ICON

Hyperconnect the World

Contents

Abstract

The advent of the blockchain technology has introduced the world of decentralization and is challenging our preconceived perspectives of the current social, political, and economic systems, most notably, the central banking system. The rapid advancement of this technology has begun to blend world borders and statute, providing glimpses of an improved, alternative future. Yet, the technology is still at its infancy and is confronted with limitations in terms of performance, ease of use, and service quality.

Generally, the majority of blockchain projects place emphasis on their decentralization methodology and lack evidence of adoption in the real world due to their technological and business limitations. The ICON Project ("ICON", "ICON Network", "we", "our", "us") aims to overcome such challenges and help advance our society towards true hyperconnectivity.

This paper outlines our vision and philosophy of the ICON Project and details on the supporting proprietary technologies that have been in development over the past few years. More importantly, we discuss actual implementation with dozens of reputable institutions that are already in the ICON Network. This demonstrates our progress beyond the initial concept stage and validates our team's strong execution ability; a major factor that differentiates ICON from the majority of blockchain projects today.

ICON is inspired by Gilles Deleuze and Felix Guattari's rhizome – "the world with no center point and the world where any point is a mere connection to other points." ICON is a connector of disparate cryptocurrencies with different blockchain governances, and furthermore, a connector of the crypto world to our real world. ICON embraces the new and the unfamiliar, the principle of radical inclusion – accept new ideas and decisions made by the new republic established by ever-changing crypto-to-real world connections.

1. Introduction

1.1. Vision

The vision of the ICON Project is to introduce the new era of decentralization by redefining the meaning of communities and creating a new world by connecting such communities. Communities today are commonly defined by its social and political functions and limited to the economic boundaries set forth by world nations. Through ICON, communities can go beyond and be free from traditional economic system and promote frictionless value exchanges with other communities, eventually resulting in maximum total utility of society. ICON is not limited to the real world, but it directly connects and communicates with the crypto world creating the most robust network that can scale without limits.

The ICON Project aims to build a decentralized network that allows independent blockchains with different governances to transact with one another without intermediaries. Anyone can create a new blockchain project and join the network. A new blockchain project is free to connect with existing projects and create new unique worlds, or blockchain multiverse. ICON itself can be viewed as both a living organism and an ecosystem.

ICON is a vision with a proven track record and has progressed beyond the initial concept stage. ICON already boasts communities comprised of reputable institutions – banks, securities, insurance, hospitals, universities, and more. A future with faster money remittance and frictionless value exchange of securities, medical records, academic data, insurance fees is within our reach.

With ICON, we now enter into a world of true hyperconnectivity.

1.2. Background

Overview

The advent of the blockchain technology has introduced the world of decentralization and is challenging our preconceived perspectives of the current social, political, and economic systems, most notably, the central banking system. The rapid advancement of this technology has begun to blend the world borders and statute, providing glimpses of an improved, alternative future. Yet, the technology is still at its infancy and is plagued with shortcomings in terms of performance, ease of use, and service quality.

Generally, the majority of blockchain projects place emphasis on their decentralization methodology and lack evidence of adoption in the real world.

There are fascinating projects such as Steem that operates a crypto world, a virtual service on top of its own blockchain. However, other projects that attempt to connect to the real-world are feeling performance limitations, and hence, realizing the need for more research and development. To overcome such limitation of connecting the real world to crypto world, ICON was started.

Ethereum[1]

Launched in 2015, Ethereum was the first project to introduce the concept of 'Smart Contract' in the blockchain world opening the unforeseen possibilities of Decentralized applications(DAPPs). Ethereum is widely considered the greatest milestone in blockchain technology since the first introduction of Bitcoin by Satoshi Nakamoto; therefore, is referred to as Blockchain 2.0. It paved blockchain application beyond simple cryptocurrency transaction to a wider use of the technology including in the financial services industry.

Various DAPPs have been developed, most notably a USD$170 million decentralized and autonomous venture capital fund called the DAO project. Unfortunately, DAO was hacked in June 2016 and Ethereum went through hard-fork to restore the stolen funds. Many issues, particularly on Proof-of-Stake consensus, are still under discussion among the Ethereum developers, which includes the founder Vitalik Buterin, and miners.

Despite the facts above, Ethereum is gaining popularity as a ICO platform due to the simplicity of ERC20 Token generation. But ironically, the popularity of certain ICOs such as Status.im has resulted in overload of the entire Ethereum network.

Bancor[2]

Bancor provides Decentralized Exchange (DEX) that allows real-time cryptocurrency transactions based on fair price deriving algorithm that uses Ethereum reserves. With the concept of exchanging Ether and Bancor Token(BNT) via DEX, Bancor raised over USD$150 million in ICO.

Bancor has succeeded in supporting different business models such as ETFs, by exchanging cryptocurrencies based on reserves. However, we believe it faces significant challenges due to the high transaction fees and performance limits when running on Ethereum. Transaction fees and speed limits when running on Ethereum.

EOS[3]

EOS is a blockchain platform that primarily focuses on scalability issues of Ethereum. It is a Proof-of-Stake consensus algorithm that generates blocks in every 3 seconds and removes the transaction fees to invigorate DAPPs.

EOS, even at its current developmental stage, is anticipated by many for its potential to replace Ethereum. But so far, there appears to be no substantial difference from Ethereum other than the consensus algorithm. Furthermore, its smart contract platform is based on virtual machines like Ethereum; therefore, we need to see if EOS is capable of handling massive, real-time transactions.

2. ICON

2.1. Hyperconnect the World

The ICON Project began with the goal to enrich our everyday lives through "connection". The history of mankind's technological innovation is related to our history of connection. The creation of postal service made it possible to connect each other's thoughts without having to physically meet. Telephones made it possible to connect each other in real time regardless of the distance, and wireless communication added freedom of mobility. And with the advent of the Internet, real-time connection to everything, not just people, has become possible anywhere in the world. Despite these breakthrough innovations, today's level of connection is still not perfect. With the ICON Project, we are now moving closer to a more seamless connection.

We live in a world where it is possible to buy a cup of latte at Starbucks with one swipe of a credit card. But in fact, there is a more complex process behind the scenes. The information acquired from POS terminal including card number, expiration date, billing address, and CVC are stored and transmitted to the databases of seven (7) intermediaries such as a front-end processor (FEP) company; various fees are incurred at each stage of the process. The credit card network is a centralized system that depends on security and reliability of trusted third parties.

ICON is a decentralized network rather than the existing centralized network. Transactions on the ICON Network are verified by a ledger shared within the community network itself, not controlled by a centralized authority. This minimizes the involvement of unnecessary intermediaries, which significantly reduces the fees. In addition, decentralization ensures autonomy and independence of the community. In order to be connected to a centralized system, it is inevitable to passively accept the policies and system determined by the centralized organization. For instance, to use VISA or MasterCard for payment, it is necessary to use their designated system and follow their policies. However, the ICON Network allows each community to autonomously determine the appropriate systems and policies, while reliably connect to other communities when needed.

ICON aims to eradicate the various boundaries that have been existed in the centralized system. Imagine stock investors in Korea trading Apple stocks in real time with US stock investors, or medical researchers at Korean university hospitals obtaining permission to work with diabetes patients' data from Sydney and London. "Tokenization" of assets and rights are being accelerated, and as a result, the dynamics of cross-border connections is being redefined. Existing currencies, tangible assets such as real estate and automobiles, intangible assets such as patents, copyrights, and trademarks, our legal rights such as voting rights and citizenship, and even DNA data or blood test results can benefit from tokenization[4]. This forces us to rethink everything, even obscures the space-time boundary, and makes distinguishing tangibles from intangibles meaningless. It is possible to trade 0.2 apartments with 0.8 cars, and insurance fee can be directly paid by uploading 5 posts on an SNS.

2.2. Hyperconnect Korea

The Republic of Korea presents an ideal environment for blockchain technology and cryptocurrency disruption. Korea is the top ranked ICT (information and communications technologies) country in the world[5] and the 11th largest economy[6]. Due to such reasons, Korea has been a key test market for global tech companies such as Facebook[7]. In addition, Korea is now quickly becoming a leader in digital currencies[8], and as of July 17, 2017, the country's top three (3) crypto exchanges all rank in the top ten in global daily trading volume[9].

ICON has established itself as the dominant market leader in Korea via theloop, a Korea-based for-profit blockchain technology company behind ICON (*2.8 Implementation of loopchain*). And this is only the beginning as we have various strategic plans set in motion to hyperconnect Korea, Asia, and then

eventually, the world. The ICON team believes that the fundraiser can greatly accelerate the growth of the ICON Network in Korea and further support our ambition for global expansion.

2.3. How to Design

The ICON Project is not simply a connection of blockchain nodes, but a deep study or an investigation of community-to-community connectivity. ICON started with the mission to create a protocol, or cryptocurrency, to be actively utilized in the real world within and between actual communities. There were three (3) considerations when designing of the ICON Network:

1) Components of the ICON Network

2) How to connect

3) How to operate

We first define the elements that constitute the ICON Network, then investigate the way each element is connected. We also look at how the ICON Network operates with a focus on the effective governance

2.4. Components of the ICON Network

Components of the ICON Network: ① Community, ② C-Node (Community Node), ③ C-Rep(Community Representative), ④ ICON Republic, ⑤ Citizen Node

Community

Community is a network comprised of different nodes with the same governance system. Financial institutions, governments, schools, e-commerce platform, healthcare, Bitcoin, and Ethereum can all be considered a Community. Each community has different compositions and scales of nodes, according to their characteristics and circumstances.

