Proof of Concept of Blockchain Technology in the Field of Finance Using Hyperledger Fabric 1.0

TORIYAMA Shinichi, OKABE Tatsuya, TANAKA Shuntaro, KANEKO Yusuke

Abstract

A blockchain is a distributed ledger system that allows the participants to share and record data without using a centralized management system. This paper introduces a PoC that was performed through inter-company collaboration operations in order to verify the applicability of blockchain to the IT systems of financial institutions with high system requirements for quality. The results have proven that Hyperledger Fabric 1.0, which was the blockchain platform adopted in the PoC, can meet many system requirements for operability/maintainability and security, but also that, it still has some issues that need to be addressed, such as resistance to falsification and implementation of a cryptography function.

Keywords

Blockchain, Hyperledger Fabric, inter-company collaboration

1. Introduction

A blockchain is a distributed ledger system proposed by Satoshi Nakamoto to serve as the basis of Bitcoin. It is a mechanism that allows participants to share and record data without using a centralized management system[1]. As of 2018, various enterprises even outside the financial field are conducting R&D and PoC (Proof of Concept) of this technology.

This paper introduces the PoC jointly conducted by NEC Corporation, Sumitomo Mitsui Financial Group, Inc. and The Japan Research Institute, Limited in order to verify whether a system incorporating blockchain can meet the quality standards of financial businesses with high system requirements for quality, including the reliability and security of IT systems.

2. Purpose and Process of PoC

The purpose of the PoC was to determine the feasibility and effectiveness of the construction and operation of a system using blockchain by setting up an inter-company collaboration system involving financial institutions as the use case. The reason why we focused on inter-company collaboration is that it has a high affinity with blockchain in the following properties.

- Automation of check processing with high authenticity
- Saving of workflow execution history with high authenticity

2.1 Selection of evaluation items

We then selected the items to be verified by considering the following two points that are indispensable for the implementation of IT systems for financial institutions.

(1) Operability/maintainability

Verification was conducted under an environment that was built so as to identify the operation functions (node startup/shutdown, failure notification, etc.) required for the blockchain inter-company collaboration system.

(2) Security

The blockchain inter-company collaboration system was verified in the verification environment so as to

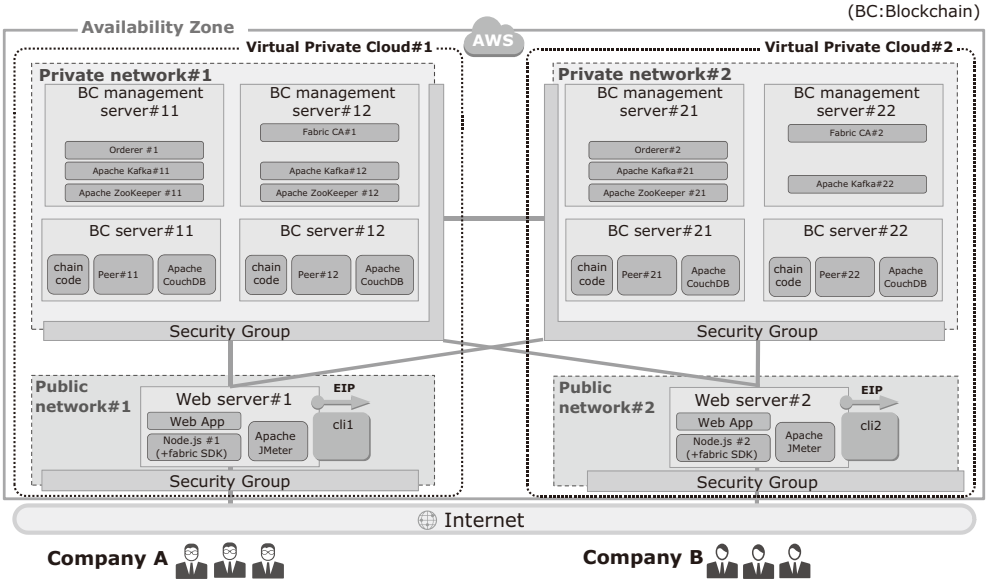

Fig. 1 Overall view of verification environment.

determine its compliance to the security functions (data secrecy, access limitation, illegality tracking, etc.) to be provided by the system.

