ConnectionChain: Security Technology for Securely Linking Blockchains

● Shingo Fujimoto ● Jun Kogure

Blockchains, which are used to manage virtual currency, are expected to be used in many different fields as a distributed ledger technology that enables secure transactions among multiple blockchain participants through a decentralized operation. To increase the value of blockchains, it is necessary to link various blockchains. However, such linking at an application level is insufficient to ensure transparency, as shown by the possibility of unauthorized operations by system operators. There is also a need to deal with errors that may occur when these operations are performed. Fujitsu Laboratories has developed ConnectionChain, a security technology for securely linking and operating different blockchains. This paper presents the features of ConnectionChain and its prototype systems.

1. Introduction

Blockchains are a form of distributed ledger technology (DLT) for managing transactions and records used for virtual currency. As a technology that can facilitate collaboration among multiple blockchain participants (hereafter, players), its application to a variety of fields in addition to finance is expected.

Bitcoin, a type of virtual currency that uses a blockchain, has been operating continuously without a single shutdown since its launch in 2009. However, there have been many reports to date of disappearing or leaked coins at virtual currency exchanges. Yet, it has become clear that such incidents have occurred because of improper operations by system administrators rather than a problem with the blockchain technology itself. Operating a blockchain safely can be difficult, and for this reason, many platform technologies and cloud services are being prepared.

Against this background, Fujitsu Laboratories has developed ConnectionChain as a security technology for safely connecting different blockchains.

This paper first describes the blockchain mechanism and associated issues. It then introduces the features of ConnectionChain and its prototype systems for subsequent trials.

2. Blockchain mechanism

This section describes the blockchain mechanism.

2.1 Data recording in a blockchain

A blockchain consists of computers called “nodes” that interconnect with each other on a peer-to-peer (P2P) network. Each node holds a copy of a ledger for managing various types of digital assets, which gives the blockchain high availability. A blockchain also uses hash functions[note 1)] and public-key cryptography[note 2)] to prevent data tampering.

A blockchain records target data, i.e. transaction data, in the ledger in units of “blocks,” each of which groups multiple items of transaction data (**Figure 1**). Each block of data is protected by a hash value calculated by a hash function. This hash value covers not only the transaction data to be recorded but also the hash value of the immediately previous block (prior block). In other words, the hash value given to each

note 1) Technology for guaranteeing consistency by making it easy to detect tampering in accordance with differences in output hash values.

note 2) Technology that permits only a player owning a private key to create a signature and enables the validity of that signature to be verified with a public key.

