JAPAN EXCHANGE GROUP

JPX WORKING PAPER

Applicability of Distributed Ledger Technology to Capital Market Infrastructure

Atsushi Santo†, Ikuo Minowa‡, Go Hosaka†, Satoshi Hayakawa§, Masafumi Kondo†,
Shingo Ichiki†, Yuki Kaneko¶

August 30, 2016

Vol. 15

† Fintech Laboratory, New Business Development, Corporate Strategy, Japan Exchange Group , Inc.
(jpx-fintech@jpx.co.jp)
‡ IT Development, Tokyo Stock Exchange, Inc.
§ IT Development, Osaka Exchange, Inc.
¶ Clearing & Settlement Development, Japan Exchange Group , Inc.

This material was compiled based on the results of research and studies by directors, officers, and/or employees of Japan Exchange Group, Inc., its subsidiaries, and affiliates (hereafter collectively the "JPX group") with the intention of seeking comments from a wide range of persons from academia, research institutions, and market users. The views and opinions in this material are the writer's own and do not constitute the official view of the JPX group. This material was prepared solely for the purpose of providing information, and was not intended to solicit investment or recommend specific issues or securities companies. The JPX group shall not be responsible or liable for any damages or losses arising from use of this material.

Acknowledgement

We would like to take this opportunity to express our deep appreciation to our PoC test partners, IBM Japan, Ltd., Nomura Research Institute, Ltd., and CurrencyPort Limited, and test participants from the Japanese financial industry*, as well as other external experts for their inputs and invaluable opinions in preparing this paper.

* Japan Securities Depository Center, Inc., Mizuho Securities Co., Ltd., Monex, Inc., Nomura Securities Co., Ltd., SBI Securities Co., Ltd., The Bank of Tokyo-Mitsubishi UFJ, Ltd. (in alphabetical order)

Contents

I. Introduction

Virtual currencies such as Bitcoin have become a popular topic of conversation all over the world. People were initially interested in virtual currency itself, but its underlying technology, blockchain or distributed ledger technology (DLT), has attracted a lot of attention recently from various industries exploring applications other than virtual currency. There is no reason to limit the application of DLT to virtual currency, and the existing centralized consensus process can be replaced by DLT in theory. Due to DLT's innovative concept and wide range of applications, it is said that it will bring a 'paradigm shift to the fifth generation' of IT evolution.

One of the areas attracting people's attention is the application of DLT to capital market infrastructure. DLT technical features are considered to be appropriate for the layers of capital market operations especially those for the post-trade process. Some people have pointed out that DLT may replace existing infrastructure for reasons beyond simple efficiency. Global exchanges, CCPs, CSDs, banks, brokers, and market facility providers have proactively explored DLT applications through PoC (proof of concept), and investment in technology providers or participating consortiums.

Cost reduction is one of the potential advantages of utilizing DLT for capital market infrastructure. According to M Mainelli et al. [2016][1], the total cost of clearing and settlement processes all over the world has reached 40 billion dollars annually, and most of the cost comes from data reconciliation and manual operations. This cost could be decreased by utilizing DLT in the post-trade process. The Australian Stock Exchange (ASX) has invested 8.5% in Digital Asset Holdings and announced that DLT application is one of the options for replacing its post-trade service infrastructure.

M Mainelli et al. [2016] also pointed out that eliminating existing infrastructure operators is not realistic even if the technical issues were resolved since they also play the role of law enforcement and dispute resolution. The transition cost of replacing the whole infrastructure is another issue. SWIFT [2016][2] acknowledged the technological advancements in DLT but concluded that further research and development is needed to apply DLT on full scale to capital market infrastructure.

The Japan Exchange Group, Inc. (JPX) established an internal research group late last year and has studied the applicability of DLT to capital market infrastructure. Through two PoCs[3] with six other domestic financial institutions, during April to June 2016, we have tested whether a streamlined process on securities market, security issuance, trading, settlement, clearing, and ownership registry, could be realized in a DLT environment. Through our research and PoCs, we have concluded that DLT has the potential to transform capital market structure by encouraging

---

[1] http://www.swiftinstitute.org/wp-content/uploads/2016/05/The-Impact-and-Potential-of-Blockchain-on-the-Securities-Transaction-Lifecycle_Mainelli-and-Milne-FINAL.pdf

[2] https://www.swift.com/insights/press-releases/swift-and-accenture-outline-path-to-distributed-ledger-technology-adoption-within-financial-services

[3] One is with IBM Japan using Hyperledger and the other is with Nomura Research Institute and CurrencyPort using consortium/private DLT based on Ethereum.

new business development, improving operation efficiency, and contributing to cost reduction.

We have written this report to contribute to further technological advancements and the ongoing global efforts for DLT application to capital market infrastructure by describing our findings, issues to be resolved, and the future innovations that we expect.

Proposals for new DLT platforms continue to emerge alongside the increasing amount of R&D worldwide. Our evaluation of DLT is based on the information at the time of publication, and it might be changed due to future technological advancements or our lack of understanding.

JPX has operated in capital markets for about 140 years since the Tokyo Stock Exchange and Osaka Exchange started their operations in 1878. Japanese capital market infrastructure has evolved several times to be more effective by using IT, including full computerization in 1999 and dematerialization of securities in 2009. We would like to continue contributing to the design of the future capital markets by leveraging our experience and expertise.

II. Outline of Blockchain/DLT

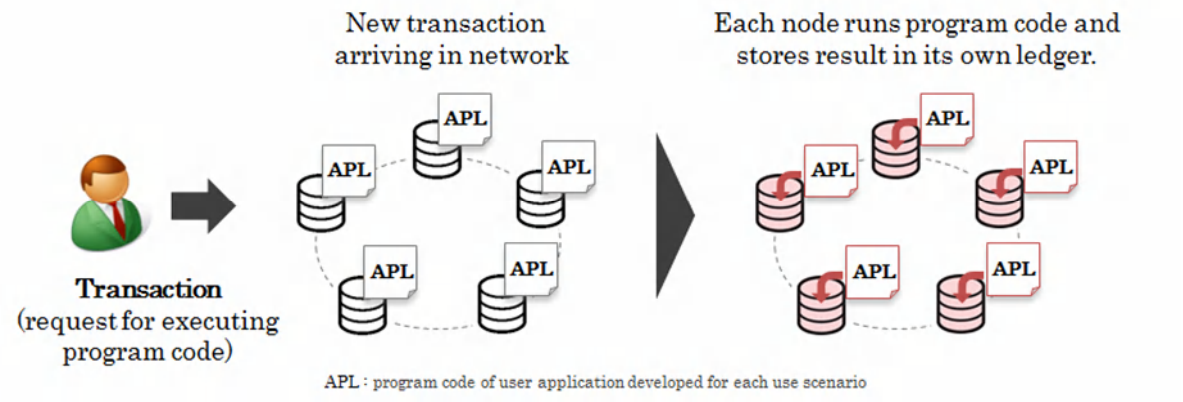
DLT enables network participants to validate the transfer of rights between each other and share those records in an immutable manner by utilizing cryptographic technology. This technology originated from the paper 'Bitcoin: A Peer-to-Peer Electronic Cash System'[4] published under the pseudonym Satoshi Nakamoto in November 2008.

