Deloitte.
デロイト トーマツ

Contact
Yuta Takahashi
Teresa Aohori
Marketing & Communications
Email: DTC_PR@tohmatsu.co.jp

News Release
FOR IMMEDIATE DISTRIBUTION

Verification report on KYC advanced platform utilizing blockchain technology by the Blockchain Study Group

TOKYO, JAPAN, 13 July, 2018 — The Blockchain Study Group, conducted by Deloitte Tohmatsu Group, Mizuho Financial Group, Inc., Sumitomo Mitsui Financial Group,Inc. and Mitsubishi UFJ Financial Group, Inc., announce the completion of the verification report on KYC advanced platform utilizing blockchain technology. In order to conduct the verification test, the Blockchain Study Group applied to "Fintech PoC (Proof-of-Concept) Hub[(*)]" established by the FSA (Financial Services Agency) in October 2017. After receiving the official approval from the FSA in November 2017, the Blockchain Study Group started to work on the verification test under the support of the FSA, who provided advisories on the experiment.

[*]The FSA established "FinTech PoC Hub" to eliminate the hesitation and concern that FinTech firms and financial institutions are inclined to have in conducting unprecedented tests. The Hub offers continuous support in cooperation with other relevant authorities as necessary by forming a special working team within the FSA for each selected PoC project.

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.

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.

Please refer to the link below or see attached file for the full report.

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

Overview of the Verification Test and Results

■ **Name of verification test**
Verification test on the construction of an advanced "Know Your Customer" (KYC) platform using blockchain technology

■ **Term of verification test**
July 2017 – March 2018

■ **Participants of verification test**

· **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

· **Observers**
Financial Services Agency, Bank of Japan

■ **Overview of the verification test**

· **Overview and detailed framework**

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.

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

2. The consortium conducts filtering/screening[3] 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[4] 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[5] 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[6] 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.)

· **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

---

[1] "Specified transaction" in this verification test assumes the opening of an account.
[2] 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 license).
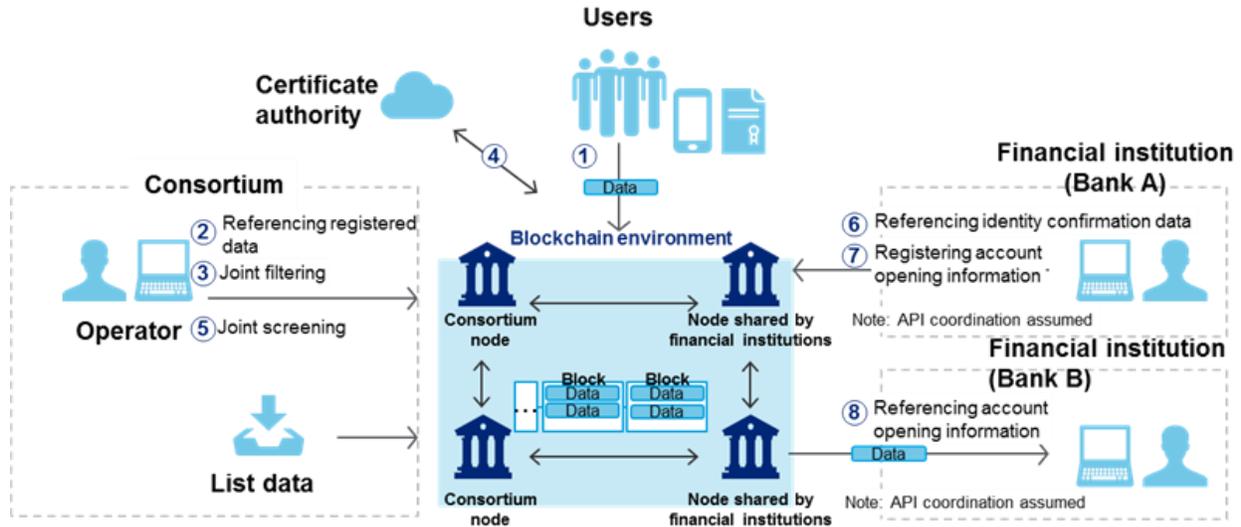[3] The verification test uses the following definitions. "Filtering" = comparing the identity confirmation details provided by the customer with a list of sanctions subjects or similar (test data created based on items listed by the Ministry of Finance, under the assumption that they will be expanded 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.
[4] The assumption is that the customer will display a digital certificate received as proof of completing the registration of ID information.
[5] Financial Institution A's decision will also be based on additional information independently collected by A.
[6] 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").

verification test is premised on the use of Hyperledger Fabric[7], and the environment used was constructed on top of the Japanese Bankers Association's Collaborative Blockchain Platform.

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)

---

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

Function	Explanation
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

■ **Overview of results**

I) Operational

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.

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.

<u>**Observations regarding legal positions**</u>

▽ **In cases which the consortium confirms identity confirmation details (businesses utilize confirmation results)**

Regarding "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 "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.

▽ **In cases which businesses confirm identity confirmation details (consortium supports mutual use of confirmation results)**

With regard to "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 "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.

Functional perspective

In functional terms, it was proven that blockchain technology can be satisfactorily applied to the simplified 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.

Non-functional perspective

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 include functions such as ones for monitoring stability and performance, linking with open-source software 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.

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.

■ 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.