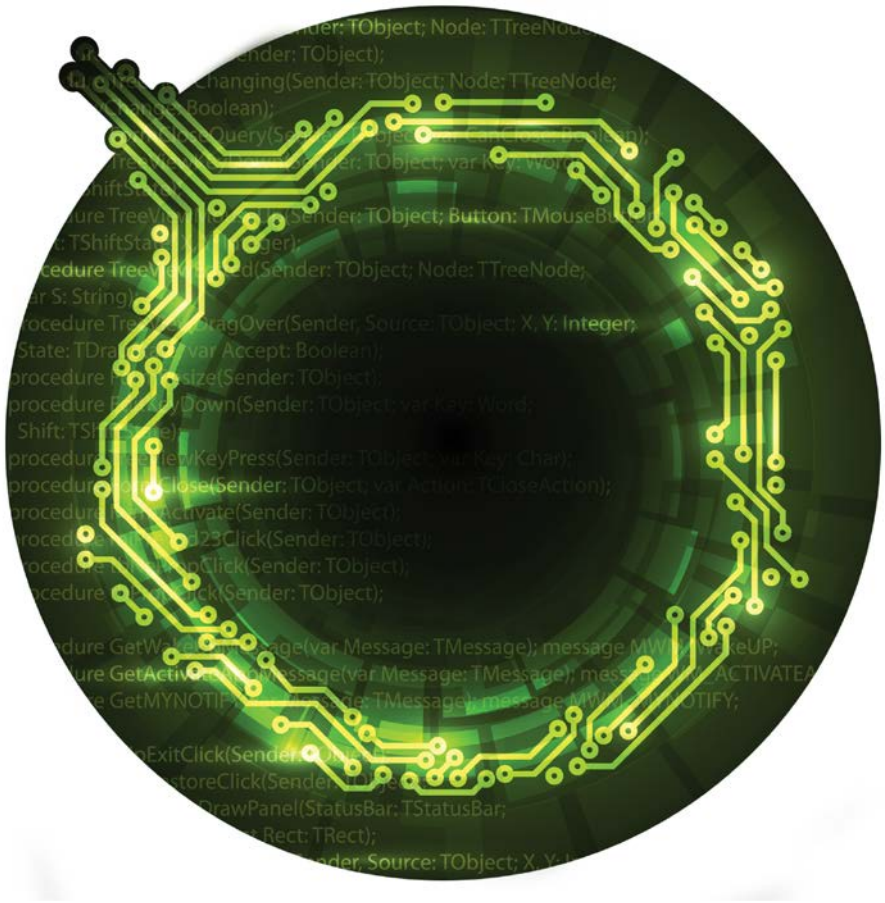

Report on Practical Experiment of Blockchain Technology in Japanese Domestic Interbank Payment Operation

Blockchain Study Group

Mizuho Financial Group, Inc.
Sumitomo Mitsui Banking Corporation
Mitsubishi UFJ Financial Group, Inc.
Deloitte Tohmatsu Group

November 30, 2016

Contents

1. Outline of the Blockchain Study Group

(1) Background and objective of the study group

Recently in the financial industry, FinTech innovation is developing significantly, creating a fusion of the finance industry and IT. Replacement of conventional financial services and emergence of unprecedented innovative financial services with FinTech are observed. Among those, blockchain technology which is used for virtual currency including bitcoin has high affinity to operations related to funds transfer, settlement, securities transaction, etc. because of its features such as “resistance to alteration,” and “high availability” in transactions. Therefore the technology is strongly expected to be leveraged in the financial industry in the future.

Led by the financial industry, blockchain technology is being actively researched including practical experiments. Global competition for the practical use of the technology and achieving the position of de facto standard became fierce. Financial institutions in Europe and the United States are especially enthusiastic.

In this situation, the Blockchain Study Group was established in December 2015, recognizing that blockchain technology is one of the elemental technologies which are necessary for Japan to grow further continuously. The study group’s final objective is to contribute to domestic financial institutions’ establishment of the foundation of blockchain technology, and to improve their technology to the level equivalent to that of financial institutions in Europe and the United States. The study group aims to identify the scope of blockchain’s application to financial system and to determine direction toward practical use.

(2) Position of the study group

Mizuho Financial Group, Inc., Sumitomo Mitsui Banking Corporation, Mitsubishi UFJ Financial Group, Inc., and Deloitte Tohmatsu Group participate in the Blockchain Study Group and promote research on blockchain technology.

