# Realizing Interoperability in Next-Generation Finance

## Secure and Efficient Settlement Between Multiple Digital Currencies

April 2022

Datachain, Inc.

Datachain

# Table of Contents


Summary · · · · · 3
1. Background · · · · · 3
2. Issues with Existing Methods to Achieve Interoperability · · · · · 4
3. Proposed Methodology and Architecture · · · · · 5
    Smart Contracts and Consensus · · · · · 5
    On-chain Verification · · · · · 5
    Inter Blockchain Communication (IBC) · · · · · 6
    Proxy-based Architecture · · · · · 7
    Cross Framework · · · · · 8
4. Use Cases (Exchange Platforms for Multiple Digital Currencies) · · · · · 10
    Inter Blockchain Communication (IBC) Ecosystem · · · · · 10
5. Discussing Methods in Use Cases · · · · · 13
    Outline of the Flow of Steps in a Transaction Based on the Use of Universal Payment Channel · · · · · 13
    Challenges with the Flow of Steps in Transactions Based on the Use of Universal Payment Channel · · · · · 14
6. Other Envisaged Use Cases · · · · · 15
    Money Transfer Processing with Multiple Platforms · · · · · 15
    Settlement of Payments for NFTs and Other Assets · · · · · 15
    Granting Dividends, User Fees, and More · · · · · 15
    Realizing a Cross-chain Wallet · · · · · 15
    Coordinating with a KYC System · · · · · 15
7. Future Developing Topics · · · · · 16
8. Conclusion · · · · · 16

# Summary

As the world of finance continues to undergo digitization, we expect to see blockchain-based systems increasingly adopted and implemented in such areas as securities and trade, including with respect to platforms for the issuance and circulation of digital currency in the settlement domain. Blockchain enables the sharing of data or procedures of some kind among stakeholders with nodes, but it seems unlikely that all forms of data and procedures can be shared on a single blockchain in light of the attributes of the applicable domain and handled data, such that enhancing interoperability between blockchains or between a blockchain and an existing system will be necessary to have processing carried out between blockchains or between a blockchain and an existing system. Such processing includes simultaneous multicurrency settlement processing and simultaneous securities transfers and settlement processing. This concept paper proposes a solution architecture with a focus on interoperability and presents its applicability to subject matter consisting of an exchange platform that enables settlement processing between different currencies as an example of its use. In addition, comparisons with other schemes for the realization of interoperability and use cases where exchange platforms have been extended are also discussed.

# 1. Background

Blockchain-type architecture is being adopted and introduced in various financial and nonfinancial domains, including digital currency. Investments in 2021 in the blockchain field are expected to exceed 30 billion dollars[1] globally, a significant increase over the 5.4 billion dollars invested in 2020, and grow in Japan to 78.3 billion yen from the 41.5 billion yen invested in the previous year[2]. In October 2020, the Japanese government set up the Trusted Web Promotion Council under the purview of the Cabinet Secretariat's Headquarters for Digital Market Competition and has been developing prototypes and studying use cases through this council[3]. This council sees blockchains as a technology that enables the verification of disclosed data among multiple business participants and would like to see this technology grafted onto the Internet as a whole and used accordingly by 2030.

The expansion of blockchain architecture in this way can be seen in numerous use cases, including the settlement (such as digital currency), traceability (traceability in the course of distribution), authentication, and nonfungible tokens (NFTs). In each use case, data are shared and transactions between companies and users are realized through the deployment of original blockchains and smart contracts (conditional business logic) based on industry regulations, national regulations, industry practices, and other elements. If such an environment could be further connected to external data or systems, more value could be provided to participating companies. For example, if trading services companies were to automate the payment of bills of lading through the execution of smart contracts, the linking of systems with accurate information on trade operations involving lading, export licenses, and bills of lading with systems that undertake settlement actions will be needed. In the area of trade where use is being promoted, it has already been announced that there is a goal of achieving interoperability between TradeWaltz and

1 KPMG [pulse of fintech H2 2021]
https://home.kpmg/xx/en/home/insights/2022/01/pulse-of-fintech-h2-2021-global.html
2 Yano Research Institute, Ltd. [Conducted a 2021 survey on the blockchain-utilizing services market (2021)]
https://www.yano.co.jp/press-release/show/press_id/2914
3 Trusted Web Promotion Council [White papers and publications issued by various assemblies]
https://www.kantei.go.jp/jp/singi/digitalmarket/trusted_web/index.html

TradeLens as multiple blockchain systems used as trading platforms in Thailand[4]. In other use cases as well, it is expected that interoperability and interconnection between multiple blockchains and between blockchains and existing systems[5] will be important.

## 2. Issues with Existing Methods to Achieve Interoperability

There are probably three main methods of realizing interoperability as shown in Figure 1[6]. The first is the Trusted Third Party method/TTP method whereby the information in each blockchain is linked by a specific trusted third party; this method is the easiest to implement. At the same time, this method concentrates trust in the TTP, which means that the costs required for system availability and permanence and for establishing organizational governance are expected to be high. Consequently, the costs incurred for transactions between blockchains increase to become a burden for service providers and general consumers, which could then impede the development of services built on a blockchain. Thus, interoperability needs to be realized by means that are not dependent on a specific party for trust.

There is a method of realizing interoperability by way of trustless[7] means known as the hashed timelock contract (HTLC)[8], which is based on the use of hashlocks and timelocks. However, this method is problematic in that it limits use cases to, for example, the transfer of substitution tokens[9], and it sacrifices the efficiency of liquidity for timelocks and deposits. While the issues concerning HTLC for token transfers will be mentioned below in a discussion based on subsequent use cases (Chapter 4), the relay method has been put forth as a method that resolves these issues and generates trustless interoperability in use cases that are more generic.

