Verification report on the construction of an advanced “Know Your Customer” (KYC) platform using blockchain technology

Blockchain Study Group

Mizuho Financial Group Inc.

Sumitomo Mitsui Financial Group Inc.

Mitsubishi UFJ Financial Group Inc.

Deloitte Tohmatsu Group

July 13, 2018

1. Overview of the Blockchain Study Group

(1) Background and goals of establishing the study group

The financial industry has recently seen remarkable development in the field of FinTech, a term used in reference to innovative technologies combining finance and IT. Such developments are bringing about the emergence of innovative financial services as alternatives to existing services. Among these, blockchain technology, used in cryptocurrencies such as Bitcoin, appears to be highly compatible with operations related to matters such as transfers, payments, and securities transactions due to its characteristics, which include resistance to falsification and high availability. Going forward, expectations for the use of blockchain in the financial sphere are high.

Centered on the financial industry, we are seeing vigorous research into blockchain technology, including verification testing, with global competition intensifying as various actors seek to achieve practical implementation and to define de facto standards. European and North American financial institutions have been particularly active in this regard.

In such an environment, we see blockchain as one of the technological elements necessary for the continued growth of the Japanese economy. The ultimate goal of the Blockchain Study Group is for Japanese financial institutions to contribute to constructing the foundation of this technology while raising their technological prowess to a level on par with their European and North American counterparts. This study group was founded in December 2015 with the initial aims of specifying the scope of blockchain use in financial systems and establishing a path to practical implementation.

(2) Position of the study group

The members of the Blockchain Study Group, which conducts research into blockchain technology, are Mizuho Financial Group Inc., Sumitomo Mitsui Financial Group Inc., Mitsubishi UFJ Financial Group Inc., and the Deloitte Tohmatsu Group.

The study group selects banking services to which blockchain technology could be applied, drafts prototypes, confirms operations and conducts operational verification, and evaluates results. If the usefulness of blockchain technology is established through this process, the group is also prepared to develop official specifications with a view to practical utilization in the future.

The drafting of prototypes does not depend on the technology of any specific blockchain operator, as operators are selected from a pool of several candidates on the basis of criteria established by the study group, after which prototypes are drafted through technical cooperation with the operators.

The basic policy of the study group is to establish a path to the practical implementation of blockchain technology through the study of said technology. Its aim is to contribute to the development of the financial industry in Japan.

(3) Current theme

Following the “Report on Practical Experiment of Blockchain Technology in Japanese Domestic Interbank Payment Operation by the Blockchain Study Group[1],” issued in November 2016, the Blockchain Study Group conducted a new project, “Verification of the Application of Blockchain Technology to Advanced ‘Know Your Customer’ (KYC) Platforms,” from July 2017 to March 2018.

As a matter concerning the prevention of money laundering (Anti-Money Laundering or AML), combating the financing of terrorism (CFT), and implementing economic sanctions, regulations related to identity confirmation (KYC) are being tightened internationally. Regulations, including those targeting individuals, are being made stricter in Japan as well, and a consequent increase in the workload of financial institutions is expected. This is where the establishment of infrastructure which can be shared among financial institutions can be expected to improve the efficiency and quality of identity confirmation.

[1] “Report on Practical Experiment of Blockchain Technology in Japanese Domestic Interbank Payment Operation by the Blockchain Study Group” (November 30, 2016)
https://www2.deloitte.com/jp/en/pages/about-deloitte/articles/news-releases/nr20161130.html

In view of such a background, and in light of the expected high compatibility of blockchain technology, characterized by its resistance to falsification and high availability, with improving the efficiency of identity confirmation, the study group selected “construction of an advanced ‘Know Your Customer’ (KYC) platform” using blockchain technology as the theme for its next research project. It aimed to build a prototype KYC system using said technology, and decide upon the system’s specifications. Criteria such as sufficiency (functional feasibility, performance, security, etc.) and cost reduction effects were used for examination at the result verification stage, and the study group evaluated the usefulness of the new blockchain-based system.

2. Evaluation and examination of the verification test

(1) **Overview**

In addition to consolidating operations such as referencing lists of individuals subject to economic sanctions, currently conducted separately by each financial institution, into a newly established, jointly operated organization (referred to as “consortium” below), we expected to establish a framework for simplifying KYC-related operations through steps such as allowing participating financial institutions to confirm with each other whether the customer in question has already undergone identification procedures. Such confirmation would require a declaration of intent by the customer.

