Report of the Review Committee for the Possibility and the Challenges of Utilizing Blockchain Technology

In View of the Possible Transformation that Blockchain Technology Will Bring to Banking Operations

March 16, 2017

Review Committee for the Possibility and the Challenges of Utilizing Blockchain Technology

(Secretariat: Japanese Bankers Association)

Introduction

While FinTech, a new fusion of finance and technology, has progressed in recent years, much attention has been paid to blockchain technology as a prominent technology that may transform banking operations and systems in the future.

Blockchain technology is generally described as a technology that aims to accurately maintain transaction histories by connecting all past transaction histories like a single chain through cryptographic technology, so that in order to tamper with the record of a past transaction, newer transactions must all be tampered[1]. It is extremely difficult to destroy or tamper with the data of systems that utilize this technology and it is possible that substantial zero downtime systems may be realized with this technology. Because of these features, blockchain technology is expected to be applied not only to the financial sector but to various other operations and systems as well going forward.[2]

In the report of the Working Group on Payment and Transaction Banking (announced December 22, 2015) and the Japanese Government's "Japan Revitalization Strategy 2016: For the Fourth Industrial Revolution" (cabinet decision as of June 2, 2016), policies for the collaboration of the banking industry with financial administration authorities to deliberate the possibility and the challenges of utilizing blockchain technology have been formulated in view of incorporating the advancement of IT into the financial sector, in order to promote the sophistication of financial services which would increase convenience for users and strengthen the growth potential of the Japanese economy.

In light of this, the Japanese Bankers Association established the Review Committee for the Possibility and the Challenges of Utilizing Blockchain Technology whose members are from the banking industry as well as IT companies, FinTech companies, blockchain industry groups, financial infrastructure managers, lawyers, academics, relevant authorities, and deliberated at the committee on the possibility of utilizing blockchain technology in the banking sector and the challenges that would be faced.

This report, as the outcome of the Review Committee, considers the possibility of utilizing blockchain technology in the banking sector as well as the challenges while recommending the public-private sector joint initiatives in view of the possible changes that blockchain technology will bring to banking operations.

---

[1] Page 5 of the report for the Working Group on Payment and Transaction Banking (December 22, 2015)

[2] According to a survey by the World Economic Forum, there is the view that by 2027 approx. 10% of the world's GDP will be recorded on blockchain technology (World Economic Forum's "Deep Shift: Technology Tipping Points and Societal Impact" (Sep. 2015)).

Table of Contents

The List of Members of Review Committee for the Possibility and the Challenges of Utilizing Blockchain Technology (as of March 2017)

Member	Tomoaki Nakayama	General Manager, IT Innovation Dept., Sumitomo Mitsui Banking Corporation
	Eiichi Kashiwagi	General Manager, Digital Innovation Division, Mitsubishi UFJ Financial Group, Inc.
	Nobuhisa Abe	Project Team Leader, Incubation Project Team, Mizuho Financial Group, Inc.
	Hiromitsu Umehara	Director / General Manager, Corporate planning department, The Shizuoka Bank
	Susumu Sasaki	General Manager, Channel Development Division, Fintech Promotion Office, North Pacific Bank, Ltd.
	Norifumi Yoshimoto	General Manager, Fintech Business Planning Dept., SBI Sumishin Net Bank, Ltd.
	Yutaka Masuda	Secretary General, Japanese Banks' Payment Clearing Network
	Hiroji Uchida	Representative executive officer and President, densai.net Co.,Ltd.
	Yoshiharu Akahane	Senior Manager, Systems Planning Group, Technology Strategy Promotion Section, Business Strategy Department, Financial Segment, NTT DATA Corporation
	Motohiko Kaizuka	Leader, Blockchain Solutions, IBM Japan, Ltd.
	Yuzo Kano	Representative Director, Japan Blockchain Association / CEO, BitFlyer, Inc.
	Yasunori Sugii	Deputy Director, Blockchain Collaborative Consortium / CEO, CurrencyPort Inc.
	Takashi Okita	FinTech association Japan / CEO, SBI Ripple Asia Co., Ltd.
	Yasuyuki Ogyu	Director, Deloitte Tohmatsu Consulting LLC

	Kanta Matsuura	Professor, Institute of Industrial Science, The University of Tokyo
	Hitoshi Okada	Associate professor, National Institute of Informatics
	Yoshihiro Kataoka	Attorney at Law, Kataoka & Kobayashi
	Nobuyuki Kinoshita	Senior Advisor, Aflac Japan
	Toshitake Inoue	Director for Credit System, Financial Services Agency
	Jutaro Kobayashi	Director General, Planning Department, The Center For Financial Industry Information Systems
	Yumiko Nagasawa	Executive director, Foster Forum
Observer	Naoyuki Iwashita	Deputy Director-General, Payment and Settlement Systems Department / Head of FinTech Center, Bank of Japan
	Atsushi Santo	Head, Fintech Laboratory, Corporate Strategy Department, Japan Exchange Group, Inc.
Secretariat	Japanese Bankers Association	

Outline of Meetings

The following bodies were established to conduct discussions for this report.[3]

Review Committee for the Possibility and the Challenges of Utilizing Blockchain Technology

- This committee conducted high-level discussions regarding the orientation of deliberations and the draft report submitted by the Research Committee which was established under the Review Committee.

Research Committee for the Possibility and the Challenges of Utilizing Blockchain Technology

- This committee conducted practical and expert discussions regarding the draft report.

The outline of meetings of the Review Committee and Research Committee are as follows.

1st Research Committee, August 4, 2016

- Information session, "Presenting the Problems regarding the Themes for the Research Committee"
- Information session, "Results of the Japanese Bankers Association's Questionnaire Survey"

1st Review Committee, December 20, 2016

- Information session, "Proposed Orientation of the Blockchain Review Committee Report"
- Information session, "Status of Deliberation of the Possibility of Utilizing Blockchain Technology in Other Nations"
- Information session, "Results of the Japanese Bankers Association's Questionnaire Survey"
- NTT DATA, "Characteristics and Challenges of Blockchain Technology"
- IBM Japan, "Utilization of Blockchains for Settlement and the Considerations thereof"
- Deloitte Tohmatsu Consulting, "Initiatives at the Blockchain Study Group"[4]

2nd Research Committee, January 25, 2017

- Information session, "Possibility and Challenges of Utilizing Blockchain Technology (1)"
- Japanese Banks' Payment Clearing Network, "Introduction of the Zengin System and the Challenges with Utilizing Blockchain Technology"
- Densai Net, "Overview of Densai Net and the Challenges in Applying Blockchain Technology"
- SBI Ripple Asia, "Overview of Ripple Solution and the Consortium for Unification of Domestic and Foreign Exchange"
- SBI Sumishin Net Bank, "Overview of Blockchain Proof of Concept"

3rd Research Committee, February 3, 2017

[3] The office for both is the Japanese Bankers Association.
[4] A private study group comprised of the Mizuho Financial Group, Inc., Sumitomo Mitsui Banking Corporation, Mitsubishi UFJ Financial Group, Inc. and the Deloitte Tohmatsu Group.

- Information session, “Possibility and Challenges of Utilizing Blockchain Technology (2)”
- Kataoka, Lawyer, “Blockchain Technology and Legal Issues Relating to Financial Institutions”[5]

4th Research Committee, February 20, 2017

- Information session, “Proposed Blockchain Review Report”
- Deloitte Tohmatsu Consulting, “Impact of Blockchain Technology on the Financial Sector”

2nd Review Committee, March 8, 2017

- Information session, “Proposed Blockchain Review Report”
- Bank of Japan, “Report by BIS’s Committee on Payments and Market Infrastructures: ‘Distributed ledger technology in payment, clearing, and settlement – An analytical framework’”[6]

We would like to express our deepest gratitude to those who cooperated with the Review Committee and Research Committee with valuable suggestions and presentations.

[5] Handouts can be viewed at the website of Kataoka & Kobayashi (http://www.klo.gr.jp/lawyers/dat/yk170316_paper.pdf).
[6] English version (http://www.bis.org/cpmi/publ/d157.pdf)

Summary

- Blockchain technology or distributed ledger technology (DLT) has the potential to significantly transform the future of banking operations and systems. Various financial institutions both inside and outside Japan are currently considering implementation of this technology. In the Japanese banking industry, many banks are now carrying out Proof of Concept and taking other measures to study and deliberate the possibility of utilizing this technology.
- On the other hand, bank systems require a high level of stability, reliability and accuracy. Further considerations still need to be made in technological, operational, security and legal aspects to implement this technology.
- Considering the distributed ledger feature of blockchain technology as well as the fact that much of banking operations and transactions assume interbank networks and that integration would reduce the costs of some operations, it can be said that it is important to advance both competitive initiatives of individual banks and initiatives in which the public sector works together with the private sector to overcome these challenges.
- Given the above, the Review Committee proposes the following initiatives to the public and private sectors.

Public-Private Sector Joint Initiatives on Blockchain

(1) Establishment of a Collaborative Blockchain Platform (tentative name) in the banking industry

Examinations into the possibility of utilizing blockchain technology/DLT are moving from the phase where banks were individually considering utilization to a phase where consortium-type examinations are being held through interbank cooperation. It is therefore expected that deliberation for the establishment of a Collaborative Blockchain Platform (tentative name), as an environment of Proof of Concept aiming collaboration and cooperation, by the next fiscal year will be advanced, mainly by the banking industry. By developing such an environment, it is expected that active examinations be advanced for implementation of blockchain technology/DLT regarding the sectors where utilization is expected such as through new settlement and money transfer services, KYC and financial infrastructure including the Zengin system[7] and the Densai Net System[8].

(2) Strategy for adapting to the international standard

The selection of a blockchain/DLT platform that considers the possibility of international proliferation is important in examining new services and mechanisms that look to future collaboration and cooperation with overseas financial institutions. It is expected that initiatives will be progressively advanced in preparation for the establishment of the Collaborative Blockchain Platform (tentative name) in the banking industry upon examination and selection of a worthy blockchain/DLT platform and in consideration of the trends in international standards and the

[7] The nation-wide online network system for banks dealing domestic funds transfers which is operated by Japanese Banks' Payment Clearing Network (Zengin net)
[8] The electronically recorded monetary claims system which is operated by Densai Net

features of different platforms.

(3) Deliberating the possibility of utilization in financial infrastructure

With regards to financial infrastructure such as the Densai Net system and Zengin system, it is important to advance deliberations on the possibility of utilization proactively with planned scheduled basis in view of the possibility of future improvements of infrastructure, cost reduction. Seeing the role and positioning of this technology as future financial infrastructure, it is expected that financial infrastructure managers will decisively advance these initiatives without delay. Regarding the Densai Net system, it is expected that efforts targeting a radical improvement in the efficiency of the system will be advanced with a view to conduct Proof of Concept for the Collaborative Blockchain Platform (tentative name) while, regarding the Zengin system, deliberations on the utilization of blockchain technology/DLT will be conducted on an ongoing basis.

(4) Collaboration with relevant authorities for utilization of blockchain technology/DLT

If Proof of Concept for implementation are to be conducted, the programs, mechanisms, business rules must take into account the final legal conformity in deliberations. It is expected that the relevant authorities will back the initiatives of the private sector to implement blockchain technology/DLT such as through proactive support in individual Proof of Concept and deliberations for implementation by organizing the legal issues.

(5) Collaboration with the central bank for the utilization of blockchain technology/DLT

It is expected that the central bank will engage in dialogue with a wide range of participants in the financial industry including the banking industry to utilize blockchain technology/DLT in financial infrastructures from the viewpoint of including, but not limited to, ensuring safety and increasing efficiency of settlements. It is also expected that the central bank will from time to time inform the banking industry about the international discussions concerning blockchains to ensure that the initiatives led by the banking industry is consistent with international discussions regarding settlements.

(6) Establishment of a safety measures standard concerning application

It is expected that information security-related institutions will advance research and study on blockchain technology/DLT, while keeping an eye on trends of Proof of Concept, the status of new use cases from both a responsibility aspect and technological aspect of safety measures, as well as organize the application (interpretation, operation) of such assuming the new safety measures standard that is scheduled to be revised.