2.2 Verification environment

The outline of the verification environment is summarized below. The overall view is shown in **Fig. 1**.

- Configuration: 2 organizations, total of 10 servers with 5 in each organization
- Built on the AWS (Amazon Web Services). All of the servers have an instance type of t2.medium (3.3 GHz x 2v CPU, 4 GB memory)[2].

The blockchain platform used was Hyperledger Fabric 1.0 (hereinafter "Fabric 1.0") which is open source software (OSS)[3][4]. Fabric 1.0 can be divided roughly into the processing block and data block and is composed of three elements including the "smart contract", "business data", and "historical data". With Fabric 1.0, the "smart contract" is described as a chaincode and the "business data" is stored as a database in the Key Value Store (KVS) format. An example of configuration is shown in **Fig. 2**.

For the verification environment, the following two items were developed in addition to the user interface screen.

- **Caller application**
  Written in the JavaScript language, this app processes the requests from the user interface screen and calls the chaincode.
- **Chaincode**
  Written in the Go language, this executes the business logics.

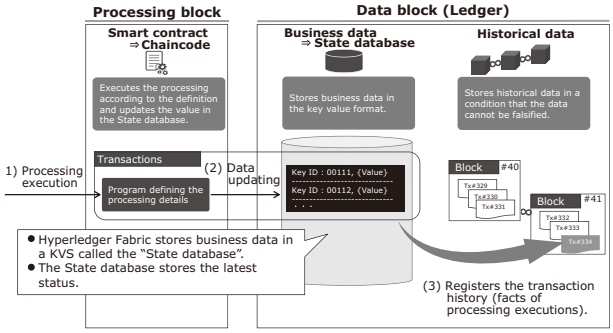

Fig. 2 Configuration of blockchain of Fabric 1.0.

3. Results of PoC

Table 1 summarizes the results of the verified items. While it was proven that Fabric 1.0 can meet many system requirements for operability/maintainability and security, it was also found that some requirements have not yet been met. This section discusses the results in detail.

3.1 Operability/maintainability

Table 2 shows the details of the results. One of the points to be noted is that a node storing falsified data cannot detect the falsification itself. This was because the hash-chain verification during block addition of the node was insufficient. However, propagation of falsified data to other nodes did not occur. In addition, two problems in the specifications of Fabric 1.0 were discovered in the verification using the actual system.

Table 1 Results (Overall summary).

#	Verified items	Goal (Requirement)	Results
1	Data backup & archiving possibility	It should be possible to store data spanning ten years.	△ Table2
2	Effects of app addition/ modification on services	Services should not shut down during addition or modification of apps.	○
3	Restoration after node failure	In case of node shutdown, re-access to the system should be possible without affecting services.	○
4	Service monitoring possibility	The system for monitoring the whole service should be clarified explicitly.	○
5	Existence of single point of failure	Services should not shut down due to a single failure.	○
6	Effects of single organization failure on services	Services should not shut down due to a failure of a single organization.	△ Table2
7	Permissible number of node failures	The number of node failures caused by a single failure should be below the permissible number.	○
8	Falsification resistance	No node should be falsified even when a single node is falsified.	△ Table2
9	Cryptography	The mechanism for ensuring data secrecy should be provided.	△ Table3
10	Authority management	The mechanism for limiting accesses should be provided.	△ Table3
11	Falsification detection	The mechanism for tracking illegalities should be provided.	△ Table3

(○: No problem. △: Problematic <workaround available>. ×: Problematic <workaround not available>).

Table 2 Detailed results of unachieved items (Operability/maintainability).

Verified items	Verified results	See Table 1
Data backup & archiving possibility	Disk addition or archiving becomes necessary when the transaction amount is high.	1
Effects of single organization failure on services	When all the servers in one organization are down in the two-organization system, shutdown of services occurs (because the block generations are stopped due to the split-brain syndrome of the distributed messaging system).	6
Falsification resistance	The falsified data is not self-detected by the falsified node, and the falsified data continues to be processed. The falsified data is not self-detected by the falsified node, and the falsified data continues to be processed.	8
Isolation between apps and platform	The caller app is modified every time the number of organizations is changed.	*
Exclusive control of transactions	Isolation between the master data (read) and transaction data (appended) in the KVS is necessary.	*

(*Items that were proved additionally by the verification)

3.2 Security

Table 3 shows the details of the results. While the problems related to falsification resistance were pointed out in Section 3.1 above, it can be said that Fabric 1.0 is insufficient in certain functions including data secrecy, access limitation, and illegality tracking. These functions may be added in a future upgrade of Hyperledger Fabric.