C-Node

C-Node (Community Node) is the building block of a Community that affects the consensus or decision-making process of Community governance. C-Nodes are available to both individuals and organizations (banks, brokers, insurers, schools, governments, etc.), and Node policies are determined by the members of each Community.

C-Rep

C-Rep (Community Representative) is the representative unit of Community that functions as the component of governance of ICON Republic. It has the right to vote on verification and governance of transactions in ICON Republic. C-Rep is selected according to the decision of each community, and C-Rep can be changed from one node to another. In other words, C-Rep duties are transferable depending on the situation and purpose of each governance. Furthermore, C-Rep will receive incentives for its maintenance and activation of ICON Republic.

ICON Republic

ICON Republic is the connector of different communities. It is comprised of representatives called C-

Rep, and other Citizen Nodes. ICON Republic's governance is determined by C-Rep votes, and hence, decentralized. ICON Republic functions as a communication channel between communities, and does not affect the governance of the communities.

Citizen Node

Citizen Node is a component of ICON Republic. Anyone can participate as Citizen Node by DAPPs created on *loopchain*. However, Citizen Node does not have voting rights for the governance of ICON Republic, and has only the right to create a transaction. Citizen Node can also be C-Rep with the right to vote if certain conditions are met.

2.5. How to Connect

The types of connections in the ICON Network are: ① Connection between nodes within a single Community, ② Connection between nodes within ICON Republic, ③ Connection between Community and ICON Republic, ④ Connection between different Communities

Connection between nodes within a single Community

Communities have the freedom choose or customize a blockchain that fit their need. Therefore, each Community such as finance, government, school, e-commerce, healthcare, Bitcoin, and Ethereum, can be organized into different blockchains and can utilize different consensus algorithms.

Connection between nodes within ICON Republic

ICON Republic is supported by *loopchain*. ICON Republic is designed to connect various communities both in the real world and crypto world, so that it adopts the consensus algorithm that allows real-time transaction processing. ICON Republic has governance which is different from that of each community, and operates on LFT (Loop Fault Tolerance) consensus algorithm.

Connection between Community and ICON Republic

Community and ICON Republic are connected in real-time via DEX (Decentralized Exchange). DEX sets currency reserves to provide exchange ratio in Community and ICON Republic in order to facilitate exchange values in real time based on that ratio. When it comes to the connection of Community that cannot reach a consensus in real time (e.g. Bitcoin, Ethereum, and Ethereum-based Cryptocurrency), the agreement within ICON Republic is suspended until consensus is completed.

Connection between different Communities

Connection between different Communities is available in ICON Republic. ICON Republic is connected to each community in real-time through DEX (Decentralized Exchange), while C-Node is also connected in real-time to other C-Nodes in different Communities via C-Rep and ICON Republic on the basis of ICX.

2.6. How to Operate

Community

Each community operates independently based on its own governance according to the characteristics of its own blockchain. Separate from ICON Republic, Communities can reach its own consensus to decide the consensus algorithm, consensus-participating Node, operation of a cryptocurrency in a Community.

ICON Republic

Governance of ICON Republic is determined by the consensus process of C-Reps, with the scope of governance limited to ICON Republic. ICON Republic does not affect the governance of other communities, but involves in the issuance and rewards policies of ICON Exchange Token ("ICX")

2.7. What to Expect

A wide variety of communities are beginning to be formed around the world for various business purposes and relationships in the field of finance, public service, logistics, healthcare, IoT, energy, manufacture, e-commerce, and much more. With the development and spread of blockchain technology, the number of these communities is expected to accelerate. In such an environment, many tasks are handled through Smart Contracts, and the role of centralized agencies and intermediaries is expected to either shrink or disappear.
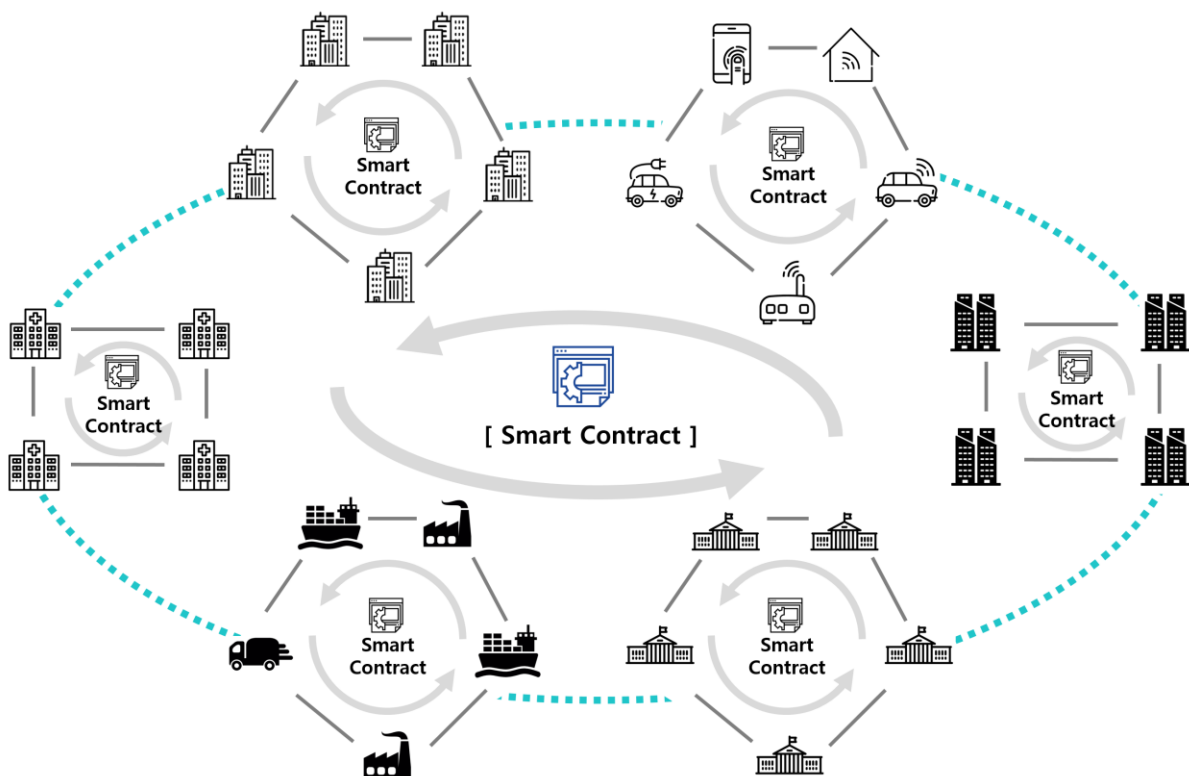
Smart Contracts not only revolutionizes the way members work within communities, but also affects the way communities work with other communities. In general, most communities begin with the goal of improving the work efficiency among the members, but in many cases, they evolve naturally in the direction of increasing interactions with the members of other communities. In this case, instead of handling external affairs through a separate centralized institution, Smart Contracts can reliably liaise the relationships.

Many pundits call blockchain technology a megatrend, and ICON has already positioned itself as the leader by creating an environment where all communities in ICON Republic are interconnected in real-time through Smart Contracts. Furthermore, as the number of communities connected through the ICON Network increases, the number of transactions increases exponentially, resulting in maximum utility of the network.

2.8. Implementation of loopchain

We are in the process of implementing our blockchain technology in various industry communities made up of reputable institutions, including capital markets, insurance, university, and healthcare. Each community has started to embrace the blockchain technology to solve existing inefficiencies and began to recognize the possibilities of expanding beyond respective communities by connecting with other communities. In a sense, ICON is a natural evolution of thriving blockchain ecosystem and is the solution to the need of bridging disparate blockchain communities.

Capital Markets

'Korea Financial Investment Blockchain Consortium,' the first industry-wide blockchain consortium backed by 25 securities firms, is leading the innovation of domestic capital markets with *loopchain*, a blockchain technology developed by theloop. The first blockchain service to be launched by the consortium in 2H 2017 is a BSI-based authentication, which enables direct authentication and generation/verification of digital signatures without the third party. The consortium plans to expand its blockchain services to other capital market processes, including post-trading and trading, through SCORE, the *loopchain*'s smart contract execution environment.
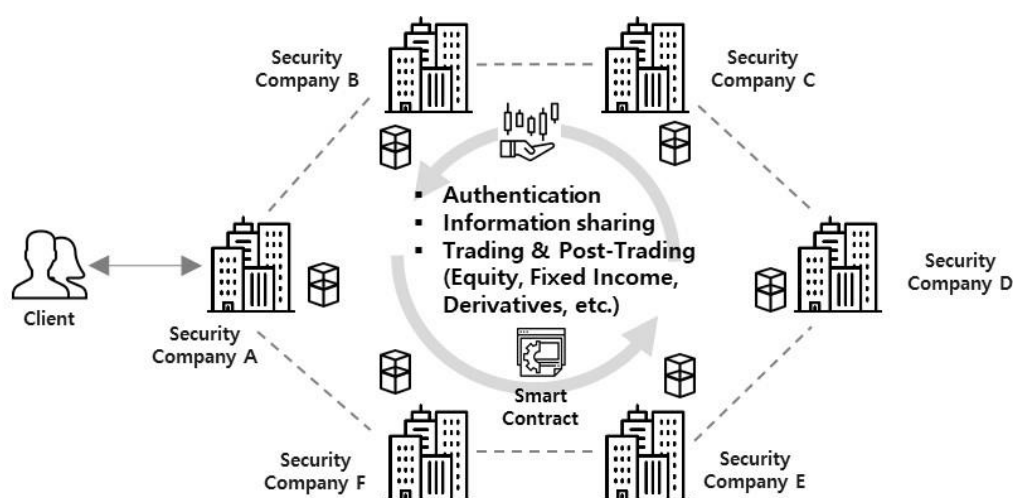
Throughout the global capital market, countless transactions are constantly being carried out through large group of intermediaries and centralized institutions. Because of these intermediaries, the transaction becomes lengthy and back-office work becomes complicated. In general, the clearing and settlement process (post-trading process) for stock transaction will take t+2 to t+3 days, and the United States alone spends over 9 billion dollars every year.