Fiat currencies are controlled by central entities (governments or central banks), and the trust in the central entities is the basis of currency issuance and circulation (centralized system). However, virtual currencies do not necessarily have such involvement by controller, and mutual trust is the basis of the system (decentralized consensus system).

DLT consists of five technological features: (1) database to record ledger, (2) cryptographic hash function[5] to digest data, (3) public key cryptography[6], (4) P2P[7] network, and (5) consensus algorithm[8]. Various DLTs have been developed by combining these features, and various use cases for DLTs other than virtual currency have been proposed.

For some use cases, executing complicated business processes or trading conditions is necessary. Currently some DLTs can use a Turing-complete programming language executable on each node. A 'smart contract' function enables users to create business applications that can be deployed and executed on distributed nodes[9] (Figure 1).

Figure 1: Overview of smart contract



While the network of Bitcoin blockchain is open to the public, use cases of B2B business often require limited network access. Depending upon the policy of network accessibility, DLTs can be categorized as 'public' and 'consortium/private' (Table 1). Public DLTs cannot prevent malicious participants gaining access in advance, whereas consortium/private DLTs can allocate nodes

[4] https://bitcoin.org/bitcoin.pdf

[5] Function that produces fixed-length output from variable length input.

[6] Cryptographic system that uses pairs of keys: public keys that may be disseminated widely paired with private keys which are known only to the owner.

[7] Communication architecture in which interconnected nodes transmit and receive data among each other. Nodes are equally privileged, equipotent participants in the architecture.

[8] Series of procedures that allow network participants to reach consensus about transactions on validation and adoption to ledger as block.

[9] Leading example is Ethereum which provides proprietary programming language named Solidity.

only to trusted parties or a single entity. Due to the difference in accessibility policies, appropriate consensus algorithms vary.

Since anyone can create new blocks in public DLTs, workloads like proof of work (PoW) are often built into the consensus algorithm to avoid malicious participants overwriting past data. In general, the effort of doing some work is rewarded by issuing virtual currency to the block creator.

Table 1: Comparison between public DLT and consortium/private DLT

	Public	Consortium/Private	
Network Participation	Open	Permission is required	
Features	No central entities	[Consortium] Used among permissioned entities	[Private] Used within a specific entity

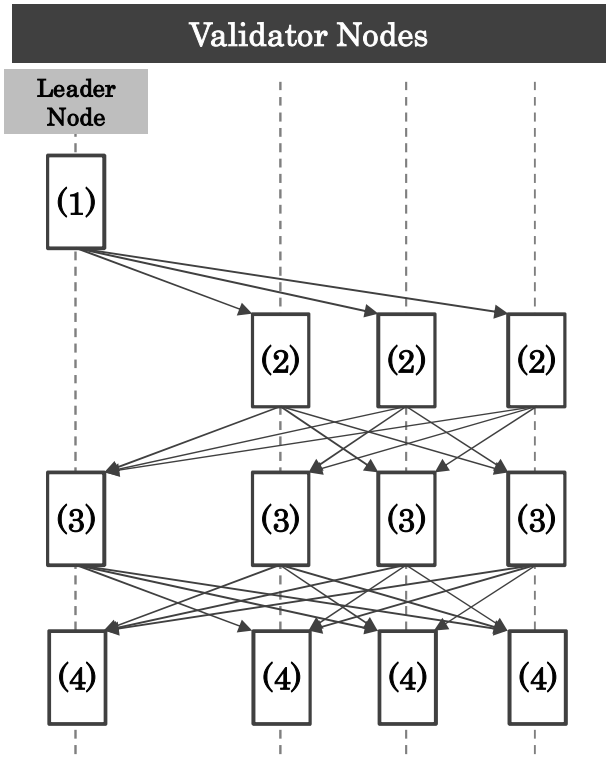
On the other hand, consortium/private DLTs can limit block creation to designated participants. It is also possible to restrict possession of multiple nodes to a single person or entity. These access control considerations enables use of a faster consensus algorithm where a leader node designated by a simple rule generates a new block[10], and then the block is validated by a predefined ratio of nodes.

Now many consortium DLTs use a consensus algorithm based on practical byzantine fault tolerance (PBFT) proposed by M Castro et al. [1999][11]. In the original PBFT algorithm, consensus is reached with the approval of roughly 2/3 of nodes, which ensures robust consensus as well as fault-tolerance capability to endure up to (n-1)/3 node failures when there are n nodes (Figure 2). Since computationally intensive calculation is not necessary, consensus can be achieved faster than with PoW.

[10] The rule differs depending on the type of DLTs such as changing in round-robin or fixing until failure on leader node.

[11] http://pmg.csail.mit.edu/papers/osdi99.pdf

Figure 2: Flow of consensus algorithm based on PBFT



n : total number of validator nodes
f : (n-1)/3, maximum number of validator nodes that may be faulty

(1) Generate new block and broadcast it to other validator nodes

(2) Validate block and broadcast result (confirm or not) to other validator nodes

(3) Wait for message from 2f nodes with same result and broadcast result to other validator nodes

(4) Add block to own ledger when 2f+1 nodes (possibly including its own) have received confirmation from 2f nodes

III. Proof of Concept

DLT usage in capital market infrastructure has yet to be properly tested. We have conducted a PoC to gain further insight beyond current research or studies from publicly available information.

1. Adopted DLT Platform

Virtual currencies and securities have different product specifications and trading/settlement procedures, so the functional requirements of DLTs are accordingly different.