The study group selects banking operations to which blockchain technology can be applied, establishes a prototype, and checks/evaluates the operation. When the study verifies that the blockchain technology is capable of use, it is also within the scope to develop formal specifications based on the prototype for practical use in the future.

The development of the prototype does not rely on a specific blockchain service provider’s technology. The prototype is developed with the cooperation by a blockchain service provider which is chosen from multiple candidates based on the requirements identified by the study group.

The study group’s goal is to support the growth of the domestic financial industry by determining the direction of the practical use of blockchain technology through its research.

2. Overview of blockchain technology

(1) Characteristics of blockchain technology

Blockchain technology is a P2P distributed database with a consensus algorithm.

P2P distributed database

In order to improve availability unlimitedly, distribution of the platform is necessary. A cross border platform with distributed hardware/regions/geopolitical risks enables a stable platform.

Consensus algorithm

In order to acquire validation of accurate transactions (hereinafter "transactions"), process including "Proof of Work" is necessary. Achieving correct consensus across participants is required where some participants send false information.

(2) Variations of consensus algorithms and their characteristics

There are four major consensus algorisms used in blockchain technology: "Proof of Work (hereinafter PoW)", "Proof of Stake (hereinafter PoS)", "Proof of Importance (hereinafter PoI)", and "Practical Byzantine Fault Tolerance (hereinafter PBFT)."

PoW

PoW, which is used in bitcoin, the origin of blockchain technology, is a framework with which network participants verify and validate the accuracy of transactions in bitcoin P2P[1] network to enable transfer of value without intermediation of administrators.

The participants (hereinafter "nodes") who validate transactions are called miners. Transactions validated by them are recorded in a unit called block and blockchain consists of blocks which keep records and which are linked as a chain. Blockchain forks when multiple miners link blocks simultaneously. A chain which has a certain number of blocks[2] linked after the fork is deemed to be irreversible. On the other hand, blocks which belong to the shorter blockchain (and transactions stored in them) are discarded and become invalid.

Creating blocks requires mining, an operation which is simple but requires very large computer resources. Therefore, it is said that it is virtually impossible to modify blockchain, since malicious miners need vast computer resources to expand false blockchain deliberately and validate it.

PoS

PoS is a consensus algorithm which is an application of PoW. The algorithm decreases difficulty of mining in accordance with coin retention amount and coin retention period, and thus decreases wasted computer resources.

---

[1] Peer to Peer network. Each peer is connected directly to other peers and communicates each other with equal privilege.

[2] Generally, in the bitcoin, approval procedure (block addition) is performed at intervals of 10 minutes, and it is regarded as definite when 6 times can be confirmed (about 1 hour elapsed).

PoI

PoI is a consensus algorithm which is an application of PoW and PoS. In order to moderate accumulation of coins by large-amount coin holders, the difficulty of mining is adjusted considering recent frequency of coin usage, in addition to coin retention amount and period (under PoS, there is a concern that large-amount coin holders accumulate coins and keep them from circulation, because large-amount coin holders always get advantage in mining).

PBFT

A framework under which authority to create a block is dominated by specific nodes (hereinafter "core nodes") and transactions are validated by the conference[3] of core nodes. The core nodes must be operated by trusted organizations. Though this framework does not have features such as "consensus which can be made without intermediation of specific administrators" as PoW, PoS, and PoI have, it enables agile and reliable transfer of value. However, it is generally said that, if a network adopts PBFT, you need to pay attention to availability since there is a concern that a failure of the core node may lead to a failure of the whole network.

Chart 1: Sorts and features of consensus algorithms

Consensus algorithm	Features		
	Availability	Process performance	Possibility of blockchain fork
PoW	Each node has the authority to create blocks, therefore the network is able to operate continuously if at least one node is working	In order to assure resistance to alteration while each node has authority to create blocks, a degree of difficulty for creating blocks is required. Such difficulty requires time before transactions are validated	Blockchain forks if multiple nodes create blocks simultaneously
PoS/PoI	Each node has the authority to create blocks, therefore the network is able to operate continuously if at least one node is working (although difficulty of creating blocks varies by nodes, each node has the authority)		
PBFT	The authority to create blocks is dominated by core nodes. Therefore, if a given number of core nodes stops, continuous operation is not possible	Blocks are created exclusively by specified and trusted nodes (core nodes). Therefore, validation of transaction can be achieved in a relatively short time	Blockchain does not fork since one block is created at a specific timing by the conference of core nodes

[3] A framework which prescribes that, among the blocks which are compiled from transactions in the network, blocks agreed as accurate by about 2/3 of core nodes or more are validated

(3) Scope of disclosure

The scope of disclosure of how widely participants can participate in the Blockchain network, has three forms. “Public network” which is used in bitcoin allows general public to participate, “private network” and “consortium network” limits participants to a single organization or group, or multiple organizations or groups.