4 TradeWaltz [Japanese trading platform TradeWaltz and Thai trading platform NDTP sign a system-integration terms of reference agreement (TOR): Toyota Tsusho will cooperate for commercial distribution, and TradeLens will be utilized and linked in the area of digital bills of lading]
https://www.tradewaltz.com/news/1426/

5 World Economic Forum [Bridging the Governance Gap: Interoperability for blockchain and legacy systems]
https://www.weforum.org/whitepapers/bridging-the-governance-gap-interoperability-for-blockchain-and-legacy-systems

6 Comprehensive deployment of blockchains for supply chains: Part 6. A framework for blockchain interoperability.
https://www2.deloitte.com/content/dam/Deloitte/jp/Documents/financial-services/bk/WEF_A_Framework_for_Blockchain_Interoperability_JP_2020.pdf

7 What Does Trustless Mean?
https://www.gemini.com/cryptopedia/trustless-meaning-blockchain-non-custodial-smart-contracts

8 Project Stella: Search for the future of DLT and financial market infrastructure
https://www.boj.or.jp/announcements/release_2019/data/rel191008b1.pdf#page=11

9 What is fungible? Three categories for understanding tokens. What are nonfungible and hybrid tokens?
https://www.coindeskjapan.com/21635/

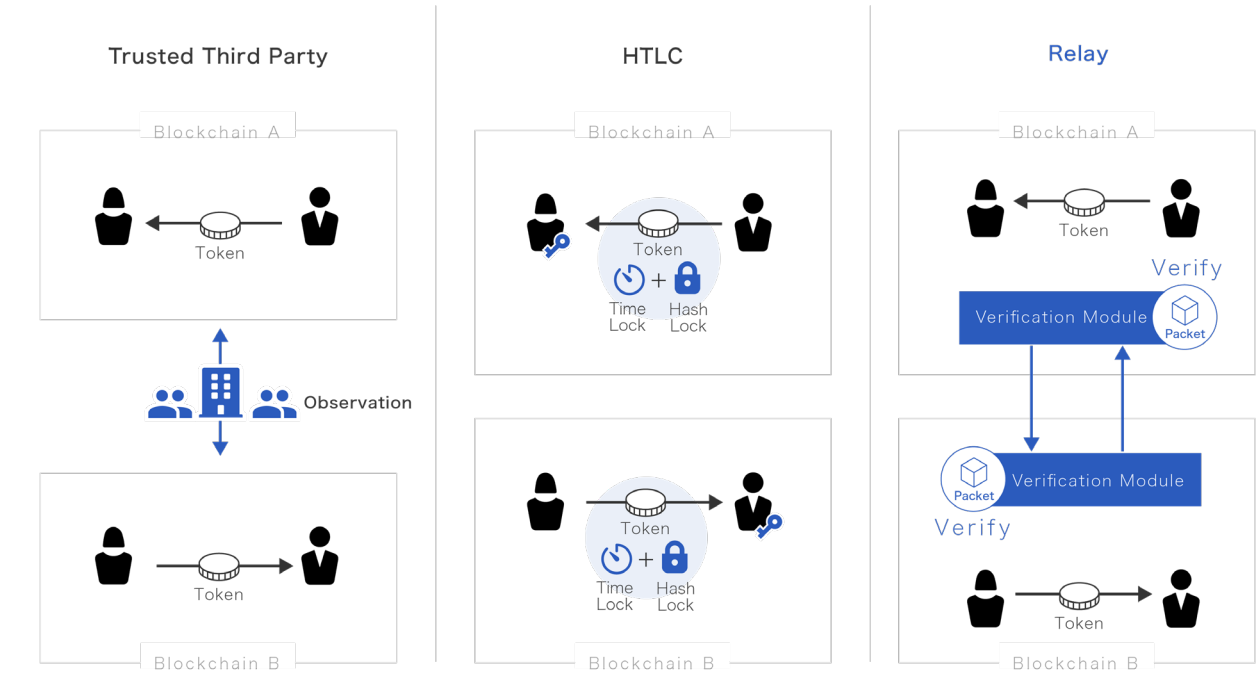


Figure 1: Methods of realizing interoperability between blockchains

# 3. Proposed Methodology and Architecture

## Smart Contracts and Consensus

First, let us provide an overview of the way blockchains (distributed ledgers) work and their properties. In order to create a common ledger at multiple nodes, ledgers are updated according to the same rules in a blockchain and by consensus between nodes. Specifically, let us look at an example. Based on the user's account balance information or other record agreed upon in the current step (t), a money transfer or other such transaction is changed based on common rules between nodes, which are known as smart contracts. Even in a new step (t+1), the ledger is constituted in a way in which the record is agreed upon.

Example:
(1) In step t, Alice holds 100 tokens.
(2) Alice transfers 50 tokens to Bob.
(3) In step t+1, 50 tokens are recorded as Alice's new balance.

Through this process, transactions can be processed while ensuring the correctness of the ledger between nodes. On the other hand, an external company or user who is not participating in the blockchain does not usually undergo such an agreement process. For this reason, even if a given record (such as the fact that Alice's balance is 50 tokens) were obtained by an external company or user, it would not be possible to verify the correctness of this record. This problem is a factor impeding interoperability between systems.

## On-chain Verification

The basic idea behind on-chain verification is that it is a solution to ensure the correctness of an agreement or change in the target blockchain through the performance of verification work similar to participating nodes in the blockchain on the recipient side of information outside the blockchain. The implementation of this idea in a

blockchain smart contract is referred to as on-chain client[10]. The use of this mechanism allows the state of the target blockchain to be verified and the record consisting of Alice's balance to be incorporated into the recipient-side blockchain.

## Inter Blockchain Communication (IBC)

By applying the aforementioned mechanism, communication between mutually verifying blockchains can be realized. Inter Blockchain Communication (IBC) has been proposed as such a communication protocol and put into practical use as part of the Cosmos ecosystem[11]. In IBC, specifications are prescribed for, among other items, packets as the unit of communication and connection channels as the unit of connection. IBC enables trusted communication between blockchains, including in terms of authentication and sequencing.

As an outline of processing with IBC, the following steps would be taken in the event that blockchain A wishes to communicate with blockchain B:

i. A packet for B is recorded on blockchain A.
ii. An on-chain verification of the packet information is performed on blockchain B to verify that the packet information has been correctly recorded on A, whereupon the packet is accepted.
iii. Processing based on the communication from A is performed on the B side and the reply to A is recorded as a packet.
iv. The same verification process as provided for in (ii) is performed on the A side and the reply packet is then accepted.

It should be noted here that A records the packet for B on A and does not engage in so-called transmission processing whereby it writes to B. In fact, processes known as relayers access the blockchains of both A and B to actually mediate information. Since, as outlined earlier, the other party's blockchain will be subject to on-chain verification, if relayers tamper with the information, the tampering can be detected when verification is conducted.
There are various consensus rules in public blockchains and enterprise blockchains, and each of these sets of rules will need to be accommodated in conducting the verification process. Datachain comprises an on-chain client for major enterprise blockchains and has contributed codes to Hyperledger Labs in the form of the YUI project[12].