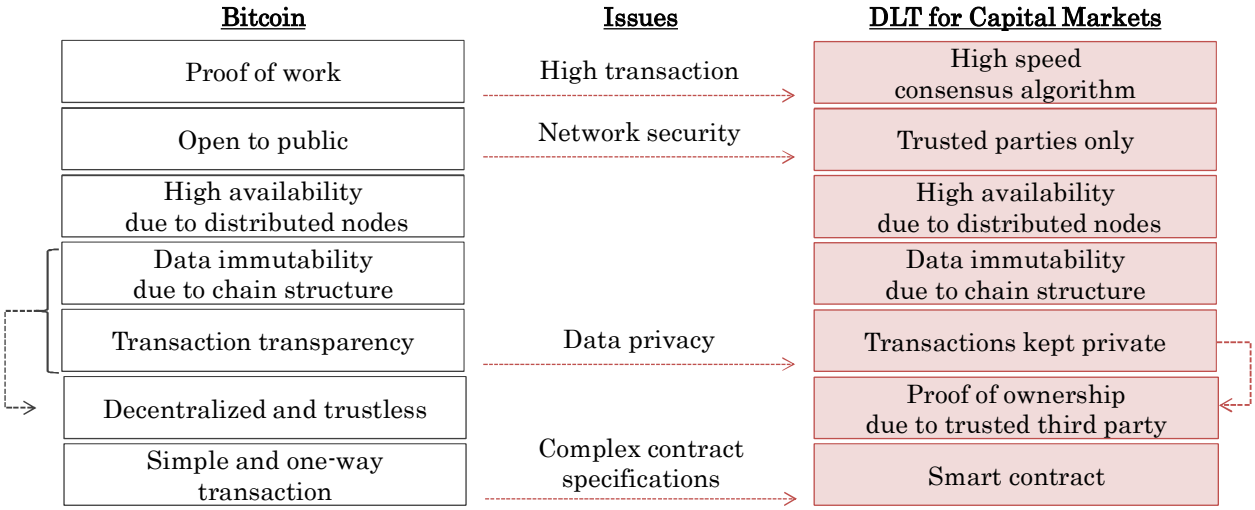
The throughput capability of a virtual currency[12] is insufficient to process current daily securities settlement volumes. We think that the improvement in throughput with PoW is limited in the long term, so we adopted faster PBFT-based consensus algorithm. Protection against node occupation or attack from outside is secured by adopting a permissioned network where only trusted entities are allowed to participate.

Although the anonymity of participants is secured, it is unlikely that infrastructure users would accept sharing material information, such as a large transaction or bilateral OTC trading conditions including prices, in real time. Therefore, it is desirable to incorporate multi-layer data privacy control so that a normal user can see only his/her transactions while administrators can see all transactions and certify the user's transactions/ownership.

Furthermore, financial products have more complex specifications than virtual currencies, and their business processes include relatively complex agreements or confirmation steps, so utilizing smart contracts is necessary.

Having considered these factors, we decided to adopt a consortium DLTs for our PoCs.

Figure 3: Framework of DLT for capital markets



[12] The throughput on Bitcoin blockchain is about seven transactions per second at the time of this writing.

2. Outline of PoCs

We have implemented two PoCs that covers issuance, trading, settlement, registry, and corporate actions. There were slight differences in the coverage or implementation method among the two PoCs, but for simplicity we will summarize our PoC coverage as below.

The PoC environment was built on a public cloud service where the number of nodes was close to the minimum required for the consensus process. We gave node access permission to the exchange/CCP/CSD as an administrator/validator. Their member financial institutions were designated as validators, and listed companies were designated as non-validators and given read-only access. While the security settlement was regarded as finalized by validating it and recording it on DLT, cash payment was recorded on DLT as a token transfer, assuming that the necessary messages will be passed to the off-DLT payment system. Unlike the existing system that records only the financial intermediaries' name, investors' account information was recorded along with settlement information directly in our system, which enables individual investors' ownership information to be updated in real time. KYC (know your customer) and AML (anti-money laundering) were assumed to be conducted by financial institutions outside of DLT.

(a) Securities Issuance

- An administrator registers issuer (listed company) information and records new securities issuance to the issuer's account on DLT upon request outside of DLT.
- The new issuance is first allocated to financial institutions (as underwriters) that then sell them to investors. All rights transfers are recorded on DLT.

(b) Corporate Actions (Dividend and Stock Split)

- An administrator invokes the corporate action process on the DLT upon request from the issuer outside of DLT.
- The amount of money tokens as dividend or security as a result of a stock split is calculated based on the ownership registry at the specified date and time, and then the DLT record is updated.

(c) Ownership Registry

- Shareholder registries (the name and the number of shares) are updated in real time.
- An administrator can see all shareholder registries, and each issuer can see only its own shareholder registry.

(d) Trading (Reconciliation)

- Orders are recorded on DLT. If an incoming order takes any of the tradable orders recorded on DLT, the pair of orders is recorded as a transaction (order matching on bulletin board).
- A bilateral transaction as a result of negotiation outside of DLT is recorded on DLT by one

party, and the other party confirms it (bilateral reconciliation).

(e) Securities Settlement (Clearing)

- Security transfer is regarded as finalized once validated on DLT.
- It is possible to control settlement status by requesting sign-off from the administrator for the DVP (delivery versus payment) process or net out multiple transactions for the net settlement system.

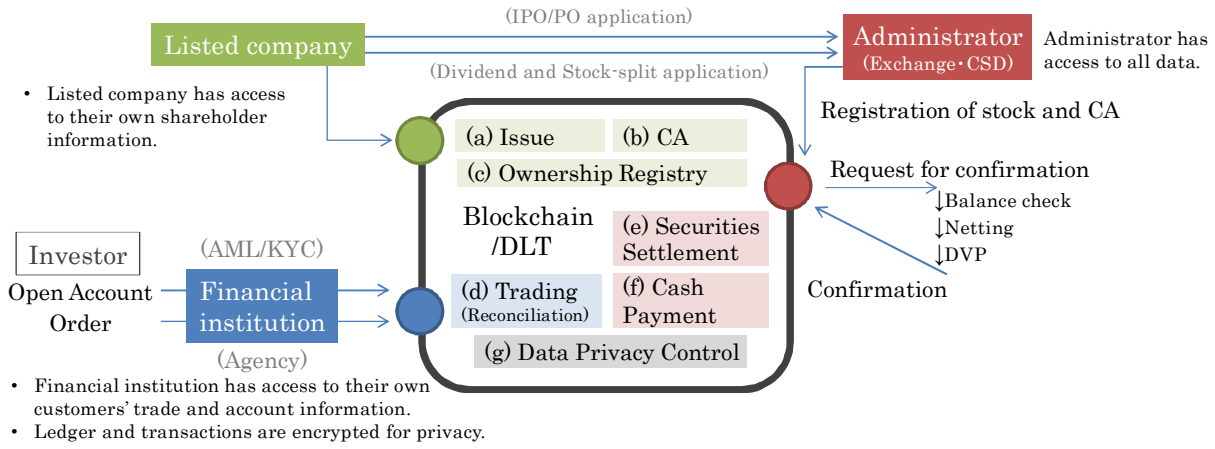
(f) Cash Payment

- Payment is recorded as a token transfer in DLT, and those records are considered to be passed to the existing payment system outside of DLT.
- It is possible to control the settlement status by requesting sign-off from the administrator for the DVP process or net out multiple transactions for the net settlement system.

(g) Data Privacy Control

- A financial institution cannot access other institutions' client information or unrelated transaction records.
- An issuer (a listed company) has read-only access privilege to its shareholder registry and can see the name and the number of shares in real time. The issuer is not allowed to access other issuers' registry or transaction information.
- An administrator has access privilege to all information on DLT.