Chart 2: Accessible zone

Accessible zone	Explanation
Public	General public nodes are allowed to participate in blockchain P2P network
Consortium	Specified organizations or groups are allowed to participate in blockchain P2P network
Private	A single organization or group is allowed to participate in blockchain P2P network

(4) Blockchain’s functional features and application

Blockchain’s features are resistance to alteration, high availability, fault tolerance, and cost reduction. These features are expected that blockchain technology is applied to finance services (including currency, payment and settlement [EDI], issuance and distribution of stocks and bonds, and trust), and to other industries (including property transfer ledger [real property, automobile, digital property, etc.], document management, notarization, traceability, and IoT).

Resistance to alteration

Data between nodes will not change once a consensus has been achieved.

High availability

Even if a part of the nodes fail, the network continues to respond as far as other nodes are alive.

Fault tolerance

System does not fail even if the network between the nodes is broken, etc.

Cost reduction

System cost, administrative cost of contract, payment and settlement operation, maintenance cost, etc. are reduced by distributed processing.

3. Evaluation and considerations of practical experiment

(1) Overview of practical experiment

The goal of this practical experiment is implementation of “payment,” the initiating process of funds transfer using blockchain technology. The funds transfer will be realized with participation of sending and receiving banks’ in blockchain environment[4] and by their exchange of transfer messages through the environment. Though “clearing” and “settlement” operations follow after payment in actual operations, operations related to those two operations are out of the scope of the practical experiment.

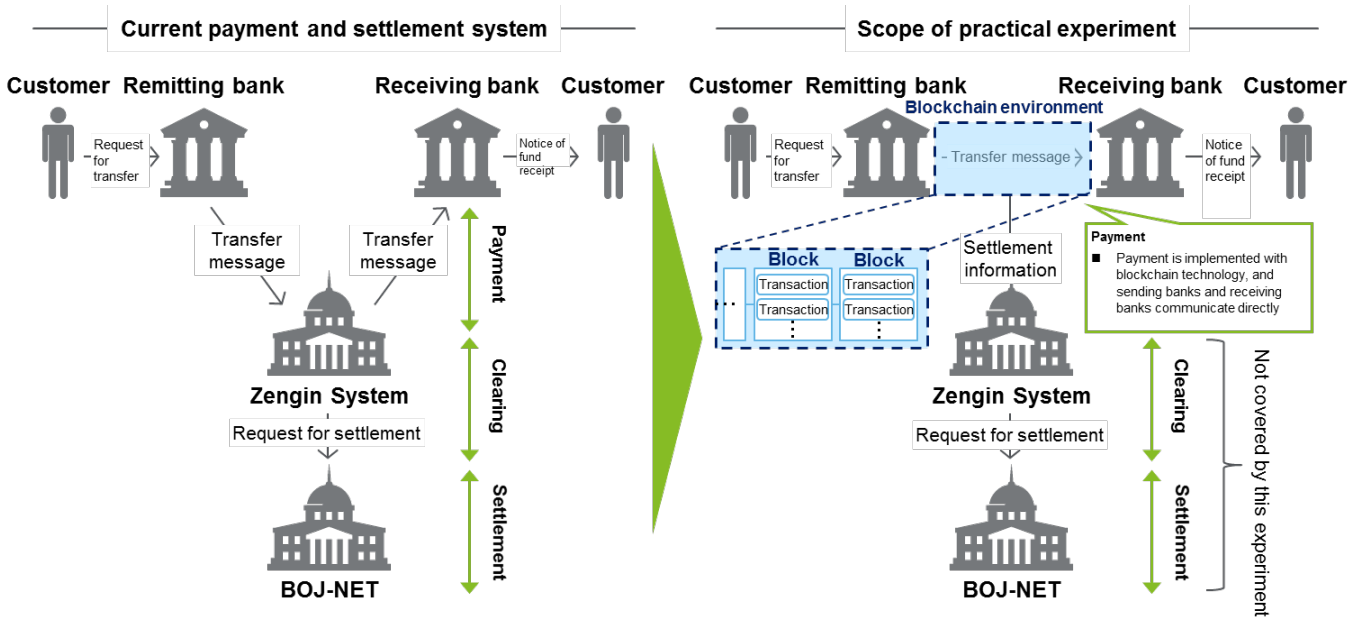

Figure 1: Scope

[4] Scope implemented by blockchain technology (Scope in which validation of transitions, storing into blocks, and sharing of transaction blocks on P2P network) among the experiment environment which is constructed in practical experiment.