(7) Forming a blockchain community

There is a need to promote understanding on the challenges of the banking sector's utilization of this technology among IT companies, blockchain associations and operators, academics, researchers, relevant authorities and others and to encourage further studies, technological developments for resolving challenges and implementing this technology. As such, it is expected that in the banking industry, there will be backing of Proof of Concept through the collaboration and

cooperation of banks while the formation of a community will be promoted such as through the establishment of a framework to share the outlines of the experiment results, technological trends obtained through the Proof of Concept within the whole industry. Furthermore, in the field of academic research, it is expected that there will be further promotion of research and sharing of research results and that researchers in this field will be proactively nurtured.

1. Introduction

1.1 Purpose of this Report

The purpose of this report is as follows.

- To aggregate the challenges in utilizing blockchain technology and the knowledge of experts as currently understood by individual banks and to organize, as a review committee, the possibility and the challenges of utilizing blockchain technology in the banking sector.

- By publicly announcing this report to widely promote understanding of the challenges in the utilization of blockchain technology in the banking sector among IT companies, blockchain associations and operators, academics, researchers, relevant authorities and others, and to encourage further study, research, technological development for resolving challenges and implementation.

- To propose public-private sector joint initiatives that will be necessary for implementation in view of the potential change that blockchain technology will bring to banking operations and systems.

Please note that, while blockchain technology is expected to be applied not only to the banking sector but various other operations and systems such as securities transactions and real estate registration, this report examines blockchain technology with the spotlight particularly on the banking sector.

1.2 Assumed Definition of Blockchain Technology/DLT in this Report

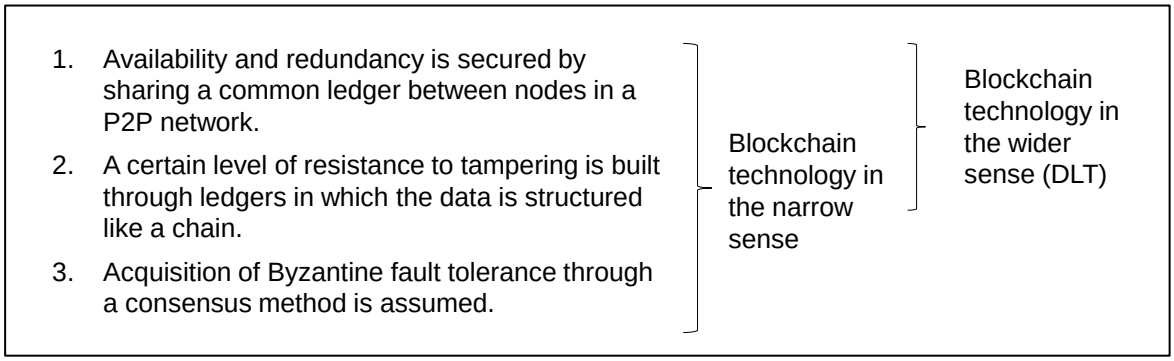
Blockchain technology is generally described as a technology that aims to accurately maintain transaction histories by connecting all past transaction histories like a single chain through cryptographic technology so that in order to tamper with the record of a past transaction, the newer transactions must all be tampered.[9]

There are many different forms of blockchain technology depending on the purpose of use. In utilizing blockchain technology in the banking sector, not only is blockchain technology in the narrow sense, for example, as the technological foundation of cryptocurrencies like Bitcoin, being considered, but also, blockchain technology in the wider sense, namely distributed ledger technology (DLT) which adopts parts of the technological features of blockchain technology.

With the above in mind, this report will examine the following possibilities and challenges for utilizing blockchain technology/DLT.

[9] Page 5, footnote 7 of the report for the Working Group on Sophisticated Payment and Transaction Banking (December 22, 2015). There is no definition that has been widely and internationally agreed upon.

[Figure 1] Basic Scope of Blockchain Technology/DLT Targeted by this Report

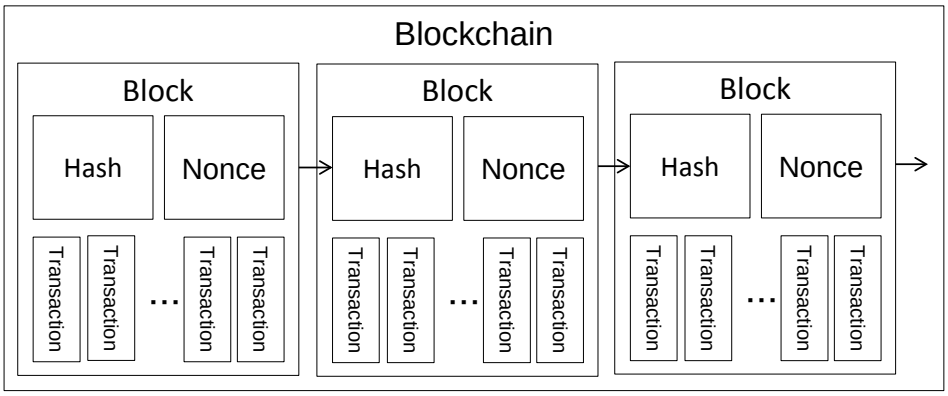


2. Basic Mechanism of Blockchain Technology/DLT

2.1 Basic Mechanism

In a blockchain, transaction histories (blocks) are recorded through cryptographic technology as linked like a single chain from past to present. A single block is comprised of an aggregate of agreed upon transaction records and the information which links block to block (hashes, nonces). A blockchain refers to multiple blocks linked together.

[Figure 2] Basic Mechanism of Blockchains



A hash is a value generated from the information of the previous block through ahash function[10]. If a new block was to include the previous blocks, the file size would increase each time a block is linked. However, the increase of file size is limited through the use of hashes. The ordering of the blocks is maintained through these hashes[11].

A nonce is a parameter given to a hash calculation when a new block is created. In proof of work (PoW; see page 14 for details), tampering with a block is made difficult by imposing nonce mining operations which must meet predetermined criteria with large calculation loads for the generation of a new block.

When a participant conducts some sort of transaction, the content of the transaction will be broadcast to all participating nodes in the decentralized environment of the P2P network. A new block is generated when the content of the transaction is approved through a previously negotiated method (consensus algorithm[12]).

In the mechanism of a distributed ledger which supports blockchain technology, the ledger data is held by various participating systems and there is constant synchronization. When more than one user requests input into the same data at the same time, a general database would hold back the

[10] A function which generates a fixed-length pseudorandom number from a given text
[11] However, the information in the previous block cannot be generated through the hash.
[12] A mechanism that assures the correctness of shared data and uniquely identifies it. There are many different types (for details see the next page).

request of one party and process the other's request (exclusion control). However, in a distributed ledger, the consensus algorithm would determine which request would be prioritized.

2.2 Component Technologies

Blockchain technology/DLT combines multiple component technologies. The main components are (1) distributed ledgers, (2) smart contracts, (3) anti-counterfeiting and encrypting technology, (4) consensus algorithms and (5) P2P networks.

(1) Distributed Ledgers

Unlike centralized management systems, transaction records in blockchains are held by participants of a P2P network (distributed ledger). While conventional technology has restrictions with regard to multiple participants holding the same information, blockchain technology/DLT enables the same information to be shared without letting it be tampered with.

(2) Smart Contracts

Smart contracts refer, in the wider sense, to contracts that are programmed and that can be automatically executed and, in the narrow sense, to agent programs that operate on blockchains or distributed ledgers. Smart contracts are described according to the operational requirements in corresponding blockchains/distributed ledgers with individual operational fields.

(3) Anti-Counterfeiting and Encrypting Technology

Anti-counterfeiting and encrypting technology is used when transaction information is entered into a network to prove that it is one's own transaction. An electronic signature is made using public-key cryptography and calculations are made with hash functions.

(4) Consensus Algorithms

Consensus algorithms are used to solve the problems which arise when a consensus is being built on a single result by several nodes in a decentralized environment. There are various types of consensus algorithms (see [BOX 1] for the details) and the appropriate type is chosen based on the purpose of use of blockchains/distributed ledgers and the operational conditions.

(5) P2P Networks

Blockchains/distributed ledgers are maintained by a P2P network in which there is no particular server or client and where each participating node communicates directly on an equal basis rather than a client-server network in which there is a particular management body.

[BOX 1] Principal Consensus Algorithms and Features

Proof of Work (PoW)

PoW is a mechanism in which the first party to solve a particular problem requiring a large amount of calculation

can create the block. It is able to deal with many participating nodes. If multiple blocks are created at the same time, the block which the majority of participating nodes accepts is recognized. This allows it to avoid problems particular to decentralized environments. However, finality concerning the sharing of information on the P2P network cannot be fully ensured as there is a time lag between the participating nodes[13]. For example, if a new block has been accepted by the majority of participants, the block that had formerly been recognized will be nullified and the new block should take its place. Therefore forks may arise in the chain. Since a certain amount of time is required for approval, this does not happen in real time.

Proof of Stake (PoS)

With PoS, authorizers owning larger amounts of assets are prioritized to create blocks, based on the idea that participants with more assets are not likely to impair the reliability of the system since they would want to protect the value of their assets. PoS therefore has the benefits of reduced hash calculation load as well as having a smaller consumption of resources compared to PoW. However it is basically similar to PoW in that it cannot ensure finality (forks may arise in the chain) and that it lacks real time property.

Proof of Importance (PoI)

PoI is a consensus algorithm that is employed by the cryptocurrency NEM, New Economy Movement. Blocks are generated based on the "importance" of the user in the network. This "importance" is determined by the user's balance in the account and number of past transactions. There are rules regarding the balance and number of transactions to prevent misuse so that merely a large balance will not result in greater "importance." The system for prioritization is thus more complex than with PoS. The same challenges with ensuring finality are present as with PoW and PoS (forks may arise in the chain). However, functioning (processing speed) is more easily secured compared to PoW as blocks are generated according to "importance."

Practical Byzantine Fault Tolerance (PBFT)

With the PBFT algorithm, one of the network's participants becomes the primary (leader), sends requests to all participants including itself and confirms blocks by collecting the results of the requests and adopting the value which holds a majority. The number of nodes required to confirm a block is predetermined; if f is the number of illegitimate nodes, the number of whole nodes required is $3f + 1$. An upper limit is usually required since, as the number of participants increases, the amount of messages required to form an agreement increases exponentially while the time required for an agreement is extended as well (10 to 20 participants is generally considered to be appropriate). As blocks are generated following the agreement, no forking will result in the chains and the uncertainty in determining finality after forking, a weakness of PoW and PoS, is resolved. PBFT is employed by consortium-type blockchain platforms such as Hyperledger Fabric and Eris.

2.3 Platform Types

Platforms for blockchains/distributed ledgers are classified into three different types, namely (1)

[13] Bitcoin uses PoW and is designed so that 10 minutes is required to create one new block. The finality is established after six more blocks are generated following the recording of a transaction in a blockchain.

public, (2) consortium and (3) private, depending on the participants' scope of disclosure and restricted contents. The appropriate type is selected based on use cases. Furthermore, applying restrictions to the scope of disclosure allows a consensus algorithm to be selected that is more suitable for the use cases of financial institutions.

(1) Public

Public platforms are open and anybody may participate. Since the risk of misuse cannot be eliminated, a consortium algorithm must be employed to decrease the incentives for tampering. Bitcoin, which is a well-known case of utilization of blockchains, is an example of a public platform.

(2) Consortium

Consortium platforms only allow those which satisfy certain conditions to participate. By limiting participants to those that may be trusted, the risk of misuse by participants is reduced and a consensus algorithm that is more suitable for the use cases (fast processing speed, able to ensure finality) can be selected. Consortium platforms are generally appropriate for utilization in the enterprise field.

(3) Private

Private platforms are managed within a single organization (such as an in-house system). Confidentiality of information is ensured as information is not shared with those outside of the organization. Private platforms are considered for use mainly as a replacement for centralized systems.