Insurance

The top-tiered life insurance company in Korea and major university hospitals are working together on a blockchain pilot project to incorporate theloop's blockchain technology into the insurance claims and payment process. This project aims to automate the entire insurance claiming process, from patient authentication to sending medical records to insurance providers, through blockchain technologies without any intermediaries. The pilot project will be implemented through SCORE, and plans to launch in early 2018 initially for select insurance products. The project received a government grant from the Ministry of Science, ICT and Future Planning in April 2017, and is expected to gain further momentum by adding more products and inviting other insurance providers to the consortium.

Blockchain is driving the innovation of the insurance industry throughout its value chain[10]. Innovation of claims and payment services not only can reduce the cost by improving the efficiency of the transaction process but also will greatly enhance consumer experience, thereby improving the overall satisfaction of the insurance industry.

Compared to those of other financial industries, transactions within the insurance industry frequently involves external parties (both in terms of data and transfer of funds). However, these external organizations generally operate on isolated system infrastructures unique to each institution, which hampers efficient transactions. By ensuring interoperability and mutual reliability of different systems, blockchain dramatically improves the efficiency of transactions between various organizations. As such, we believe blockchain technology will continue to attract vast amount of interest from the insurance sector and accelerate the transformation of the industry ecosystem.
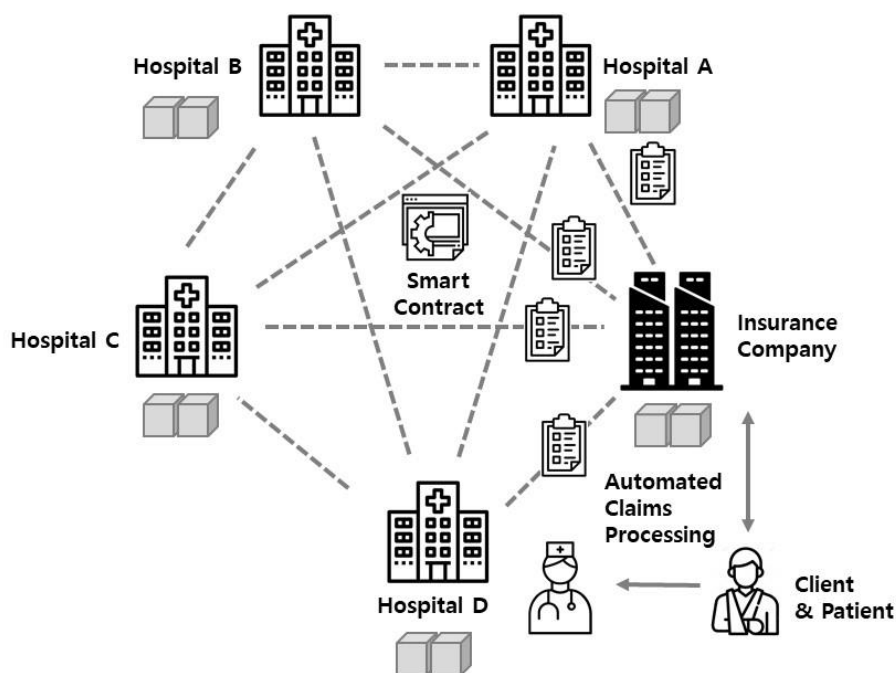
University

U-Coin ('University-Coin') is a cryptocurrency for university students in major universities in Korea. Scheduled to launch its pilot test by the end of 2017, U-Coin received a grant by the Ministry of Creation and Science in April 2017, and is expected to expand its services to other universities in Korea. Furthermore, U-Coin will expand its ecosystem by creating other cryptocurrency-based services that can be used in nearby communities and university towns, including cryptocurrency vending machines and easy payment/transfer systems.

University students are one of the most receptive to new technologies and have always been at the forefront of experiencing new innovations. Especially, with the pace of innovation accelerating, there are disparities between age generations in how they adopt and embrace new technologies. Similarly, the university students will play a significant role in the spread of this innovative technology.
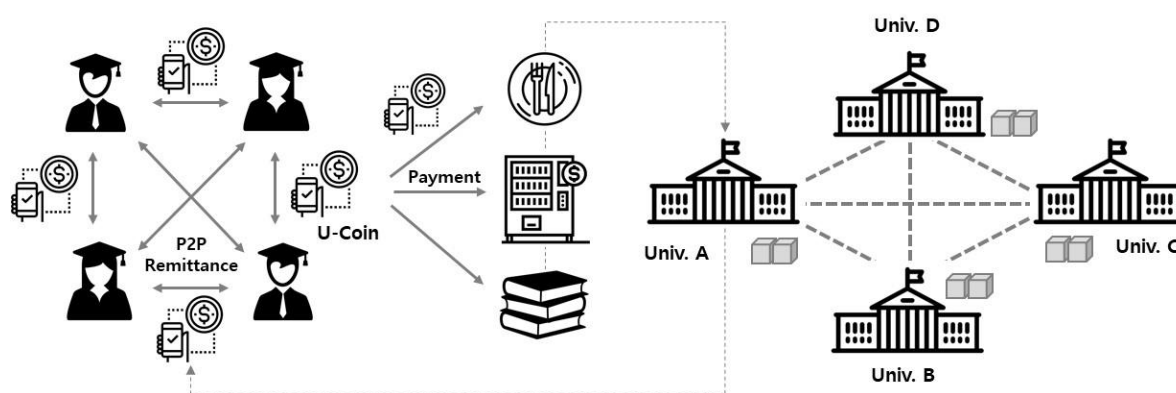

Healthcare

Precision Medical Hospital Information System (P-HIS) is the largest Healthcare blockchain consortium in Korea, joined by major domestic hospitals, and *loopchain* will provide the underlying blockchain technology.[11]. This project aims to build the network to share precision medical data in a secure manner, and plans broaden the scope of medical data distribution globally through global networks, including ODHSI (Observational Health Data Sciences and Informatics)[12]. This consortium is building a safe and transparent distribution system of medical information based on blockchain and promoting the introduction of cryptocurrencies to the ecosystem.

While sharing medical information is essential in improving the overall quality of medical services (e.g. prevention, diagnosis, treatment, research, etc.), improper disclosure or indiscriminate use of sensitive personal information can cause great damages. With the explosion of genomic information from next-generation sequencing ('NGS') and medical data from wearable devices, both interest and discussion about ways to securely share medical information have reached its all-time high.

Blockchain technology is emerging as an alternative solution to this sensitive and complex problem. Blockchain ensures the interoperability between different hospital systems, and manage the access rights to data and records reliably. We believe a secure distribution of medical information through blockchain and a fair reward system for those who share their data through the network will invigorate the medical ecosystem.
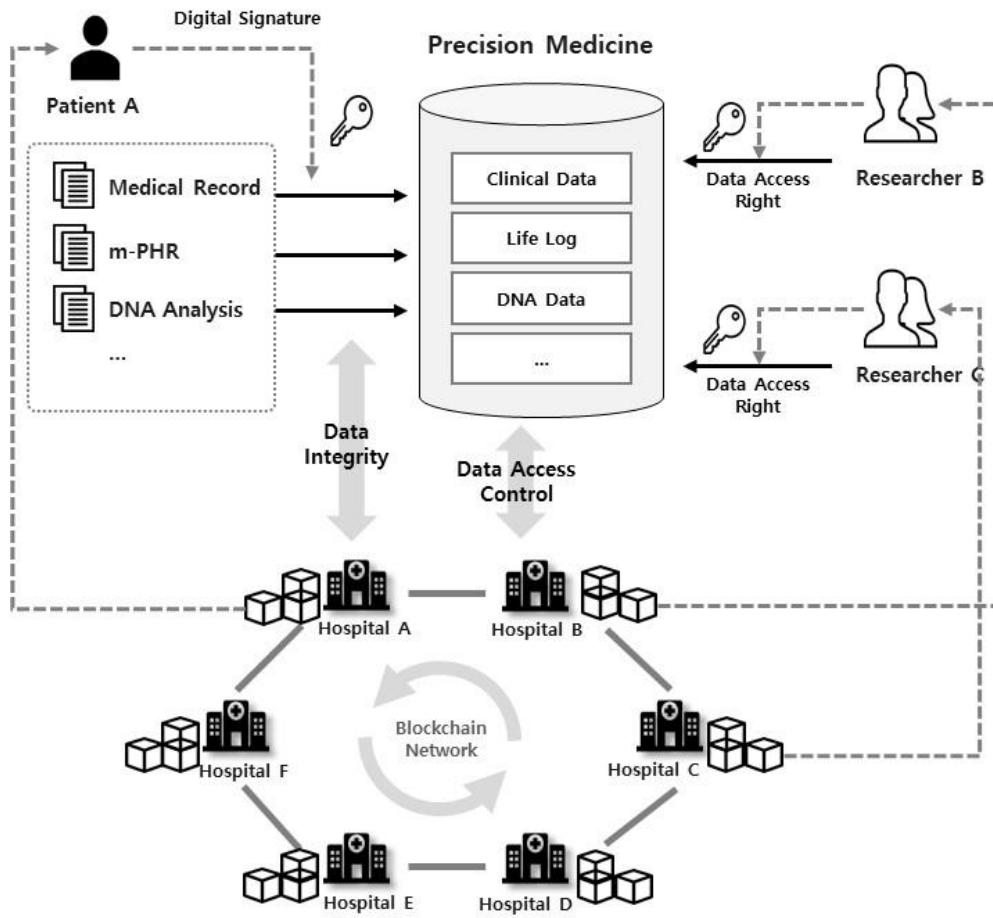
3. ICON Architecture

3.1. Introduction

ICON constitutes a network where various blockchain-based independent Communities are connected via C-Rep to form a greater community, or ICON Republic. In basic ICON architecture, Nexus supports ICON Republic while Portals support C-Reps allowing blockchains to be connected to Nexus so that tokens can be transferred with speed and trust. A Nexus can connect to another Nexus, and this allows blockchain networks to scale and expand in diverse ways.