[Reference] Current settlement system

The settlement execution process in the settlement system is classified into three categories: (1) payment, (2) clearing, and (3) settlement, realized by the bank, Zengin System, and BOJ-NET. The outline of each operation and operators is shown below. In the practical experiment, while referring to this scheme, a part of the process is constructed in the experiment environment.

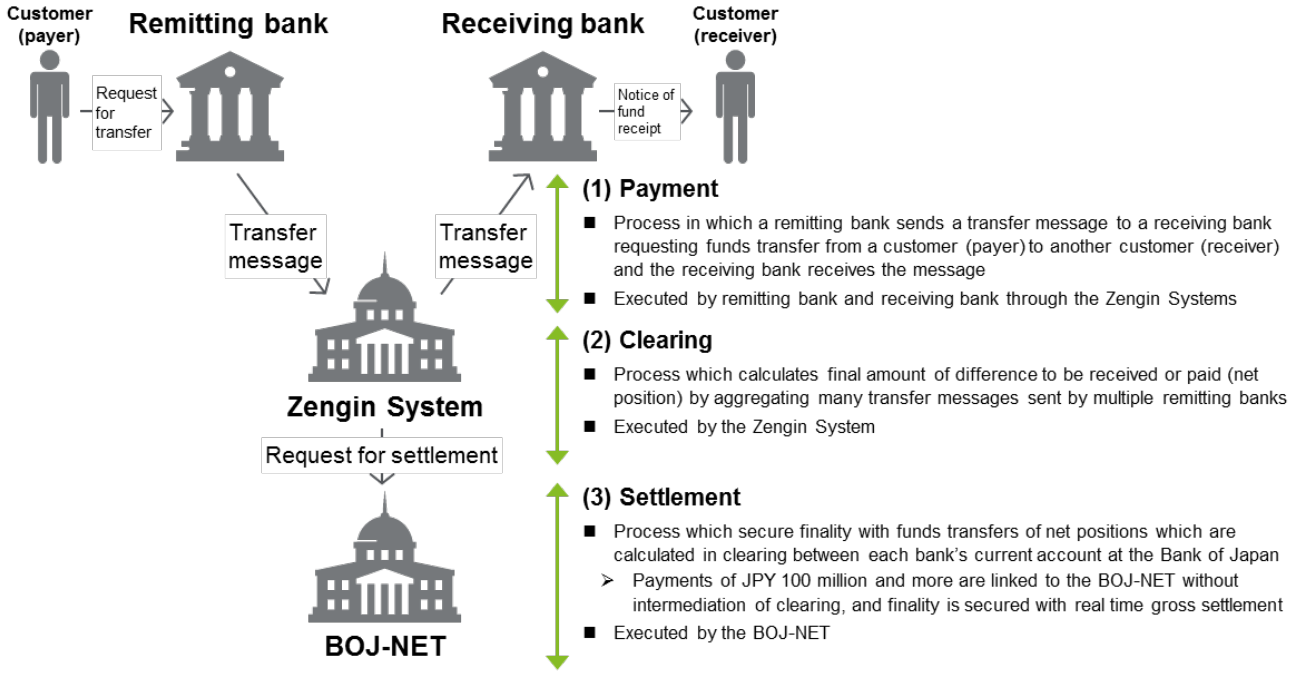

Figure 2: Scheme outline of settlement system

Chart 3: Japan's payment system[5]

Outline of payment systems			Services		Scale of payments		
Name of the system	Start of operation (year)	Operator	Operating hours	Method of settlement	Transaction volume (thousands per day)	Transaction value (JPY trillion per day)	Transaction value (JPY millions per transaction)
BOJ-NET	1988	Bank of Japan	8:30-21:00 (12 hours and 30 minutes)	Gross settlement (RTGS mode/Liquidity-saving features [LSF] mode)	69	136	1,957
Zengin System	1973	Zengin-Net	8:30-15:30 (7 hours) * 24 hours a day, 365 days a year operation is planned to start in 2018	Net settlement * payment to the recipient account is made in real time	6,346 * 20,000 or more on peak days	12	2

[5] Source: Masashi Nakajima and Junichi Shukuwa, *All about Payment Systems, 3rd Edition* (Toyo Keizai Inc., 2013) and PAYMENT AND SETTLEMENT STATISTICS(December 2015) (compiled by Deloitte Tohmatsu Consulting)

(2) **Constructed experiment environment**[6]

Real-time processing of several hundred transactions per second[7] without failure is required in interbank transaction operations. Considering the nature of the operations described above, a framework which is similar to PBFT[8] is adopted as the consensus algorithm of this experiment. While PoW, PoS, and PoI leave a risk that transaction validation is reversed by blockchain fork, compared with the above three frameworks, the framework adopted does not create the fork, assuring transaction finality (state of completion and irreversibility of transaction) instantly, and is expected to provide relatively high performance.