10 Refers to light clients operating on an on-chain basis. See the following for more information: https://www.coinbase.com/ja/cloud/discover/dev-foundations/blockchain-client-types#Light-clients.
11 Cosmos: https://cosmos.network/
12 Hyperledger Lab: YUI https://github.com/hyperledger-labs/yui-docs

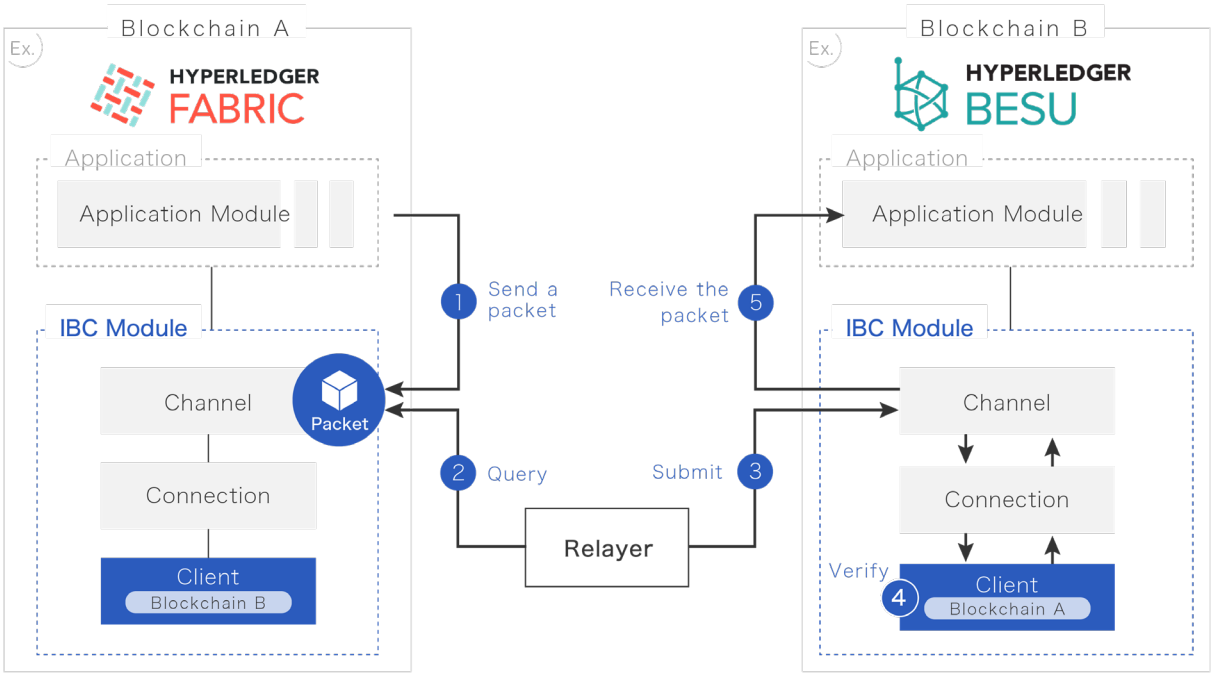


Figure 2: IBC module configuration

## Proxy-based Architecture

In IBC as seen in the previous section, communication between blockchains A and B takes the form of the introduction of an on-chain client in both A and B. If we were to assume the presence of a third blockchain referred to as blockchain C, then similar mechanisms would, in general, need to be configured between A and B, A and C, and B and C. As the number of combinations increases, we can expect that difficulties in terms of design, development, and operations will arise. We propose a proxy-based architecture in order to address the above challenges associated with general one-to-one IBC connections. This architecture is predicated on the use of a hub system (blockchain) for verification and communication among multiple blockchains. This hub system uses IBC to communicate with each blockchain via a relayer and thereby realizes communication between each combination of blockchains. As shown in Figure 3, the proxy also operates an on-chain client and takes over the verification of communication between blockchains in this form of IBC connection.

The following are some of the advantages that can be obtained by adopting this architecture.

1. It can be difficult to configure an on-chain client depending on the smart contract system that has been adopted for a blockchain. The use of a proxy to take over verification[13] will enable communication that can be trusted even in such cases.
2. Additional on-chain clients can be introduced to a proxy to enable communication for new types of blockchain.
3. The adoption of a hub-and-spoke-based communication structure will allow blockchains joining a network to connect to already-connected blockchains.

13 It should be noted that transparency guarantees achieved by, among other approaches, having a node in the proxy system and disclosing the code log, are a prerequisite for preventing the proxy from becoming a black bo

