Fujitsu bolsters blockchain security technology

October 19 2016

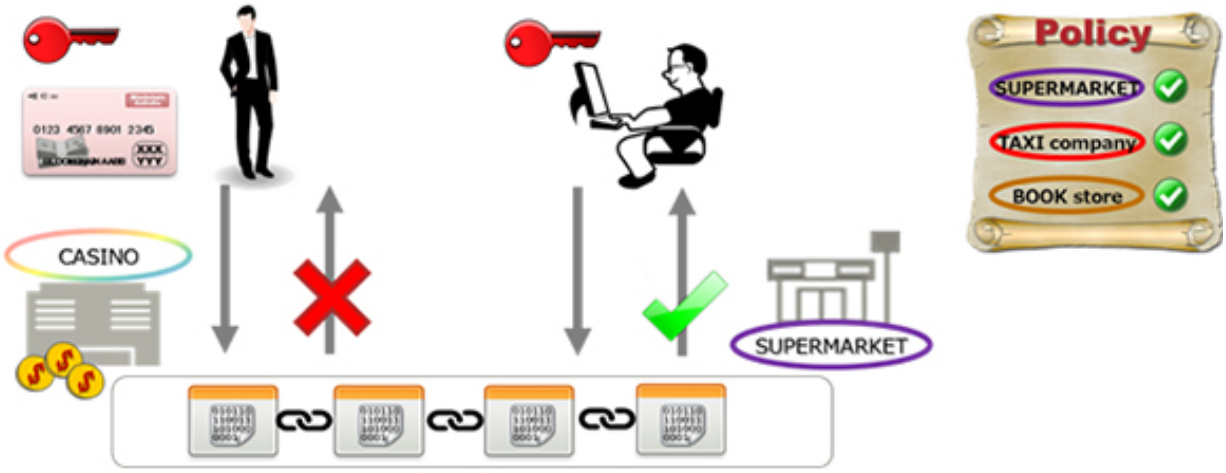


Figure 1: Electronic payment that can only be used at specific stores. Credit: Fujitsu

Fujitsu Laboratories has developed blockchain-based security technologies to safely and securely handle confidential data between multiple organizations. The most prominent characteristic of a blockchain is that it provides information sharing with high transparency and reliability, without management by a specific trusted organization.

On the other hand, in financial trading applications, there are operational issues related to safely executing trades, such as key management. In addition, document management applications preserving the original

state of documents lead to issues in creating a system that could limit which people would be allowed to reference the information recorded in the blockchain. With a view to applying the blockchain to a variety of fields, Fujitsu Laboratories has now developed two technologies: a transaction restriction technology based on pre-established policies to restrict trading, such as by restricting users, and a document encryption technology, which allows only relevant parties who hold multiple distributed keys to securely access the information recorded in the blockchain.

With transaction restriction technology, operations preventing the misuse or abuse of keys become possible, enabling safer use of the blockchain. With document encryption technology, it is also possible to create a workflow where documents are acknowledged by collective decision making or between specified organizations, or where they can be restored when keys are lost. The application of these security technologies will enable Fujitsu Laboratories to contribute to expanding the applicable fields where blockchain can be used, beyond finance to a variety of areas, such as logistics, supply chain, and official document management.