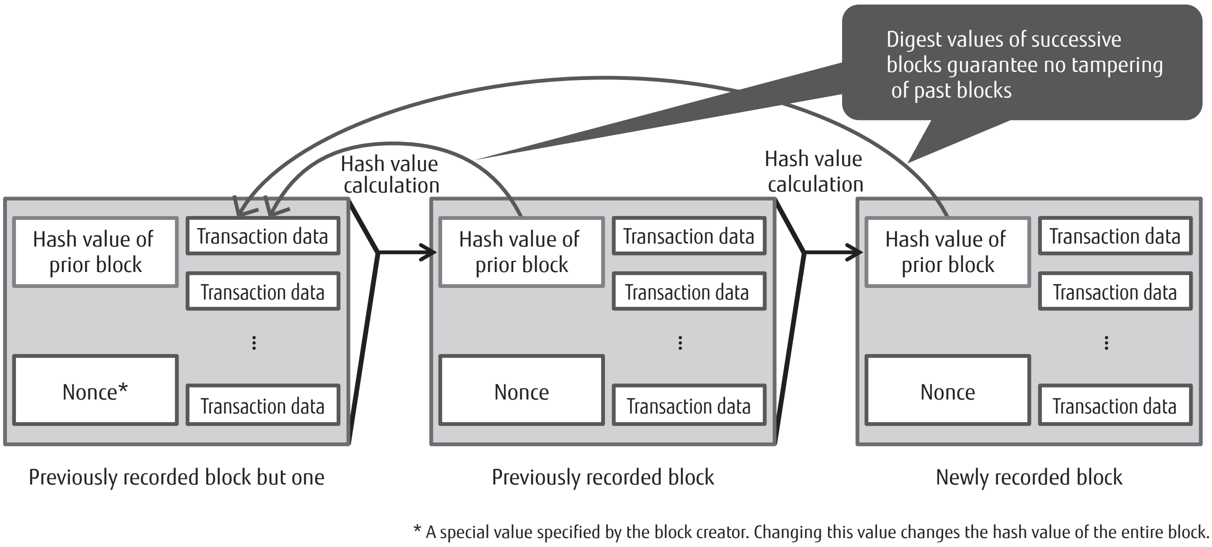

Digest values of successive blocks guarantee no tampering of past blocks
Hash value calculation
Hash value calculation
Hash value of prior block
Transaction data
Transaction data
Nonce*
Transaction data
Hash value of prior block
Transaction data
Transaction data
Nonce
Transaction data
Hash value of prior block
Transaction data
Transaction data
Nonce
Transaction data
Previously recorded block but one
Previously recorded block
Newly recorded block
* A special value specified by the block creator. Changing this value changes the hash value of the entire block.

Figure 1
Blockchain mechanism.

block indirectly protects the immediately previous block. This interlocking chain provides added protection for the data recorded in the blockchain.

2.2 Blockchain features

The following describes the blockchain features enabling secure data management.

1) High-reliability P2P-based network

A conventional data management system generally operates by centralized data management under a system administrator, which makes it difficult to deal with fraudulent activities like data tampering or concealment. Blockchains, on the other hand, can detect tampering of transaction data through a chain of hash values calculated from the data of previously recorded blocks. In addition, the ledger consolidating the results of executing transactions is stored on each node, which compares the ledger it holds with that of other nodes in a process of mutual monitoring. The end result is a high-reliability network for transaction data.

2) Public and shared transaction ledger

Ensuring data consistency in conventional data management systems is difficult when sharing data by means of a ledger. In a blockchain, however, each node has a copy of the ledger via a P2P network so that each player can check for data consistency using its own ledger.

3) Robust verification of data operations

As described above, a conventional data management system operates under centralized management, and as a result, there have been occurrences of erroneous data operations or fraudulent operations by system administrators. Blockchains, in contrast, have a function called a “smart contract” that distributes authority to multiple participating nodes and performs data operations in accordance with predetermined processing rules. With this function, a ledger operation will be reflected only when the result of processing at each node has been verified and the results at all nodes are in agreement.

3. Issues in using blockchains

This section discusses issues in the use of blockchains as background to the development of ConnectionChain.

3.1 Ensuring transparency in connecting blockchains

It is said that more than 2,300 types of virtual currency were in circulation throughout the world as of September 2019.[1)] Virtual currency can be purchased using actual money and converted to other types via a virtual currency exchange. In Japan, legislation on the operation of virtual currency exchanges including a registration system is progressing on the basis of guidance from related ministries and agencies, but incidents of virtual currency leaks are nonetheless occurring frequently.

Furthermore, in addition to virtual currency, the types of digital assets managed by blockchains have been increasing, and have come to include package delivery status and access rights to data content. The management of such digital assets other than virtual currency, while not accompanied by the transfer or exchange of assets, involves the recording of asset state transitions. However, the validity of that recording is often guaranteed outside of blockchains, so deciding on strict operation rules is difficult. As a result, transparency in the processing performed when making connections between blockchains in this case cannot be ensured.

3.2 Exception processing in ledger operation

Although dependent on the type of blockchain, a certain amount of time is generally needed to settle a ledger operation. In addition, there are cases in which a transaction can span multiple blockchains even if the players in that transaction are not mutually trustworthy. In such a case, it is convenient to have an escrow transaction that can initiate the transaction after guaranteeing that the associated charge can be paid and that can cancel the receipt or payment of the charge if the entire transaction should fall through for some reason.