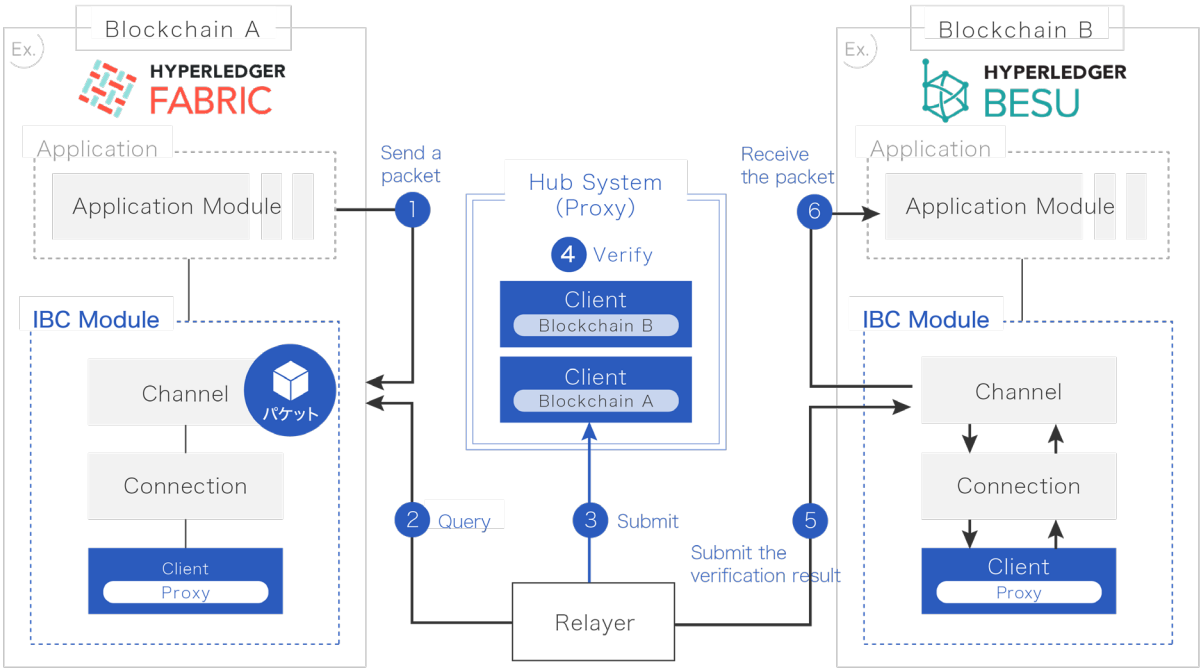


Figure 3: IBC proxy-based architecture

## Cross Framework

The use of IBC to facilitate trusted communication between blockchains permits various applications based on the use of such communication to be realized. One example of this is concurrent processing across multiple systems as might be seen with the two-phase commit protocol. To achieve this, Datachain has released open-source software known as the Cross Framework to be run as middleware.

While you should refer to the development document[14] for more information on the Cross Framework, an outline is provided as follows: (1) a mechanism to realize such processes as locking and commit is added to the management of the state of blockchains, and (2) a function to control the execution of smart contracts for this mechanism is incorporated into the IBC-based communication protocol. This scheme enables smart contracts on multiple blockchains to be processed by each blockchain on a coordinated basis. This enables the realization of such processes as the so-called atomic swap[15] process and the process whereby the outcome of the execution of one smart contract is used as the basis for conditional branching with other smart contracts.
The hierarchical structure of software presented in this section is summarized in Figure 5.

14 https://github.com/datachainlab/cross-docs

15 Refers to the process whereby assets on blockchain A are sent from Alice to Bob and assets on blockchain B are sent from Bob to Alice. Conceivably necessary for concurrent payment and settlement processing.