[Figure 3] Types of Platforms for Blockchains/Distributed Ledgers

	Public	Consortium	Private
Managing body	No manager	Several organizations	Single organization
Participation	Open	Authorization required	
Consensus algorithm	PoW, assuming possibility of participants that would misuse the platform	Distributed consensus algorithms such as PBFT (able to adopt consensus algorithms that do not assume participants that would misuse the platform)	
Finality	Chains will fork and finality is uncertain (stochastic)	Finality may be ensured by employing consensus algorithms such as PBFT	

3. Status of Deliberation of the Possibility to Utilize Blockchain Technology/DLT both inside and outside Japan

3.1 Overview

Blockchain technology/DLT has the potential to significantly transform the future of banking operations and systems. Various financial institutions both inside and outside Japan are currently considering implementing this technology[14].

Until around 2016 such deliberations had primarily been through technological verification through Proof of Concept and the testing of prototypes but 2017 has seen projects that have moved into the phase of examination for actual implementation. According to a survey by IBM[15], of 200 leading financial institutions worldwide, 14% are expected to implement blockchain technology/DLT by 2018 and 70% are expected to move to implementation by 2020.

[Figure 4-1] Principal Fields Considering Utilization of Blockchain Technology/DLT

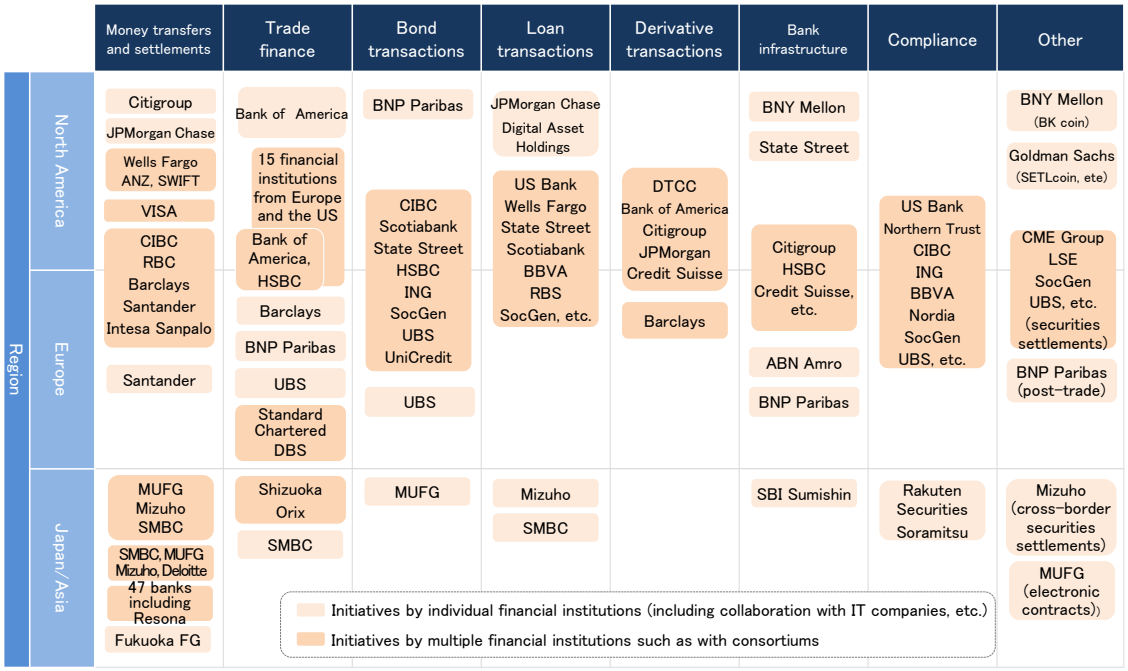
Classification		Principal trends in transactions	Proofs of Concept	Examples of implementation
Financial services	Currency	There is acceleration not only in the issuance of cryptocurrencies but also currencies for central banks to facilitate settlements and companies' own currencies or points.	[Cryptocurrencies] UBS, Deutsche, BNY Mellon, Santander	[Cryptocurrencies] Bitcoin
	Money transfers and settlements	Efforts for cross-border remittances in which shortened settlement time is sought but immediacy is not necessary are especially active globally.	[Domestic transfers] SMBC, Mizuho, MUFG	[International remittance] Santander (Ripple)
	Loans	Efforts center on those in the fields of trade finance and syndicate loans which are expected to be used for the management of contract terms and records of successive transactions.	[Syndicate loans] Mizuho	[Trade finance] KBC Bank (Belgium)
	Financial products transactions	Efforts center on the realization of transactions of unquoted shares and credit in which speed is not an issue as well as in post-trade processing which is expected to increase operational efficiency.	[Post-trade processing] BoA, Citi, JP Morgan, Credit Suisse	[Unquoted shares trading] Nasdaq
Financial information management		Establishment as well as renewal of infrastructure that integrates into information held by financial institutions such as in management of private information, management of corporate information and KYC.	[Corporate information management] Kompany.com	[KYC] ConsenSys

Source: Materials from presentation by Deloitte Tohmatsu Consulting at the Fourth Research Committee

[14] Concerning Japanese banks, in a questionnaire survey which the Japanese Bankers Association conducted in June and July of 2016 targeting its members, 66 of 99 responding banks (approx. 67%) replied that they are conducting some form of deliberation including study and research activities.

[15] IBM Institute for Business Value "Leading the pack in blockchain banking" (2017)

[Figure 4-2] Deliberation Status of Utilization of Blockchain Technology/DLT by Financial Institutions Worldwide (as of March 2017)



The above figure was prepared based on various reports and press releases.

3.2 Overview of Individual Initiatives

3.2.1 R3

R3 is a consortium led by the U.S. startup R3CEV. Established in September 2015, its purpose is to establish infrastructure utilizing new technology for the financial sector and to research the correspondence of regulations. As of December 2016 there are more than 70 participating companies including Barclays, BBVA, J.P. Morgan, UBS, Bank of America, Deutsche Bank, HSBC, Mitsubishi UFJ Financial Group, Mizuho Financial Group, Sumitomo Mitsui Banking Corporation and Nomura Securities[16].

The consortium's activities that have been announced so far include validating the possibility of DLT which utilizes the Ethereum platform, conducting Proof of Concept for bonds (commercial paper) which utilize five different platforms (Chain, IBM's platform, Intel's platform, Ethereum and Eris) regarding their issuance, transaction in secondary markets, redemption and Proof of Concept for shared KYC[17] services. However, these have not yet reached the stage of operation in production environments.

Led by the R3 consortium, the distributed ledger platform Corda was developed for the financial sector and in November 2016 it was released as an open-source platform.

[16] http://www.r3cev.com/press/2016/12/14/credicorp-joins-r3-distributed-ledger-consortium
[17] Abbreviation for "Know Your Customer."

3.2.2 The Hyperledger Project

The Hyperledger Project is a consortium established in February 2016 for the purpose of promoting blockchain technology/DLT. Led by the Linux Foundation, it conducts research and development through the collaboration of more than 30 IT companies, financial institutions worldwide, including from Japan.

While R3's activities focus on specifically to the financial sector, the Hyperledger Project's aim is to meet the requirements of a variety of sectors such as manufacturing, insurance, real estate contracting, IoT, license management and energy transactions.

Initiatives utilizing the platform developed by the Hyerledger Project include Proof of Concept in trade financing led by UBS and Proof of Concept[18] in securities by the Japan Exchange Group. Furthermore, the Mizuho Financial Group announced in June 2016 that it will conduct verification operations for cryptocurrency in the field of settlement services[19].

3.2.3 Ripple

Ripple is a FinTech startup established in San Francisco in 2012. It aims to create new secure and low-cost settlement infrastructure that can process international settlements which are small but frequent, utilizing distribution technologies such as blockchains.

Of the top 50 global banks, 15 participate in or have demonstrated participation in the international settlement network created by Ripple. More than 90 banks globally have completed Proof of Concept. Moreover, the cryptocurrency XRP issued by Ripple can be used as a bridge currency for interbank settlements. Demonstration experiments concerning the utilization of XRP have been completed by R3 with the participation of 12 banks.

In Japan, the Consortium for Unification of Domestic and Foreign Exchange, which employs Ripple as the platform technology, was established in October 2016. There are 47 financial institutions participating as of March 2017.

3.2.4 Other

Besides the initiatives mentioned above, the current status of principal deliberations for the possibility of utilizing blockchain technology/DLT by individual financial institutions or through the collaboration of multiple financial institutions is as outlined below.

[18] http://www.jpx.co.jp/corporate/research-study/working-paper/tvdivq0000008q5y-att/JPX_working_paper_No15.pdf
[19] https://www.mizuho-fg.co.jp/release/20160622release_jp.html

[Figure 5] Status of Principal Deliberations on the Possibility of Utilization by Japanese Financial Institutions (as of March 2017)

Announced	Implementing bank (participating bank)	Overview
December 2015	SBI Sumishin Net Bank	Launched a Proof of Concept for the establishment of future backbone operation systems that utilize blockchain technology
February 2016	Mizuho Financial Group	Launched a Proof of Concept targeting syndicate loan operations through the collaboration of 4 domestic companies
February 2016	Mizuho Financial Group	Launched a Proof of Concept for cross-border document information sharing between multiple nations as well as original currencies through a collaboration with overseas IT service providers (completed in February 2017)
March 2016	Mizuho Bank	Implemented Proof of Concept for streamlining cross-border settlement processes in securities transactions together with Fujitsu
March 2016	Fukuoka Financial Group	Launched inspection of possibility of application to new financial services such as exchanging points and various settlement services
June 2016	Mizuho Financial Group	Launched evaluation of possibility of application of blockchains in settlement operations as well as the feasibility of cryptocurrencies
July 2016	Mizuho Financial Group	Launched a Proof of Concept for international remittance as a collaborative project in the R3 consortium
July 2016	Shizuoka Bank ORIX Bank Corporation	Completed a Proof of Concept for blockchain application with the theme of trade finance
August 2016	The Bank of Tokyo-Mitsubishi UFJ	Launched Proof of Concept in Singapore for the utilization of blockchain technology targeting the digitization of checks
November 2016	Mizuho Financial Group, Mitsubishi UFJ Financial Group, Sumitomo Mitsui Banking Corporation (Blockchain Study Group)	Implemented a Proof of Concept for blockchain technology in domestic interbank transfer operations
November 2016	The San-In Godo Bank	Launched a Proof of Concept for electronic money using blockchains
January 2017	The Bank of Iwate	Launched a Proof of Concept for services utilizing blockchain technology
February 2017	Sumitomo Mitsui Banking Corporation	Launched a Proof of Concept for the possibility of application of blockchain technology in the field of trade

The above figure was prepared based on the press releases of the banks.

Note: The above does not cover all of the initiatives in the banking industry. Initiatives that have not been officially announced such as press releases are not included, although they are reported.

4. The Possibility and the Challenges of Utilizing Blockchain Technology/DLT in the Banking Sector

4.1 Issues for Utilization

When it comes to an existing or a new operation or transaction, whether a centralized management system or blockchain technology/DLT is appropriate will depend on the operation or transaction's nature, characteristic. In utilizing blockchain technology/DLT in the banking sector, the issues originating in the nature of these technologies are as follows[20].

[Figure 6] Issues in Utilizing Blockchain Technology/DLT

Classification	Issue
(1) Function	✓ Performance requirements and data synchronization ✓ Finality
(2) System safety, Security	✓ Zero downtime (availability and redundancy) ✓ Resistance to tampering, irreversibility and traceability
(3) Ensuring data confidentiality	✓ Sharing and management of transaction records ✓ Encryption and authority management
(4) Implementation	✓ Operation and governance ✓ Resources and capacity
(5) Cost effectiveness	

It is currently standard for bank operations and transactions to be managed by a centralized system and database (centralized management system). Deliberation of the possibility of utilizing blockchain technology/DLT in some operations and transactions will inspect the advantages of blockchain technology/DLT compared to centralized management systems in terms of the above issues[21].