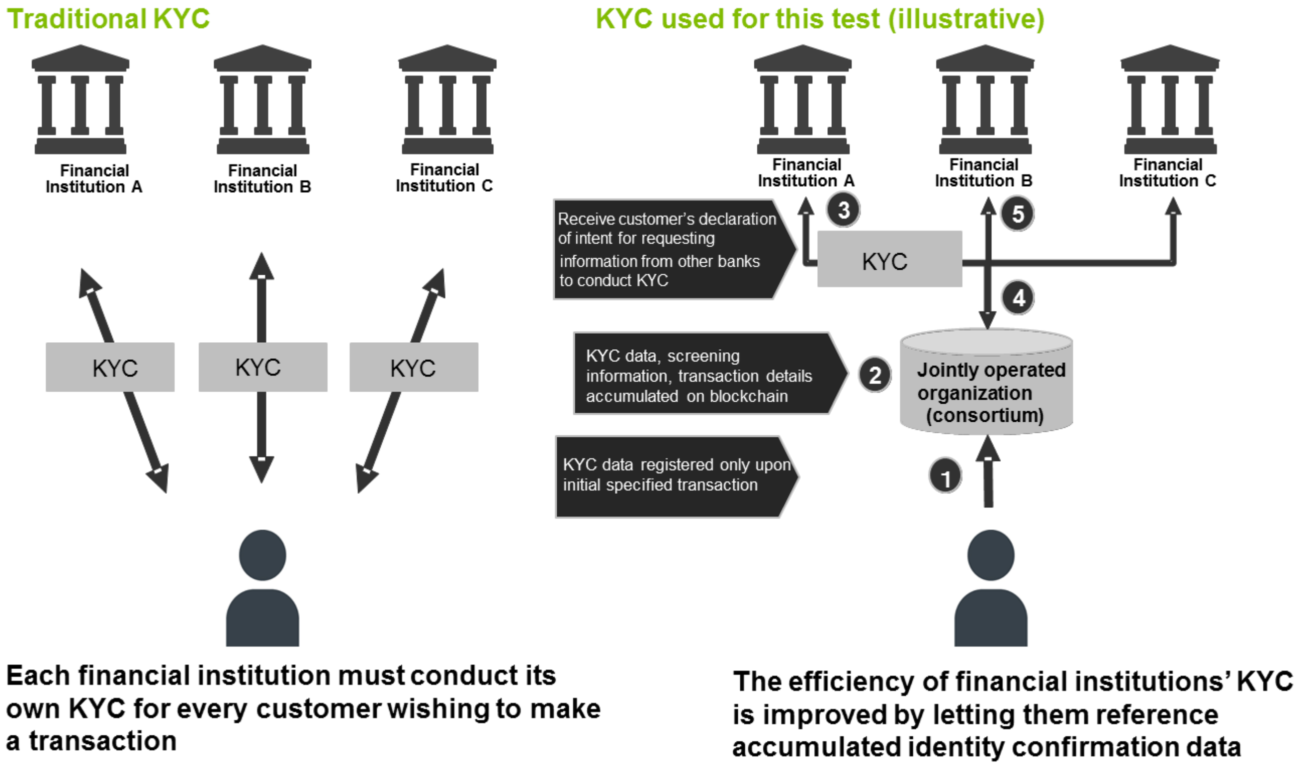

Traditional KYC
Financial Institution A
Financial Institution B
Financial Institution C
KYC
KYC
KYC
Each financial institution must conduct its own KYC for every customer wishing to make a transaction
KYC used for this test (illustrative)
Financial Institution A
Financial Institution B
Financial Institution C
Receive customer's declaration of intent for requesting information from other banks to conduct KYC
3
5
KYC
4
KYC data, screening information, transaction details accumulated on blockchain
2
Jointly operated organization (consortium)
KYC data registered only upon initial specified transaction
1
The efficiency of financial institutions' KYC is improved by letting them reference accumulated identity confirmation data

Figure 1: Diagram of the KYC system to be verified

(2) **Detailed framework**

The following assumes a situation in which a customer conducts a new transaction with a financial institution participating in the consortium. Treatment of existing customers, who are already conducting transactions with financial institutions participating in the consortium, will be examined at a later date.

1. Before conducting a specified transaction[2], the customer is asked to fill in the required identity confirmation details[3] via the consortium’s online registration form.

[2] “Specified transaction” in this verification test assumes the opening of an account.

[3] The verification test was limited to individual customers, who were assumed to be providing identity confirmation details, additional information related to identity confirmation, and images of identification documents (driver’s licence).

2. The consortium conducts filtering/screening[4] based on lists such as ones for individuals subject to economic sanctions. In case no matches are found, the individual is registered as "N/A" (this is referred to as filtering/screening information below) on the blockchain.
3. When the customer in question initiates a specified transaction with Financial Institution A, based on a declaration of intent[5] by said customer, the consortium provides Financial Institution A with said customer's identity confirmation data and filtering/screening information. In addition to conducting KYC for the customer, Financial Institution A uses the aforementioned information to make a decision[6] on whether the transaction can be carried out (if errors in the blockchain record are found when conducting KYC for the customer, the consortium will have to get back to the customer to conduct step 1 again).
4. When Financial Institution A conducts a specified transaction such as opening an account, it goes through the consortium to record the details of said transaction in the customer information on the blockchain.
5. When the customer initiates a specified transaction with Financial Institution B, based on a declaration of intent by said customer, the consortium provides Financial Institution B with said customer's identity confirmation data and filtering/screening information. Financial institution B goes through the consortium to confirm[7] that KYC for the customer has been conducted by financial institution A. This confirmation can be used as KYC by financial institution B (if it decides to do so). (At that point, Financial Institution B verifies that no risk of impersonation exists by referencing the customer's transaction history, recorded on the blockchain, and checking that the customer is not engaging in suspicious behavior, such as conducting similar transactions at several financial institutions.)

(3) **Constructed testing environment**

Registration of the user's (individual customer's) identity confirmation data, referencing and management of the registered data by the consortium, referencing of the information by financial institutions, and the function of registering/referencing account opening information were implemented using blockchain technology and tested (some parts of the test were simulated). This verification test is premised on the use of Hyperledger Fabric[8], and the environment used was constructed on top of the Japanese Bankers Association's Collaborative Blockchain Platform.