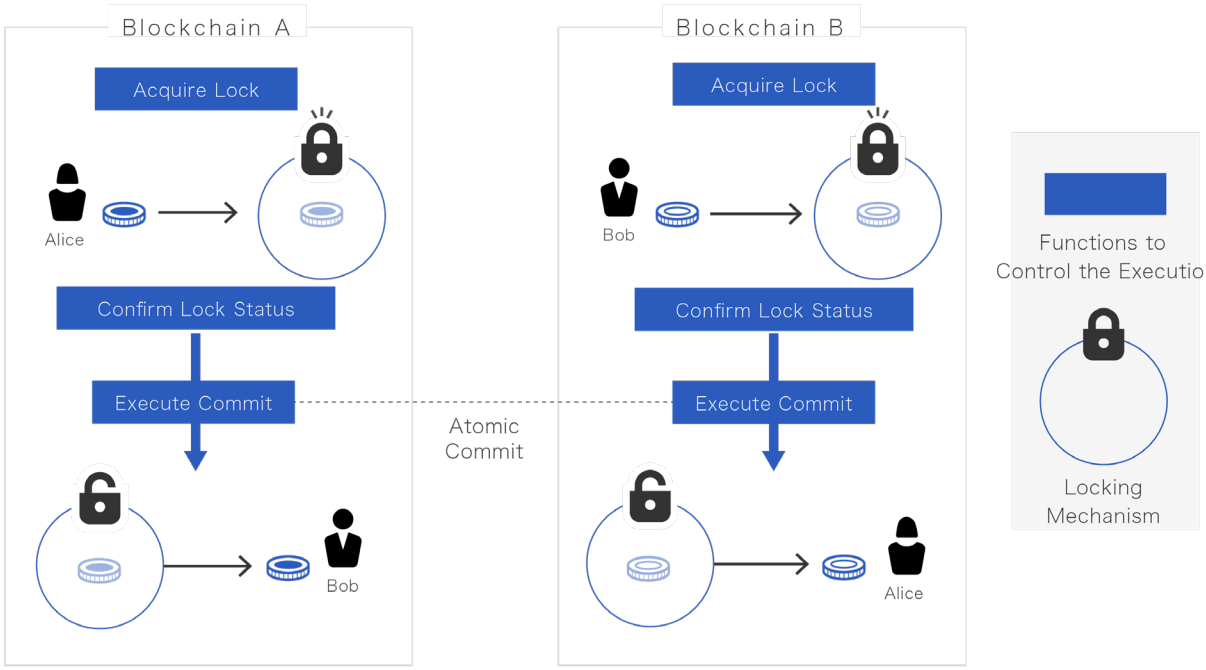


Figure 4: Outline of the Cross Framework

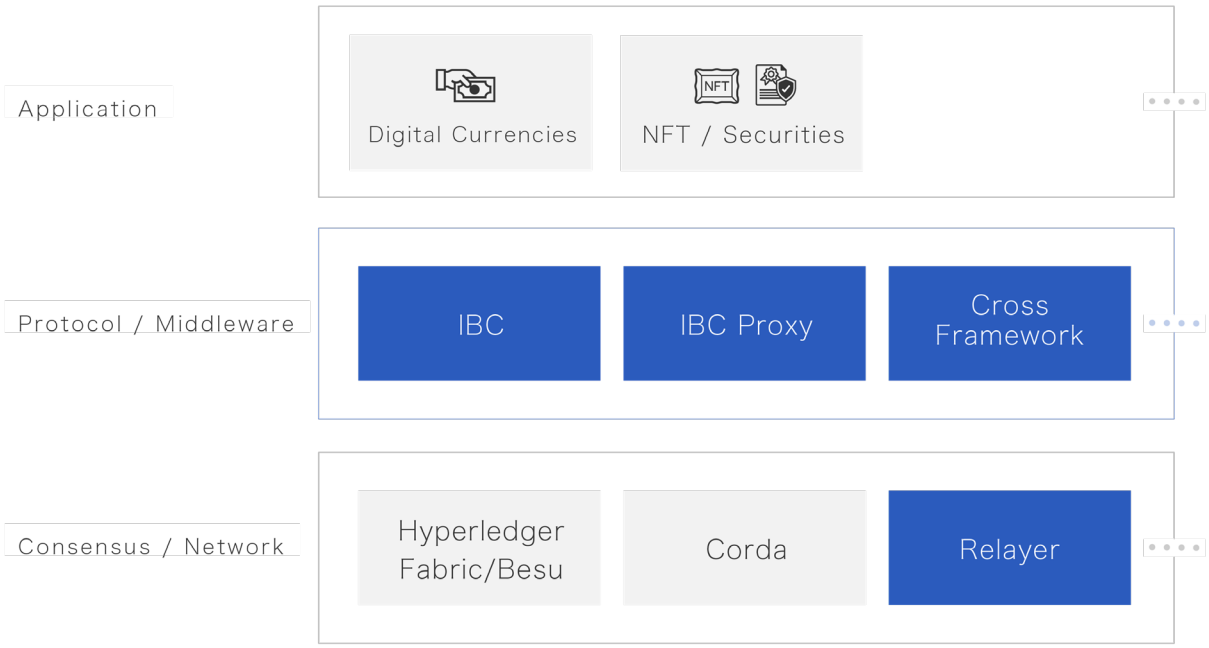


Figure 5: Organization of the proposed architecture

### Inter Blockchain Communication (IBC) Ecosystem

IBC is an inter-blockchain communication protocol designed by Cosmos for the realization of the Internet of blockchains. It plays a key role in supporting the Cosmos ecosystem worth in excess of 100 billion dollars. Blockchains built using the Cosmos SDK (software development kit) are equipped with IBC. Since becoming enabled on main networks in March 2021, IBC has been involved in actively transferring assets among more than forty blockchains. The building of blockchains using Cosmos SDK has also been adopted by enterprises and by such entities as the Blockchain-based Service Network (BSN), which is being promoted as a national strategy in China; Line Plus Corporation, a subsidiary of Line; and the USDF Consortium, which was established for the purpose of enabling a number of US-based banks to offer a stablecoin called USDF. In light of these initiatives, the selection of a platform with a focus on the growing necessity of realizing interoperability among heterogenous blockchains is considered to have also become important in the domain of enterprises.

# 4. Use Cases (Exchange Platforms for Multiple Digital Currencies)

We saw in previous chapters that it is possible to realize interoperability for various case uses in order to guarantee correctness between multiple blockchains by utilizing IBC to interconnect multiple blockchains, adopting a proxy-based architecture that makes operations more efficient, and placing the Cross Framework atop this architecture. In this section, we will explore exchange platforms for digital currencies as use cases.

When we talk about a digital currency as a means of payment on a digitized blockchain that is tied to a sovereign currency unit issued by a sovereign state, such as the Japanese yen or American dollar, it is desirable from the perspective of users that multiple digital currencies can be selected and that the levels of the exchangeability and liquidity of currencies are high. Presently, there are multiple digital currencies on multiple blockchains and multiple digital currencies that can be used for payment purposes. In January 2022, PayPal, a major US-based online payments system, made the news when the company that operated this system announced to great fanfare that it was going to look into developing a digital currency[16]. It is expected that the number of digital currencies used for making payments will continue to increase in the future.

In such a situation, a safe and efficient exchange platform that establishes payments among multiple digital currencies is required to enhance payment convenience. Specifically, we can illustrate the use of an exchange platform in the following payment scenario. If Alice holds emerging α Coins and Bob's shop has β Coins, which are also used by many of the staff members of Bob's shop, different currencies may be selected for payment by Alice and receipt by Bob, such that a mechanism for exchanging these currencies is needed to enhance user convenience. User convenience in this context includes not allowing the possession of α Coins by Alice to ruin Alice's opportunity to purchase and not incurring a cost to switch to β Coins before purchase.

As touched on in the section on existing methods in the previous chapter, there is an issue of trust in intermediaries in any payment exchange based on the use of a TTP. Specifically, the following risks exist in transactions carried out on an exchange platform:

16 Bloomberg [PayPal Explores Launch of Own Stablecoin in Crypto Push]
https://www.bloomberg.com/news/articles/2022-01-07/paypal-is-exploring-launch-of-own-stablecoin-in-crypto-push

- Counterparty risk related to the business continuity of the TTP wherein Alice has made a payment, but no deposit has been made on Bob's side.
- Risks arising from the increased complexity of processing due to the need to go through an off-chain system in between despite the fact that the TTP itself is an intermediary with no malicious intent.
  (Example: Where an off-chain TTP transmits information, there is a need to manage such intermediate states as the status of incoming and outgoing payments and the appropriate scale of liquidity management. There is a risk of system delays and outages due to the difficulty of designing so as to eliminate abnormal systems.)

On the other hand, it is possible to apply a combination of IBC, proxy-based architecture, and the Cross Framework as mentioned in the previous section as architecture to this case. Such an approach could reduce costs compared to settlement processing based on the use of a TTP (Figure 6).