Figure 4: Overview of PoC environment



IV. Evaluation of DLT

1. Evaluation of DLT as Fundamental Technology

In this section, we will evaluate DLT as a technology for capital market infrastructures based on our findings gained through our research and PoCs from the following six aspects: (1) applicability to each layer of capital market, (2) throughput, (3) consensus process, (4) data privacy, (5) availability, and (6) cost.

(1) Applicability to Each Layer of Capital Market

Since securities have more complex contract specifications and work flow than virtual currency, it is necessary to utilize a smart contract. Both DLTs that were tested in the PoCs implemented smart contract function in environments that were constructed with Turing-complete language, thereby, allowing it to provide the fundamental functions of the capital market mentioned in the previous chapter[13]. However, the extent of applicability was different for each business and functional layer.

(a) Trading (Reconciliation)

The distinctive aspect of the trading process in the securities market mostly lies in how to design an effective pre-trade order matching process. In order to raise the probability of order matching and getting a competitive price, market operators try to collect as many orders as possible. The underlying concept of order aggregation does not really fit with DLT's decentralized processing architecture, and it is hard to bring improvement if there is already an effective centralized order processing facility.

The trading practice of frequently canceling/revising orders in the market also makes it difficult to apply DLT to the trading process due to the immutability of the DLT ledger. Considering these issues, we think it is better to conduct the pre-trade process out of DLT.

For OTC bilateral trading, however, such intense price competition is not required, and the cancel/revise rate is relatively low, so DLT is applicable. The reconciliation process among related parties could be a promising use case.

(b) Clearing and Settlement

Unlike the trading process, there is no necessity to aggregate orders, so the decentralized process of DLT will bring some benefits such as high availability. This layer is considered to be the most important use case, and we will examine it in more detail in the next section.

[13] While smart contract can realize a wide variety of functions with Turing-complete programming language, error handling functions such as time-out should be implemented appropriately in preparation for unexpected software bug such as infinite loop.

(c) Securities Ownership Registry

While Bitcoin blockchain records only transaction flow, DLTs tested in the PoC recorded state information as well. Although the implementation method is slightly different among DLTs, these flow and state data are efficiently stored by tree structure and its snapshot at specified date and time can be easily referable (Figure 5). This feature allows for retroactive traceability of securities ownership and ownership levels without any special need to record snapshot data at such point in time.

(d) Corporate Actions

Thanks to the feature mentioned in (c), a list of shareowners at a specified date can be retrieved retroactively, and it is possible to invoke corporate actions such as dividend payment or stock split by using the list. DLT would make the corporate action processes simpler and could reduce operation cost.

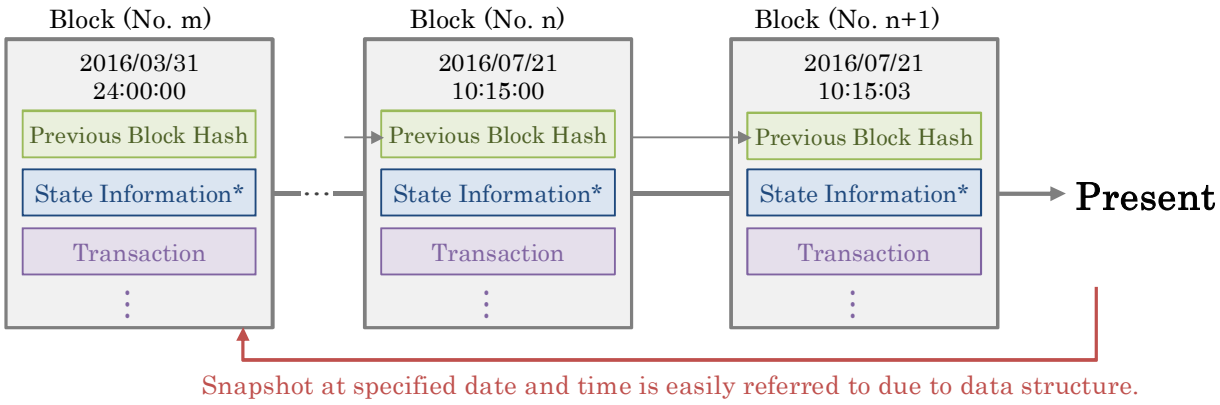
Considering the above features, applying DLT to the post-trade process could make the existing work flow much more efficient in the future.

However, we have also identified several concerns that might prevent DLT deployment. There is a business requirement of time-trigger events such as a periodic interest rate payment or maturity of a derivatives contract. Each node should invoke a transaction at the specified time, but the lack of clock synchronization among the nodes might prevent invoking the transactions at the same time. The process of listening to outside feed, such as a floating interest rate or underlying price for exercising an option, is often necessary. If all nodes independently listen to the outside feed, they might get slightly different values due to a timing difference. Random number generation in a complex valuation might return a different result if each node runs an application independently[14].

Assigning these roles to a single node could be a solution, but this will also bring the concern that the node would be a single point of failure.

[14] Because the result of transaction is compared in digest value calculated by hash function among validator nodes, the data on ledger that each validator node own have to be completely consistent in byte-sequence level.

Figure 5: Reference of state information at time of generation of past blocks



* Generally, only hash value of root node in tree data structure is stored in block.

(2) Throughput

Transaction throughput is one of the major issues when considering the application of the DLT usage in capital market infrastructure. Although the throughput requirement varies depending on each product's average transaction frequency, it is normally desirable to have a capacity to process a few thousand to tens of thousands TPS for global stock market post-trade infrastructure.

The throughput capacity in DLT, which determines how many transactions can be processed per unit time, is generally affected by how the consensus algorithm works. Taking Bitcoin as an example, the throughput capacity is defined as follows.

Throughput capacity = maximum number of transactions per block*
/ average time to process a block