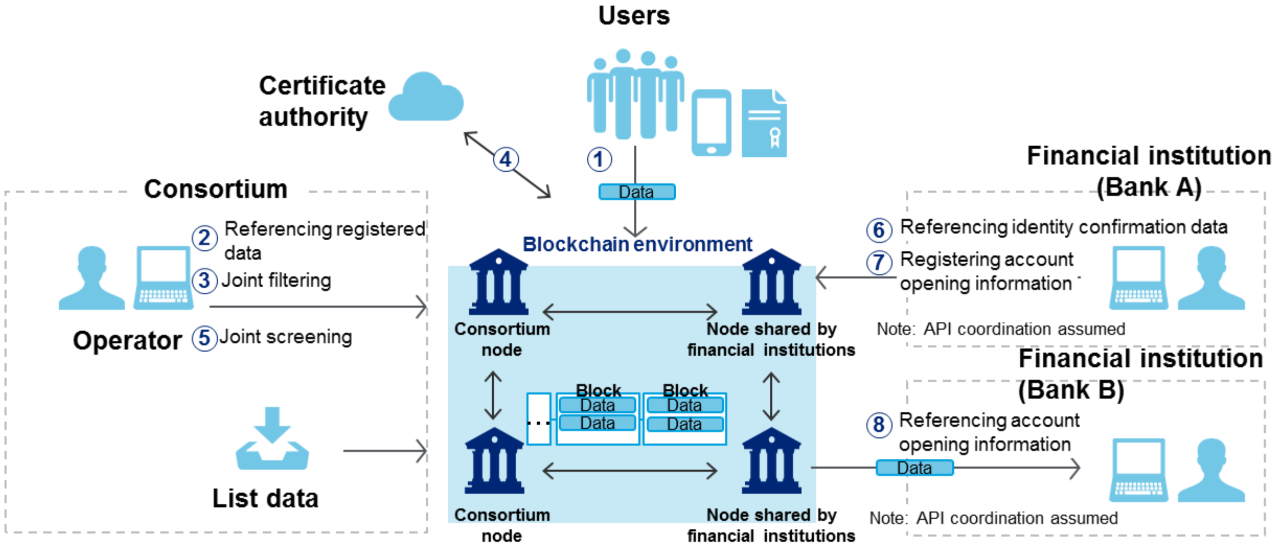

Users
Certificate authority
④
①
Data
Consortium
② Referencing registered data
③ Joint filtering
Operator
⑤ Joint screening
List data
Blockchain environment
Consortium node
Node shared by financial institutions
Block
Data
Data
Block
Data
Data
Consortium node
Node shared by financial institutions
Financial institution (Bank A)
⑥ Referencing identity confirmation data
⑦ Registering account opening information
Note: API coordination assumed
Financial institution (Bank B)
⑧ Referencing account opening information
Data
Note: API coordination assumed

Figure 2: Diagram of the testing environment constructed

[4] The verification test uses the following definitions. "Filtering" = comparing the identity confirmation details provided by the customer with a list of sanctions subjects or similar (test data created based on items listed by the Ministry of Finance, under the assumption that they will be expanded in the future), and indicating "N/A" (meaning no hits on the list, does not include investigation or decision) or "Other." "Screening" = comparing accumulated identity confirmation details with a list and indicating "N/A" (same as above) or "Other." A decision to designate the customer "approved" or "rejected" is then made by the relevant bank.

[5] The assumption is that the customer will display a digital certificate received as proof of completing the registration of ID information.

[6] Financial Institution A's decision will also be based on additional information independently collected by A.

[7] When Financial Institution B goes through the consortium to confirm the customer's account situation, whether the names of financial institutions at which the customer already has an account financial institution A in this case) are to be displayed will be examined going forward (the verification test was conducted with pseudonyms such as "financial institution X").

[8] Hyperledger Fabric is a blockchain framework implementation and one of the Hyperledger projects hosted by The Linux Foundation.

Chart 1: Overview of major functions implemented in the testing environment

Function	Explanation
1. Registration of identity confirmation data	・ Users fill in their identity confirmation data on an online form, which is then sent to the blockchain environment
2. Referencing of registered data	・ The consortium references data stored on the blockchain and checks for defects in the registered details
3. Joint filtering	・ Filtering is conducted based on list data, and “N/A” and “Other (complete match / partial match)” results, along with supplementary comments, are saved on the blockchain
4. Issuing of digital certificates	・ Digital certificates are issued by the certificate authority and users notified
5. Joint screening	・ When list data is updated, all registered user information is screened and the results (same as for filtering) are saved on the blockchain.
6. Referencing of identity confirmation data	・ The financial institution receiving a request for the opening of an account (Bank A) references the user’s identity confirmation data on the blockchain.
7. Registration of account opening information	・ If the financial institution (Bank A) decides to open the account based on the results of its independent filtering/screening, it registers that information (if the account could not be opened, the information is registered in a format not accessible by other banks)
8. Referencing of account opening information	・ The financial institution (Bank B) confirms that the customer has opened an account at another bank, makes a decision to omit a part of the independent filtering/screening process based on that information, and opens the account

(4) **Participants of the verification test**

The scope and conditions of the verification test were examined and decided upon by the project owners and members (the three “megabanks,” regional banks, securities firms, and Deloitte), and the system was built by Hitachi and JBA based on these decisions. The observers provided opinions and advice regarding points of contention and other issues.

Project owners (Blockchain Study Group)

- Mizuho Financial Group Inc.
- Sumitomo Mitsui Financial Group Inc.
- Mitsubishi UFJ Financial Group Inc.
- Deloitte Tohmatsu Group

Project members (in Japanese syllabary order)

- SMBC Nikko Securities Inc.
- Daiwa Securities Co. Ltd.
- The Chiba Bank Ltd.
- Nomura Securities Co. Ltd.
- The Bank of Fukuoka Ltd.
- Mizuho Securities Co. Ltd.
- Mitsubishi UFJ Morgan Stanley Securities Co. Ltd.