3.2. Conceptual Model

With ICON, numbers of blockchains are connected around Nexus via Portal. Nexus is a *loopchain*-based blockchain. It realizes a decentralized governance by allowing Portals and different nodes to participate. Blockchain Transmission Protocol (BTP) facilitates transactions among independent blockchains connected to Nexus through respective Portals. This structure, connecting a network with one type of governance to another network, is same as that of Internet that connects every computer into one communication network by establishing 'Networks of Networks'.
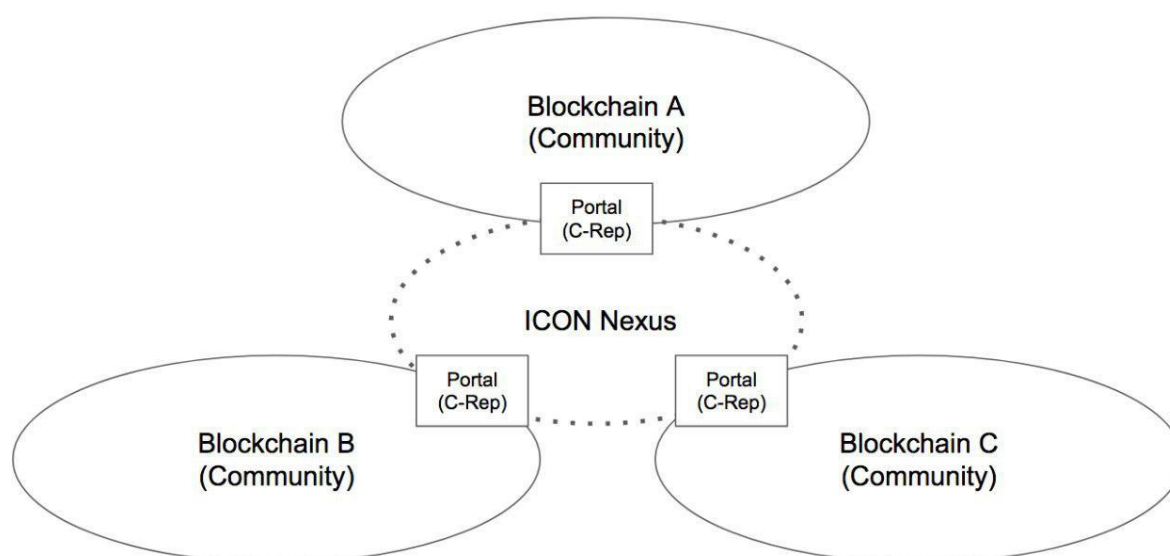
Internet is a computer network system across the globe that connects the world with standard Internet protocol called TCP/IP. Likewise, ICON uses BTP as the standard protocol. In order to construct a massive network of blockchains, it guarantees independent governance to different blockchains and makes mutual connections only when they are needed. It does not connect every participant to a single blockchain.

3.3. Nexus

Nexus is a Multi-Channel blockchain comprised of Light Client of respective blockchains. Each blockchain is connected to Nexus via Portal and each Portal, basically the representative of independent networks, participates in Nexus blockchain network as a node. Since Nexus is built on the basis of *loopchain*, its consensus is reached based on LFT consensus algorithm, one of the *loopchain*

features with unique functions of grouping and voting rights adjustment. Nexus includes a Representation channel through which operational policies are proposed and selected by voting. Each Portal, as the C-Rep representing its community, participates in the Representation channel.

Tokens called ICX (ICON Exchange) are embedded in Nexus and the interconnected blockchains can use ICX to transfer values. Nexus incorporates Reserve channels that can issue ICX according to the policies. In principle, every node that constitutes Nexus can issue ICX token by participating in Reserve channel. As a blockchain itself, Nexus can be connected to another Nexus, allowing different blockchains with different governance structures to execute transactions and exchange values.

3.4. Portal

As a component that connects independent blockchain to Nexus, Portals are connected to Nexus through BTP. Depending on the policy of respective blockchain, Portal can be organized by a single node or multiple nodes, or it can make another form of consensus network to serve the different needs.

This structure can be thought as a SWIFT[13] system where each country has its own currency system but multiple banks within one country are able to be connected through the SWIFT network. Likewise, the number of nodes in Nexus can also be single or plural. Nodes are managed in one group by *loopchain*'s grouping function and the voting of the nodes should comply to the Nexus policy. Portal represents its own blockchain as a C-Rep and votes for the policies via Representation channel to realize a decentralized governance.
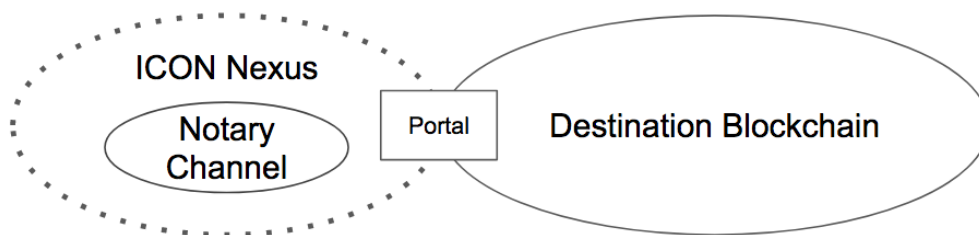
3.5. BTP (Blockchain Transmission Protocol)

BTP is a protocol to connect transactions among blockchains that are linked to Nexus. It is through the Notary channels in Nexus that the Transmitter blockchain transfers the transactions to the Receiver blockchain.

In this sense, Nexus nodes with voting rights to the Notary channels possess multiple channels, where the Light Client of each blockchain connected to Nexus is counted as one channel. A Notary channel is implemented based on Multi-Channel function of *loopchain*. It can identify the transactions confirmed by respective blockchains through the blockchain's Light Client connected to Nexus.
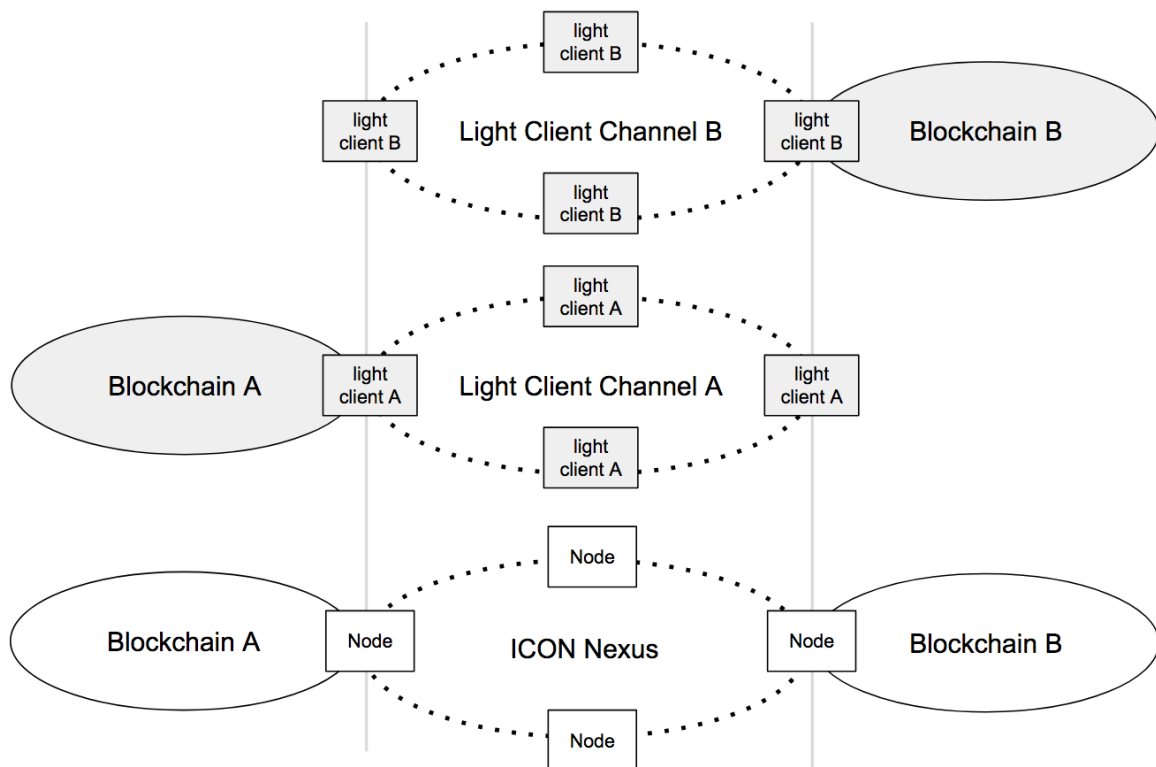
Multiple signatures of nodes with voting rights to Notary registration request are contained in blocks and these blocks form blockchains of Notary channel. The block data with the transactions registered to Notary channel will then be transmitted to the Receiver blockchain via Portal. When the Receiver blockchain verifies the relevant block data, it validates the signature of each node based on the certificates of nodes from Notary channel. If two-thirds or more of the signatures are confirmed according to the Notary channel standards which follows the LFT consensus algorithm, the agreement will be confirmed and the requested transaction will be executed.