In such time-absorbing or escrow transactions, it must be kept in mind that some transactions may not complete. One means of dealing with such a situation is to use a smart contract as described earlier to suspend an incomplete transaction and return the transaction back to where it started. However, this function operates only on a single blockchain, and as a result, it has not been possible to handle transactions across multiple blockchains or to execute exception processing at the time of an error.

4. Features of ConnectionChain

To resolve the issues described in the previous section, Fujitsu Laboratories developed ConnectionChain security technology for securely connecting blockchains.

4.1 Highly-transparent blockchain connections

With the aim of enhancing the transparency of connection processing between different blockchains, we adjusted the existing smart contract function that has so far been used on single blockchains only. We achieved the execution of this extended smart contract for connecting multiple blockchains on ConnectionChain.

ConnectionChain uses a “connection node” for operating on a connected blockchain as a single node. A connection node has a function for receiving instructions from the smart contract and performing ledger operations such as asset transfer and a function for receiving block data targeted for connection and recording the results of ledger operation in an evidence management ledger. This scheme enables a series of ledger operations spanning different blockchains to be verified by viewing the evidence management ledger (**Figure 2**).

4.2 State management in support of error processing

ConnectionChain can deal with cases in which a

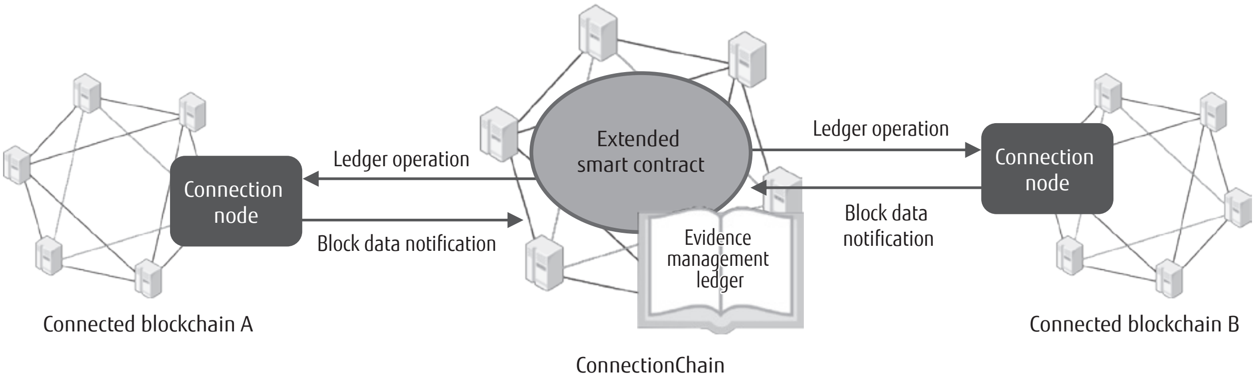


Figure 2
Extended smart contract in ConnectionChain.

transaction has not been fully completed, for example, by providing a function for putting a transaction into a pending state or restoring the state before the transaction began. This function incorporates the concept of escrow payments in which secure payments are made via a third party. The main point here is that ConnectionChain prepares an account that only it can operate on for the connected blockchain.

In this way, if the need to put a payment on hold arises, ConnectionChain will move assets to the escrow account that it can access instead of moving those assets to the intended destination. In addition, ConnectionChain can determine whether payment conditions have been satisfied and automatically transfers the deposited assets to the intended destination or retransfers the assets to a player's account.

5. Application of ConnectionChain technology

In this section, we introduce two prototype systems as specific examples of using ConnectionChain.

5.1 Virtual currency settlement system

A virtual currency settlement system provides a function for exchanging virtual currency. The development of such a system originates in the recent appearance of "regional digital currencies" that can be used by certain municipalities in Japan. The issuing of such regional digital currencies is being accompanied by many trials to promote consumption by local residents. The prototype system used in the trial introduced here is a settlement system supporting payments by regional digital currencies managed by different blockchains. The system enables regional digital currency that an individual holds to be used outside of that region.