Function/environment providers

- Hitachi Group
- Japanese Bankers Association[9]

Observers

[9] Provided JBA’s Collaborative Blockchain Platform testbed environment

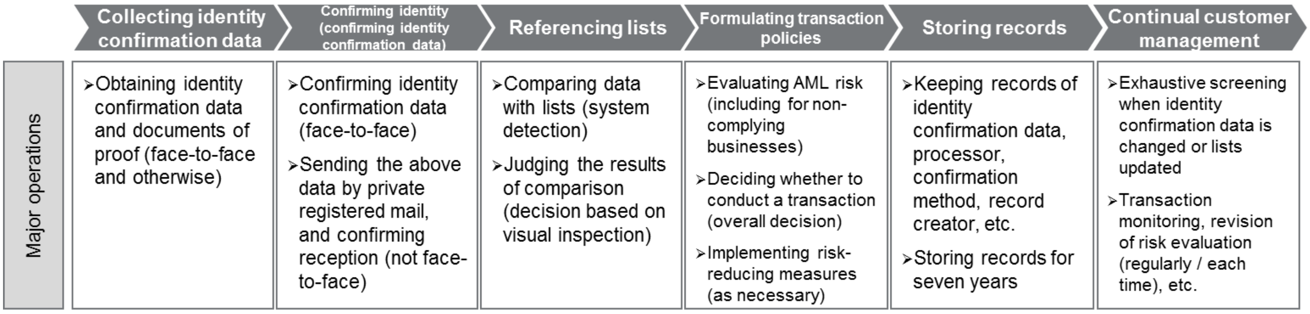
- Financial Services Agency
- Bank of Japan

(5) **Verification results and examination**

Ⅰ) **Operational**

Views on legal position

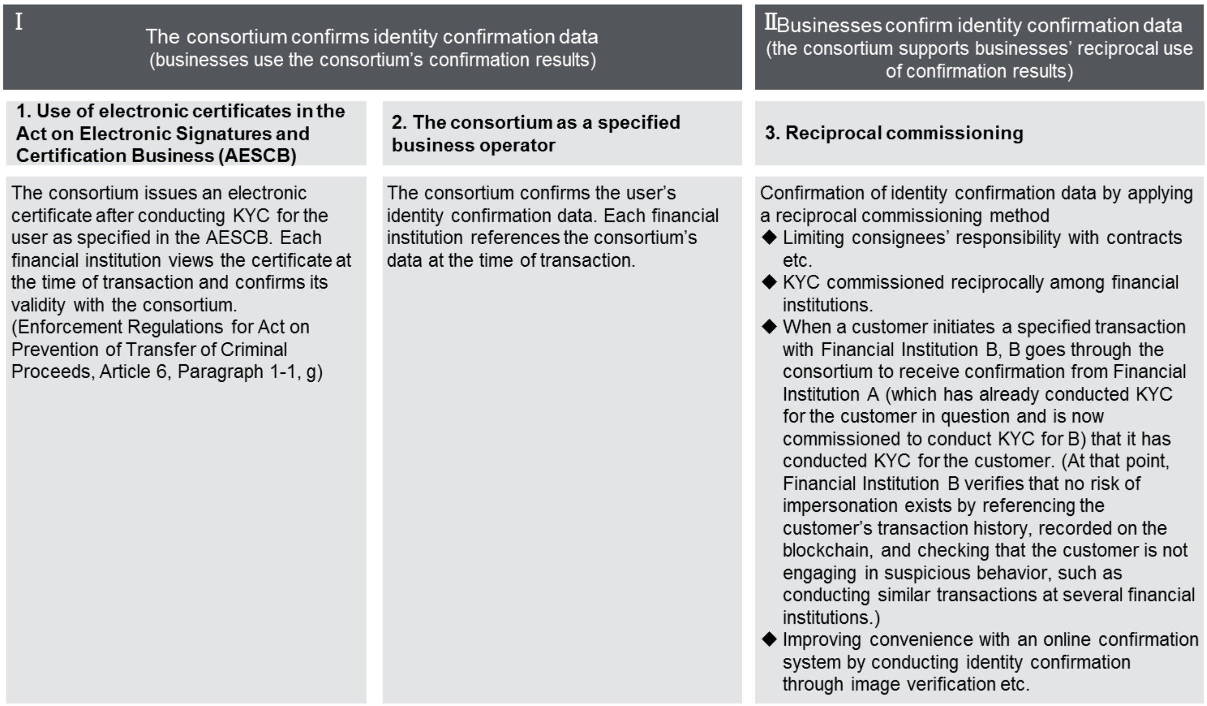
From an operational perspective, and considering effectiveness and convenience by focusing on the core KYC processes of collecting identity confirmation data and confirming identity, the roles (responsibilities) of the consortium were tied in with its legal position and clarified as a matter of priority.



	Collecting identity confirmation data	Confirming identity (confirming identity confirmation data)	Referencing lists	Formulating transaction policies	Storing records	Continual customer management
Major operations	➢Obtaining identity confirmation data and documents of proof (face-to-face and otherwise)	➢Confirming identity confirmation data (face-to-face) ➢Sending the above data by private registered mail, and confirming reception (not face-to-face)	➢Comparing data with lists (system detection) ➢Judging the results of comparison (decision based on visual inspection)	➢Evaluating AML risk (including for non-complying businesses) ➢Deciding whether to conduct a transaction (overall decision) ➢Implementing risk-reducing measures (as necessary)	➢Keeping records of identity confirmation data, processor, confirmation method, record creator, etc. ➢Storing records for seven years	➢Exhaustive screening when identity confirmation data is changed or lists updated ➢Transaction monitoring, revision of risk evaluation (regularly / each time), etc.