Multiple signatures of nodes with voting rights to Notary registration request are contained in blocks and these blocks form blockchains of Notary channel. The block data with the transactions registered to Notary channel will then be transmitted to the Receiver blockchain via Portal. When the Receiver blockchain verifies the relevant block data, it validates the signature of each node based on the certificates of nodes from Notary channel. If two-thirds or more of the signatures are confirmed according to the Notary channel standards which follows the LFT consensus algorithm, the agreement will be confirmed and the requested transaction will be executed.
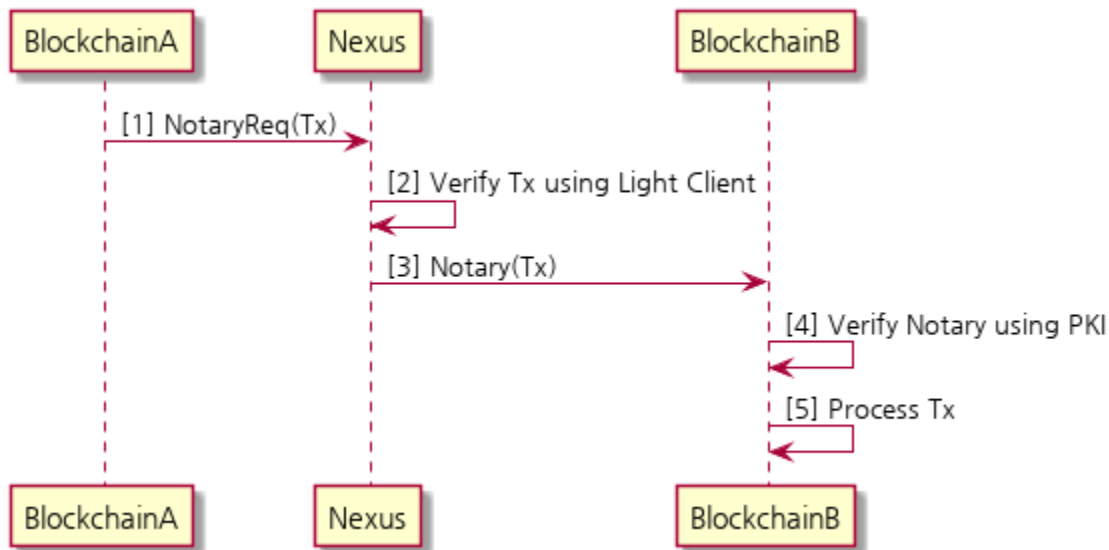
3.6. DEX (Decentralized Exchange)

DEX[14] is a trading market that executes transactions automatically on a blockchain, rather than a centralized exchange that relies on a trusted third party, typically represented by cryptocurrency exchanges. Although centralized exchanges are easy to use and are available of various types of transactions such as reserved transactions and margin transactions, users have to completely trust the exchange and anonymous transactions are difficult to take place since users have to sign up before use. In particular, users are the ones who suffer from the damage when accidents such as hacking break out, as in the case of the Mt.Gox incident[15]. DEX, on the other hand, enables automated transactions without the need to trust a particular exchange, supports completely anonymous transactions, and is free from problems such as server breakdown and hacking. Bitsquare[16] and Bitshares[17] are some examples of DEX, but they had some issues of users always having to be online during the transactions, in addition to issues regarding liquidity.

As a blockchain network that links multiple blockchains with their own unique governance, ICON provides DEX based on ICX. It enables transactions among different cryptocurrencies by determining the exchange rate through Reserve based on the Bancor Protocol[18].

For transactions between ETH and ICX, DEX can be comprised of nodes with voting rights to Reserve Smart Contracts within Ethereum and ICON. In this case, the price of ICX is determined according to the following equation:

$$ReserveBalance = ReserveRate \times ICXVolume \times ICXPrice$$

$$ICXPrice = \frac{ReserveBalance}{ReserveRate \times ICXVolume}$$

If one purchases ICX with ETH via DEX, the Reserve Balance composed of ETH increases and the ICX Volume decreases, resulting in an increase in the ICX Price. Conversely, buying ETH with ICX reduces the Reserve Balance and increases the ICX Volume, resulting in a decrease in the ICX Price. Please refer to the Formulas for Bancor system[19] for the details on the purchase price and ICX token number calculation.

If ICX is listed and traded on another exchange, its value at the corresponding exchange and the value

at ICON DEX may be different. In this case, arbitrage transactions which lead to ETH inflow and exchange will take place, thereby resulting in similar price levels of ICX.

Such an ICX-based DEX scheme enables trading of the cryptocurrencies of various independent blockchains connected to ICON. In the case of blockchains that use BFT[20] series consensus algorithms in particular, such as *loopchain*, exchanges are processed in real time. For example, if there is a blockchain for financial institutions connected to Nexus and a cryptocurrency called Fcoin used only among the concerned financial institutions, Fcoin DEX service is provided based on the Reserve made up of Fcoin and ICX, in which Fcoin and ICX can be traded in real time. Moreover, since the converted ICX can then be used for exchange with other cryptocurrencies connected to ICON, transactions among different cryptocurrencies are ultimately realized.

Another key feature of ICON DEX is that it can establish an A.I. Analysis Model[21] based on the accumulated data such as total call volume, transaction frequency, and price involved in transactions among different cryptocurrencies. Such data enable various adjustments of features such as the Reserve Rate and the Reserve composition ratio of each cryptocurrency, which in turn create a stable cryptocurrency that can be used in real life.

3.7. Nexus Public Channel

Nexus includes a Public Channel opened to anyone. It is embodied in Nexus through the Multi-channel function of the *loopchain*. Anybody can participate in the Public Channel as the name implies. Users participating in the Public Channel can not only participate in ICX transactions, but can also create and use various DAPPs[22]. The concept of DAPPs in Public Channel is similar to that of Ethereum, but there are differences in how it is deployed and executed. Ethereum includes the compiled codes in the transaction data and executes the codes with Virtual Machine (VM). On the other hand, in Public Channel, DAPPs are developed and registered in the DAPPs Store in advance; nodes that want to participate in the transaction must download and install DAPPs from the DAPPs Store in order to use it.

Nodes participating in the Public Channel are divided into Light-Client-based nodes that can register and confirm transactions and Full Nodes which validate the transactions. Full Nodes are chosen by Representation channels, the consensus channels of Nexus, and receive incentives when they validate transactions. In addition, Light Client nodes can also receive incentives according to various criteria such as the transaction size or the amount of ICX deposit.
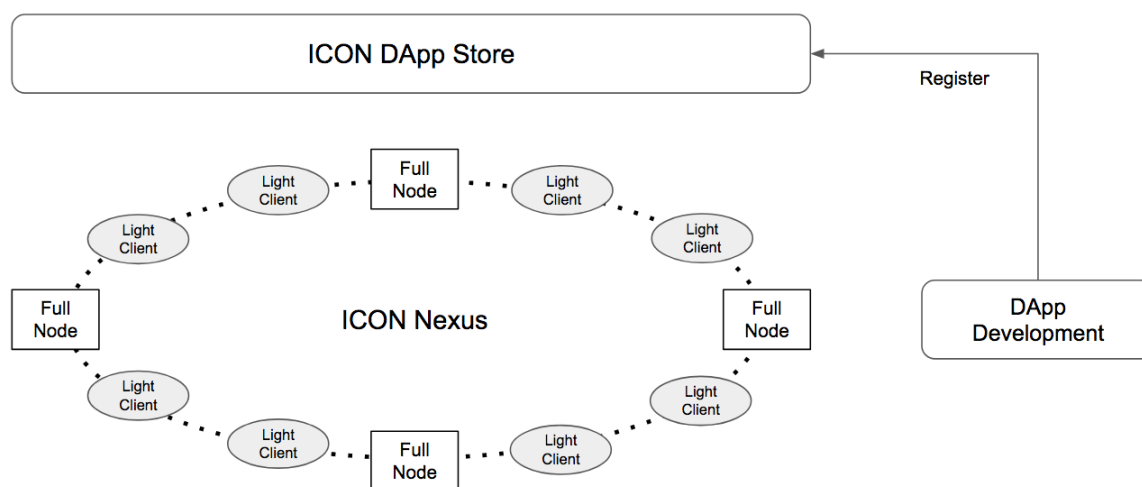
3.8. Governance

ICON essentially aims for a decentralized governance. Each blockchain connected to Nexus holds its own governance, and Nexus progresses discussions with an equal level of representation on behalf of each independent blockchain like an indirect democracy [23]. To this end, Nexus also includes Representation channels to propose policies and cast votes, Reserve channel to issue and manage ICX, in addition to Notary channels to process BTP.