4.1.1 Issues Regarding Function

4.1.1.1 Performance Requirements and Data Synchronization

- Consensus algorithms and their processing speed often become the main factor determining processing performance. If it is too slow, the performance requirements are not met. If it is too fast, the burden of the system and communication for the processing of synchronization, approval becomes too big. Therefore, consensus algorithms and systems must be designed depending on the operations and transactions, taking into considering their balance.

- Since consensus algorithms that do not result in the forking of chains (PBFT; the same follows hereafter) are designed so that the results of the participants in the blockchain/distributed ledger are tallied, the formations of agreements in whole will require more time when there are

[20] Please refer to [Reference Materials 2] at the end for legal issues.

[21] In this section these are indicated as a general feature of blockchain technology/DLT. Please note that these may not apply in some cases to individual products since there are many issues to which solutions are being sought in this field where technical innovations are making rapid progress. Also, these issues may be interrelated and so are not necessarily separate points. Measures to resolve one issue may affect other issues.

participants with slow processing or when there are many participants. Therefore the processing speed required for actually carrying out the assumed operations and transactions may not be ensured. When a consensus algorithm that results in forking (PoW, PoS, PoI; the same follows hereafter) is employed, the more participants there are in the blockchain/distributed ledger, the more forking there will be from the time lag in synchronization and the greater the possibility of frequent inconsistency of data between participants.

- In order to improve processing performance with increased computer performance, enhancement of functions in programming such as increasing the amount of data shared per unit time is needed. However, with regards to public blockchain platforms in particular, since an agreement of the majority of the participants is required, changes in specifications is difficult and technological development such as increased computer performance may not always result in improved processing performance.

- In general, processing performance is a trade-off with security and availability. For example, increasing the number of participants in a public blockchain indicates increased availability but the processing performance may decrease if the system design is not adjusted.

4.1.1.2 Finality

- Finality (settlement finality) generally refers to a state in which a settlement is completed without conditions and is irrevocable[22]. While consensus algorithms that generate forking in chains are able to adapt in cases where there are many participating nodes, because of their mechanisms it cannot completely eliminate the possibility of overturns in transaction details (finality cannot be ensured)[23]. Therefore, in consideration of the safety and security of transactions, the relationship with finality is an important issue when incorporating blockchain technology/DLT to financial services providing settlement functions.

- With regards to this issue, the following points need to be clarified in light of the current conceptions of cash equivalent transactions.

  - When to deem a transaction as final
  - How to deal with overturns in transaction details
  - How to determine the time of implementation of transactions
  - How to deal with and how to recover in situations where a participant received a transaction

[22] Finality may also refer more widely to finality between parties, finality with a third party, fund settlement finality or irrevocability of a payment order. For details, please refer to Takuya Shima The Legal Concept 'Settlement Finality' in Funds Transfers System" (http://www.fsa.go.jp/frtc/nenpou/2006a/11.pdf).
English version (http://www.fsa.go.jp/frtc/nenpou/2006a/11e.pdf)

[23] With Bitcoin, for example, a transaction recorded in a block is confirmed only after six more blocks are generated (some parties will confirm the transaction prior to there being six more blocks) and there is still a certain possibility that the transaction may be overturned.

but the transaction was not recorded due to failure

- Transaction details will not be overturned in consensus algorithms that do not result in the forking of chains. However, discrepancies in the content of ledgers may arise in cases such as where there are delays in information of some nodes due to failure. If the information on the ledger is read at such a time, the consistency of data between nodes may not be maintained.

- Due to system design, a significant amount of time may be required without intention for a transaction to be recorded in a block and there is a possibility that discrepancies may arise in the order of transactions as well as the order of their recording in blocks. Therefore the foreseeability of whether or not a service is sure to be implemented may be decreased[24].

4.1.2 Issues Regarding System Safety and Security

4.1.2.1 Zero Downtime (Availability and Redundancy)

- Since the same information (ledger) is shared between multiple participants (nodes) in blockchain technology/DLT, the effects of the suspension or failure of the ledgers of some participants[25] on the management and operation of the entire system are able to be controlled. As such, the realization of systems with availability and redundancy (substantially zero downtime) are generally considered to be relatively simpler in blockchain technology/DLT[26].

- The availability of blockchains/distributed ledgers will be limited even if they operate nonstop if there is stop time in peripheral systems and services. Also, if the number of participants decreases this will affect the resistance to tampering even while redundancy and availability are maintained.

- In exchange with availability and redundancy, participants in distributed systems must perform both the role of client and of server and, additionally, when failure occurs, must autonomously change their role and implement decision-making by majority vote. As such, the operations of distributed systems are generally more complex than centralized management systems.

4.1.2.2 Resistance to Tampering, Irreversibility and Traceability

- The data structure of blockchains/distributed ledgers is such that it can easily ensure resistance to tampering and irreversibility. Therefore blockchains/distributed ledgers may be able to realize resistance to tampering and irreversibility of the same level as centralized management systems with simpler compositions and at a lower cost. However, regarding the standard of tamper

[24] With Bitcoin the transactions with higher fees are prioritized in authorization and the situations exist where those with lower fees are not authorized (such as with records being deleted after 72 hours).

[25] However, since blockchains/distributed ledgers maintain their reliability through majority rule, management methods for dealing with cases where the number of participants is lower than what is needed to establish reliability must be considered.

[26] The conditions for establishing availability (such as the number of operating units) depend on the consensus algorithm, type of participation (private, public or consortium).

resistance, methods must be chosen according to operational conditions due to the impact of the consensus algorithm.

- Blockchain technology/DLT may increase traceability and transparency of transactions and may be used as audit trails.

- Since the significant irreversibility makes corrections difficult, deliberation from technological and management standpoints for how to make corrections or deletions when wrong information has been inputted or how to maintain the reliability of the information recorded in ledgers is necessary.

- Depending on the consensus algorithm, if there is a group of participants accounting for more than a certain percentage computer resources (CPU) comprising the blockchain/distributed ledger, the participants in that group may in effect become the manager of the blockchain/distributed ledger, giving rise to the risk that they may intentionally tamper with the ledger[27].

4.1.3 Issues Regarding Data Confidentiality

4.1.3.1 Sharing and Management of Transaction Records

- The feature of blockchain technology/DLT in which multiple participants share the same information (ledger) is an advantage in operations, transactions that assume the sharing of information between participants (or in which added value is gained through such).

- On the other hand, the following may be issues in operations and transactions that do not assume the sharing of information between participants.

  - Legal arrangements concerning the holding of ledger records by participants other than the transacting party
  - The essentials of information sharing upon joining a blockchain/distributed ledger
  - How to ensure deletion of information upon withdrawal from a blockchain/distributed ledger

- In blockchains/distributed ledgers, there may be detachment in the reception of a transaction from its recording time and, generally, in distributed systems the times do not completely match between participants. As such, there needs to be prior agreement between participants and legal arrangements regarding the method of recording times and the interpretation of times in various conditions.

- Acknowledgement of all participants is necessary for confirming the retention of the same

[27] Therefore, deliberation regarding the necessity and method of understanding the characteristics of blockchain participants on a continual basis as well as the method of avoiding extreme fluctuations in the number of blockchain participants is required.

information by all participants and there is generally a limitation in immediacy compared to centralized management systems. There is also a method of recognizing inconsistencies between members but this bears other challenges such as forking chains.

4.1.3.2 Encryption and Authority Management

- Since multiple participants share the same information (ledger) in blockchains/distributed ledgers, in principle the information recorded in the ledger is disclosed to all participants. While it is possible to conceal some or all of the transactions through authority management and encryption, the technology for concealing information in cases where information is to be disclosed only to the participant that is the transacting party is still currently under development. Also, since the implementation of encryption technology is a trade-off with processing performance, the impact on processing performance must be considered.

- Combinations of the following security requirements are being proposed for implementation.

[Figure 7] Trends in Security Technology

Security requirement	Implementation method
User authentication	User authentication through user ID and login
Transaction authentication	Confirming which user implemented each transaction through digital certification
Privacy protection	Anonymizing implementers of transactions through anonymous certification
Data concealment	Encryption of transaction details
Access control	Controlling users' implementable transactions and data access privileges (read/write)

- Even if information is obscured to participants other than the transacting party through encryption, the legal issues must be clarified since the encrypted information itself is still shared among all participants. Also, since a greater number of parties retain blockchain ledgers/distributed ledgers compared to centralized management systems, there are more instances when the encrypted information will become available to those that would attempt to decode the information and so the risk of decoding is increased[28].

- When a centralized management system is used to centrally manage privileges, the centralized management system may be a single point of failure even if the ledger itself ensures availability and redundancy.

- Even if encryption is used through the latest technology, future improvements in computer functions and advancements in decoding technologies could possibly result in a situation where

[28] However, the distributed ledger platform Corda developed with the lead of the R3 consortium enacts measures that allow data to be held only by the transacting party. This assures confidentiality but gives rise to challenges in terms of availability.

current encryption technologies are lacking in security (loss of assurance of safety) and countermeasures are therefore needed in systems that assume long-term use.

4.1.4 Issues Regarding Implementation

4.1.4.1 Operation and Governance

- Since multiple participants share the same information (ledger) in blockchains/distributed ledgers, operation and governance becomes more complex compared to centralized management systems as there is a greater number of parties overall for operations and administration.

- The irreversibility of blockchains means that once a program has been placed in a blockchain it cannot be changed. Measures must be devised for how to deal with changes and corrections.

- Agreement between relevant parties is needed for the following matters.
  - Methods of determining specifications of and renewing programs
  - Procedures and processing details for when the number of participants in a blockchain/distributed ledger changes
  - Process for managing incentive (particularly with PoW)
  - Methods of management for when there is system failure or when a threat has actualized (recovery and investigation of the cause)
  - How to allocate system management fees
  - For consortium platforms, standard for selecting participants and KYC methods
  - Handling of determination time of information
  - Response and legal measures for when transactions are not implemented according to the records in the blockchain/distributed ledger
  - Necessity and specification of experimental environments mimicking actual environments for the protection of actual systems after operations begin

- Deliberations are also required for how to constantly monitor the operating status (participants, synchronization of the ledger, speed of consensus) of blockchains/distributed ledgers.

4.1.4.2 Resources and Capacity

- Since blockchains/distributed ledgers must record transactions that are not related to itself, the capacity of information required for maintaining the ledger increases in proportion to the number of participants. Therefore, a large capacity is needed for information compared to centralized management systems[29].

- Further development of data storage minimization technologies is required in order to ease

[29] However, the distributed ledger platform Corda developed with the lead of the R3 consortium aims to resolve this point.

resource restrictions.

- Some consensus algorithms require a large amount of computer resources and electric power for consensus building. The participants in the blockchain/distributed ledger bear the burden of the resources needed for consensus building as the cost for ledger operation. In particular for consortium platforms, deliberation for allocating resources fairly is needed.

- Speeding up of processing through system enhancement tends to be difficult compared to centralized management systems. Particularly with public platforms, consensus algorithms may affect processing performance and finality according to the number of participants[30].

4.1.5 Issues Regarding Cost Effectiveness

- In systems used in banking operations, ensuring redundancy and availability, countermeasures for tampering and ensuring traceability are considered to be important matters. In order to meet these conditions, conventional centralized management systems use system multiplexing and other measures. With blockchain technology/DLT, it is said that the same conditions may be met with relatively lower costs. As such, it is expected that fundamental streamlining of banking systems will become possible through the utilization of blockchain technology/DLT.

- However, the following points must be considered with regards to cost comparison.

  - Cost reduction measures must be compared since centralized management systems also have cost reduction measures such as in switching the host computer to an open-type computer or using cloud services.
  - Costs required for consensus building and communication costs for keeping the ledger up to date must be considered.
  - When establishing a new system using blockchains/distributed ledgers, various elements must be considered and deliberations must be made based on total cost of ownership (TCO) including system, office and operation aspects.
  - Deliberations must be made not just for IT infrastructure but also with regards to the fundamentals of infrastructure and cost reduction effects through improvements of operational processes.

- When switching a centralized management system to a system that uses blockchain technology/DLT, the following may also be issues in their relation to cost.