Table 3 Detailed results of unachieved items (Security).

Verified items	Verified results	See Table 1
Cryptography	An encryption mechanism should be provided additionally because the data (history, KVS) is open to the public. The private key should be managed in encrypted rather than plaintext form.	9
Authority management	User authentication is necessary when the system is controlled by a general user.	10
Falsification detection	An audit log is required for use in investigations in case of an illegal action.	11

4. Considerations on PoC Results

The results of the PoC suggests the necessity of further study and verification, such as by implementing an external system that supplements the currently lacking functions in order to employ Fabric 1.0 as a financial service platform. **Fig. 3** shows an example of system configuration designed after viewing the obtained results.

4.1 Operability/maintainability

(1) Falsification resistance

As the hash-chain verification, which is the key to the falsification resistance of the blockchain, is insufficient with Fabric 1.0, addition of functions is necessary to enable application to the IT systems used for financial institutions.

(2) Data archiving

With Fabric 1.0, both the "historical data" and "business data" continue to increase. Each system using the blockchain is therefore required to measure the amount of data increase and the degradation level of the response performance against the increasing data amount. In consideration of the measurement results, it is necessary to examine the necessity of archives.

4.2 Security

(1) System configuration

With the system configuration of Fabric 1.0, it is required to place the KVS server in the internal network in order to improve the resistance against attacks to the database storing the business data (**Fig. 4**).

(2) Audit log

Fabric 1.0 does not have the function to record the audit log, but since the IT systems for financial institutions are often required to trail data accesses, it is therefore essential to introduce additionally a

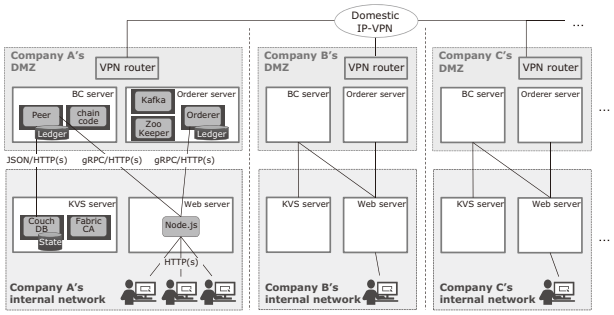

Fig. 3 System configuration after viewing the PoC results.

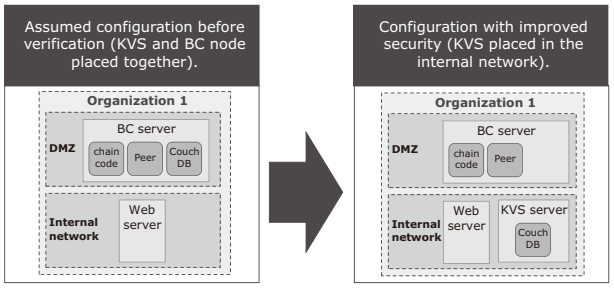

Fig. 4 Placed segments.

mechanism for taking the audit log.

(3) Key control

Fabric 1.0 does not have the function to control the private keys. In general, the security of blockchain platforms is guaranteed on the premise that the private key cannot be stolen. Therefore, when it is used with financial services, the private key control method should be examined separately. This issue can be dealt with by, for example, using the PKCS (Public Key Cryptography Standards) in the control of the keys.