In accordance with consensus algorithm adopted, nodes participating in the blockchain environment are divided into two classes, application nodes which create transactions and core nodes which validate transactions and create blocks. Banks participate in the environment as application nodes.

Application nodes: Operated by banks performing the payments
Core nodes: Operated by trusted neutral organizations

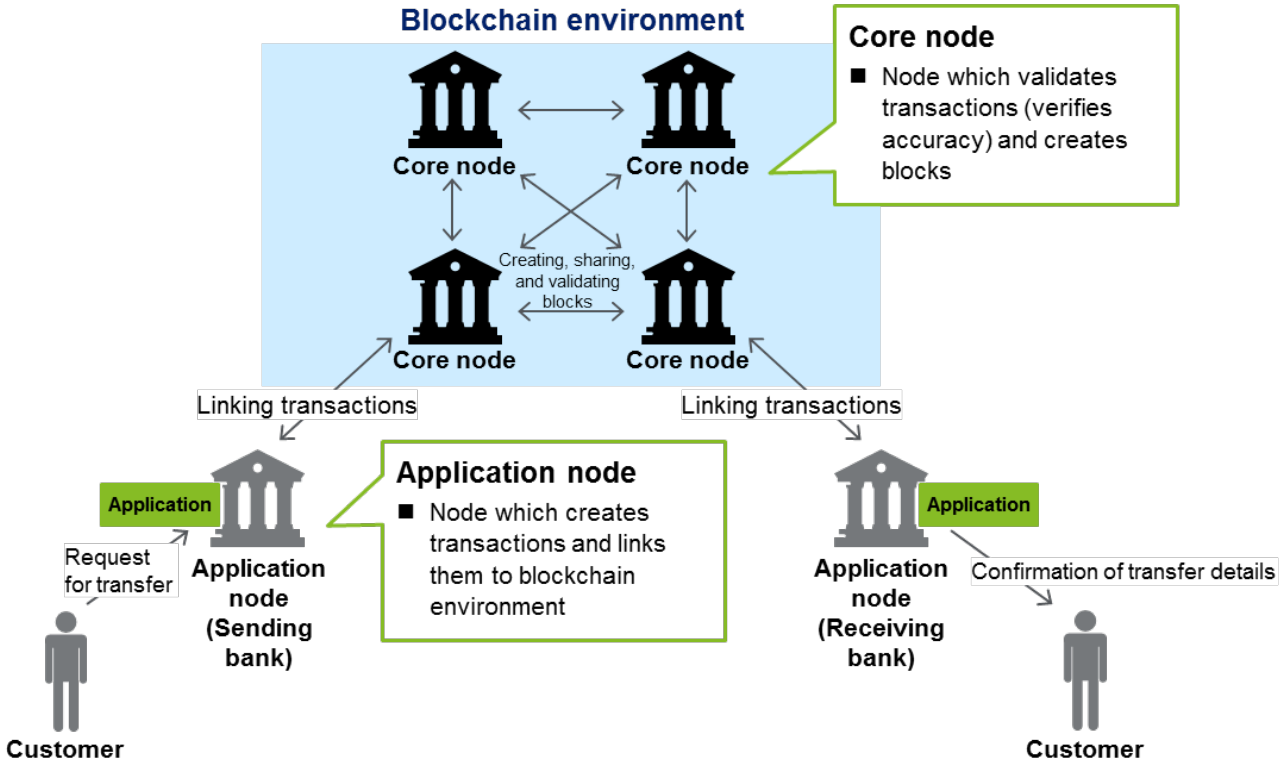

Figure 3: Concept image of constructed experimental environment

[6] The experiment environment was constructed in cooperation with bitFlyer, Inc.
[7] Actual daily volume of interbank payment in 2012 was about 1.35 billion transactions (Source: 「Pamphlet of Zengin System (Published in March 2014)Zengin-Net」) which stands for 216 transactions per second in average (based on business days and business hours).
[8] Though the algorithm is similar to PBFT, it was independently developed by bitFlyer, Inc.