Figure 3: General operational flow for KYC

As a basic principle, ensuring the effectiveness of KYC (confirming substantiality and identity) at its current level, or at a level above that sufficient for the relevant authorities, was premised on the necessity of taking into account user (customer and business) convenience.



Ⅰ The consortium confirms identity confirmation data (businesses use the consortium's confirmation results)		Ⅱ Businesses confirm identity confirmation data (the consortium supports businesses' reciprocal use of confirmation results)
1. Use of electronic certificates in the Act on Electronic Signatures and Certification Business (AESCB)	**2. The consortium as a specified business operator**	**3. Reciprocal commissioning**
The consortium issues an electronic certificate after conducting KYC for the user as specified in the AESCB. Each financial institution views the certificate at the time of transaction and confirms its validity with the consortium. (Enforcement Regulations for Act on Prevention of Transfer of Criminal Proceeds, Article 6, Paragraph 1-1, g)	The consortium confirms the user's identity confirmation data. Each financial institution references the consortium's data at the time of transaction.	Confirmation of identity confirmation data by applying a reciprocal commissioning method ◆ Limiting consignees' responsibility with contracts etc. ◆ KYC commissioned reciprocally among financial institutions. ◆ When a customer initiates a specified transaction with Financial Institution B, B goes through the consortium to receive confirmation from Financial Institution A (which has already conducted KYC for the customer in question and is now commissioned to conduct KYC for B) that it has conducted KYC for the customer. (At that point, Financial Institution B verifies that no risk of impersonation exists by referencing the customer's transaction history, recorded on the blockchain, and checking that the customer is not engaging in suspicious behavior, such as conducting similar transactions at several financial institutions.) ◆ Improving convenience with an online confirmation system by conducting identity confirmation through image verification etc.

Figure 4: Potential legal positions

Observations regarding legal positions

Regarding "1. Use of electronic certificates in the Act on Electronic Signatures and Certification Business," the AESCB requires the organization issuing electronic certificates to confirm the identity of the customer for whom a certificate is to be issued by either a) having the customer display identification documents (in person), b) sending an envelope to the customer's home address via private registered mail and having the customer reply by mail, or c) having the customer's identity confirmed through Japan's public key infrastructure (PKI). The fact that options a) and b) do not allow for the process to be concluded online is one of the user convenience issues associated with this approach. On the other hand, the convenience of PKI means that its use should be examined in more detail.

As for “2. The consortium as a specified business operator,” because Japan’s Act on Prevention of Transfer of Criminal Proceeds requires that “specified business operators” conduct KYC, the option of having the consortium, which does not engage in specified transactions with customers, conduct KYC as such a “specified business operator” was deemed unrealistic.

With regard to “3. Application of a reciprocal commissioning method,” opinions were voiced concerning the existence of parties opposed to commissioning other financial institutions to conduct KYC. This issue was considered solvable by establishing a system that follows the procedures laid out in Figure 4. In other words, once Financial Institution A has completed KYC for a customer, it stores an image of said customer’s identification documents on the blockchain, and when the same customer initiates a specified transaction with Financial Institution B, in addition to commissioning Financial Institution A to conduct KYC for the customer, Financial Institution B can conduct its own verification of the identification documents on the blockchain to check for anything suspicious.

On the other hand, it was recognized that further examination is necessary regarding matters such as the clarification of commissioning details (contract formats, duties, etc.) to be agreed upon between financial institutions.

The legality of “3. Application of a reciprocal commissioning method” is supported by Article 13 of the Enforcement Ordinance for the Act on Prevention of Transfer of Criminal Proceeds, which states that “when Specified Business Operator B commissions Specified Business Operator A to conduct a specified transaction with a customer, if A has confirmed the identity of said customer during a previous transaction and maintains a record of said confirmation, re-confirming the identity of the customer is not required (confirming that identity has been confirmed is sufficient).” We have received confirmation from the relevant authorities for the interpretation that “commissioning” in this case also includes commissioning a party to conduct KYC only, without affording it the right to conclude a contract, and believe that there are no legal problems associated with this.

Ⅱ) System

From a system perspective, while the scope of verification this test allowed for was limited, no fatal flaws were detected at this point, and it can be said that using the advanced KYC platform for actual operations appears possible.

<u>Functional perspective</u>

In functional terms, it was proven that blockchain technology can be satisfactorily applied to the simplified[10] advanced KYC platform defined by the level of requirements for this test. Gradual improvement of the prototype and specifications will be pursued based on multiple criteria taking into account user convenience (improvement of usability, response to exceptional cases, etc.), and a certain level of results were confirmed through user acceptance testing (UAT). We believe that a continued focus on improving user convenience is necessary in moving toward practical implementation in the future.