* maximum block size / average size of transactions

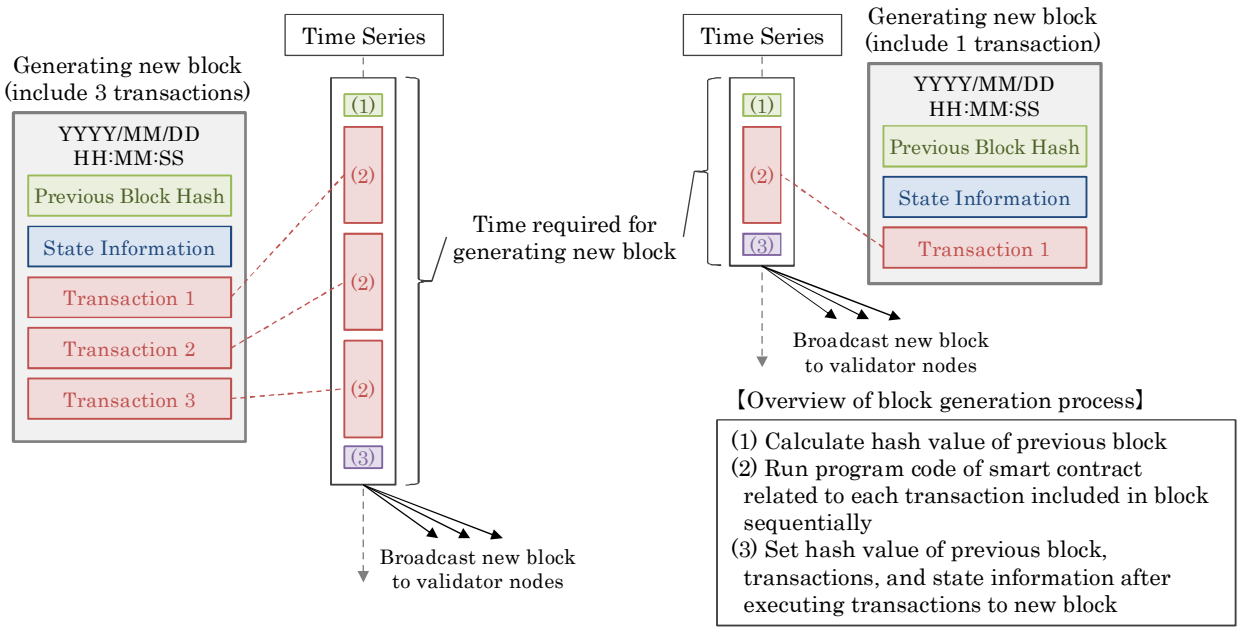
In order to increase throughput capacity, it is necessary to either increase the maximum number of transactions per block or adopt a faster consensus algorithm. The former could be achieved by raising the block size, but this will lead to consuming a larger network bandwidth during the consensus process. The latter also has some concerns. The time to generate a new block mostly consists of the duration of PoW, and setting a shorter duration for this process will weaken security and might cause inflation as a result of the higher pace of the virtual currency supply.

On the other hand, the consortium/private DLTs built on permissioned network do not necessarily need a consensus by PoW and can use a faster consensus algorithm. If the consensus algorithm is fast enough, network latency becomes a non-negligible factor. This indicates that geographical node concentration will improve the throughput, but it will sacrifice the high availability of the infrastructure. The infrastructure operator needs to strike a balance between throughput and availability.

We have implemented a high traffic test by injecting large amounts of transactions, and the test produced a maximum of tens to a hundred transactions per second. We have analyzed the detailed processes in Hyperledger during the high traffic test and found that the CPU resource was not fully used; the bottleneck was the serial execution of the smart contract (Figure 6). While a simpler use case like Bitcoin holds all the information directly in transaction data, a more complex use case using a smart contract will run a program that is instructed by the transaction. In order to improve throughput, it is necessary to run the program efficiently. Although the serial execution of a smart contract was a primary bottleneck in this PoC, other factors including the number of total validator nodes or the geographical distribution of the nodes would affect the throughput in theory. We hope further investigation will see progress in this area.

The trading system for listed stock market, which has to process high message traffic in real time, typically increases the total throughput capacity by allocating tasks to multiple servers to process transactions in parallel. Since each node has a single configuration, applying the technology to high volume listed stock markets is not easy to achieve even if technical improvements are expected. On the other hand, the technology is sufficient even at the current capability of DLT for post-trade process where real-time processing at the millisecond or microsecond level is not necessary. Also, the technology is sufficient for the OTC market where relatively fewer transactions occur.

Figure 6: Performance bottleneck due to sequential execution of smart contract



(3) Consensus Process and Network Access

The appropriate combination of consensus algorithm and network access varies depending upon the use case.

The public DLTs cannot eliminate malicious participants beforehand; thus, robust protection

against data manipulation is required. Selecting PoW or its derivatives as its consensus algorithm is reasonable. The consortium/private DLTs limit its node access only to trusted players or internal operators, which can secure immutability of ledger and enable the adoption of an effective consensus algorithm like PBFT to process higher traffic.

In the existing framework, financial institutions serve as intermediaries for their clients, but it is still effective and practical to fulfill the KYC/AML requirement even if the financial infrastructure is built based on DLT. The consortium/private model is a reasonable option in this context as well.

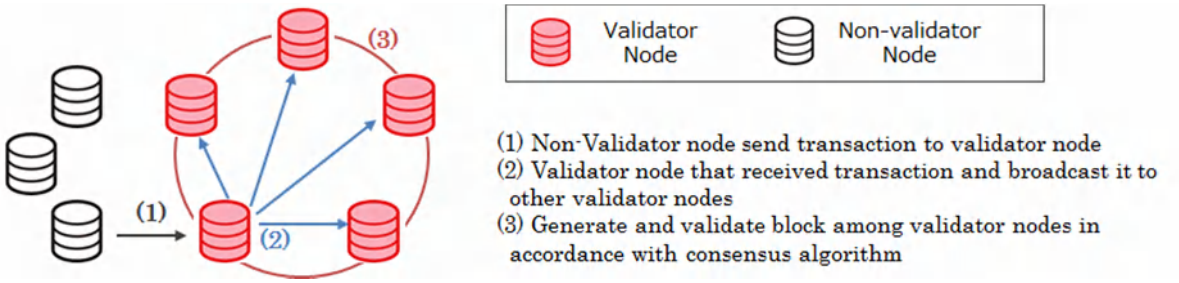
The PBFT-based algorithm, often used by consortium/private DLTs, takes each consensus by validation from roughly two-thirds of the permissioned nodes. This enables to prevent a 'fork' of the chain, which will secure stable and immediate finality. This is also an advantage when considering the application of DLT for a capital market infrastructure.

In the PBFT-based consensus algorithm, 'validator nodes' are responsible for storing ledger and participating in the consensus process, while 'non-validator nodes' can invoke a transaction but are not allowed to participate in the consensus process[16] (Figure 7). For the use case of a capital market infrastructure, we think it is appropriate that nodes are operated by financial institutions and an infrastructure administrator. However, it is not necessary that all financial institutions possess validator nodes. Either possessing a validator node or a non-validator node is the choice of each financial institution.

The number of validator nodes has impact on network bandwidth because message traffic for the consensus process is proportionate to it. The message that the leader node broadcasts, a newly generated block, to other validator nodes at the beginning of the consensus process is relatively large because it includes the content of the transactions. On the other hand, while the messages containing the validation results that each validator node transmits is small because it includes only the digest value of the block, there is high traffic volume due to communications among the validator nodes.

If consensus participation is not rewarded by virtual currency, how to incentivize financial institutions to possess validator nodes would be an issue.

Figure 7: Difference of roles in validator node and non-validator node



[16] Based on the definition in some type of DLTs such as Hyperledger at the time of this writing.

(4) Data Privacy

Bitcoin as the most popular public blockchain records the full history of a transactions with anonymous ID in a publicly available manner. This makes it possible to trace how many bitcoins are possessed by a specific ID. High transparency and an immutable ledger is the foundation of the decentralized nature of bitcoin in proving individual ownership.