This system enables a user to use a regional digital currency settlement system via a web browser without having to install a special application on a smartphone. Additionally, compared to the operation of a paper-based region-specific coupon system, in which printing can incur high costs to deter counterfeiting, this system has the advantage of a low-cost secure operation.

As an example, we describe a use case in which two shopping districts that use different regional digital currencies are connected as part of a promotional campaign (**Figure 3**). In this example, a resident, Hanako, is thinking of using regional digital currency A that she holds to purchase a book at bookstore X that handles regional digital currency B. With existing technology, Hanako would first have to exchange her currency at a regional digital currency exchange before making payment at bookstore X. This would require Hanako to create an account to receive regional digital currency B from the

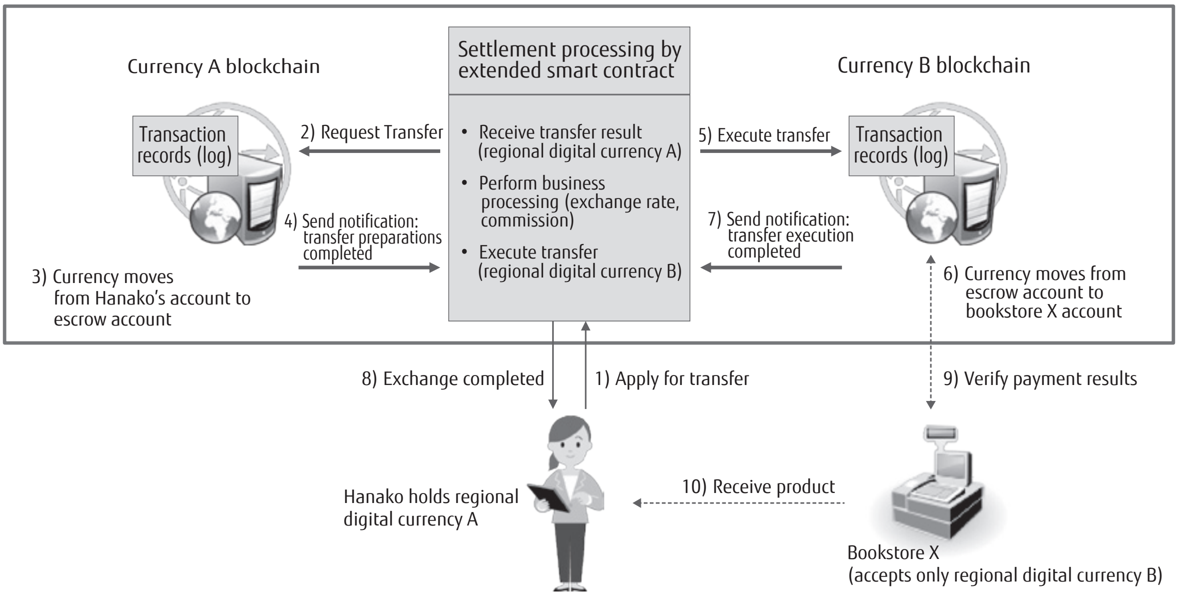

Currency A blockchain
Settlement processing by extended smart contract
Currency B blockchain
Transaction records (log)
2) Request Transfer
• Receive transfer result (regional digital currency A)
• Perform business processing (exchange rate, commission)
• Execute transfer (regional digital currency B)
5) Execute transfer
Transaction records (log)
4) Send notification: transfer preparations completed
7) Send notification: transfer execution completed
3) Currency moves from Hanako's account to escrow account
6) Currency moves from escrow account to bookstore X account
8) Exchange completed
1) Apply for transfer
9) Verify payment results
Hanako holds regional digital currency A
10) Receive product
Bookstore X (accepts only regional digital currency B)

Figure 3
Example of using regional digital currency.

exchange. Furthermore, in the event that the book she wanted to purchase is sold out, Hanako may be left with regional digital currency B that she has no other need for.