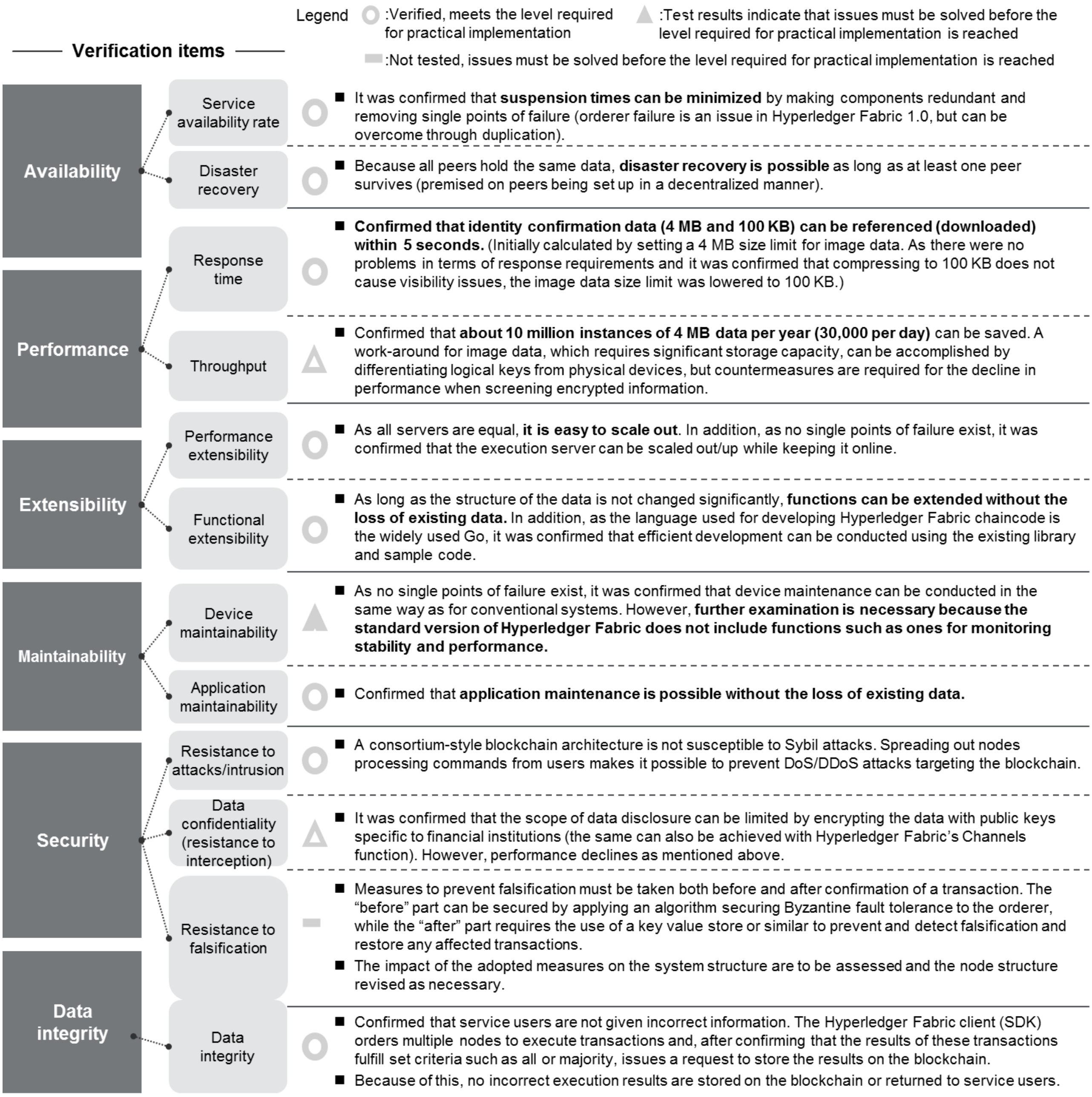
<u>Non-functional perspective</u>

Performance was evaluated by running batch processing as an equivalent to joint screening. While taking into account the effect on online processing such as referencing and otherwise handling blockchain information when registering personal information and opening accounts, the test confirmed that by adjusting the time of batch processing operations for joint screening, the necessary operations can be conducted on the scale required in this test (1,000 financial institutions, about 10 million instances of data per year [30,000 per day]).

Working toward practical implementation, with regard to throughput, the test confirmed that it is necessary to examine image separation and a scale-out/scale-up architecture to counter the decline in performance that occurs when screening large amounts of data and encrypted information. With regard to device maintainability, it was confirmed that as the standard version of Hyperledger Fabric does not

[10] Meaning that the test results are to be considered a simplified standard, considering that certain limitations and restricting conditions were placed on the environment constructed, operations, and the lists of sanctions subjects etc. used for filtering (test data was created based on items listed by the Ministry of Finance, under the assumption that they will be expanded in the future).

include functions such as ones for monitoring stability and performance, linking with open-source software[11] and examining the issues based on debate within the Fabric community is necessary. We believe that continuous examination of these matters will be necessary going forward.



Legend ○ :Verified, meets the level required for practical implementation △ :Test results indicate that issues must be solved before the level required for practical implementation is reached ▬ :Not tested, issues must be solved before the level required for practical implementation is reached