Representation channel

Representation channel is a blockchain channel composed of nodes that participate as a C-Rep and thus have the right to vote. It is a consensus system that decides the rules of all issues take place in Nexus. It is basically through C-Rep that blockchains connected to Nexus hold the voting rights. Other nodes such as nodes that support off-chain transactions [24] of ICX exchange and banks can also participate in Representation channels. In a Representation channel, one can manage node policies regarding node addition and removal in Nexus, adjust ICX transaction fee, manage node selection and removal from Notary channel, Representation channel, and Reserve channel. In addition, one can also discuss the policy regarding voting rights of nodes from different channels. The policy that sets up the voting right is similar to an Electoral College System. By allocating the number of votes eligible in proportion to the community size and the transaction scale, it can reinforce the status of relatively small communities.

Reserve channel

Reserve channel is a blockchain channel composed of nodes that can generate ICX in Nexus. When the Genesis block is created, ICX will be issued according to predefined rules and the issued ICX will be stored in Public Treasury of Nexus. At this stage, an A.I. analysis model will be established based on total money supply and transaction size to decide the issue amount according to inflation rate and exchange rate.

Anyone can participate in Reserve channel and participating nodes can issue bonds that can purchase ICX issued from Nexus. The bond limit is determined based on its contribution to invigorate the ICON Network. Afterwards, the nodes participating in Reserve channel can issue their own bonds as much as they need, exchange them for ICX, and distribute ICX. Nexus can withdraw the bonds, which was issued by these nodes and exchanged for ICX, can exercise the bonds to withdraw ICX as needed in order to manage total money supply.

Incentives

Transaction fees of ICX transaction and other types of transactions from different channels are stored in Public Treasury of Nexus together with ICX, which is steadily generated by Reserve channel.

ICX stored in Public Treasury is exchanged for bonds of nodes participating in Nexus and distributed to the respective nodes. The limit of the bond depends on how much the node has contributed to invigorate the ICON Network. A scoring system called IISS (ICON Incentives Scoring System) is applied here with a variety of criteria: the node's 1) frozen ICX, 2) C-Rep status, 3) ICX exchange volume, 4) ICX exchange volume of the whole community if it has one, 5) ICX volume traded through DEX if it has one, and so on. Scoring model calculated according to these standards of IISS will be consistently updated to invigorate the ICON Network to the maximum on the basis of A.I. prediction model[25].

According to IISS, the more actively the nodes participate in the ICON Network, the more ICX they can secure.

Nodes participating in Reserve channel can use the acquired ICX as the basis for business such as banking. One can issue bonds of higher limit based on ICX transaction volume and the ICX secured by enlisting customers in a variety of deposit products, and then secure more ICX based on the relevant bonds to pay for interests on the deposits.

A variety of services, in addition to banking, can be operated through DAPPs of Public channel. Besides making profit from charging fees on the services, one can also benefit from securing ICX allocated by IISS, which may activate a variety of services. One can also receive predefined incentives in ICX after participating in Representation channel to conduct proposal and cast vote.

4. Inside ICON

At the core of ICON is *loopchain. loopchain* is a high-performance blockchain that can provide real-time transaction, which is based on enhanced Smart Contract.

4.1. loopchain

Bitcoin[26], most synonymously used for virtual currency, is a distributed ledger that actually verifies the reliability of blockchain technology. Early blockchain technologies mainly focused on virtual currencies. This led to the introduction of various virtual currencies which are actively traded through private exchanges. Unfortunately, the early blockchain technologies have failed to attract traditional financial institutions to implement this technology into their operations. However, with the introduction of Ethereum[27] and the concept of Smart Contract[28], the blockchain technology has entered a new phase with explosive interest from the industry. Smart Contract can allow transactions to be executed without trusted third party, and the blockchain technology, which previously remained as a mere ledger for transactions, was transformed into an application platform.

We have seen various attempts to embody transactions without trusted third party using public blockchain platforms, such as Ethereum, within the finance industry. However, the transaction speed of 7~15 TPS (transactions per second)[29] and the public nature of nodes greatly limited the implementation of the blockchain technology to highly regulated financial sectors. In order to overcome such limitations, the need for enterprise blockchain technologies where only validated nodes can participated in the transaction emerged. Hyperledger Fabric[30] and R3 Corda[31] have been leading this effort to introduce enterprise blockchain technology to various industries including finance, supply chain, and public sectors.

Since majority of industries have different operational requirements and governance structures, an enterprise blockchain with flexible features is necessary to accommodate such diverse needs. This idea was the start of *loopchain. loopchain* is a high-performance enterprise blockchain with Smart Contract features that can be customized according to operational needs and linked with other distributed ledger networks.

4.2. Features

Consensus

LFT (Loop Fault Tolerance) is an enhanced BFT (Byzantine Fault Tolerance)[32]-based algorithm that promotes faster consensus and ensures the finality of the consensus without the possibility of forks within the network. LFT supports faster consensus by creating a group among trusted nodes. LFT can accommodate diverse consensus structure by allowing such groups or nodes to freely determine the number of votes.

SCORE (Smart Contract On Reliable Environment)

SCORE is an enhanced Smart Contract feature of *loopchain* that ensures high-performance contracts to run directly in the node operation environment without a separate Virtual Machine (VM). SCORE is easily deployable and can be created for various applications as it runs separate from the underlying blockchain processes.

Multi-Channel

Multi-channel[33] feature allows independent channels to be created within the same blockchain network and execute request, consensus, and Smart Contracts. Since the channel is established with only two business nodes, integrity and assurance are ensured on a channel-by-channel basis, and transaction data is held only by actual transaction parties.

Tiered System

Apart from the initial authentication process to participate in a blockchain network, each transaction is validated and secured through PKI-based authentication. *loopchain* can also set different access privileges to create nodes with specific functions (e.g. audit, supervision) to monitor certain transactions, if necessary, without participating in the actual transaction.

4.3. Consensus

Background

Bitcoin, the first service to implement blockchain, has achieved the consensus of all bitcoin nodes transaction ledger in a network of a global scale using algorithm of Proof of Work[34]. However, the algorithm of Proof of work used in Bitcoin experienced difficulties under the circumstances requiring efficiency and spontaneity of payment due to low processing speed, inefficient energy usage, and partial network split.

To resolve this type of the problem, we started to use BFT (Byzantine Fault Tolerance)[35] series consensus algorithm mainly used for a traditional state machine replication. For data consensus, BFT series consensus algorithms (famous for PBFT (Practical Byzantine Fault Tolerance)[36]), make consensus by voting for validation of data and sharing the results. Tendermint[37] announced blockchain consensus algorithm that modified PBFT algorithm into DPOS (Delegated Proof Of Stake). In addition, IBM Fabric, a private blockchain project for enterprise, chose PBFT as a consensus algorithm in version 0.6. and attempted to utilize SBFT (Simple Byzantine Fault Tolerance) that simplified PBFT as a consensus algorithm for Orderer service in version 1.0.

LFT (Loop Fault Tolerance)

LFT is a traditional BFT consensus algorithm that improved Raft[38] algorithm, one of the State machine replication[39] algorithms that is often used as Fault Tolerance mechanism in the current distributed environment, to be Byzantine Fault Tolerant and optimize itself to the nature of blockchain network.
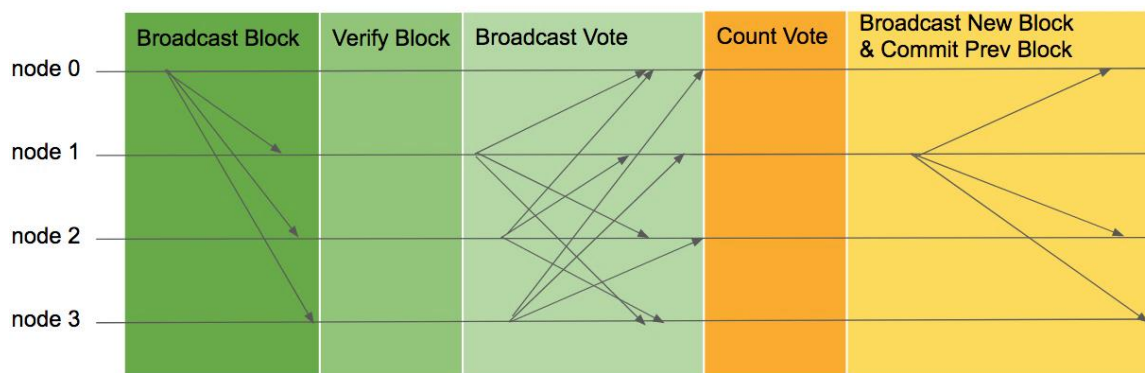
The object that organizes the blockchain network is called node. These nodes are responsible for generation, validation, retention of blocks and each node can create a signature that can distinguish its own message. Most of the networks using consensus BFT series algorithms can be divided into leader nodes and validation nodes. Leader nodes vote for validation of a block by verifying the contents that leader has made. LFT can be also divided into leader nodes and validation nodes.

In the initial stage of the network, verification nodes transfer the transactions that need to be executed to the leader node. The leader node then creates a block from collected transactions and transfers the block to all the other verification nodes with its own signature. When each verification node receives the block, they 1) confirm the creation of the block, 2) check if the block level and the prior block hash are correct, and 3) validate the block data. If step 1 to 3 are correct, 'vote data' is generated and shared to all nodes. It is important to transmit vote data to every node. If leader node is Byzantine, it is possible to separate certain nodes from the network by transmitting blocks only to the nodes that is above the quorum. To prohibit this sort of problem, vote data is transmitted to every node. A node without any block can know if the block is created or not and also request the block to the others.

