid risks such as price fluctuation. Previous studies investigated shortening the time by using data sharing via centralized management although it was not realized due to the high system operation and management costs.

The joint verification experiment with Mizuho Bank established a system that recorded a case of execution in a block using the Open Assets Protocol, as shown in **Figure 2**. All the participants involved in the transaction confirmed that it was possible to share the execution information (which evolved into tamper-resistant information) in a short period. This indicated that the entire process could be shortened to less than one day as opposed to three days.

4. Additional fields of application

In addition to its application in the financial field, blockchain technology can be applied to a broad range of fields, such as distribution, supply chain management, document management, and healthcare. It also has potential application to the sharing economy and the Internet of Things (IoT). The technology itself has evolved along with the growing range of application. In addition to digital currency (Bitcoin), various new blockchain frameworks have emerged, including Hyperledger Fabric Framework, which is one of Hyperledger projects[1)] hosted by The Linux Foundation and Ethereum.[2)] These frameworks deal with information involving more general values or rights or including a mechanism termed a "smart contract," which enables automatic contract execution under preset conditions.

Looking at supply chain management as an example, we see that blockchain technology can be used to integrate data (trade records, processing history, and transportation history) that are independently managed by multiple organizations such as material suppliers, manufacturing/processing service providers, and distributors. Two of the expected benefits include efficient manufacturing in accordance with demand and timely recall management by ensuring that the supply chain is traceable from raw material to retail sale. With respect to IoT, blockchain technology can be used to reduce management costs by utilizing smart contracts in which materials are automatically ordered

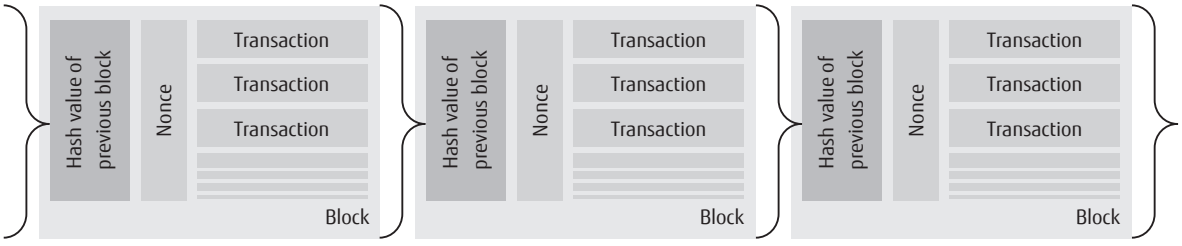

Figure 1
Blockchain structure.