Our prototype virtual currency settlement system could resolve these issues by executing an extended smart contract that would enable "payment of a fee denominated in regional digital currency B to be made in regional digital currency A." Such a contract would enable Hanako to purchase the book at bookstore X without having to worry about the transfer mechanism of regional digital currency or the exchange rate and without having to create an account in regional digital currency B.

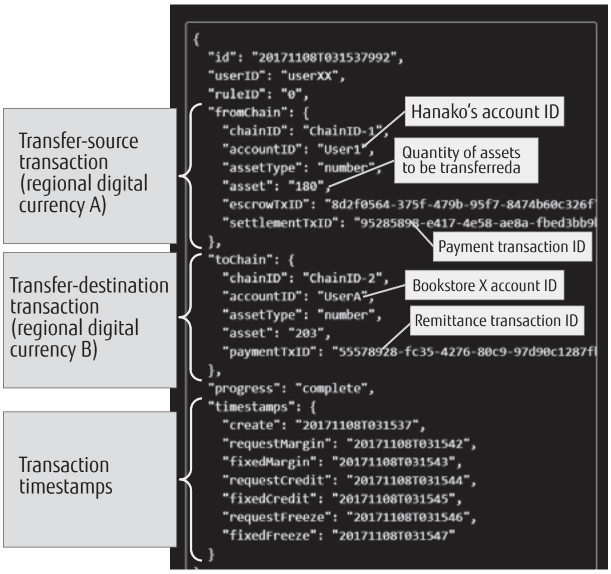
The ConnectionChain transaction record that records the results of executing an extended smart contract is shown in **Figure 4**. In this transaction record, the results of a series of operations executed automatically by ConnectionChain are recorded in the form of transaction IDs and timestamps in the blockchains performing the operations. This makes it possible to verify the validity of a transaction at any time.

In addition, if the book could not be sold at bookstore X for whatever reason, the extended smart contract can cancel the purchase by returning the virtual currency deposited by Hanako to her account.

5.2 Billing system for data usage

The second prototype system enables automatic billing for data usage fees. This system consists of two connected blockchains; one for data management (hereafter, data management blockchain) and the other for payment tokens (hereafter, token management blockchain).

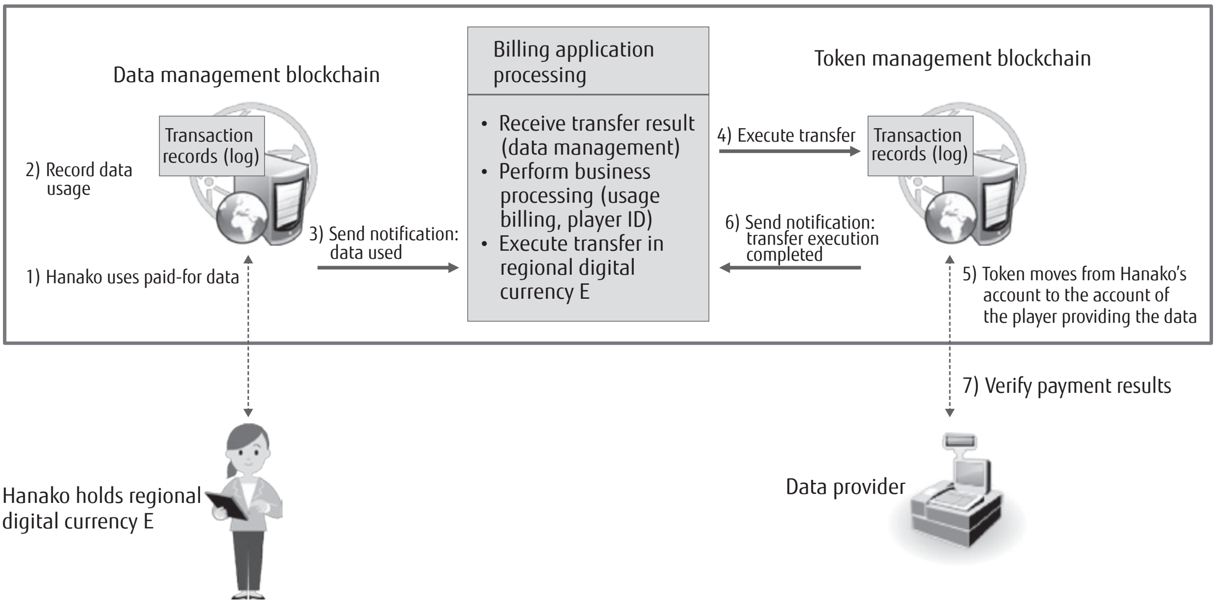
In the example shown in **Figure 5**, Hanako



```
{
  "id": "20171108T031537992",
  "userID": "userXX",
  "ruleID": "0",
  "fromChain": {
    "chainID": "ChainID-1",
    "accountID": "User1",
    "assetType": "number",
    "asset": "180",
    "escrowTxID": "8d2f0564-375f-479b-95f7-8474b60c326f
    "settlementTxID": "95285898-e417-4e58-ae8a-fbed3bb9
  },
  "toChain": {
    "chainID": "ChainID-2",
    "accountID": "UserA",
    "assetType": "number",
    "asset": "203",
    "paymentTxID": "55578928-fc35-4276-80c9-97d90c1287f
  },
  "progress": "complete",
  "timestamps": {
    "create": "20171108T031537",
    "requestMargin": "20171108T031542",
    "fixedMargin": "20171108T031543",
    "requestCredit": "20171108T031544",
    "fixedCredit": "20171108T031545",
    "requestFreeze": "20171108T031546",
    "fixedFreeze": "20171108T031547"
  }
}
```