In the experiment environment, following operations and functions are implemented to realize simplified transfer operation considering banking operations of money transfer payment in settlement systems as reference.

Chart 4 : Main functions implemented in the experiment environment

Operation	Function	Explanation
Credit transfers on the day	Creating and sending transfer message	● Remitting banks (application nodes) create transactions related to same-day transfer ● In the transactions, transfer information about customer accounts, sending and receiving banks, etc. and EDI information are set ● Created transactions are sent to core nodes, etc.
	Interbank funds transfer	● Various checks (including double payments and insufficient balances) are performed by core nodes which received the transactions ● Multiple core nodes build consensus to create blocks ● Created blocks are broadcasted to all nodes, etc.
Postdated credit transfers	Creating and sending transfer message	● Remitting banks (application nodes) create transactions related to post-date transfer (any given future date can be designated) ● In the transactions, transfer information about customer accounts, sending and receiving banks, etc. and EDI information are set ● Created transactions are sent to core nodes, etc.
	Interbank funds transfer	● The core node which received the transaction store the transfer message until the designated transfer date ● Various checks (including double payments and insufficient balances) are performed by core nodes on the designated day ● Multiple core nodes build consensus and create blocks ● Created blocks are broadcasted to all nodes, etc.
Same-day transfer / post-dated transfer	Viewing various information	● Remitting and receiving banks (application nodes) view transfer information, EDI information, etc. related to their own organizations

(3) Results and considerations

Ⅰ) From the view of functions

Implemented functions' feasibility was assessed through execution of experiment in the experiment environment. It is proven that all the functions implemented worked without issues and the functions development in blockchain technology can be sufficiently applied to the simple transfer operations.

However, in this experiment environment, in comparison with the whole payment and settlement system, the scope is limited to the payment area, and the contents of operations are also limited to implementation of

simple functions. In future, it is expected that more precise assessment can be achieved toward realization by examination of linking method to clearing (Zengin System) and settlement (BOJ-NET) and implementation method of transfer operations which are closer to actual operations.

II) **From the view of technology**

In terms of technology, considering the level required for actual operations of interbank payment services, though the range that could be verified in this practical experiment is limited, fatal defects were not identified and it is considered that blockchain technology can be applied to the area.

In the assessment to the experiment environment constructed this time, it was proven that the performance throughput in particular achieved 1,500 transactions per second and that the level sufficient for actual operation[9] is expected. However, in other areas, some issues are required further examinations to achieve required level. It is expected that more precise examination results toward realization can be acquired by proceeding continuous consideration further.

Figure 4: Assessment axes and assessment results from the view of technology

[9] Processing performance target is 5 million transactions per hour(Source: 「Pamphlet of Zengin System (Publishd in March 2014)Zengin-Net」), which stands for 216 transactions per second in average (based on business days and business hours).
[10] Ratio of uptime divided by annual operating hours
[11] Recovery from damage including disasters/preparations to contain damage minimum
[12] Construction of functions which can easily respond to new products and addition of services which are expected in advance
[13] Capability to respond to unpredicted request for addition and change of functions, etc. easily (It depends on documents' and program codes' comprehensibility, etc.)
[14] Firewall
[15] Other areas which are not relevant to blockchain technology

III) **From the view of costs**

On the assumption that multiple core nodes (central system) are connected to application nodes (bank system) equivalent to 144 banks[16], cost reduction effect by blockchain technology was examined by clarifying the difference of costs of two systems, one of which is constructed with blockchain technology and the other is constructed with conventional technology (without blockchain technology).