Verification items			
Availability	Service availability rate	○	■ It was confirmed that **suspension times can be minimized** by making components redundant and removing single points of failure (orderer failure is an issue in Hyperledger Fabric 1.0, but can be overcome through duplication).
	Disaster recovery	○	■ Because all peers hold the same data, **disaster recovery is possible** as long as at least one peer survives (premised on peers being set up in a decentralized manner).
Performance	Response time	○	■ **Confirmed that identity confirmation data (4 MB and 100 KB) can be referenced (downloaded) within 5 seconds.** (Initially calculated by setting a 4 MB size limit for image data. As there were no problems in terms of response requirements and it was confirmed that compressing to 100 KB does not cause visibility issues, the image data size limit was lowered to 100 KB.)
	Throughput	△	■ Confirmed that **about 10 million instances of 4 MB data per year (30,000 per day)** can be saved. A work-around for image data, which requires significant storage capacity, can be accomplished by differentiating logical keys from physical devices, but countermeasures are required for the decline in performance when screening encrypted information.
Extensibility	Performance extensibility	○	■ As all servers are equal, **it is easy to scale out**. In addition, as no single points of failure exist, it was confirmed that the execution server can be scaled out/up while keeping it online.
	Functional extensibility	○	■ As long as the structure of the data is not changed significantly, **functions can be extended without the loss of existing data.** In addition, as the language used for developing Hyperledger Fabric chaincode is the widely used Go, it was confirmed that efficient development can be conducted using the existing library and sample code.
Maintainability	Device maintainability	△	■ As no single points of failure exist, it was confirmed that device maintenance can be conducted in the same way as for conventional systems. However, **further examination is necessary because the standard version of Hyperledger Fabric does not include functions such as ones for monitoring stability and performance.**
	Application maintainability	○	■ Confirmed that **application maintenance is possible without the loss of existing data.**
Security	Resistance to attacks/intrusion	○	■ A consortium-style blockchain architecture is not susceptible to Sybil attacks. Spreading out nodes processing commands from users makes it possible to prevent DoS/DDoS attacks targeting the blockchain.
	Data confidentiality (resistance to interception)	△	■ It was confirmed that the scope of data disclosure can be limited by encrypting the data with public keys specific to financial institutions (the same can also be achieved with Hyperledger Fabric's Channels function). However, performance declines as mentioned above.
	Resistance to falsification	▬	■ Measures to prevent falsification must be taken both before and after confirmation of a transaction. The "before" part can be secured by applying an algorithm securing Byzantine fault tolerance to the orderer, while the "after" part requires the use of a key value store or similar to prevent and detect falsification and restore any affected transactions. ■ The impact of the adopted measures on the system structure are to be assessed and the node structure revised as necessary.
Data integrity	Data integrity	○	■ Confirmed that service users are not given incorrect information. The Hyperledger Fabric client (SDK) orders multiple nodes to execute transactions and, after confirming that the results of these transactions fulfill set criteria such as all or majority, issues a request to store the results on the blockchain. ■ Because of this, no incorrect execution results are stored on the blockchain or returned to service users.

Figure 5: Overview of verification items and results for non-functional requirements

[11] Software for which the source code is made available for free, giving anyone the rights to change and redistribute it.

Costs perspective

Working forward from comparing the workload currently required for KYC operations and the workload expected once the consortium is in place, we expect to verify the size of the expected decrease in costs, the system construction and implementation costs that will be incurred when the test environment is implemented in practice, and how the costs saved and incurred compare with each other. However, as the details of the operations to be conducted by the consortium are yet to be clearly defined, and the accompanying blockchain functions required not yet specified, we decided to only conduct an initial trial calculation during this verification test. It was also agreed that sharing storage of the table of records (i.e., having the consortium store it) would reduce costs to a certain extent.

(6) **Future issues and points of contention**

Clarifying future points of contention and continuing to examine the issues identified in relation to advanced KYC using blockchain technology can be expected to lead to more detailed mapping of the path toward practical implementation.

Operational

a. Legal position
As several points of contention were identified in relation to the legal position of the consortium when the effectiveness of KYC and user convenience were taken into account (refer to the section examining legal positions), further examination of this issue is necessary going forward.

b. Organizational principles
It is necessary to examine who will bear responsibility in the consortium and how it is to be organized (ISAO[12] organization also to be considered). It is also necessary to examine the conditions for participation in this framework.

c. Human resources and skills
Depending on the position and role of the consortium, it may be necessary to consider bringing in AML specialists.

d. Referencing lists
While not denying that the consortium may provide such a service, it was recognized that referencing logic and judgment criteria are matters not amenable to sharing. Going forward, it will be necessary to examine the need for the consortium to engage in list referencing, and whether such activities would be appropriate.

e. Continual customer management
It is necessary to examine involvement with matters such as batch updating of changed identity confirmation data (address changes, etc.) and the creation and storage of confirmation records.

System

Functional perspective

f. Improvement of user-friendliness by taking into account expected users
It is necessary to examine viable machine recognition technologies, such as improving functions supporting the automatic input of addresses and the like, automatic scanning of text on identification documents, and alteration of the surface of official documents in video and confirming the authenticity of such documents by scanning feature information—none of which rely on visual confirmation. It is also necessary to examine to what extent identification documents other than driver’s licenses (such as passports) could be accepted.

[12] The term “Information Sharing and Analysis Organization,” or ISAO, refers to a framework for sharing information such as past incidents, best practices, and risks associated with cyber threats, and cooperating in order to improve resistance to threats. It can also refer to the organization supporting these activities (ISAO) or to its associated standards (ISAO Standards Organization, or “ISAO SO”). It is preferable that the organizational form of the consortium, which will be handling significant amounts of personal data, would be outlined with the ISAO standards in mind.

g. Improving the traceability of identity confirmation / personal identification
Whether traceability, which includes to what extent personal information is up to date and changes to said information, can be ensured will be confirmed on the actual system, and other sources of value verified. It is also necessary to continue examination of whether the accuracy of identity confirmation (at the level required for KYC) can be improved by incorporating biometric authentication.

h. Linkage with certificate authorities and the My Number system
Using the NFC function of an existing (Android) device to scan My Number cards, and connecting said device with the KYC consortium and the JPKI test environment, it is possible to conduct verification tests to continually extract technological and operational issues going forward.