5. Conclusion

By examining an inter-company collaboration system as the use case, the present paper clarified how much Fabric 1.0 can and cannot meet the quality standards required by financial businesses, and indicated the points to note in the building of IT systems for financial institutions adopting the blockchain. Blockchain is expected to have a wide scope of application other than virtual currency transfer. It is expected to be introduced in various business fields all over the world, such as in sharing valuable information and in implementing a sharing economy in society that leverages the "smart contract" function. Nevertheless, before blockchain can be applied to real businesses, there are still issues to be cleared, such as the items clarified by the PoC described in the present paper. Since blockchain has only a few use cases other than virtual currency, it may be necessary to launch an external security audit and identify risks in greater detail by re-inspecting the functions that are necessary but not presently provided. In order to enable application of the blockchain in real businesses, NEC will carry out (1) an additional PoC with the system as a complement to clarify the PoC described herein, (2) expansion of the application scope by considering social environment trends, and (3) promotion of diffusion of Hyperledger Fabric based on feedback of obtained knowhow. NEC is determined to contribute to the development of business through the creation of a bright society that can meet the challenges of the future. Furthermore, the Sumitomo Mitsui Financial Group and The Japan Research Institute aim to use new information technologies proactively, thereby adapting to an increasingly fast-changing environment, and ultimately to become a more competitive and innovative financial group and continuously upgrade the quality of customer service.

Reference

1) Satoshi Nakamoto:Bitcoin: A Peer-to-Peer Electronic Cash System
https://bitcoin.org/bitcoin.pdf
2) Amazon Web Services (AWS)
https://aws.amazon.com/
3) Master Documentation
https://hyperledger-fabric.readthedocs.io/en/release-1.0/
4) Hyperledger
https://www.hyperledger.org/

Authors' Profiles

TORIYAMA Shinichi
Manager
Financial Systems Development Division

OKABE Tatsuya
Assistant Manager
Financial Systems Development Division

TANAKA Shuntaro
Advanced Technology Laboratory
Development Promotion Division
The Japan Research Institute, Limited

KANEKO Yusuke
IT Innovation Department
Sumitomo Mitsui Financial Group, Inc.

The details about this paper can be seen at the following.

Related URL:

NEC Corporation
https://www.nec.com/

Sumitomo Mitsui Financial Group,Inc.
http://www.smfg.co.jp/english/

The Japan Research Institute, Limited.
https://www.jri.co.jp/english/

Information about the NEC Technical Journal

Thank you for reading the paper.
If you are interested in the NEC Technical Journal, you can also read other papers on our website.

Link to NEC Technical Journal website

Japanese English

Vol.13 No.1 Sustainable Data-driven City Management

Vol.13 No.1
November 2018

Special Issue TOP

Remarks for Special Issue on Sustainable Data-driven City Management
Start-up of Data Utilization-type Smart Cities

Papers for Special Issue

Vision for Data-driven City Management
Global Perspective for Data-Leveraged Smart City Initiatives
A Paradigm Shift in City Management Practices Targets the Sustainable Society

Demonstration and Implementation Examples of Data-driven Smart Cities
Case Study of Data-driven City Management in Cities Abroad
Building a Common Smart City Platform Utilizing FIWARE (Case Study of Takamatsu City)
Initiatives to revitalize regional economies by advancing "*OMOTENASHI*"
— Hospitality offered to foreign visitors to Japan
Case Studies of Data Utilization by Municipal Governments:
Applying Data in Various Fields Such as Financial Affairs, Childcare, and Community Revitalization

City Management Technologies
FIWARE, Information Platform for Implementing Data Utilization Based City Management
FogFlow: Orchestrating IoT Services over Cloud and Edges
Security Requirements and Technologies for Smart City IoT
European Trends in Standardization for Smart Cities and Society 5.0
City Evaluation Index Standards and their Use Cases

Co-creation with Local Communities
An Introduction to "Partnership for Smart City Takamatsu" as a Platform to Engage in Local Co-creation Activities
Launch of Setouchi DMO — A Co-Creation Venture That Goes beyond the Conventional ICT Framework
Community Co-creation Based on a Comprehensive Cooperation Agreement
A Common-Sense Approach to the Future — Study Group for Co-creation of New Municipal Services

General Papers

Spin-Current Thermoelectric Conversion — Informatics-Based Materials Development and Scope of Applications
Reducing the Power Consumption and Increasing the Performance of IoT Devices by Using NanoBridge-FPGA
Development of Nano-carbon Materials for IoT Device Applications
Proof of Concept of Blockchain Technology in the Field of Finance Using Hyperledger Fabric 1.0

NEC Information

NEWS
2017 C&C Prize Ceremony