[30] With PoW, for example, miners that discover nonces that firstly meet the conditions appear sooner when the number of participants increases. This results in increased processing performance as well as increased communication load (however, with Bitcoin the conditions for nonces are adjusted every two weeks so that the interval between blocks generated averages out to be 10 minutes). With PBFT, there is a wait until the number of approvals needed is obtained. Therefore, processing performance is reduced when the number of approvals needed increases. If the number of approvals needed is not increased with the increase of participants, Byzantine failure will not occur.

- The scope of transition
- Internally and externally establishing interfaces and functions for collaborating with peripheral systems
- Consistency with existing operation flows
- Consistency of saving formats of information[31]

4.2 Points for Utilization in the Banking Sector

The advantages of blockchain technology/DLT as compared with centralized management systems differ by use case. In general, though, the following are thought to be operations and transactions suited for blockchain technology/DLT.

[Figure 8] Operations and Transactions Suited for Blockchain Technology/DLT

Suited operations and transactions

- ✓ Operations and transactions which provide some sort of value through sharing a ledger (such as distributed information collaboration, streamlining business processes and ensuring traceability)
- ✓ Operations and transactions that do not need to happen in real time

Unsuited operations and transactions[32]

- ✓ Transactions that need to be processed in milliseconds
- ✓ Operations and transactions comprising only one organization (these can be handled by normal systems)
- ✓ Substitutes for simple data bases, middleware and transaction processing systems

When utilizing blockchain technology/DLT in the banking sector, the appropriate type (public, consortium or private) and consensus algorithm are selected by use case in light of these characteristics and issues.

There are many systems that are used in the banking sector for operations and transactions. This section will deal with remittances, KYC, core banking systems and financial infrastructure, four topics that are being deliberated in Proof of Concept and implementation for the possibility for utilizing blockchain technology/DLT. The main areas where implementation is possible by use case and the points of consideration are as follows.

Currently Blockchain technology/DLT is moving forward with rapid technological advancements. Note that the following are based on the technological standards of the present, are considered from a general standpoint and that not all possibilities for utilization and points of consideration are

[31] It may not always be the case that the format for recording information on blockchains/distributed ledgers and the format in which information is saved in conventional technologies can be matched.

[32] Unsuited operations and transactions are not necessarily inapplicable since the issues may be solved through adjustments in mechanisms.

covered.

4.2.1 Remittances

(1) Considerations for the Possibility of Utilization

Regarding domestic remittances, since real time transfers between banks have been realized in Japan, blockchain technology/DLT is basically not superior in terms of performance requirements[33]. On the other hand, since blockchain technology/DLT may realize strong tamper resistance and high availability systems, which are crucial for settlement systems, at low costs, it could be utilized as a measure to realize a low-cost transfer service (low-value remittance) with lower performance requirements. Also, in examining the provision of transfer services with additional functions, utilization of blockchain technology/DLT is expected to be beneficial in that it will not be influenced by the specifications of existing systems while the initial investment of participants can be relatively easily reduced.

Regarding foreign remittances, considering the current standard of performance requirements, it is very likely that even with the processing performance of blockchain technology/DLT, a performance standard above the current level can be achieved. As multiple financial institutions are mediating to relay commercial and financial information, it is expected that operation costs, fees can be reduced by utilizing blockchain technology/DLT's feature of sharing and managing recorded information. Also, by allowing blockchains/distributed ledgers to be shared also by non-bank parties (supply chains) and linking transaction information with settlements, services with high added value could be developed and provided such as in the field of trade finance. Integrally providing domestic and foreign transfer services, which has been difficult so far, is now on the horizon.

(2) Points of Consideration and Challenges

The point for implementation is the verification of total cost effectiveness including (1) technologically achievable performance level and function and (2) cost for implementation and data confidentiality. These will ultimately be reflected in transfer costs to be borne by clients and thereby influence what kind of transfer service can be realized at what price.

In introducing mechanisms using blockchains/distributed ledgers in foreign remittances, examinations and agreements from various angles including operations and systems will be necessary when collaborating with parties from foreign countries with different business practices and laws. Moreover, since the impact of network speed is strong with consortium blockchains/distributed ledger, careful verification of system operations is needed especially in foreign remittances.

4.2.2 KYC

(1) Considerations for the Possibility of Utilization

[33] On the other hand, blockchain technology/DLT may be a way in which issues can be solved depending on performance standards in countries where real time transfers have not been realized.

KYC[34] is currently implemented by individual banks and clients are bearing procedural burdens as there are cases where different banks have different procedures. Utilizing the features of blockchains/distributed ledgers of information sharing and strong tamper resistance, timely and accurate information sharing across banks and reduction of client procedural burdens may be realized. In terms of backing up information, a reduction of hardware costs may be possible if distributed management is realized through blockchains/distributed ledgers.

KYC information requires encryption from a technological standpoint but since relatively lower processing performance is required compared to remittance transactions, the usual problem of the trade-off between security and processing performance is thought to be less likely to occur.

(2) Points of Consideration and Challenges

KYC information generally requires higher confidentiality of information and the development of technologies to meet these conditions, including security measures, is needed. When sharing information between multiple banks based on the consent of clients[35], due to the feature of the service the issue will be whether or not the consent of the clients can be obtained.

A clarification of legal issues is needed both for private platforms and consortium platforms. For example, clarification of where responsibility lies in the handling of private information, responsibility boundary between participants and making rules for how to solve problems can be raised. Each needs to be deliberated based on the relevant laws and regulations.

4.2.3 Core Banking Systems

(1) Considerations for the Possibility of Utilization

Since core banking systems which process the core operations of banks require high reliability and stability, cost benefits may arise such as through the elimination of backup devices, if zero downtime can be realized, using the high availability of blockchains/distributed ledgers. The current mechanisms in operation and governance may be followed if a private platform is employed. This may reduce the impact upon introduction to relatively small.

When account information is allowed to be shared with client companies, this enables direct linking of ledgers with those client companies. For example, if account information is shared on a distributed ledger with a client company, operations of receipt and payment of money which the client company conducts through its own accounting treatment will be shared and reflected on the account information without the financial institution having to command the receipts and payments.

(2) Points of Consideration and Challenges

Application of blockchains/distributed ledgers to existing systems requires that high security

[34] Management of client information when an account is made, updated information when the address or name is being changed, transfer checks based on the Act on Prevention of Transfer of Criminal Proceeds, list of those subject to sanctions based on the Foreign Exchange and Foreign Trade Control Law.

[35] On the other hand, if KYC information is not shared between multiple banks, the platform will necessarily be private and the feature of sharing information, an advantage of blockchains/distributed ledgers, cannot be utilized.

(including encryption) is secured while the same performance level is maintained. With the current level of technology, it is difficult to secure processing speed and standards of security that can withstand implementation at medium and large banks and so innovation will be needed.

As core banking systems serve the central function of banking systems, utilization of blockchain technology/DLT requires that connection with peripheral systems is also validated. Furthermore, when large amounts of past data held by existing systems are to be managed through blockchains/distributed ledgers, methods of transferring and holding data must also be deliberated.

4.2.4 Financial Infrastructure

(1) Considerations for the Possibility of Utilization

Utilization of blockchain technology/DLT as a replacement for centrally managed financial infrastructure that is currently used between banks is generally thought to require a large amount of investment and longer time[36]. On the other hand, since financial infrastructure requires high reliability and stability, centralized management systems require large amounts of investment, including for backup site facilities. Therefore, if zero downtime is realized utilizing the high availability feature of blockchains/distributed ledgers while paying attention to the decrease of performance requirements, cost reductions may be possible.

It is thought that blockchain technology/DLT can be an option for partial transfer in specific operations and systems if their characteristics and limits are also taken into account.

(2) Points of Consideration and Challenges

Centrally managed financial infrastructure currently used between banks processes large numbers of transactions at high speed. On the other hand, blockchain technology/DLT are generally considered to be unfit for these types of transactions. Replacement with blockchains/distributed ledgers will only be appropriate after it meets the technological challenges of satisfying other functional requirements while securing the same level of performance requirements.

[36] World Economic Forum “The future of financial infrastructure” (2016)

[BOX 2] Possibility of Application in the Zengin System

1. The Zengin System (Data Telecommunications System in Japan)

- The Zengin System is a central system which processes domestic remittances (domestic transfers to other banks) of financial systems online and in real time. It is managed and operated by the Japanese Banks' Payment Clearing Network (Zengin Net). Financial institutions across Japan[37] are connected to each other through this network. Requests of transfers received from clients to financial institutions all across Japan are sent and received through the Zengin System to financial institutions online and in real time and real time receipt of payments to accounts is realized.

- Data such as notifications of transfer related to remittances is currently sent through the Zengin System's telegraphic fund transfer or through the new file transfer. The mechanisms of telegraphic fund transfers are such that data of notifications of transfers is sent and received online and in real time one transaction at a time. The processing capacity of the system is five million transactions per hour (approx. 1,389 transactions per second) and 25 million transactions per day. For the new file transfer, data of notifications of transfer such as for stock dividend transfers is transferred in bulk on a specific date and the system has the capacity to process 26 million transactions per day.

2. Future Policy for Zengin Net

- While there are still technical challenges including the performance requirements in utilizing blockchain technology/DLT in the Zengin System at the current stage, it is Zengin Net's policy to continue deliberating the utilization of blockchain technology/DLT while holding the following views.
  - In considering the use of blockchain technology/DLT, it is believed better to incorporate this technology as a new mechanism rather than as a simple replacement of existing systems.
  - As the Zengin System is a fund settlement system that can accurately and speedily process both large and small settlements, the utilization of blockchain technology/DLT must be considered carefully and with an eye on the expectations and trust that users have in these existing services.
  - The impact on the systems of connecting member banks must be considered

[37] There are currently 1,296 financial institutions (as of the end of December 2016) participating in the Zengin System. These include not only banks but also credit unions, credit associations, labor credit associations and agricultural cooperatives. Nearly all deposit-taking financial institutions in Japan utilize this system.

(including the impact on cost).

- Considerations must be made for business system compliance of clearing institutions for interbank fund transfers called for by the BIS's Principles for Financial Market Infrastructure and the Financial Services Agency's Comprehensive Guidelines for Supervision of Financial Market Infrastructures.
- As the emergence of new transfer services that utilize blockchain technology/DLT is expected going forward, the role and positioning of blockchain technology/DLT as settlement infrastructure should be continually verified.

[BOX 3] Possibility of Application to the Densai Net System

1. The Densai Net System

・ The Densai Net system has the role as an institution that records electronic monetary claims. Its main operation is to hold registry, make electronic records and disclose matters in a monetary claim upon the requests of users. Densai Net, the operating body, conducts its operations as a specialized joint-stock corporation designated by the relevant cabinet ministers, namely the Prime Minister and Minister of Justice.

・ The performance requirements at the current level are as follows (as of the end of December 2016)

(1) Number of users: Approx. 444,000 companies / Approx. 599,000 contracts
(2) Number of participating financial institutions: 609[38]
(3) Number of joint relay centers: 3
(4) Operating hours (online transactions): 7:00 to 24:00[39]
(5) Performance target[40] (Online transactions): Update operations: 3 seconds; Reference operations: 1 second
(6) Operation data storage area: Approx. 5TB[41]

2. Future Policy of Densai Net

[38] These are 7 city banks/trust banks, 105 regional banks/second regional banks, 265 credit unions, 105 credit associations, 123 JA/credit federations of agricultural co-operations/The Norinchukin Bank and 4 other financial institutions.
[39] The second Saturday of every month is the scheduled non-operating day. Business hours other than the core hours (9:00 to 15:00 of weekdays) depend on the participating financial institutions.
[40] Performance target assuming a maximum load of 50 online applications per second.
[41] This is the storage capacity of the main disk device and not the total storage capacity of the Densai Net system.

・ The following are some of the issues upon applying blockchain technology/DLT to the Densai Net system.