Transfer-source transaction (regional digital currency A)
Transfer-destination transaction (regional digital currency B)
Transaction timestamps
Hanako's account ID
Quantity of assets to be transferreda
Payment transaction ID
Bookstore X account ID
Remittance transaction ID

Figure 4
Example of asset transfer records in regional currency exchange system.



Data management blockchain
Transaction records (log)
2) Record data usage
1) Hanako uses paid-for data
3) Send notification: data used
Billing application processing
• Receive transfer result (data management)
• Perform business processing (usage billing, player ID)
• Execute transfer in regional digital currency E
4) Execute transfer
6) Send notification: transfer execution completed
Token management blockchain
Transaction records (log)
5) Token moves from Hanako's account to the account of the player providing the data
7) Verify payment results
Hanako holds regional digital currency E
Data provider

Figure 5
Billing system linked to data usage.

performs an operation to obtain data using the data management blockchain. Specifically, whenever Hanako performs a data-acquisition operation, transaction data is recorded in the data management blockchain. This blockchain is connected to the token management blockchain for billing purposes (regional digital currency E) by a smart contract that bills in accordance with the amount of data used. In this way, ConnectionChain detects data usage via the connection node of the data management blockchain every time a transaction is recorded. Then, in accordance with the bill set in the smart contract, ConnectionChain automatically transfers assets from Hanako's account in the token management blockchain to the account of the player providing the data.

6. Conclusion

This paper introduced the ConnectionChain security technology developed by Fujitsu Laboratories for securely linking different blockchains.

Blockchain technology enables secure transactions among multiple players, so it is exactly in use cases involving many players that its true value comes to light. ConnectionChain is a technology that provides security for more complex online transactions without losing the inherent features of blockchains, and that can therefore uncover even more possibilities in the use of blockchain technology. Going forward, Fujitsu aims to accumulate more results through trials with the aim of achieving a practical implementation of ConnectionChain and contributing to the co-creation of business in this area.

References

1) CoinMarketCap: Cryptocurrency by Market Capitalizations. *https://coinmarketcap.com/*

Shingo Fujimoto
Fujitsu Laboratories Ltd.
Mr. Fujimoto is currently engaged in blockchain application research.

Jun Kogure
Fujitsu Laboratories Ltd.
Dr. Kogure is currently engaged in blockchain application research.