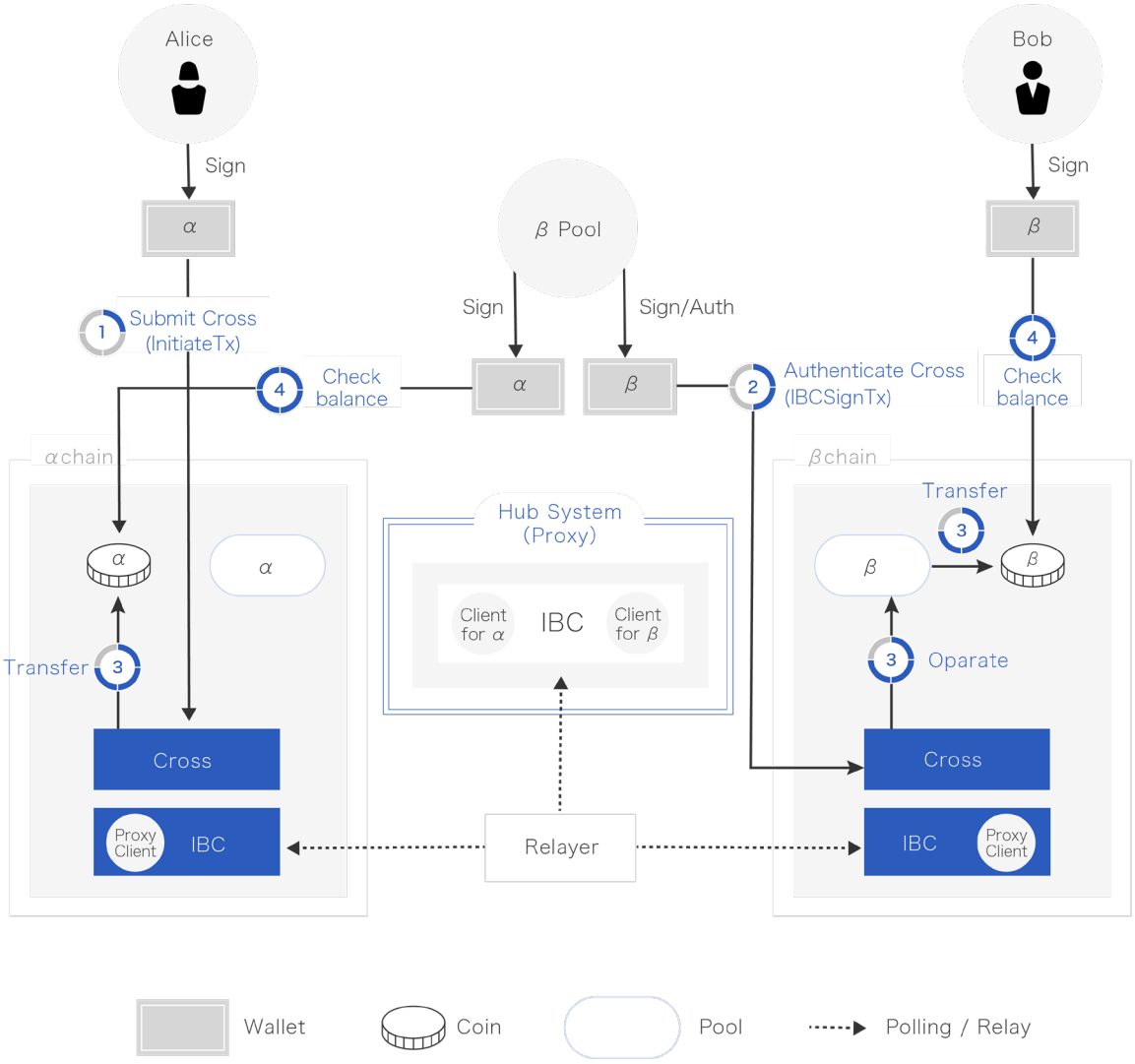


Figure 6: Architecture envisaged for an exchange platform

This architecture is a simple one that focuses on transactional parts in use cases involving an exchange platform. In other words, it does not encompass parts consisting of user registrations, prepayment deposits, the ensuring of liquidity, or the redemption of digital currencies. The transaction entails a payment by Alice and a receipt by Bob by way of the following four steps:

1. **[Submit Cross]**
   After the transaction amount and exchange rate are agreed upon, a Cross Framework transaction will be initiated by Alice.
2. **[Authenticate Cross]**
   The liquidity-providing β pool detects the event in question by some trigger, such as an off-chain notification. If the detected transaction initiation are as agreed upon, authentication is carried out according to the authentication method for the β chain connected with IBC.
3. **[Transfer]**
   Based on the authentication results, the Cross Framework processes smart contracts on both the α chain and β chain on a coordinated basis to get α Coins and β Coins to be transferred concurrently.
4. **[Check the balance to confirm the results of the transaction]**
   Alice and Bob can check the results of the transfer.

The envisaged sequence of steps presented above is shown in Figure 7.