- Verification of the benefits for and incentives of users, Densai Net and the participating financial institutions is necessary.
- How to realize the implementation of confidentiality must be considered including the use of encryption. In addition to meeting the challenges in system design and encryption technology, consideration must also be given to legal issues such as whether or not the implementation is in line with existing laws and regulations.
- There is a need to consider how to work with cost sharing and responsibility of maintenance and operation of the software and hardware of financial institutions if systems with blockchains/distributed ledgers are built.
- The blockchain/distributed ledger feature of high tamper resistance may be a restriction as corrections of records may occur in Densai Net transactions and so countermeasures must be considered.
- It is possible that the format in which information can be recorded on blockchains/distributed ledgers and the format of past data currently held by the Densai Net system may not be able to be integrated (see footnote 31 earlier) and so deliberations are necessary for how to transfer and hold data.
- Since the current Electronically Recorded Monetary Claims Act specifies that recording in registry is a requirement for a monetary claim to become effective, there needs to be clarification in how to deal with registry in distributed ledgers. Because service provisions of Densai Net are conducted based on the Electronically Recorded Monetary Claims Act, Act on the Protection of Personal Information, Act on Prevention of Transfer of Criminal Proceeds and other relevant laws and regulations, compatibility with relevant laws and regulations and the necessity of legal revisions must be widely verified as the operations.

・ One of the policies of Densai Net's second medium-term management plan (fiscal 2017 to fiscal 2019) is to firstly verify the possibility of use of blockchain technology/DLT in the Densai Net system as well as the advantages/disadvantages, issues and impact upon use, in light of the debates at the Japanese Bankers Association's Research Committee for the Possibility and the Challenges of Utilizing Blockchain Technology and then to advance initiatives targeting drastic systems streamlining while looking to the possibility of reducing infrastructure costs.

4.2.5 Other

Besides the use cases mentioned here, there are various other surveys, studies and initiatives regarding the possibility of utilizing blockchain technology/DLT that are being conducted by individual institutions[42]. In addition, in recent years there has been an increase of initiatives through interbank collaboration such as the joint Proof of Concept for domestic interbank transfer operations by the Mizuho Financial Group, Mitsubishi UFJ Financial Group, Sumitomo Mitsui Banking Corporation and the Deloitte Tohmatsu Group as well as the consortium for unification of domestic and foreign exchange by SBI Ripple Asia and Japanese banks.

[42] See “3.2 Overview of Individual Initiatives”

5. In View of the Possible Transformation that Blockchain Technology will Bring to Banking Operations

5.1 Necessity of Initiatives Engaging both the Private and Public Sectors

Blockchain technology/DLT has the potential to significantly transform the operations and systems of banking in the future. In the Japanese banking industry, many banks are now carrying out experiments and taking other measures to study and deliberate the possibility of utilizing this technology.

On the other hand, bank systems require a high level of stability, reliability and accuracy. Further considerations need to be made in technological, operational, security and legal aspects before this technology can be utilized or implemented. Moreover, collaboration between different parties is necessary if these issues are to be solved through business rules and operations.

Considering the distributed ledger feature of blockchain technology/DLT as well as the fact that much of banking operations and transactions assume interbank networks and that integration would reduce the costs of some operations, it can be said that it is important to advance both competitive initiatives of individual banks and initiatives in which the public sector works together with the private sector to overcome these challenges.

Given the above, the Review Committee proposes the following initiatives to the public and private sectors.

5.2 Recommendations of the Review Committee (Public-Private Sector Joint Initiatives on Blockchain)

5.2.1 Establishment of a Collaborative Blockchain Platform (tentative name) in the Banking Industry

There are currently various Proofs of Concept being conducted by individual banks for the verification of the possibility of utilizing blockchain technology/DLT. Given the distributed ledger advantage and feature of blockchain technology/DLT, the development of new services that go beyond individual banks and look to interbank networks as well as the commonization of non-competitive operations and systems for the purpose of cost reduction can be potent areas where the utilization of this technology is expected in the future.

Currently, examinations of the possibility of utilizing blockchain technology/DLT is moving from the private phase where banks were individually considering utilization to a phase where consortium-type examinations are being conducted through interbank cooperation[43]. From the perspective of supporting such initiatives, it is therefore expected that deliberation for the establishment of a Collaborative Blockchain Platform (tentative name), as an environment of Proof of Concept aiming collaboration and cooperation, by the next fiscal year will be advanced, mainly by the banking

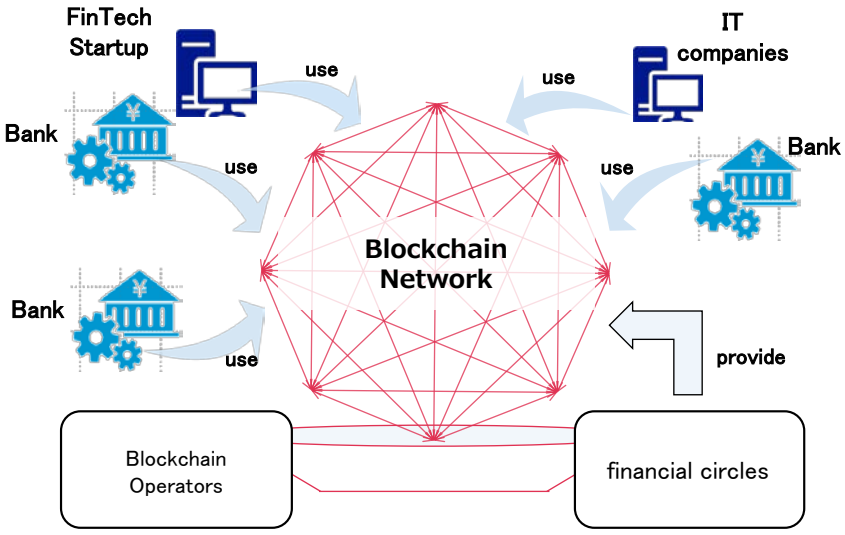
[43] Generally, deliberations for utilization of this technology by individual banks assumes private blockchain platforms while deliberations for collaborative utilization between banks assumes consortium blockchain platforms.

industry, for the purpose of facilitating collaboration and cooperation for implementation as well as to decrease development costs[44].

In the Collaborative Blockchain Platform,

- The banking industry will collaborates with blockchain operators and develops the environment of Proof of Concept and the framework of information network (Blockchain Network)
- It will be enabled that IT companies, FinTech startups and banks collaborate and cooperate to carry out trials and Proof of Concept to develop financial services that utilize blockchain technology.

[Figure 9] Image of a Collaborative Blockchain Platform



(Note) Details will be deliberated in the banking industry

By establishment of this environment, it is expected that active consideration be advanced for implementation of blockchain technology/DLT regarding the sectors where utilization is expected such as through new settlement and money transfer services, KYC and financial infrastructure including the Zengin System and the Densai Net system.

5.2.2 Strategy for Responding to the International Standard

There are currently many standards for blockchain/distributed ledger platforms[45]. Applications that

[44] Not only are technological inspections necessary before implementing blockchain technology/DLT but legal problem solving is also essential such as for application of laws and safety measures standards. Given this matter, it is expected that the relevant authorities will give active support in clarifying the application of laws for Proof of Concept and inspections. For details please see “5. 2. 4 Collaboration with Relevant Authorities for the Utilization of Blockchain Technology/DLT”

[45] See the reference materials at the end for an overview of the main blockchain/distributed ledger platforms.

are programmed for one blockchain/distributed ledger platform will in principle not operate on platforms with different standards. Therefore, in considering new services, mechanisms that look to future cooperation and collaboration with overseas financial institutions, it is important to select a blockchain/distributed ledger platform taking into consideration the possibility of international proliferation according to its purpose. Selecting such a blockchain/distributed ledger platform will contribute to securing an international voice as users to deciding and changing specifications.

It is expected that initiatives will be progressively advanced in preparation for the establishment of the Collaborative Blockchain Platform (tentative name) in the banking industry upon selection and consideration of a suitable blockchain/distributed ledger platform and in consideration of these trends in international standards and the features of different platforms.

5.2.3 Deliberating the Possibility of Utilization in Financial Infrastructure

Regarding the utilization of blockchain technology/DLT in financial infrastructure, not only technological aspects, but several elements, such as safety, stability and reliability as infrastructure and the impact on connecting banks, must be considered from various angles. It is important to advance deliberations on the possibility of utilization proactively with a planned schedule in view of the possibility of future improvements of infrastructure, cost reduction.

Densai Net's second medium-term management plan (fiscal 2017 to fiscal 2019) states that Densai Net will examine the possibility of use of blockchain technology in the Densai Net system as well as the advantages/disadvantages, issues and impact upon use, in light of the debates at the Japanese Bankers Association's Research Committee for the Possibility and the Challenges of Utilizing Blockchain Technology and then to advance initiatives targeting fundamental system streamlining while looking to the possibility of reducing infrastructure costs[46]. It is expected that Densai Net will move forward with the initiatives above with a view to implement Proof of Concept for the Collaborative Blockchain Platform (tentative name).

It is also said that Zengin Net which manages and operates the Zengin System will continue to deliberate the utilization of blockchain technology/DLT.

As the emergence of new services utilizing blockchain technology/DLT is anticipated going forward, in view of the role and positioning of this technology as future financial infrastructure it is expected that financial infrastructure institutions will decisively advance these initiatives without delay[47].

5.2.4 Collaboration with Relevant Authorities for the Utilization of Blockchain Technology/DLT

If Proof of Concept for implementation are to be conducted or if clarifying challenges is to be undertaken by gathering feedback through experimental use by clients, the programs, mechanisms,

[46] To utilize blockchain technology in transactions of electronically recorded monetary claims, it is expected that the relevant authorities will give support to clarify with regard to the current Electronically Recorded Monetary Claims Act..

[47] If the possibility of new services or of cost reduction is anticipated, there could be initiatives such as the implementation of Proof of Concept for the Collaborative Blockchain Platform (tentative name).

business rules must take into account the final legal conformity in the deliberations.

On the other hand, it has been pointed out "since FinTech, as a starting point of innovation of technologies that will serve as the foundation for the provision of financial services, is something that tries to realize new ideas, in many cases, it is difficult to make arrangements with existing systems[48]." Besides this, there are various legal issues with regard to the utilization of blockchain technology/DLT[49].

It is expected that the relevant authorities will facilitate the initiatives of the private sector to implement blockchain technology/DLT such as through proactive support in individual Proof of Concept and deliberations for implementation by organizing the legal issues.

5.2.5 Collaboration with the Central Bank for the Utilization of Blockchain Technology/DLT

In deliberating the possibility of use of blockchain technology/DLT in financial infrastructures, collaboration with the central bank is also important.

It is expected that the central bank will engage in dialogue with a wide range of participants in the financial industry including the banking industry to utilize blockchain technology/DLT in financial infrastructures from the viewpoint of including, but not limited to, ensuring safety and increasing efficiency of settlements. It is also expected that the central bank will from time to time inform the banking industry about the international discussions concerning blockchains to ensure that the initiatives led by the banking industry is consistent with international discussions regarding settlements.

5.2.6 Clarification of the Security Guidelines concerning Application

In the use cases of blockchain technology/DLT, it is assumed that the degree of financial institutions' responsibility in safety measures varies. Since the Security Guidelines formulated by the Center for Financial Industry Information Systems (FISC) assumes the responsibility of financial institutions in safety measures, it is important to ascertain the degree of responsibility in safety measures of individual financial institutions in each use case. Moreover, it is assumed that technologies for which safety measures standards were not primarily considered will be newly employed.

It is expected that information security companies will research and study on blockchain technology/DLT while keeping an eye on trends of Proof of Concept, the status of new use cases from both a responsibility aspect and technological aspect of safety measures, as well as organize the application (interpretation, operation) of such assuming the new Security Guidelines that is scheduled to be revised.

---

[48] Nobuyuki Kinoshita's "Regulatory Sandbox" (NBL Jan. 15, 2017, p. 35)
[49] See [Reference Materials 2] at the end for details.