In the securities market, however, disclosing a large transactions or large positions might induce front-running activity or the ID associated with each investor might be identified by comparing the records with legal disclosure documents. In the case of OTC bilateral trading, related parties do not disclose the trading parameters (volume and price) to unrelated parties.

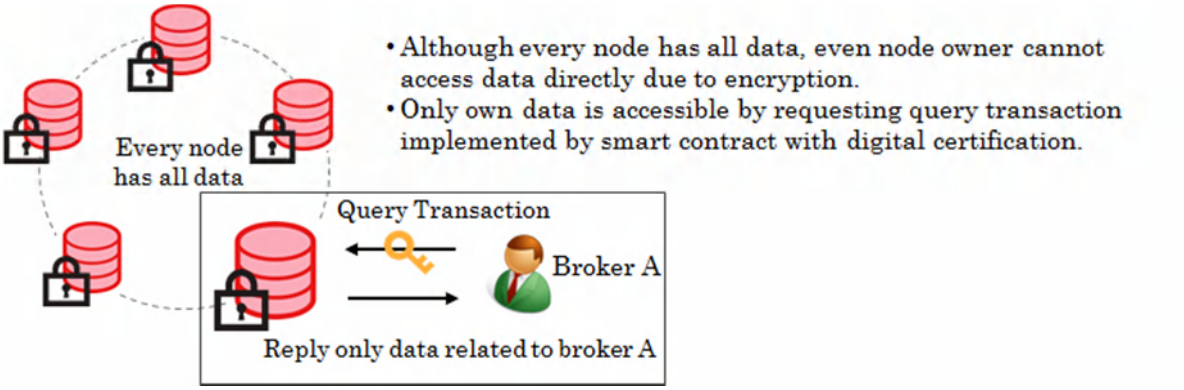
Considering these concerns or business requirements, it is preferable that all stored data is only accessible by related parties. Since this will lose the feature of ownership certification by public trust, nobody can validate his/her claim of securities ownership. Therefore, full data access privilege needs to be given to a trusted third party who is responsible for the ownership certification.

For consortium use of DLT, several financial institutions share nodes containing all transaction data. If they are not confident with the data privacy protection from the other institutions, such node sharing might not be realized.

In our PoC, the infrastructure operators, such as the exchange/CCP/CSD, played the role of certification authority in public key infrastructure and delivered certification to each financial institution. The ledger stored in each node and each transaction were encrypted and deployed with access control. The function to query past data was realized by a smart contract. Since each institution invokes transactions with the necessary certificate attached, it can see only its transaction or its client's identification (Figure 8). Also the transaction is decrypted only on a virtual machine to run the smart contract program, which is separated from the other system areas. Therefore, even the validator node owner cannot see unrelated transactions. Provided that the validator node is properly protected from attack and falsification as an existing financial IT system and decrypting transaction data without a private key is practically impossible[17], all financial institutions can share the same single ledger while hiding each transaction from others. This environment was successfully built with Hyperledger, however, DLT platforms fulfilling this level of data privacy control are considered to be limited at present.

[17] Since one's data is stored in the server owned by competitors though the data is encrypted, reliability of cryptographic technology should be assessed carefully.

Figure 8: Privacy protection achieved by encryption and digital certificates



(5) Availability

Higher availability is one of the major reasons that the exchange/CCP/CSD as a capital market operator is exploring DLT. Of course, existing infrastructure already has achieved high availability by redundant configuration or thorough maintenance of hardware, but maintaining the robust infrastructure is not that easy and needs a proportionate cost.

In the environment based on DLT, partial node failure will not stop the infrastructure operation if a sufficient number of validator nodes continue their operation. If those validator nodes can be distributed to several financial institutions beyond a single capital market operator, availability of the infrastructure will be enhanced compared with the existing server-centric architecture. It is even possible that global financial infrastructure operators could collaborate to develop services on DLT with higher availability through global distribution of validator nodes.

Sharing nodes among different institutions will also provide higher resiliency. Even if a single node loses its data due to system failure, it could be recovered by other nodes since all nodes have the same data, which is synchronized in real time.

Considering these features, the DLT could realize a more efficient industry-wide BCP solution, which currently each institution is responsible for. We would like to reiterate, however, that the consideration of data privacy as discussed in the previous subsection is critical in achieving industry-wide node sharing.

In order to fully realize higher availability with DLT, validator nodes need to be distributed to geographically separate locations in case of a wide-area disaster. We need to be aware, however, that single point of failure would still remain in a few functions, which we discussed in subsection (1) or interface between the surrounding systems. The smart contract as a business application is expected to be developed for each use case, and a complicated process could cause application failure, which would impair the high availability of the DLT.

While an administrator node is not necessary for the original Bitcoin blockchain, the DLT use case for a capital market infrastructure would work better with it. In order to utilize DLT's feature of high availability, however, the roles and responsibility of this node should be minimized. Candidates for the administrator are existing infrastructure operators such as the exchange/CCP/CSD, but not limited to them. Regulators or IT vendors could potentially play the

role of a trusted third party.

(6) Cost

We have compared the typical client-server architecture and DLT from the following four aspects: (a) application development, (b) hardware, (c) software, and (d) maintenance. As shown in the table below, the rough cost estimation indicates that the cost of hardware, software, and maintenance are expected to decrease, but the extent of the cost reduction would be limited in just replacing the IT infrastructure with DLT. The major cost savings in using DLT will come from reduction in the operational cost achieved by changing the existing business processes. It is also expected that industry-wide node sharing could reduce the total BCP cost in the industry.

Table 2: Cost comparison between client-server architecture and DLT

Viewpoint	Cost impact of adopting DLT
a. Application Development	No material change • No reason to decrease development effort just by DLT adoption. • Development cost would be identical assuming the same unit price.
b. Hardware	Likely to reduce • High-end storage server is not necessary due to DLT's multi-node data redundancy.
c. Software	Likely to reduce • Since major DLT is currently open source, middleware and database license fee are not charged.
d. Maintenance	Likely to reduce • Service level in hardware failure recovery must be relaxed due to DLT's high availability.

2. Issues and Assessment of the Securities Clearing and Settlement

In this section, we would like to discuss the applicability of DLT to a securities settlement system focusing on the following three points, (1) settlement finality, (2) DVP settlement, and (3) considerations for a large-scale process.

(1) Settlement Finality

Settlement finality is defined as "settlement that is irrevocable and unconditional" and is an important concept for the stability of the financial infrastructure.

With public DLTs, it is known that there is a risk of chain fork, which could rollback its validation status. Due to this risk, it is hard to clearly define the timing of the transfer of rights in the DLT, which would make settlement finality unstable.

The risk of chain fork could be eliminated by designing the infrastructure with consortium/private network and a PBFT-based consensus algorithm.