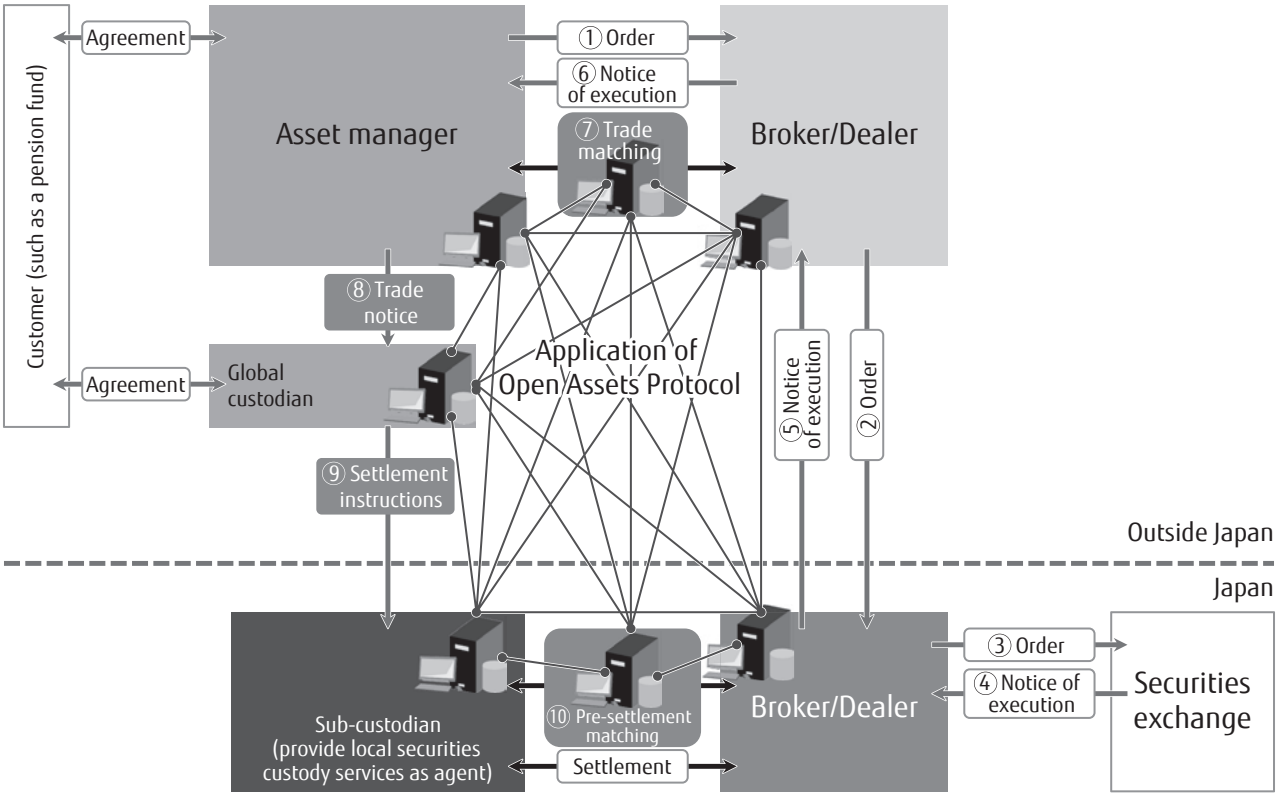

Figure 2
Flows in post-trade settlement process for cross-border transactions.

by the processing machine itself in accordance with the amount processed by the machine.

5. Challenges of blockchain technology

The efforts involved in the application of blockchain technology have highlighted several technical challenges. These include the necessity of more robust security technology that enables its safe use and faster processing speed.

(1) More robust security technology

Blockchain technology is characterized by ensuring security through verification of the transaction information by all network participants, thus preventing illegal activity. This enables an individual outside the blockchain to access a transaction executed within the blockchain. In some cases for some applications, transaction information is not accessible to an individual unless the individual is directly involved in the transaction. A significant challenge relates to the method used for guaranteeing the confidentiality of a transaction by using a blockchain.

(2) Faster processing speed

A blockchain transaction takes more time to process than a conventional transaction as validation by all network participants is required. Therefore, for those applications involving a great number of transactions, improving processing speed is a challenge.

The next section discusses more robust security technology among these challenges.

6. Privacy protection

A characteristic of blockchain technology is that data integrity is guaranteed in a system that allows the nodes constituting the network to equally validate the same data by making the data open. In other words, all the data stored in the blockchain are accessible to every participant in the blockchain network.

To realize privacy protection in a blockchain, encryption can be used to maintain confidentiality when information is made accessible to certain concerned individuals. Information related to a secret key must be shared by the concerned individuals. However, if an

individual loses the key, that individual cannot decrypt the data. Furthermore, if the key is stolen, the information is exposed to the never ending risk of decryption because the data in a blockchain cannot be deleted or modified.

7. Development of document encryption system

We developed a document encryption system using blockchain technology and using a secret sharing scheme for secret key management. In a secret sharing scheme, the secret key is divided into several fragments such that each concerned party possesses a unique piece. The information prior to the division (secret key) can be reconstructed without collecting all the fragments because they are divided in a manner in which a certain number of collected fragments can be used to recover the secret key.

Figure 3 shows the prototype system. Documents are stored in the blockchain, and some of the data is encrypted by means of public key cryptography such that only the parties involved can access the data. A private key corresponding to the public key is required to view the data, and the security is reinforced by the secret sharing scheme.

A key is divided into three pieces, and the parts are given to Party A, Party B, and the document creator. The original private key is said to be reconstructed when two of the fragments are collected. Party A and Party B can thus cooperate to view an encrypted document part.

Creation of the keys and reconstruction of the encrypted document parts are realized in the confidentiality control system, as shown in Figure 3. A web interface is used for access purposes, and the following security measures are provided in which each key holder transfers his/her fragment to the control system.

- Each key fragment is encrypted with the key holder's public key.
- While decrypting the key fragment, the key holder is required to enter a personal identification number (PIN).
- The web application (including the restored information) is shown in the browser via the Secure Sockets Layer (SSL).
- The key fragments decrypted at the terminal are sent to the confidentiality control system using the Diffie-Hellman (DH) key agreement protocol.

It is assumed that a party wants to refer to the document of another company. The encrypted parts of the document are made accessible through a web browser such that a user can work on them from a