5.2.7 Forming a Blockchain Community

Regarding blockchain technology/DLT there are currently many parties that are advancing deliberations for problem solving in technological and other aspects as well as for the application of various use cases. The possibilities and the challenges of use mentioned in this document are merely those clarified at this point in time. New possibilities of use, challenges may be revealed going forward through Proof of Concept.

As such, there is a need to widely promote understanding on the challenges of the banking sector's utilization of this technology among IT companies, blockchain associations and operators, academics, researchers, relevant authorities and others and to encourage further studies, developments for resolving challenges and implementing this technology.

It is therefore expected that, in addition to the individual study and understanding of the latest technological trends by individual banks, Proof of Concept will be facilitated in the banking industry through the collaboration and cooperation of banks[50] while the formation of a community will be promoted such as through the establishment of a framework to share the outlines of the experiment results[51], information on technological trends from a wide range of parties, obtained through the Proof of Concept within the whole industry.

Also, as there is currently a lack of scientific research (technological research, research of system design, economic research) concerning blockchain technology/DLT, it is expected that, in the field of academic research, there will be further promotion of research and sharing of research results and that researchers in this field will be proactively nurtured so that the technology can be implemented soundly and appropriately.

[50] For example, it is considered that banks hosting the Proof of Concept develop a mechanism calling for participation in joint experiments through industry organizations.

[51] In obtaining meaningful research results, it is important to clarify the purpose and significance of the demonstration experiments to be conducted and to plan and design the experiments accordingly.

[Reference Material 1]

Overview of Principal Blockchain/Distributed Ledger Platforms and Related Technologies

Eight blockchain/distributed ledger platforms that have already been implemented or that have been tested with Proof of Concept are introduced here.

1. Bitcoin Core
・Developer: Bitcoin Core (https://bitcoin.org/)
・Features: The reference implementation of Bitcoin; the first platform to apply and spread blockchain technology.

2. Ethereum
・Developer: Ethereum Foundation (https://www.ethereum.org/)
・Features: Platform for construction decentralized applications (DApps); contracts can be described with special programming language; Ethereum is flexible and is used in Proof of Concept in various fields.

3. Hyperledger Fabric
・Developer: Hyperledger Project (https://www.hyperledger.org/community/projects)
・Feature: One of the P2P DLT platforms under development by the Hyperledger Project led by the Linux Foundation under open governance and aiming to be the global standard; Ver 0.7 employs PBFT as consensus algorithm.

4. Corda
・Developer: R3 (https://www.corda.net/)
・Features: DLT platform for finances led by the R3 consortium; focuses on consensus building; not all data is shared between participants; released as open source platform in Nov. 2016.

5. Chain Core Developer(Enterprise) Edition
・Developer: Chain (https://chain.com/)
・Features: Equipped with functions assuming corporate use such as with the new consensus algorithm Simplified BFT which realizes completion of transactions in short periods and secures consistency of data, encryption of blockchains.

6. NEM
・Developer: NEM.IO Foundation (https://www.nem.io/)
・Features: Blockchain platform with its own currency function; PoI is employed as consensus algorithm; reduces power consumption and low barrier to entry through a method of determining block generators every minute according to the contribution to the network; functions such as multisig and encryption messaging as well as node evaluation systems for effective operation and management. There is a closed platform called mijin which was developed based on NEM and which employs PoS as the consensus algorithm.

7. Orb 1
・Developer: Orb (https://imagine-orb.com/)
・Features: The benefits of centralized and distributed platforms are merged through Super Peer which is authorized by the managing body; settlement finality is secured by periodically confirming transactions.

8. Interledger (ILP)
・Developer: Ripple (https://interledger.org/)
・Features: Connects existing ledgers held by financial institutions and provides mechanism of encrypted escrows; high-speed and low-cost payment is possible because of one-to-one exchange without a mediator is possible; ILP itself is standard of communications protocol and the whole does not have a single ledger (blockchain) or unique currency; the consensus section is publicly disclosed.

[Figure 10] Comparison of Principal Blockchain Platforms/Distributed Ledger Platforms

	Bitcoin Core	Ethereum	Hyperledger Fabric
Classification	Public, consortium, private	Public, consortium, private	Consortium, private
Consensus algorithm	PoW	PoW (as of March 2017)	PBFT (as of March 2017)
Finality	None. Since each node creates blocks there may be overturns in once-confirmed transactions if forking occurs in the blockchain.	None. Since each node creates blocks there may be overturns in once-confirmed transactions if forking occurs in the blockchain.	Yes. Finality exists since consensus is obtained and confirmed when updating.
Performance	Unit time between generation of blocks is 10 minutes. About an hour is required to see if a block has been confirmed.	Unit time between generation of blocks is 12 seconds. A few minutes is required to see if a block has been confirmed.	High-performance as consensus is obtained and confirmed when updating (targets 100,000 TPS per 15 nodes).
Account management	Participants are managed by each node and are not shared so there is no function of limiting inflow of participants.	Participants are managed by each node and are not shared so there is no function of limiting inflow of participants.	A membership service registers users and nodes and PKI-based certificates are issued.
Minimum configuration units	Operates starting at one unit. Two units are needed to withstand malfunctions.	Operates starting at one unit. Two units are needed to withstand malfunctions.	A minimum of four units is needed to withstand the malfunction of one unit on PBFT.
Data storage	Transaction information is stored on blockchains and transmitted.	The contracts themselves are also stored on blockchains and transmitted.	Comprised of blockchains and world state.
Confidentiality of information	None. Transaction details are publicly disclosed.	None. Transaction details are publicly disclosed.	Confidentiality is ensured. Certificates are issued for individual transactions and encryption is applied.
Smart contract development	Executed through script language. There is loop processing due to the simplicity of the language and limits on if-clause. Also, expansibility is weak[52].	A program called contract is developed with a special language called Solidity[53].	A program called chaincode is developed with the Go and Java languages. Java Script is scheduled to be added. It is directly executed by generating a native code from the source. It is executed in the Docker container.

[52] Bitcoin Core's limitations on smart contract development also have the purpose of safety and ease of verification.
[53] The source code does not depend on the platform since it operates on a virtual machine called Etherum Virtual Machine (EVM). Operations must be within a certain range of processing costs based on a fuel concept called Gas.

[Reference Material 2] Legal Points at Issue

Overview of Materials Presented by Member Kataoka (Chief Attorney, Kataoka & Kobayashi)

There is a distinction between private and public law systems and each is multilayered with different planes. Therefore in considering the legal system in relation to blockchains, it must be made clear where exactly the problem lies and which problem will be considered with which plane.

The following are basic legal issues that should be understood for the reason stated above when using blockchains for financial transactions.

1.1 Problem of the Assumption of Types of Blockchains

When considering the legal system in relation to blockchains, it must be kept in mind that there are various different types of blockchains and so problems must be examined in terms of each type as well as the legal plane that is relevant.

Blockchain platforms are generally classified into the following from actual and legal standpoints.

(1) Types in terms of the manager

1) Public: Has no manager (in principle)
2) Consortium: Has several managers
3) Private: Has a single manager

(2) Types in terms of revision of records

1) Non-revisable: Records cannot be revised (in principle)
2) Revisable: Records can be revised[54]
   A. Transfer revision: Targeted content is transferred to be replaced by revised content
   B. Deletion revision: Deletes the targeted content and records the revised content

   Among these there may be a gap between those that eliminate the targeted content and those that retain the record of deletion.

(3) Types in terms of legal effect

In considering use cases of blockchains, platforms can be classified into the following types from a legal perspective regarding the relationship of the records to legal effects.

1) Those with strong legal effects on legal rights of the records themselves due to legal stipulations.

Ex. Records of electronically recorded monetary claims (presumption of legal rights by law)

2) Those with legal effects on legal rights but not the legal rights of the records themselves, due to legal stipulations.

[54] Aside from the problem of whether to refer to these as blockchains or simply DLT aside, it is needed to separately consider the technological issues of how to revise individual transaction records in use cases where revision of transaction records is necessary and where the blocks in blockchains cannot be revised

Ex. Real estate registers (not recognized but has assertion by law; in judicial precedents there is no legal estimation concerning rights but there is considered to be actual estimation concerning actual transfer of rights)

3) Those with no direct legal effects in the records themselves

Ex. Commercial books (there are no direct legal effects, even though they may be used as evidence in lawsuits is possible)

1.2 Legal relations by type of blockchain platform

(1) Public

Since public platforms do not have a manager and only have an algorithm as a computer system, legal relations in causal relations cannot be ordered in contract law principles and so determination by the legal principles of (1) office management, (2) profiteering or (3) unlawful acts, which are debts-and-credits relations of provision of the law of obligations in causal relations, will be made. In addition, application of (4) the principle of good faith, (5) abuse of rights, (6) violation of public order or morality or (7) reasonableness which are general legal principles is possible.

(2) Consortium

Regarding consortium platforms, some or all of the original board members comprising consortiums consider it normal that agreements are determined by organizations such as associations as joint action. If there are those which originally or later join, due to this agreement as organic law or civil entity contract they will be ordered with contract law principle of the agreement.

In consortiums it is thought to be normal to determine a clause which orders with contract law principles the legal relations of basic civil substantive laws concerning the blockchains between these participating parties and the users. It is also thought that ordering by contract law principles the legal relations of basic civil substantive laws concerning blockchains between users by clause law principles will be recognized.

On the other hand, regarding consortium blockchain platforms, whether or not the stipulating of orders of civil substantive laws against perpetrators of wrongful acts will have legal effects is an issue. If it is stipulated in the clause to be one to access consortium platforms which are private, this may be ordered by contract law principles including the principle of good faith. This is a matter of future deliberations.

(3) Private

Regarding private platforms, since there is a single manager, orders are thought to be made through contract law principles (see Article 548-2 and onward of the revised civil code draft; the same applies to consortium platforms) by the clause stipulated by the manager. The same applies as with consortium platforms regarding the relationship between users.

2. Problems of the Assumption of Legal Structure and Strata of Financial Transactions

(1) Cause or Lack Thereof

In considering the legal effects of financial transactions, there is a need to distinguish between those with cause that are impacted by legal relations of cause transactions and those without cause that are not impacted. If it is a transaction without cause, even if there is a defense[55] in causal relations, that is something that should be given effect and resolved between the parties of the cause transaction and the effects do not in principle reach the parties of the financial transaction. However, remedial actions by special laws such as the Act on Damage Recovery Benefit Distributed from Fund in Bank Accounts Used for Crimes (the so-called phone fraud remediation act) are a separate matter. It is also a separate matter if there is fault in the financial transaction itself and a reverse transaction will be made.

1) Cause Transactions

In the background or cause of financial transactions are cause transactions such as the sale of things and transactions of service provision. The lending of money is a financial transaction but is not itself a cause transaction.

2) Transactions with Cause

Even if a transaction as a settlement method of a cause transaction substantially has credit functions, comprehensive credit purchase intermediaries and individual credit purchase intermediaries concerning so-called sales credit will be defended in their cause relation by civil provision of the Installment Sales Act.

Moreover, regarding sales by personal loans of finance institution as well as so-called tie-up loans that are acknowledged to be closely tied to cause acts, such loan transactions should be called financial transactions but, due to their close connection to cause acts, will also be defended in their cause relation by civil provision of the Installment Sales Act.

3) Transaction without Cause

When there is a cause transaction and a bill of exchange, a check or a promissory note is written for the sending or collection of that charge, such an act is legally composed as without cause to a cause relation. Although executing an exchange transaction for the sending or collection of the charge of a cause transaction is a type of financial transaction, this financial transaction is composed as without cause to a cause relation and will not be defended in its cause relation.

---

[55] Required Facts
As legal rights and legal effects are notional concepts, it has the structure of [*P* (*f*) ⇒*Q* (*e*)]where some legal facts are acknowledged and, as a result, the generation of certain legal effects is acknowledged. The required facts are [*P* (*f*)] and the legal effects are [*Q* (*e*)]. The required facts [(*f*)] for the arising of rights is called the cause of action (fact) and the required facts [(*f*)] that bring about legal effects that disrupt, eliminate or inhibit the legal effects of the arising of these rights is called the defense (fact). The required facts that disrupt, eliminate or inhibit the arising of legal effects of the defense are called the re-defense. This continues as re-re-defense and re-re-re-defense. As such it is acknowledged that the actual causal relations may stamped out over and over in terms of the law. Note that there are separate time factors in these required facts.