(2) DVP Settlement

Modern financial infrastructure facilitates its settlement with DVP where cash payment must be made simultaneously with the delivery of the security. In our PoCs, we have confirmed that DVP settlement in DLT is technically possible by controlling the timing of delivery and payment using a smart contract.

On the other hand, further consideration is needed from a practical perspective. Under the current Japanese settlement system, transferring dematerialized securities among participants' accounts in JASDEC (CSD) is regarded as settlement finality. It would be technically possible to build such a function with DLT, but its legal or regulatory treatment as a single source of truth needs to be clarified. Since fiat currency is not issued as a digital asset yet, achieving payment finality on DLT will needs some special consideration, such as, (1) linkage with existing settlement infrastructure, (2) money tokens, or (3) digital currency.

Plan 1: Linkage with Existing Settlement Infrastructure

Finality of cash payment is currently obtained by transferring Japanese yen as a fiat currency between bank accounts. In order to realize this process on DLT, one solution would be to generate a payment instruction messages from DLT to the existing settlement infrastructures (BOJ-NET). Unlike the following two solutions, security settlement and payment will be processed in different systems. In order to synchronize the timing of finalities, DLT communicates with the existing payment infrastructure. The completion message of the payment process will trigger completion of securities settlement on DLT. Since the payment is still processed in the existing BOJ-NET, the definition of finality does not need to be revised.

Plan 2: Money Tokens

There is an idea to use money tokens for payment on DLT. Financial institutions participating in the settlement can deposit fiat currency in a trust bank, and then the bank issues money tokens in return, which will then be used for settlement on DLT. Strictly speaking, the transfer of money tokens cannot be defined as finality, but it could be regarded as this on the premise that a receiver could seize deposited fiat currency from the trust bank in case of the payer's default. Since complicated communication with external systems is not necessary, higher efficiency on DLT can be expected than plan (1).

If the money tokens are designed to circulate outside of settling financial institutions, many more complex issues will arise such as the token exchange market or default treatment of non-financial institutions.

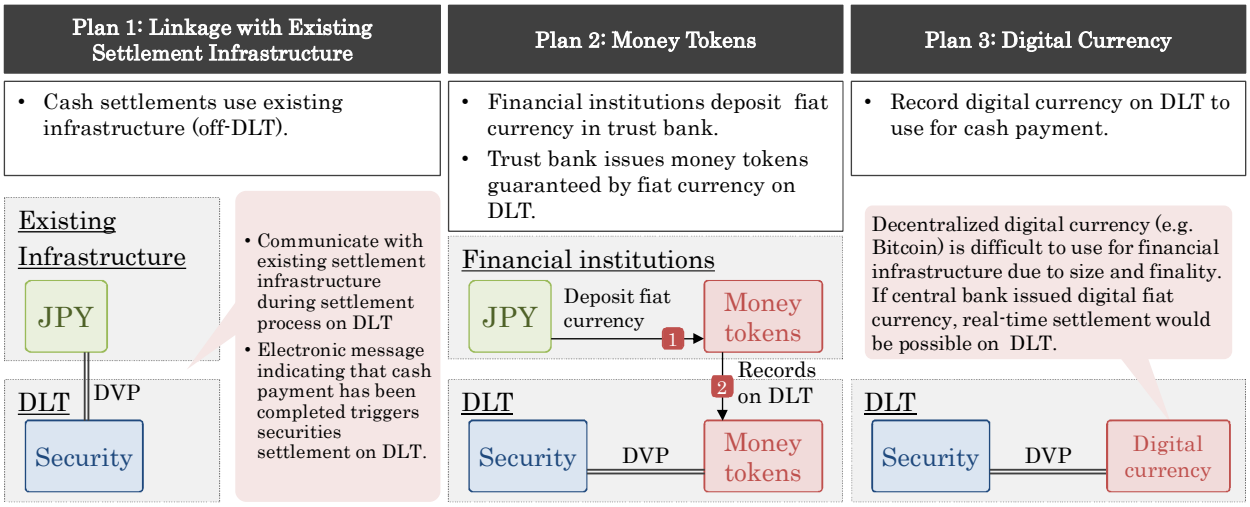
Plan 3: Digital Currency

From a technical point of view, it would be possible to utilize virtual currency for settling

transactions on DLT, but there are two practical issues. First is whether the person who receives the virtual currency on DLT is able to treat it as finality of payment. Whether it is considered as payment finality depends on the acceptability of the virtual currencies for settlement, commercial transactions, and savings, or its convertibility to fiat currency. It is a matter of public trust in virtual currencies, and unfortunately the eco-system for virtual currencies has still not reached a satisfactory level of maturity. The second issue is the size of the global virtual currency market. The value of the Bitcoin market, the world's largest virtual currency, is only about 100 billion USD (as of the end of June 2016), which makes it practically difficult to support the financial infrastructure of even just one developed country[18].

If a central bank were to issue a digital fiat currency utilizing DLT that guaranteed stable finality and sufficient supply, these issues could be fundamentally resolved. While central banks around the world and international communities such as CPMI [2015][19] are actively discussing the idea of a digital fiat currency, currently the consensus is that the number of issues that need to be addressed are far greater than that of the previous two solutions.

Figure 9: Plans to realize DVP settlement on DLT



(3) Considerations when Applied to Large-scale Post Trade Processing

Based on the technical characteristics of the DLT, it is more suitable for use in the post-trade domain in the financial markets. For the use case of small-scale post-trade process, there would not be any serious concerns even with the current state of the DLT technology.

On the other hand, the existing infrastructure has some functions to perform large-scale post-trade processing smoothly, and such functions need to be considered in the longer term, although they have been rarely examined on DLT yet. We would like to share our thoughts about issues or functional requirements for large-scale application.

[18] Yearly trading value of JGB in 2015 is 11.94 trillion JPY (buy and sell total, ref. Japan Securities Dealers Association). Daily trading value in TSE cash market in 2015 is 3.06 trillion JPY (one-way, do not include off-auction trading).
[19] http://www.bis.org/cpmi/publ/d137.htm

Point1. Impact on Liquidity in Secondary Market

It is said that the whole process from trading to settlement in capital markets will become seamless by using DLT like Bitcoin which is processing both trading and settlement in near real time.

If a security settlement is processed in real time on DLT achieving DVP, it is necessary to confirm the existence of sufficient security and cash in each account in real time.

The existing financial markets does not have a seamless process between trading and settlement, and the gap is filled by margin trading, stock lending, or purchasing power based on deposit. These trading practices increase market liquidity, but a move to real time and seamless process in settlement may lose this benefit.

Point2. Netting

In the securities post-trade process, obligations and claims are netted out among multiple-parties, and the difference is processed in the settlement. This reduces the operation cost and brings capital efficiency by decreasing the number of processing messages and the delivery/payment amount.

The real time gross settlement process does not always work well, and consideration to secure effective settlement is necessary for some markets or products by building a netting functionality into DLT.