Non-functional perspective

i. Data confidentiality measures
Storing encrypted data on the blockchain architecture disables the database's high-speed search function, while the overhead required for application-based (chaincode-based) decoding leads to a decline in transaction processing performance. These issues mean that it is necessary to examine and test countermeasures by means such as scale-out/scale-up, or by designing a system that does not require encryption.[13]

j. Throughput performance measures
Because the precision of fuzzy search declines as the size of the searchable data grows, it is necessary to examine performance verification that takes into account the delay time in consensus-building between geographically dispersed nodes.

k. Improvement of device maintainability
Monitoring of performance indicators and component resource use is essential for operational stability and identification/analysis of performance issues, but the current version of Hyperledger Fabric does not offer these functions. In addition, although redundant configuration of components is possible, Fabric-CA[14], peers, and orderers themselves do not come with functions for keep-alive monitoring, connection management, and distributed processing. Because of this, operation of the entire Hyperledger Fabric network is to be examined through linking with or otherwise making use of open-source software, and by referring to the Hyperledger Fabric community's discussion on how keep-alive monitoring can be conducted.

Costs perspective

l. Continued examination from the perspective of comparing with and improving the efficiency of current operations will be necessary when clarifying the expected new operational flow and reducing the costs associated with the storage and management of KYC-related documents. In addition to the cost reduction perspective, it may also be possible to examine matters such as a framework for charging fees for the provision of data for referencing information. Furthermore, if this project is expected to provide even further reductions in costs, examining a system structure that also incorporates technologies other than blockchain will be necessary.

[13] The verification test used encryption to control the rights of financial institutions to reference data among each other, but controlling the extent to which data is shared is also an option. The Channels function in Hyperledger Fabric 1.0 allows for the limitation of parties among which data is shared, while a method for controlling such parties is being discussed for the next version of the software. In addition, not having to encrypt the data in a database would make databases with high-level search functions (indexes etc.) possible in the future, with improvements in performance expected. Based on this, which method is preferred will be one future point of contention to be examined.

[14] The certificate authority for Hyperledger Fabric. Conducts user management in the blockchain network and issues certificates. Only users with certificates issued by Fabric-CA can participate in the network and issue transactions.

3. Summary

Verification testing the construction of an advanced KYC platform using blockchain technology confirmed that blockchain technology certainly can be applied to KYC on the basic level required by this test. However, it was also recognized that various issues, such as user demand and convenience and legal points of contention, need to be solved if practical implementation is to be achieved.

Based on the insights earned from this verification test, and considering the aforementioned issues, the Blockchain Study Group will examine whether to continue verification testing of the applicability of blockchain technology to KYC operations and mapping of the path toward practical realization.

Finally, we hope that the publication of this document (summary of the test results) will inspire widespread commentary looking ahead to practical implementation, and many subsequent verification tests in the financial industry, with all of these efforts contributing to the advancement of blockchain technology.

Appendix (glossary)

No.	Term	Category	Explanation
1	Block	Blockchain (general)	The unit recording data in a blockchain. Several transactions are stored into single blocks. Transactions stored in blocks become approved (meaning that they cannot be reversed).
2	Blockchain	Blockchain (general)	A chain of blocks on a timeline from past to present.
3	Consensus algorithm	Blockchain (general)	A process for verifying the validity of and approving transactions processed by nodes (i.e., creating blocks). Several such algorithms exist, including Proof-of-Work (PoW) used by Bitcoin.
4	Node	Blockchain (general)	A transmission device (such as a server) connected to a blockchain's P2P network (i.e., using a blockchain-based service).
5	Sybil attack	Blockchain (general)	An attack in which the adversary uses several IDs within the network to pose as several different actors and unfairly influence consensus-building among participants.
6	Byzantine fault	Blockchain (general)	A discretionary fault, such as an undelivered or falsified message. For example, such a fault can occur when a malicious participant intentionally transmits false information to prevent consensus on the correct solution for the whole.
7	Ledger	Hyperledger Fabric (component)	A file containing the results of all past transactions. All participants generally hold the same ledger.
8	Orderer	Hyperledger Fabric (component)	A module that establishes the order for executing transactions, processes transactions into blocks, and forwards them to a peer. Pluggable implementations (e.g. Kafka) can be used in establishing the order for executing transactions.
9	Peer	Hyperledger Fabric (component)	A module that executes transactions (executes chaincode) and administers the ledger.
10	Chaincode	Hyperledger Fabric (component)	A smart contract program in which the details of transaction processing are defined. Developers write logic for specific applications as chaincode.
11	Fabric-CA (Membership)	Hyperledger Fabric (component)	The certificate authority for Hyperledger Fabric. Conducts user management in the blockchain network and issues certificates. Only users with certificates issued by Fabric-CA can participate in the network and issue transactions.
12	Client (SDK)	Hyperledger Fabric (component)	A program that orders peers to issue transactions and the orderer to confirm the results of those transactions in response to requests from users.
13	Endorsement policy	Hyperledger Fabric	A policy that defines the conditions for approving the results of an executed transaction. Approved transactions are added to the ledger by peers. The policy is composed of the number of organizations and peers that must endorse the transaction. The reliability of the results of executed transactions is enhanced by the requirement that transactions be endorsed by multiple organizations and peers.
14	Key-value store	Software	A database paradigm for storing pairs of data values and keys to said values in one place. Distinguished by quick retrieval of records ("values") identifiable with their respective keys.
15	Kafka	Software	A highly scalable distributed messaging system. Used as an implement to confirm the execution order of transactions established by the orderer. Kafka is open-source and also used for purposes other than blockchain.