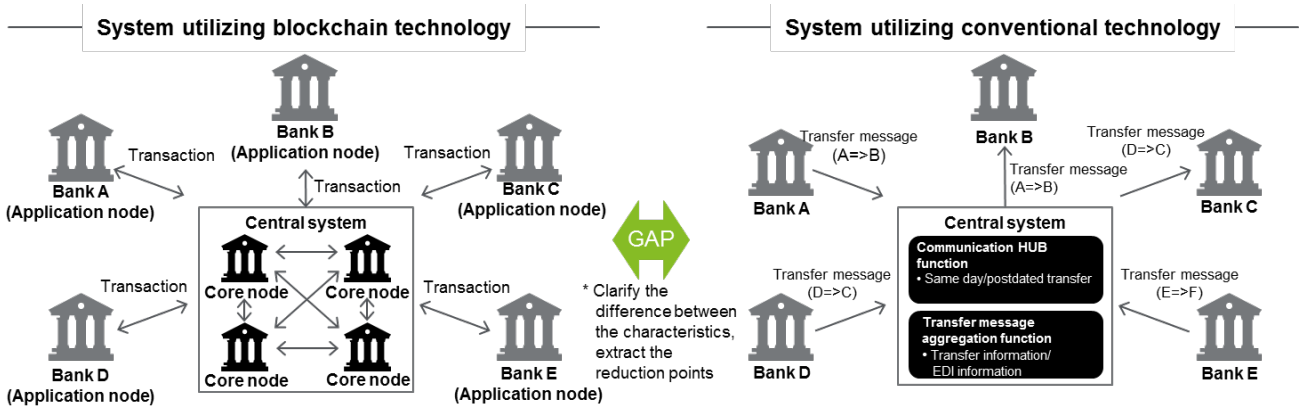

Figure 5: Concept image based on the cost reduction effect estimate

As a result, several points of cost reduction were confirmed on the central system side, and it is confirmed that system cost could be reduced by utilizing blockchain technology.

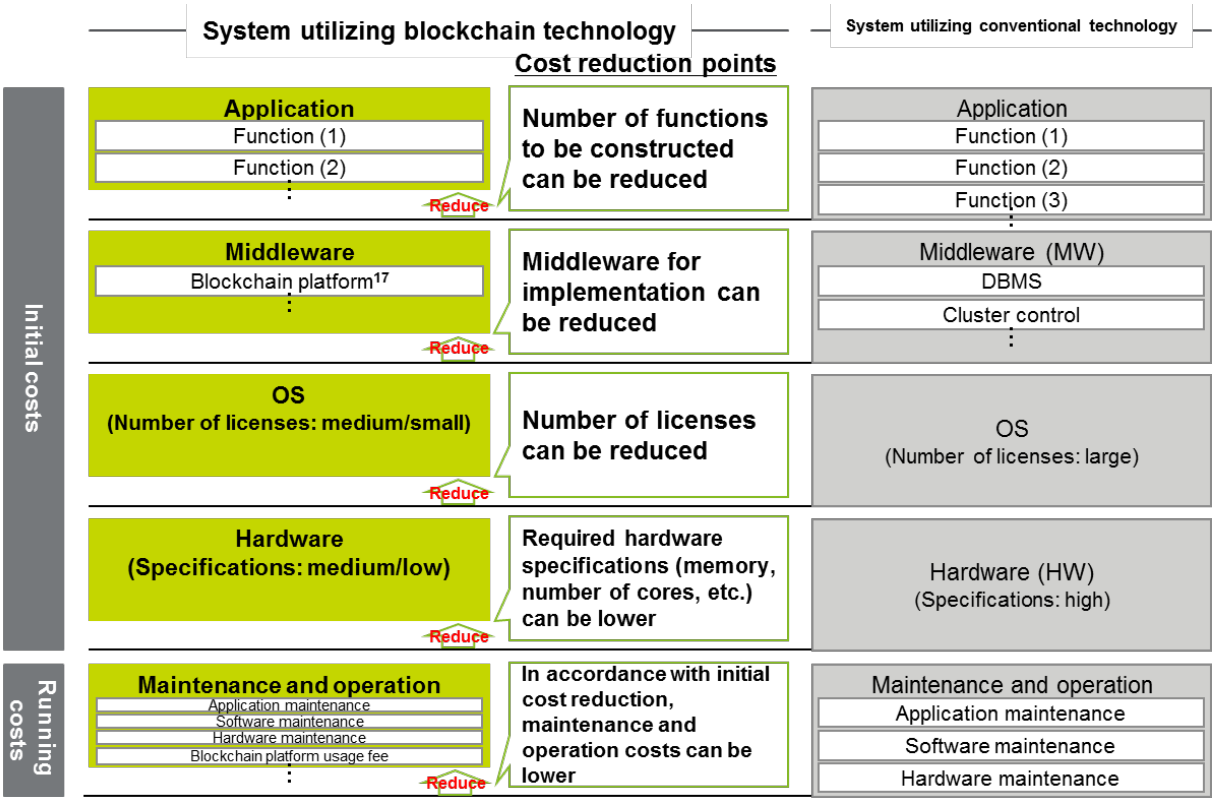

Figure 6: Expected cost reduction points

[16] The number was set considering number of participants in clearing of the current Zengin System.