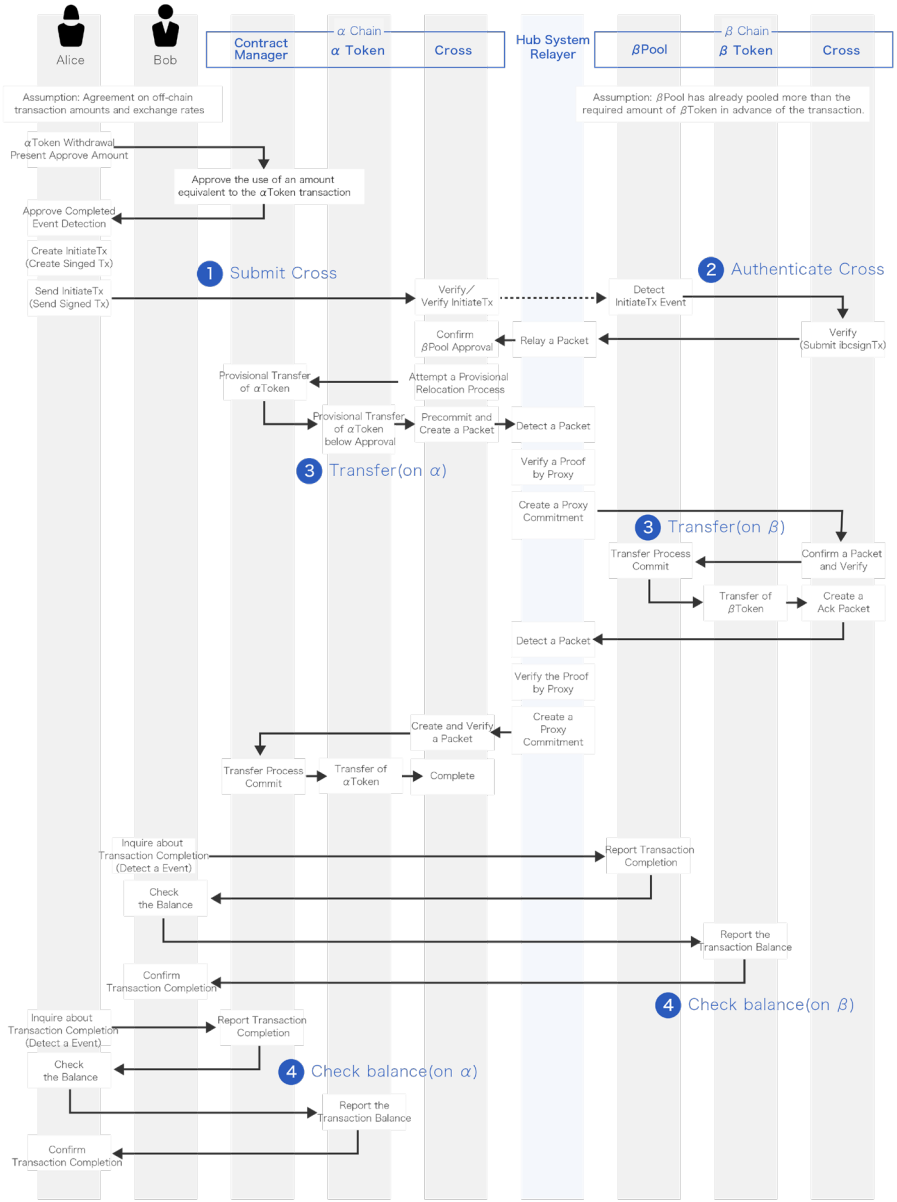


Figure 7: Flow of transaction steps carried out on the exchange platform

Liquidity needs to be supplied between α and β in order to carry out this transaction (which is represented by the β pool indicated in Figures 6 and 7). In other words, it is necessary to have a suitable amount of α Coins obtained from Alice, a user of α Coins, on the α side where the payment is made and to have pooled funds paid to Bob's shop on the β side where the deposit is made. We can expect to see a single liquidity provider or multiple liquidity providers, such as DeFi, in the above scenario as realized. This architecture can perform a settlement in either case by appropriately operating a liquidity pool, but the design of a liquidity pool lies outside the scope of this paper. Since this system takes a form that entails immediate gross settlement processing, the scale of required liquidity is likely to be greater than that of point-in-time net settlement processing. However, it may be possible to reduce this scale by adopting a hybrid mode of settlement together with point-in-time net settlement processing whereby multiple settlement system participants can offset claims and liabilities with one another and only have to settle the resulting difference.

# 5. Discussing Methods in Use Cases

We saw that it is possible to use the architecture for a digital currency exchange platform as presented in the previous section to carry out a settlement involving multiple different digital currencies without relying on a TTP.

- The correctness of the results of fund transfers on both sides between blockchains handling different digital currencies is guaranteed through the on-chain cross-checking of these results by IBC.
- The Cross Framework enables deposits from Alice into the liquidity pool and the transfer of funds from the liquidity pool to Bob to be performed atomically, and IBC guarantees the correctness of the results thereof through on-chain verification by IBC.
- Accordingly, this guarantees that, as long as each digital currency platform is working properly, a payment between different digital currencies will be performed between Alice and Bob in a way that prevents anyone from cheating.

HTLC is a different approach to realizing trustless settlement processing with multiple digital currencies and has been proposed for Visa's Universal Payment Channel[17]. However, there are inherent challenges with this approach that depend on the characteristics of HTLC. An outline of the flow of steps in a transaction where Universal Payment Channel is used to perform money transfer processing is shown in Figure 8.

## Outline of the Flow of Steps in a Transaction Based on the Use of Universal Payment Channel

As with the use case presented in the previous chapter, let us consider a case in which Alice pays with α Coins and Bob receives β Coins through the UPC Hub.

1. The UPC Hub deploys a contract to open or close the payment channel and Alice approves the foregoing.
   a. The same flow of steps is carried out between the UPC Hub and Bob.
2. Alice and the UPC Hub deposit a sufficient amount of α Coins.
   a. Likewise, β Coins are deposited between Bob and the UPC Hub.
3. Bob sends Alice the transaction details consisting of the amount, period of validity, and hash value (R) for secret R.

17 Universal Payment Channels: An Interoperability Platform for Digital Currencies
https://arxiv.org/pdf/2109.12194v2.pdf

4. Alice sends the UPC Hub a message indicating that α Coins will be sent once secret R is disclosed before the expiration of the period of validity. Upon receipt of this message, the UPC Hub sends the same message to Bob (promise).
5. Bob sends the UPC Hub a message containing secret R (secret).
6. The UPC Hub, after verifying the correctness of secret R, sends Bob a message containing the latest balance reflecting the details of the transaction (receipt).
7. The UPC Hub sends Alice a message containing secret R as obtained in 6.
8. Alice, after verifying the correctness of secret R, sends the receipt to the UPC Hub.
9. After the necessary transaction is completed, the payment channel will be closed, and the latest balance will be reflected in the on-chain data.

Alice will be able to pay Bob via the UPC Hub without the existence of a TTP through the flow of steps described above. If Bob fails to disclose secret R before the expiration of the validity period, Alice and the UPC Hub will be able to recover funds with their own signatures.

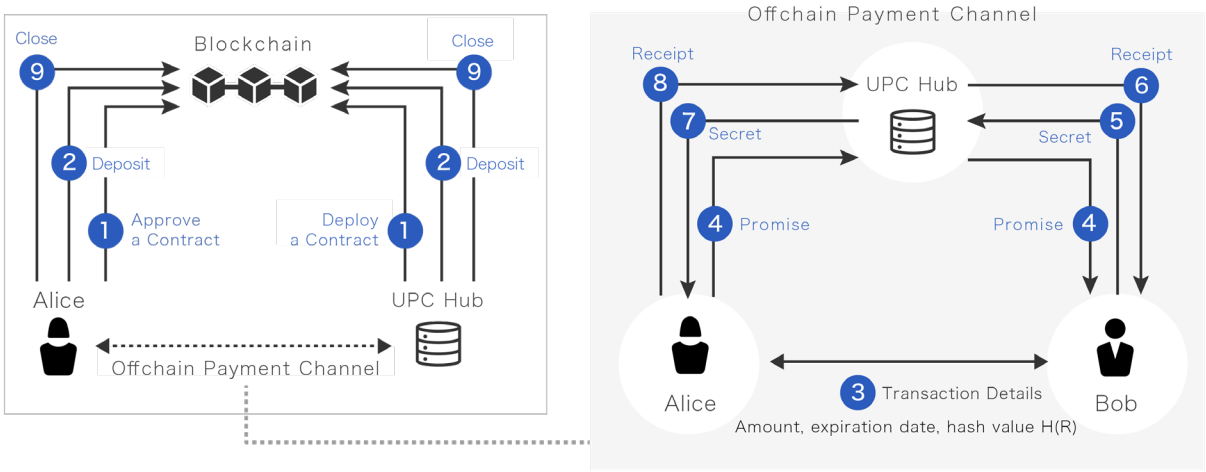


Figure 8: Flow of steps in a transaction based on the use of HTLC

## Challenges with the Flow of Steps in Transactions Based on the Use of Universal Payment Channel

As indicated above, the use of HTLC enables the realization of settlement processing with different digital currencies, but there are likely challenges to be faced in that the liquidity of funds will be sacrificed because of the deposits and timelocks and in that the risk of exchange rate fluctuations exists.