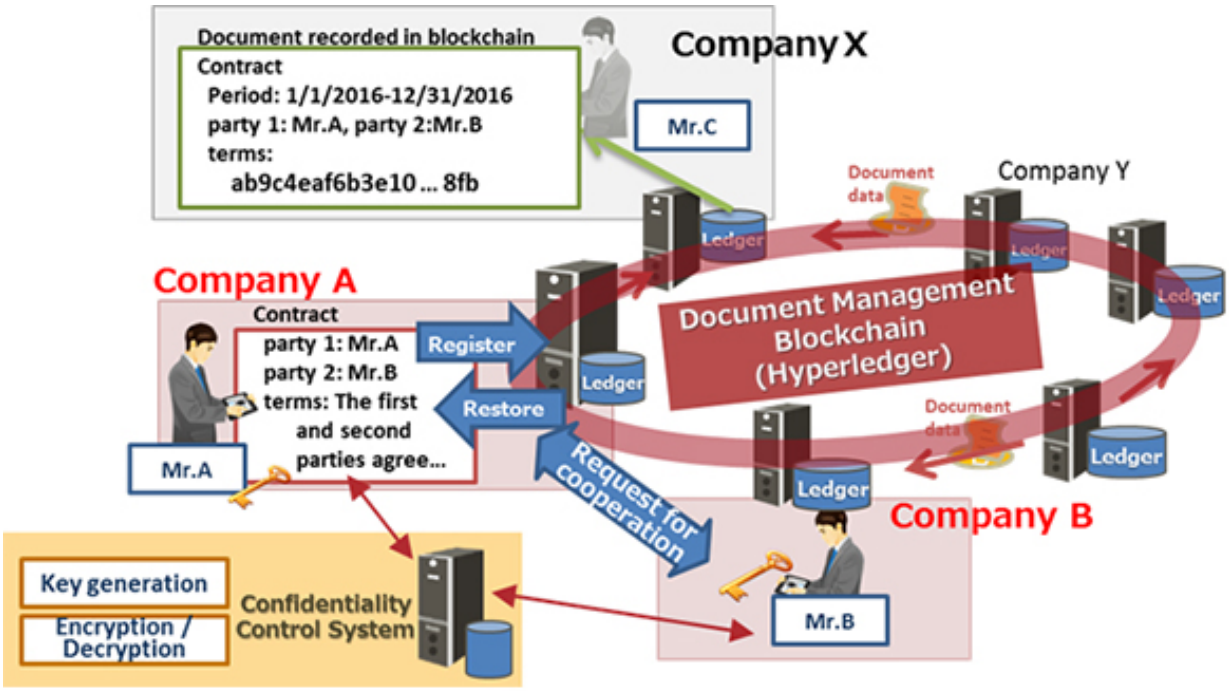
Development Background

A major characteristic of blockchain is that it offers high reliability and transparency by continually preserving records of all past transactions by multiple computers participating in a network to mutually verify and record data, making it virtually impossible to alter. It does so without any specified trusted organization or central server. This is why it has been spotlighted as a new architecture for information systems, and is expected to be applicable in a variety of fields, such as finance, logistics, supply chain, and official document management. Fujitsu Laboratories has focused on blockchain as a technology which will form a new platform for linking information, and has been working with Fujitsu

Limited on field trials and other initiatives, with a view to expanding the applicable fields in which blockchain can be utilized.

Issues

In blockchain, a digital key is needed for each user to execute exchanges or transactions, but generally speaking, if the key is lost, it becomes impossible to transfer monetary funds. One notable issue is that if a key is stolen, all of the funds in an account can be stolen. In addition, to enable transparency there is sometimes a need to make public the fact that a transaction exists between specific organizations, while keeping the transaction's details, such as monetary amounts and stock names, secret and shared exclusively between the few companies involved. However, the fact that blockchain records are shared with all users, has given rise to a major issue in how to secure the confidentiality of information.



Credit: Fujitsu

About the Technologies

Fujitsu Laboratories has now developed two technologies to enable secure transactions on blockchain. Details of these technologies are as follows.

1. Transaction restriction technology

Fujitsu Laboratories has developed a technology that can restrict transactions based on pre-established policies, such as restricting users to specific stores when executing transactions such as sending money. The technology provides a new framework that ties policies to keys used in activities such as capital transfers. The technology ensures that initiated transactions which violate policy requirements are prohibited from getting added to the blockchain as a result of verification failures at multiple computers participating in the blockchain. This makes it possible to limit damage even if a key were to be stolen (Figure 1).

2. Document encryption technology on blockchain through secret sharing-based key management

Storing documents in blockchain can guarantee that the original state of the document will be preserved, but because the content is public to blockchain users, this method is not appropriate to store documents which contain confidential information. Now, Fujitsu Laboratories has applied a secret sharing-based key management system to document encryption, where different portions of a key are held by multiple users

(Figure 2: Mr. A and Mr. B), and once a specified number of pieces have been gathered, a key can be generated. This enabled Fujitsu Laboratories to develop a blockchain document encryption technology which can control who can read the contract documents, where the confidential portions of the contracts will not be visible to ordinary users (Mr. C), and enabling document anonymity control. It can only be read when the parties involved, who hold portions of the key, work together. Fujitsu Laboratories has developed a prototype system on the Hyperledger, an open source blockchain platform (Figure 2).

Effects

With the newly developed transaction restriction technology, it is now possible to prevent the misuse or abuse of keys based on preset policies for secure blockchain operations. In addition, blockchain-based document encryption technology through secret sharing-based key management makes it possible to collaborate to find solutions to lost keys, or to create a workflow that requires acknowledgement from multiple managers when making collective decisions involving large transaction amounts. With these technologies, Fujitsu Laboratories is contributing to expanding applicable fields for blockchain, moving beyond finance to a variety of areas such as logistics, supply chain, and official document management.

Fujitsu Laboratories is carrying out trials of the applicability of blockchain to business in finance and a variety of other areas, as a cloud platform that can safely and securely handle confidential information and personal data between multiple organizations, aiming for commercialization of this technology from fiscal 2017 onwards.

Provided by Fujitsu