a. Application development costs

With conventional technology, functions including transfer message data checking and editing require application development. With blockchain technology, those functions are implemented in middleware (blockchain platform[17]) and it is expected that the functions required to be constructed are reduced. However, compared with total cost, cost reduction effect is limited as it is expected that many other functions are constructed.

b. Software (middleware/OS) purchase costs

Since hardware specifications are lowered (please refer to “c. Hardware purchase costs”), number of CPU cores are reduced. Therefore, it is also expected that the software licenses are reduced. Regarding middleware, blockchain technology, which does not require redundancy, makes cluster control[18] unnecessary. In addition, DBMS is implemented in blockchain platform. Depending on service providers’ pricing, cost reduction can be achieved (it is not clear whether there will be cost reductions in software since service providers’ pricing varies).

c. Hardware purchase costs

Though the conventional technology realizes high operating ratio with redundant structure and installation of Backup Center, it is expected that blockchain technology, by its nature, realizes high operating ratio without such measure. Additionally, compared with the conventional technology which makes a single system perform centralized processing, it is expected that blockchain technology which makes multiple systems perform distributed processing lowers hardware specification.

d. Maintenance and operation costs

Since running costs are generally proportional to initial costs, it is expected that running costs are reduced in accordance with initial cost reduction. However, it is considered that fees for blockchain platform usage can differ by service provider. In addition, if geographically distributed installation of core nodes is adopted to leverage blockchain technology’s feature, it should be noted that network usage fee can be more expensive than that of the conventional technology.

[17] Service providers’ products and OSS platforms including Hyperledger and Ethereum
[18] Middleware which controls switching to standby servers in redundant system, etc. at system trouble

IV) **Future issues and points of discussion**

Concerning the identified issues regarding blockchain technology, consideration points on the issues will be clarified and continuous review of those points will allow clearer direction to realize actual operation.

a. Interface with existing settlement systems

In actual operation, settlement systems are required to be linked to bank accounting systems to process debit and credit transactions to and from the customers' account, prior to and after application nodes and core nodes create fund transfer messages. Furthermore, fund transfer information is required to be sent to the Zengin System. However, these two requirements were not included as a subject for verification in the practical experiment. Based on these factors, settlement systems' entire operational feasibility including interface with external systems needs to be verified in the future.

b. Service availability rate and measures for disaster recovery

Target service availability rate must be determined, and the number of core nodes that are required to achieve the target needs to be clarified. When connection of application node to core node is N to 1 basis, if part of the core node stops, consequently all application nodes that are connected to the core node will stop as well. Therefore, network structure also needs to be taken into account, such as by connecting each application node to multiple core nodes. Furthermore, considering a possible widespread disaster in the future, distributed configuration of core nodes is crucial, and appropriate distribution method (number of sites, region, etc.) should be examined.

c. Process performance including the participating banks (application nodes)

Although issues in throughput were not identified at this stage, additional studies concerning the response time are considered to be required. In the practical experiment, transaction validation time was a few seconds, however this validation time does not include processing time required at the application node side, and therefore actual response time needs to be clarified considering the processing time. Additionally, feasibility on actual operation based on the presupposed response time needs to be verified, and measures to shorten the response time (validation time) must be examined whenever necessary.

d. Security measures

Since in the practical experiment, scope of encryption was narrowed down for simplified implementation, basic information such as address and amount of money transferred were open to everyone who participated in the experiment. In actual operation, confidentiality of data, from those other than the concerned parties, is considered to be essential. Feasibility of data confidentiality and impact of processing time required for the encryption, on the process performance needs to be identified.

4. Summary

Through practical experiment of domestic interbank payment operation, possibility in benefitting from cost reduction effect in system development by leveraging blockchain technology was confirmed. However, various issues exist in the application of blockchain technology to the domestic interbank payment operation, such as in methods to interface to existing bank systems and to areas outside payment, and in methods to fulfill non-functional requirements of high levels. Concerning these issues, plans for practical use of the technology is expected to be further developed through accumulation of additional studies.

The study group, based on indications gained from the practical experiment aims to verify the applicability of blockchain technology and to examine it for practical use, in a broad scope not limited to the domestic interbank payment operation.

Finally, by releasing this report (summary on results of the experiment), we expect comments leading to practical use to be shared widely. Moreover, we expect to see many and repeated practical experiments in the financial industry contributing to the improvement of blockchain technology.

The study group aims to contribute to the domestic financial industry by continuing to explore the standards of financial systems that uses blockchain technology, and to build the foundation of blockchain technology in the country, as well as to ensure technology level comparable to that of financial institutions in Europe and the United States.