- **Reduced liquidity**: The parties to the transaction (Alice and Bob) and the UPC Hub will each need to deposit an amount sufficient for the transaction; this will cause the liquidity of the funds to be sacrificed.
- **Exchange rate fluctuation risk**: If the secret is not properly disclosed either deliberately or as the result of a failure, the asset in question will not be available until the timelock is released, and there will be exposure to the risk of exchange rate fluctuations while the timelock remains engaged.

With the architecture based on the use of IBC or the Cross Framework as presented in Chapter 4, neither of the parties to the transaction, Alice and Bob, will need to make a deposit. Since the liquidity-providing pool can also be deployed for aggregated transactions, the efficiency of fund liquidity can likely be improved. Since no timelock

is needed, the parties to the transaction are not exposed to any risk of exchange rate fluctuations caused by the locking of assets.

# 6. Other Envisaged Use Cases

## Money Transfer Processing with Multiple Platforms

While we have considered the matter of currency exchange between multiple digital currencies on an exchange platform, it also seems possible to have the same currency exchanged between multiple different platforms. This type of remittance processing is probably needed when considering the architecture, such as in terms of focusing on the issuance and management of tokens, such as currencies and assets, on a given platform while using them for various applications on a different platform through smart contracts. It is believed that the use of YUI as introduced in this concept paper can realize remittance processing in both directions between platforms without having to place trust in a specific entity.

## Settlement of Payments for NFTs and Other Assets

The handling of heterogenous assets may be rendered on multiple platforms. For example, NFTs or securities tokens and digital currencies could very well be managed on different platforms. In such a case, you can imagine a use case in which you want to simultaneously perform a settlement of payments for the transfer of an NFT with a different digital currency platform. The solution architecture presented in this concept paper can also be used in carrying out such a delivery versus payment arrangement (DvP).

## Granting Dividends, User Fees, and More

Similar to the use case described above, a use case in which a dividend or user fee is provided to the holder of an NFT or securities in digital currency is conceivable. Although the NFT itself is transferred or moved onto a different chain, functions for correctly paying the dividend or user fee to the holder can be properly carried out by identifying the chain-crossing holder in question and having the exchange platform process the payment to the account belonging to this holder.

## Realizing a Cross-chain Wallet

For token operations or decentralized applications as mentioned above, systems linked to multiple systems will need to properly engage in processing, including with respect to the provision of information by users (for example, changing the processing of payments for reward tokens according to the client's area of residence and age). In order to realize such use cases, it is assumed that a system that plays the role of a portal connecting the user's wallet with each chain is needed. The architecture presented in this concept paper can conceivably be applied for this purpose.

## Coordinating with a KYC System

In the context of the configuration of a digital currency platform, operations to identify a person can be undertaken through coordination with other systems without having to place information on accounts and personal information on the platform. The architecture for communication and coordination as presented in this concept paper can accommodate such use cases and realize a flow of procedures for performing conditional branching, which would involve looking up KYC information through the exchange platform and determining whether or not to transfer money

according to the results thereof. In other words, privacy can be guaranteed since a system that grants authorization can be managed at arm's length from the payment system. When thinking about this type of coordination, a system that is linked to a blockchain-based system does not necessarily have to be blockchain based itself but could also be an existing RDB-based system. As the IBC protocol presented in this concept paper can also be applied to a linkage between a blockchain and an existing system, the properties of IBC can be harnessed to enable the realization of such properties as simultaneity, authenticity, and consistency.

# 7. Future Developing Topics

In looking to development in the future, it is important to first promote use cases as presented in this concept paper with an eye towards putting them into practical use. Among these cases, linking to existing systems is believed to be essential for reforming operational processes for enterprises by making blockchain data a single source of truth.

The course of development in the future is presented below with a particular focus on the technical aspects. As noted earlier, a state-locking mechanism is introduced in the Cross Framework as an intermediate state for the execution of a transaction. However, obtaining a lock generally incurs a cost and can induce a loss of transaction-processing performance. To resolve this issue, there are two simple fixes that can be conceived. First, you could group together multiple packets, each of which constitutes a unit of communications, and regard this group of packets as a single packet for processing. By grouping together verification processes to be carried out, you can expect to reduce the average time it takes to complete processing in connection with processing between multiple chains. The other fix entails the application of a method known as CRDT. Datachain has implemented a data structure inspired by this method and offers it as open-source software (OSS). Utilizing this method makes it possible to update such data as account balance figures without having to obtain a lock and thereby enhance transaction-processing performance.

Another challenge when it comes to proxy-based architecture lies in the need to have transparency in its operations given that it takes over the verification of communication between blockchains. Simply put, a company or user who wishes to use a function of interoperability can, by having proxy nodes, realize interoperability without relying on a TTP. However, this method has issues in that costs are incurred in connection with the maintenance and operations of nodes and in terms of privacy matters when an exchange platform for connecting various networks is configured. In dealing with this challenge, you could utilize a secure process execution environment, such as Intel SGX, and an integrity-verification method like remote attestation to guarantee that the counterpart ledger verification process is working correctly. Although both communication methods and the methods by which their safe operations can be verified are still in their infancy, combining these methods can possibly realize safer and more efficient forms of interoperability.

# 8. Conclusion

This concept paper discusses ways of realizing interoperability needed when considering blockchain-based systems with a focus on exchange platforms for multiple digital currencies. The proposed method is technology that enables communication and coordination among multiple platforms without having to rely on a trusted third party and is expected to become increasingly important with the spread of digital currencies and other blockchain systems in the years to come. In the area of digital currencies, issuers (administrators), wallet providers, decentralized application providers, and exchanges each have their own domain for the application of this technology, such that

further commercial and technical studies will need to be conducted with an eye towards the practical use and actual operations of this technology.



[Contact]
(E-mail) contact@datachain.jp


www.datachain.jp