Point3. Securing Safety Net

Existing large-scale settlement infrastructures in capital markets prepare a safety net by defining a fail procedures[20] or built-in functions to mitigate the risk of gridlock to ensure stable settlement. If trading is to occur without pre-checking availability of securities or funds in the corresponding trading accounts, similar safety nets must be built.

Resolving the settlement failures just by DLT is difficult. As with the existing securities settlement, it could be possible to mitigate the risk of the failures or accelerate their resolution by having a third party like a CCP overseeing the payment of fails charge from sellers to buyers or forcibly purchasing deliverables (buy-in) until the fail situation is resolved. Agreeing on the fails practice among DLT users will be necessary.

There would be two solutions to mitigate risk of gridlock: a) consensus algorithm improvement and b) intra-day liquidity arrangement by a third party.

The existing settlement system already has a built-in safety net to mitigate the risk of grid lock. For instance, BOJ-NET has a centralized queuing[21] and offsetting mechanism[22]. As long as we have confirmed, the majority of DLT consensus algorithms have no specific function to

[20] Market practice that do not regard it as default that securities settlement have not been completed at the settlement day, and it does not terminate the contract immediately in such situation.

[21] When payment cannot be completed due to capital shortage, the payment order will be withheld in queue on BOJ-NET.

[22] Function that searches the combination of payment orders which solves capital shortage among newly registered payment order and payment orders withheld in queue on BOJ-NET.

control transaction sequences in a block. DLT could potentially mitigate the risk of gridlock by a technical approach if the consensus algorithm can incorporate functions to alter its processing order by examining multiple transactions.

The intra-day liquidity arrangement by the central bank is a mechanism to mitigate short term capital requirement arising from the timing gap between payments and receivables. The gridlock issue could be resolved by the third party lending short term liquidity to finalize the settlement, and then the borrower will repay after receiving payment.

V. Conclusion

We have examined the potential and limitation of the DLT application to capital market infrastructure based on findings and analysis gained through JPX's internal research and PoCs. Although we have found some issues that need to be resolved, applying DLT in capital market infrastructure has great potential to contribute to generating new business, enhancing business operations, and reducing cost and even rebuild the financial business models that exist today.

Issues in Short Term

Of several technical issues we have found during conducting PoCs, non-determinism in executing smart contracts and data privacy control are the most important when considering DLT utilization in the financial markets.

Non-deterministic factors such as time-trigger events, listening to outside data feed, or random number generation might prevent consensus because such processes are actually a challenge for smart contracts running each node to reach exactly the same result. This is not negligible since those processes are very common and frequent in capital markets.

Data privacy control would be a more critical factor. Considering existing business practice in capital markets, an infrastructure disclosing all transaction data in a publicly available manner would not be accepted by existing players. Data privacy control is a very important and necessary requirement, but DLTs fulfilling this requirement are currently limited. We hope that this feature will be incorporated by other DLTs in the future.

Issues in Mid to Long Term

We would like to raise the issues in the longer term for the DLT being a core technology of capital market infrastructure.

Firstly, the throughput capacity we have gained through PoCs limits applicable field of businesses and does not reach a level sufficient to handle a high traffic volume market stably. There might be a few DLTs announcing high throughput figures in demonstration, but measurement conditions such as the use case or geographical node distributions are not clear enough. We hope for further technical advancement in DLT while taking the business requirements in this paper into consideration.

Since Bitcoin is categorized as a real time settlement system, netting, queuing, or liquidity offering functions of existing capital market infrastructures have not been sufficiently tested on DLT or shared such findings publicly. What is appropriate for DLT needs to be investigated considering several factors including user convenience and settlement stability on top of DLT technological advantages. Utilizing existing CCPs could be a solution. Furthermore, the DVP process is a necessary requirement for core use, and realizing cash payment finality on DLT will help to process high volume settlement operations safely.

Potential for Capital Market Innovation

Although we have identified several technical issues, DLT is extremely attractive as an

infrastructure technology with high availability, immutability, and high resiliency from system failure at a relatively low cost. On top of these technological features, redesigning the business process by exploring DLT would bring industry-wide efficiencies including financial service innovation or broader cost reduction.

For instance, it would be possible to generate a share ownership registry updating in real time by utilizing the characteristic of DLT of having historical data snapshots. Effective shareholder administration including voting rights or dividend payments would bring benefits for its issuers. Even trading units in the securities market might not be necessary, and trading on a value-basis might be possible. Of course, there still exists some practical and regulatory issues, however, usage of DLT would bring flexibility in financial service design and encourage innovators to bring benefits to market users. The building reconciliation process or data sharing among several entities on DLT would bring automated and effective business operations, which would lead to a big cost reduction. Although data privacy control by encryption technique is necessary, it would be possible to recover data from another financial institution's node in the event of serious node failure or data lost occurred. Building an interdependent BCP structure with DLT would reduce the redundancy cost of the whole financial industry.

DLT is the technology to share infrastructure among its user group. Each node is distributed among users while keeping the same controlling power over the infrastructure operations, which enables building a sharable fundamental layer of the industry. Even if assuming centralized entity, its role is focused more on the safeguard of the infrastructure or coordination of the group, so it is possible to share an infrastructure in a democratic manner.

We assumed the infrastructure sharing only among financial institutions in PoCs, but it could expand the range of efficiency by distributing nodes more widely to issuers or investors. Distributing nodes among global infrastructure operators would lead to a global infrastructure sharing. In line with the global trend of a sharing economy, the DLT is the technology to realize 'sharing infrastructure'.

We conclude the discussion by commenting on our attitude in exploring DLT as a technology user.

Firstly, we have to understand that DLT consists of several inter-related technical features and the best balance of those features will vary depending upon what type of business the user company designs on DLT. Bitcoin has already found well-balanced technical parameters for the use case in virtual currency. We need to explore the new balance for capital market infrastructures considering business requirements raised in this paper. While we have tested the consortium DLT in our PoCs, public DLT might be appropriate where data privacy is not required even in a capital markets use case. The argument of 'which is better between consortium and public' is meaningless, and it is desirable to choose appropriate technology by simply considering its business requirements. A journey to explore the new appropriate balance for capital market infrastructures has just begun and cannot be achievable only through theoretical research. Global efforts including PoCs will surely accelerate this fine-tuning process.

We would like to contribute to this effort continuously by leveraging expertise as an infrastructure operator.

We would also like to highlight that the DLT could bring innovation by reconstructing existing business processes to leverage its technological features. If existing entities knowledgeable in the business processes will lead the discussion, they need to take care not to eliminate the technical advantages by focusing too much on existing work flow.

Unlike Bitcoin, which has been operating since 2009, DLT application in capital market infrastructures has rarely been investigated and needs further experiment and enhancement until it matures to be a fundamental technology of capital markets. We hope that this working paper will encourage open innovation of DLT as a technology for capital market infrastructures.