(2) Legal Structure and Strata seen in Exchange Transactions

Exchange transactions (within Japan) that may be use cases for FinTech have the following legal structure and strata.

1) First plane: Cause transactions

2) Second plane: Exchange transactions of the sender, remitting bank, receiving bank and receiver (for remittance exchanges)

In this plane there are three legal relations: that between the sender and remitting bank, between the remitting bank and receiving bank and between the receiving bank and receiver[56].

3) Third plane: Fund clearing transactions between the remitting bank, fund clearer and receiving bank (the Zengin System conducts multilateral netting and the remitting bank and receiving bank then have the claim or obligation for balance of clearing to the fund settler (Japanese Banks' Payment Clearing Network (Zengin Net)))

4) Fourth plane: Fund settlements between the remitting bank, the central bank, fund settler and receiving bank (the balance of clearing (claim or obligation) of the remitting bank and receiving bank to the fund settler (Zengin Net) is notified by Zengin Net to the central bank (Bank of Japan) and the settlement is made with the third party's Bank of Japan account deposit)

In each plain of these legal relations, the former party is the cause for the later party. In principle there is no relation between the first plane and second plane. While a cause relation between the second plane and third plane is thought to exist before the effects of netting come into effect, the relation is eliminated as soon as the netting comes into effect (see Article 3 of the Act on Collective Clearing of Specified Financial Transaction Conducted by Financial Institutions (the Collective Clearing Act); with this provision the effect of netting is also held from the bankruptcy law which is a mandatory provision and there is no denial by the bankruptcy custodian). There is the provision of nonpayment of balance of clearing from Article 55 of Zengin Net's statement of operation procedures and in light of this it is thought that there is no cause relation between the third plane and fourth plane.

(3) Problems in the Conception of Finality

Finality is debated with regard to exchange settlement. Finality may also refer in a broader sense to, (1) finality between parties, (2) finality with a third party, (3) fund settlement finality or (4) irrevocability of a payment order[57].

This problem is thought to be related to the structure of exchange transaction in (1) and (2) above and their cause or lack thereof. It is also thought to refer to when the claim, obligation and loan relation between some of the parties is eliminated and that this does not stamp out the legal

[56] There is no legal relation in exchange transaction between the receiving banks and receiver and it has been interpreted (judicial precedents) that the receiver has no right of claim to the receiving bank. However, normally there is a legal relation in deposit transaction such as for the receiving of funds and for this the receiver has a right of claim for repayment of the deposit that has been inputted into the deposit account.

[57] Takuya Shima "The Legal Concept 'Settlement Finality' in Funds Transfers System" (http://www.fsa.go.jp/frtc/nenpou/2006a/11.pdf), JFSA Institute.
English version (http://www.fsa.go.jp/frtc/nenpou/2006a/11e.pdf)

relations in the legal planes. Therefore, if an exchange transaction is completed in the second plane, because the legal relation between the legal planes is without cause even if there is fault in legal action to the cause relation in the first plane and problems such as nullification, cancellation arise, the legal relation in the plane in the second exchange transaction is eliminated even if there has been legal relation procedures in the plane of the first cause relationship and so there will be no impact.

On the other hand, if there is cause in the legal relation between each legal plane, as previously mentioned (page 45 note 55 “Required Facts”), it is not known when and for what reason the legal effect in cause relation will be stamped out legally and until a sentence on the legal relation is given the legal relation with cause will not be confirmed.

Therefore, when considering the legal aspects of finality, in view of the above required facts as well, there is a need to debate after specifying the parties, legal planes and time elements. Then if the contract relation and legal relation are composed as without cause, that relation in that legal plane can be considered to have finality. Therefore, it is also impacted by the composition of the settlement system or contract. The reason that there is much interest internationally[58] and domestically with regard to finality pertains to the relationship between financial institutions and fund settlers as well as the central bank in the third and fourth planes mentioned above, from the standpoint of avoiding systemic risk[59].

As such, finality is determined based on how a settlement system’s contract is composed in each legal plane and, apart from contracts, legal relations such as the bankruptcy law and real rights laws.

3. Considerations in Legal Points at Issue by Use Case

3.1 Cryptocurrencies

(1) Cryptocurrencies and their Characteristics in Private Law

Japanese private laws such as the civil code only stipulate the concepts of “things,” “persons,” “moneys,” “real rights” and “claims.” They also stipulate the concepts of “quasi-real rights” which is the right of control over “persons” and “rights” such as pledge of claims and intellectual property rights. However, due to real rights provisions, real rights and quasi-real rights cannot become legal rights without legal provisions. Cryptocurrencies are also analogous to quasi-real rights in terms of structure since the function of effective control over “persons” and “property value” is acknowledged. However, cryptocurrencies cannot be said to be “quasi-real rights” as their property value cannot be said to be a “right.” However, since cryptocurrencies have the same structure as quasi-real rights, real rights laws themselves cannot be applied but criterion similar to real rights laws can be applied depending on general legal principles[60].

---

[58] Internationally there are the financial market infrastructure (FMI) principles (eighth principle) of the Bank of International Settlements (Committee on Payments and Market Infrastructures).

[59] In Japan, finality as the legal relation between Zengin Net, the fund settler, and the participating financial institutions is determined and secured by the contract relation based on Zengin Net’s statement of operational procedure and the Collective Clearing Act.

[60] See Professor Tetsuro Morishita “Introductory Considerations on Financial Law in the Age of FinTech: The Way of

Contract law principles are not applied to cryptocurrencies themselves as long as there is no indication of intention in some party's contract. However, legal claim relations for (1) office management, (2) profiteering or (3) unlawful acts as mentioned before may arise regarding cryptocurrencies and application of general legal principles is possible.

If there is a cause relation transaction and cryptocurrencies are to be used for its settlement, it is a separate matter if there is application of contract law principles regarding the consensus for the cause relation transaction and, if a transaction is to be made with a cryptocurrency, it is only natural contract law principles are applied to that point.

However, regarding legal relations of the cryptocurrencies themselves, as long as business customs based on international consensus is formed or legislation is promoted, the private law relations are thought to have to depend on the above general legal principles. With regard to how general legal principles will be applied to the various situations concerning cryptocurrencies, this is thought to be a future challenge that needs to be clarified going forward.

(2) Cryptocurrencies and Blockchains

While very many types of cryptocurrencies have appeared, Bitcoin has circulated most widely and, since blockchain technology is brought about by Bitcoin, we will here consider Bitcoins from among all cryptocurrencies.

Bitcoin blockchains operate on a public platform in which there is no manager and so records cannot be corrected. The function is such that if a Bitcoin record is made in a blockchain, the owner is able to effectively control and own the Bitcoin as a cryptocurrency with property value. Since this is only an essential function and not a legal effect stipulated by law, if this point is emphasized it could be the third type in the previous classification, a type that does not link to any legal effect.

On the other hand, since it is thought to meet the cryptocurrency requirement of laws concerning fund settlements in which property value is effectively held, legal protection at least in laws concerning unlawful acts is apprehended. At this level, there would be a legal effect and so it could be classified as the first type or second type as previously classification.

Here, though the property value will be acknowledged, it will have the feature of cryptocurrencies that are not classified as object, money, real rights, claims or quasi-real rights under private law.

(3) Finality of Cryptocurrencies

Regarding the finality of transfer of cryptocurrencies, as long as there is the possibility of forks arising in a blockchain, it must be said that there is no finality with a third party which cannot be stamped out in that plane or finality of cryptocurrency transfer which is similar to fund settlement finality[61].

However, when using cryptocurrencies for the settlement of transaction charges, finality between parties after some fact or point in time is acknowledged in the parties' contract and,

Corporate Law" (in celebration of the 70th birthday of Professor Kenjiro Egashira) from page 771 (especially page 807).

[61] In the case of Bitcoin's blockchains, since the possibility of forks arising is extremely low from a mathematical standpoint after six blocks have been formed, finality is then generally considered to have been established in effect. However, the possibility of being stamped out still remains.

regarding the inconvenience when such is stamped out, it is considered a possibility that it will be dealt with in the legal plane of cause relation.

3.2 Electronically Recorded Monetary Claims

Here we consider the use of blockchain technology by densai.net Co., Ltd. (Densai Net), the electronic monetary claim recording institution established by the Japanese Bankers Association, for its operations.

(1) Blockchain Type and Legal Relations

When using blockchains for Densai Net, a consortium platform is assumed in that it is assumed that there will be multiple financial institutions that comprise the nodes participating for verification. However, Densai Net is the designated electronic monetary claim recording institution in the Electronically Recorded Monetary Claims Act and as long as that positioning is unchanged the company will legally have rights as a manager as in a private platform since it will bear various legal obligations. From this standpoint, Densai Net has the privilege as the designated electronic monetary claim recording institution and although the blockchain platform is a consortium type, it is thought that it will share similarities with private platforms.

Since the operations of electronic monetary claim recording institutions themselves are legally stipulated and it is stipulated that records of electronically recorded monetary claims should be corrected, the records of blockchains must also be correctable. However, there are no specific stipulations on the method of correcting records and so it will depend on the operational rules of the designated electronic monetary claim recording institution (Article 59 of the Electronically Recorded Monetary Claims Act and Article 25-1 of the enforcement regulations of said act).

Therefore it is believed that the law will not have to be revised if a provision for the method of correction regarding the use of blockchains is added to the operational rules. However, there must be consistency between the method of correcting the records of blockchains and the method of correction required by the Electronically Recorded Monetary Claims Act.

The electronic records of electronically recorded monetary claims will give rise to rights or legal effects for transactions for transfer of rights due to sale, except when legally stipulated. It can be conceived that the multiple electronic records of each node of the blockchain itself will be the electronic record as in the Electronically Recorded Monetary Claims Act and this may in fact be realistic if the records synchronized with specific electronic records of the designated electronic monetary claim recording institution is said to be the electronic record as in the Electronically Recorded Monetary Claims Act.

(2) Financial Institutions' Duty of Confidentiality to Participating Nodes

Since the various types of data on electronically recorded monetary claims held by the Densai Net system is highly confidential information, with what scope the participating financial institutions will hold the blockchain's information as nodes will be an issue in systems design.

Also, participating financial institutions will bear the obligation of confidentiality regarding the

information. For the obligation of confidentiality for the information of corporate clients, it is thought that the Japanese Bankers Association's Investigative Report regarding Disclosure of Information in Loan Markets (April 2004) [62] will be of reference.

Furthermore, when including private information of the creditor, debtor in electronic records and when making a request to a party for the generation of an electronically recorded monetary claim, it is thought that there will be the operation of attaching consent of the party or related party as an individual regarding the provision of private information to third parties (Article 23 of the Act on the Protection of Personal Information).

(3) Responsibility of Electronic Monetary Claim Recording Institution

The responsibility of the electronic monetary claim recording institution as in the Electronically Recorded Monetary Claims Act is thought to be borne by Densai Net, the designated electronic monetary claim recording institution, if a mixed consortium-private blockchain platform is to be used for Densai Net.

If stipulated in Densai Net's operational rules, financial institutions that will be the nodes and board members participating in the consortium will bear the responsibility of contracts based on the stipulations. Moreover, it is thought that practically there should be stipulations regarding these responsibilities and their assignment thereof.

(4) Compulsory Execution for Electronically Recorded Monetary Claims

The Electronically Recorded Monetary Claims Act stipulates the compulsory execution for electronically recorded monetary claims (Article 49 Paragraph 3 of the act as well as Article 150-9 of the civil execution rules) and so consistency with this must be promoted.

Regarding this point, when considering a node as the original of the electronic record to be of the designated electronic monetary claim recording institution synchronized with the blockchain, it is thought that Densai Net will be the party in the Civil Execution Act and that no special legal treatment is required.

[62] http://www.zenginkyo.or.jp/fileadmin/res/news/news160490-1.pdf