To create blocks, leader receives vote data from nodes more than quorum. Leader creates new blocks with vote data and transmits to every node. This saves the need to transmit every data once again to guarantee that nodes more than the quorum have finished the same vote. It also allows to confirm the block by verifying the vote of new blocks. If transmitted block is not the initial one, validated node performs verification of vote data more than quorum when verifying blocks. This is when every node final commits prior blocks.

The blockchain is a technique for nodes without trust to construct a trust network through distributed data agreement. Not every state machine guarantees a response like the current state machine replication system. Each node provides a service and creates a transaction. Leader nodes can reject a transaction of a specific node when a block is created. To minimize this problem, Spinning[40] was used to reduce the number of service faults that could be caused by the Byzantine leader by replacing the leader for every block creation. In addition, we have developed a method to directly tolerate a fault handler by avoiding the complicated leader fault tolerance algorithm used in existing algorithms such as Tangora[41].

LFT is a distributed consensus algorithm for permissioned blockchain. We improved the existing BFT algorithm for the blockchain and simplified the process using block data. Details of the consensus process can be found in LFT white paper[42].

4.4. SCORE (Smart Contract on Reliable Environment)

SCORE indicates Smart Contract provided from *loopchain*. SCORE ensures a high-performance since it runs directly in real runtime but not a separate VM. It is executed on a runtime based on a container separated from basic blockchain process, so the basic blockchain process can still function properly even if there is problem with Smart Contract.

One of the key characteristics of SCORE is the repository based versioning features. Generally, when a Smart Contract is updated, data migration is required. However, with our versioning capability, Smart Contract does not require data migration with every update. This means that Smart Contract update process is easy and quick.

It provides a local repository by default for SCORE distribution, and developers can easily deploy and update Smart Contracts by using a remote repository called SCORE Store.
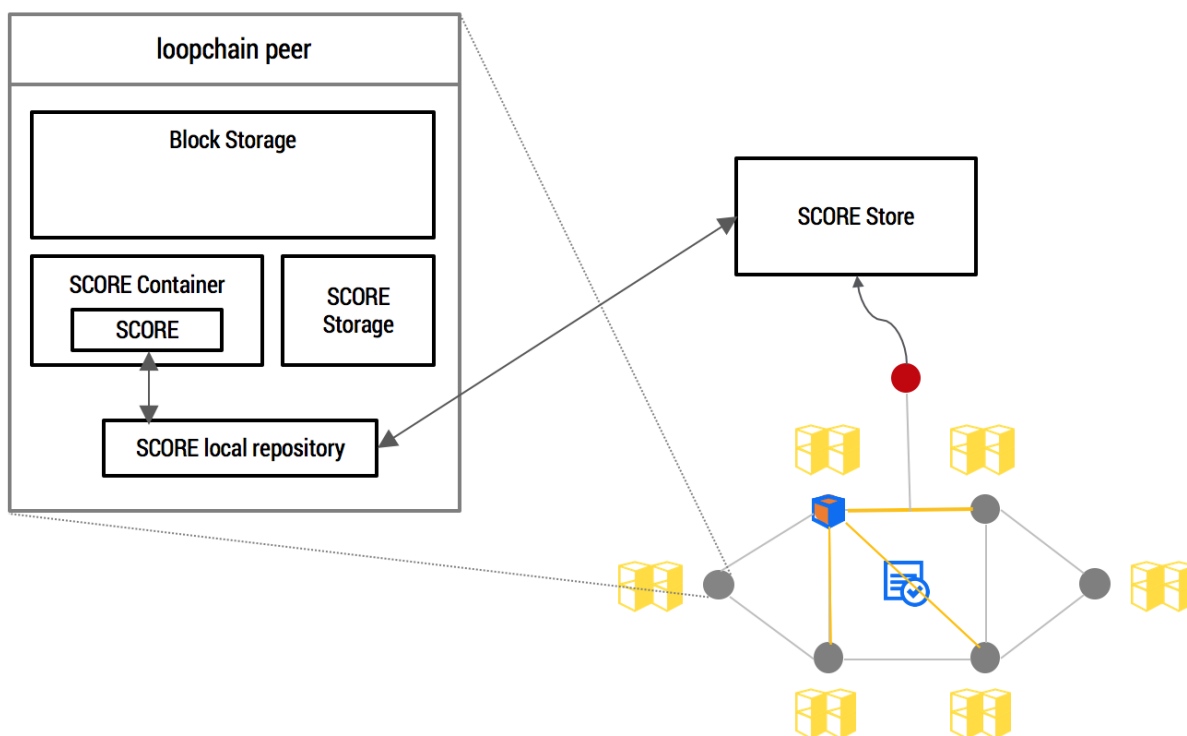
4.5. BSI (Blockchain Signature Infrastructure)

BSI is based on Smart Contract to enables the construction of digital signature infrastructures like Public Key Infrastructure (PKI). In the existing PKI, a separate Trusted Third Party (TTP) that has no relation to the transactions was needed to store keys safely and issue/manage certificates using the keys.

However, BSI does not need to manage separate keys for certificate issuance, since it issues X.509 certificates which are issued by creating digital signature on the basis of information that can process Merkle tree based Proof of Existence. In *loopchain*, BSI-based certificates are issued to nodes participating as Light Client[43], in addition to normal nodes participating validation and consensus, to use as digital signature to authentication and transaction of relevant nodes.

- **Components**
  - ✓ Users: Generate PKI-based key pairs and manage issued certificates
  - ✓ RA (Registration Authority): Identifies the user and requests for certificate issuance
  - ✓ CA (Certificate Authority) SCORE: Provides services related to certificate issuance by Smart Contracts on *loopchain* rather than separate institutions

5. Roadmap

5.1. Business Roadmap

Date	Description
2017 Q3	• Open source of *loopchain* • 1st Developers meet-up • Partnership with major bank
2017 Q4	• ICO • Listing of ICX • Financial Investment Consortium: Blockchain ID service open • U-Coin pilot service open: 3 Universities • Insurance: Blockchain based auto-claim pilot service open
2018 Q1	• 2nd Developers meet-up • Expansion of DEX reserve pool to most of major cryptocurrencies • Expansion of partnership with blockchain networks
2018 Q3	• 3rd Developers meet-up • U-Coin Expansion: 10 Universities • Financial Investment Consortium: Second service launch

5.2. Technical Roadmap

| Date	Version	Description
2017 Q3	V1 RC	• Nexus Testnet launch
2017 Q4	V1 GA	• Nexus Mainnet launch • Reserve channel open • IISS implementation • DEX(Ethereum/ICX) launch • Wallet Web/iOS/Android
2018 Q1	V2	• Representation channel open • Public channel open • A.I. advisor launch

6. ICX token

6.1. Term Summary

- Target Amount offered: 150,000 ETH

- Currency accepted: ETH Only

- Fixed Price: 0.0004 ETH per 1 ICX (2,500 ICX per 1ETH)

- Duration: Token Sale will close early if target amount is reached

- Offering Summary

Topic	Description
ICX Token	• ICX is a *loopchain*-based smart contract digital protocol that facilitates, verifies, and enacts a negotiated agreement between consenting parties within ICON
The Issuer	• ICON Foundation, a Swiss nonprofit organization
Rights	• ICX represents limited license to validate the ICON and DEX • No voting or membership rights • No sharing of revenue, dividends, equity, etc.
Refunds	• None
Redemption	• Buyback option in open market (treasury) • Regulatory redemption
Listing	• DEX (immediate with ETH) • Exchange partners

6.2. Allocation
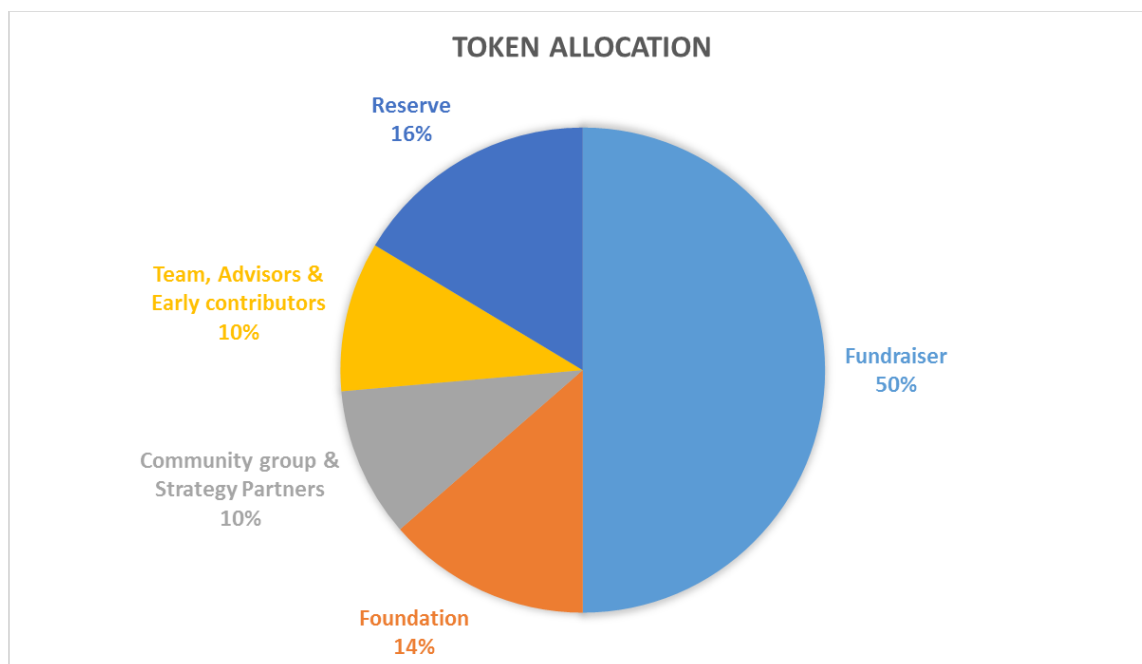
TOKEN ALLOCATION

- Expected allocation of the ICX Token are Fundraiser 50%, Foundation 14%, Community Group & Strategy Partners 10%, Team, Advisors & Early Contributors 10%, and Reserve 16%.