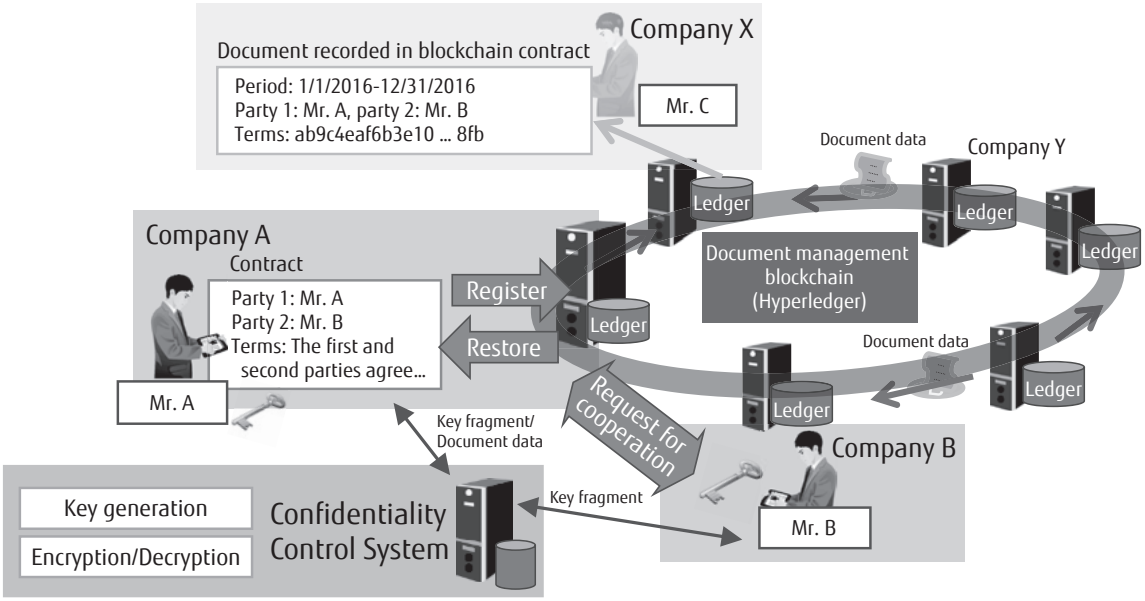

Figure 3
Document encryption in blockchain.

different office. When the prototype system is accessed, it initially shows the list of documents stored in the blockchain. Party A selects one of the encrypted document parts and enters his key fragment (1) and PIN. The document acquired with the key fragment and the blockchain is then sent to the confidentiality control system to notify Party B. When Party B is notified, he/she specifies his key fragment (2) after examining the document that Party A wishes to access. Once his key fragment (2) is sent to the control system, there are sufficient fragments for decryption. The encrypted document requested at the beginning of the process is therefore decrypted and shown in the browser of Party A.

The developed prototype system decrypts the original key by using some of the key fragments (two of the three in this case) on the basis of the secret sharing scheme. The application of this principle provides a solution to the scenario in which a terminal containing the key is lost but the key holder's superiors and other cooperators help in restoring the key. Furthermore, a workflow requiring multiple approvals is realized by considering the acquisition of a key fragment to be an approval of a request.

Another possible countermeasure technology against loss of the key involves examining a technology that links a policy limit on usage to a key. The use of a signed key for a transaction is defined in advance as a policy on file, and this policy is linked to the transaction validation key corresponding to the signature key at the system level. A transaction cannot be registered in a blockchain if it violates the policy linked to the transaction validation key. The mechanism invalidates a transaction when an individual attempts to use a signature key that violates the policy requirements. This technology enables users to limit the recipients and the maximum amount of money transmission, which reduces damage caused by monetary loss.

8. Community participation

To maximize the benefits of blockchain technology, it is necessary to create and mutually link various new business networks to grow them as a whole. This requires a base that can be a de facto standard, and the utilization of open-source software (OSS) is an attractive option

Fujitsu is participating in Hyperledger hosted by The Linux Foundation as a premier member and founder. Hyperledger is an open source collaborative effort created to advance cross-industry blockchain technologies. Fujitsu Laboratories of America is listed as the main contact, and Fujitsu Group corporations worldwide are involved in the project with participation from Japan, Europe, and Australia.

9. Fujitsu's architecture concept

"FMAB," Fujitsu's architecture concept for blockchain technology, was announced in October 2016.[3)]

The FMAB concept involves the use of different layers, such as a data management layer for a blockchain and a business function layer for a business. The layers are seamlessly linked such that the blockchain can be easily used in an enterprise domain. The Hyperledger Fabric Framework is implemented in the data management layer while the business function layer includes data access control and participating members management in which a consortium can be easily established and used. These functions aid in solving privacy issues and long standing challenges for the technology, and they reinforce trust among the consortium participants.

10. Conclusion

This paper discussed confidentiality control technology as a solution for business applications of blockchain technology and Fujitsu's efforts to commercialize blockchain products and accompanying services by introducing the extent to which Fujitsu is involved in the OSS project.

In contrast to a conventional centralized data management system, blockchain technology integrates data in a unique ledger while maintaining consistency although management is decentralized. Therefore, it is a trailblazing technology for implementing low-cost information management systems with tamper resistance and high availability, leading to next generation ICT. Future projects will involve further efforts to expand business applications by developing various component technologies and performing verification experiments.

References

1) The Linux Foundation: Hyperledger. *https://www.hyperledger.org/*

2) Ethereum Project.
https://www.ethereum.org/
3) Fujitsu: Solution for Finance with Blockchain.
http://www.fujitsu.com/jp/solutions/industry/financial/concept/blockchain/

Jun Kogure
Fujitsu Laboratories Ltd.
Dr. Kogure is currently engaged in applied research of blockchain technology.

Ken Kamakura
Fujitsu Laboratories Ltd.
Mr. Kamakura is currently engaged in data security studies.

Tsunekazu Shima
Fujitsu Laboratories Ltd.
Mr. Shima is currently engaged in applied research of blockchain technology.

Takekiyo Kubo
Fujitsu Ltd.
Mr. Kubo is currently engaged in digital business of financial system.