6.3. Use of Proceeds
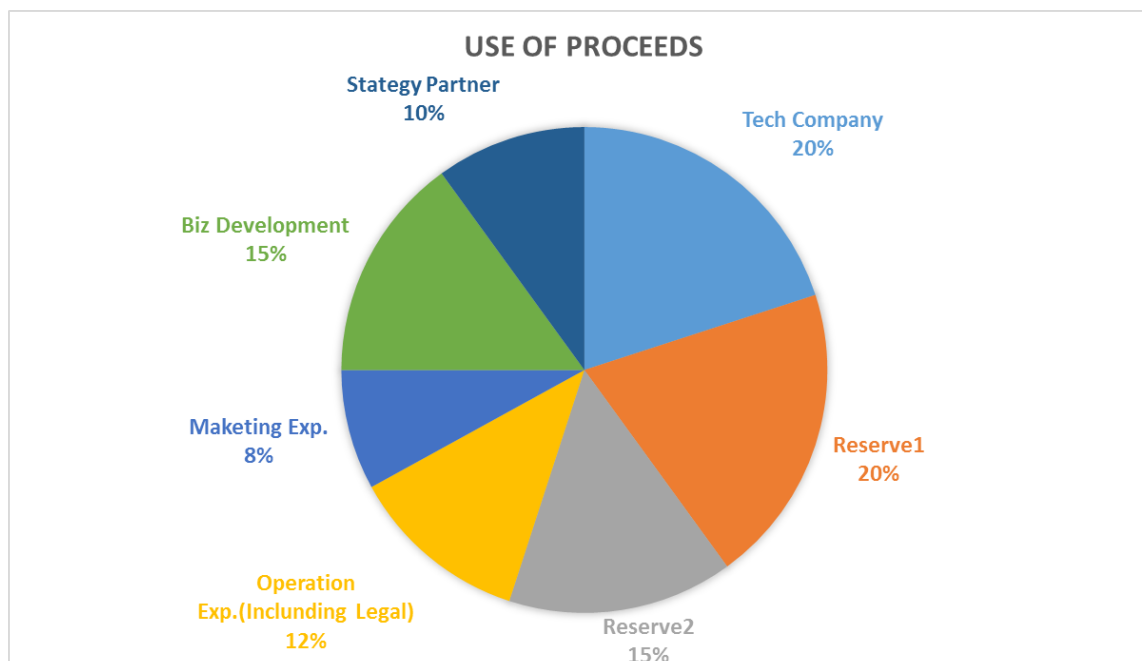
USE OF PROCEEDS

- Selected key use of proceeds are Tech Company, Reserve, Foundation Operating, Business development, and Strategy Partner.

- Tech Company: Development expense for blockchain engine, DAPPs, artificial intelligence, etc.

- Reserve: Required for real-time DEX with other blockchain network. Reserve is divided into Reserve1 (ETH Reserve) and Reserve2 (Other Reserve) Reserve1 is required for DEX with Ethereum based networks, and Reserve2 is required for DEX with other non-Ethereum based networks.

- Foundation expense: Covers operating expenses, marketing fees, legal & account fees associated with the ICON Foundation

- Business development fee: Fees associated with the global expansion of the ICON Foundation, including offices and business development related expenses

- Strategy Partner: Costs associated with ICX expansion, which are provided to the Global Business Partner

7. Issuance and Incentives

7.1. Issuance Policy

Issuance

ICX can be issued up to 20% of total volume annually with the consensus of ICON Republic, taking into consideration the ICX trading volume, DEX trading volume, freezing volume, and transaction fee. However, ICX is not directly issued but by providing nodes with the right to issuance. These rights are granted to the nodes on ICON Republic, and each node is entitled to receive ICX from the ICON Foundation by exercising its rights. Each Node may exercise its rights at any time and does not have to exercise immediately.

Rights granted to each node are determined based on the ICX Issuing Scoring System (IISS), and each node is granted in accordance to its IISS score. Nodes in ICON Republic can acquire ICX by exercising their rights.

IISS (ICON Incentives Scoring System)

IISS is an artificial intelligence (AI) based evaluation system for effective ICX distribution policy. IISS is based on a financial AI solution called 'DAVinCI,' which uses machine learning technology to enhance CSS (Credit Scoring System) of existing financial institutions. DAVinCI's AI algorithm provides an optimal prediction model for ICON Republic.

Moreover, components including ICX transaction volume, DEX transaction volume, freezing volume, and transaction fee will be used as important evaluation criteria for IISS. IISS relies on DAVinCI to continuously analyze, learn, and evolve relevant data on ICON Republic.

7.2. Transaction Fee

The transaction fee is set at 0.01 ICX per transaction to protect against DDOS attacks. The transaction fee is paid in ICX, and other tokens can be converted into ICX through DEX. Newly generated transaction fees are reserved in the Public Treasury, from which the nodes can withdraw their ICX through exercise of rights. Transaction fee can be modified through governance consensus.

7.3. Public Treasury

Public Treasury is a public wallet that is responsible for the issuance and storage of ICX. The Public Treasury operates according to the policies agreed upon by ICON Republic.

7.4. Incentives

Incentives are provided to all nodes in ICON Republic. Incentives are provided automatically through IISS and granted in the form of the right to issue ICX.

7.5. Freezing Fee

Freezing allows ICX to be deposited in the DEX Reserve Pool, allowing all participants with ICX to freeze their ICX. The volume of 'Frozen' ICX is one of the significant evaluation criteria of IISS.

Appendix

A.1. Definitions

Transaction(Tx)

- A unit of information. Contains information that needs to be saved using blockchain.

Block

- A single container containing a collection of multiple transactions. Contains one or multiple Transactions.

Peer

- Represents one peer on the P2P network. Most blockchain tasks are performed by peers.
- Create Transaction
- Exchanges Block and Transaction on P2P network

Leader Peer

- The Peer that can create a Block among Peers in the P2P network
- Creates a Block by collecting Transactions on a regular basis and distributes the Block on the Network
- Collects Transactions created by each Peer

Radio Station

- Creates Group
- Connects Peers with Group
- All running Peers connect to Radio Station to obtain the connection status of the neighboring peers in the group
- Monitors the status of each Peer

SCORE

- Smart Contract supported by *loopchain*
- A Function that alters the state value with Transaction as an input value
- Runs after the Block is verified and a new Block is added

Service System

- An application system that attempts to use a blockchain. It may be a Legacy system that has been used before, or a Service that is newly created

A.2. SCORE

SCORE Code Configuration

```python
#!/usr/bin/env python
# -*- coding: utf-8 -*-

from loopchain.blockchain import ScoreBase


class UserScore(ScoreBase):
    """ 기본 SCORE 코드
        기본 SCORE 코드는 아무런 역활을 하지 않는다
    """
    def invoke(self, block):
        pass

    def query(self, **kwargs):
        pass
```
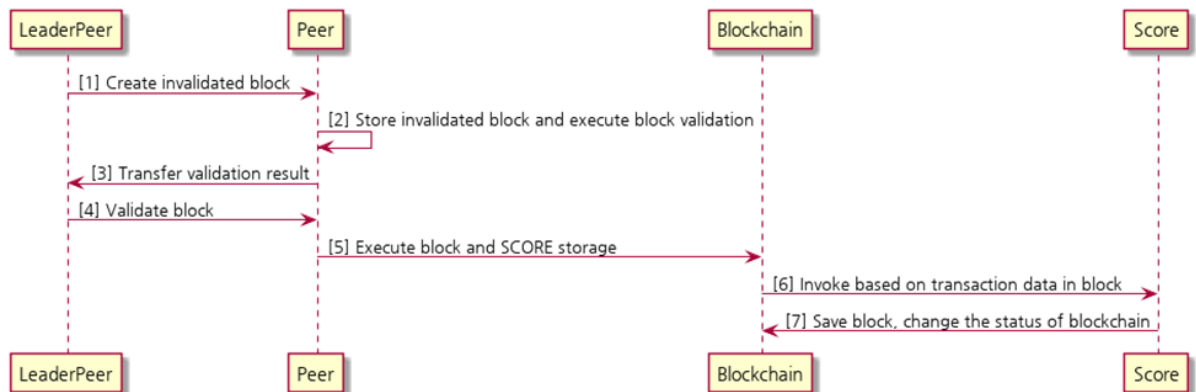
The function of each function is as follows.

- invoke() : adds data of a verified Block to a separate embedded database

- query(): query internal data

SCORE Processing Flow

Conditions

- Peer owns Score

- Provided separately

Sequence

① LeaderPeer creates an invalidated block

② Peer saves the invalidated block in a blockchain, and sends the verification result to LeaderPeer

③ LeaderPeer verifies the invalidated block based on the verification result sent by Peer(s)

④ Transfers the invoke() function of block and SCORE through Parameter when Peer saves the verified block in a blockchain

⑤ SCORE needs to inherit, write and add a class called ScoreBase. An actual transfer of information takes place.

⑥ Runs the invoke() function by putting in the data of the Transaction which is included in the block inside SCORE

⑦ Saves the result of execution in SCORE storage, or takes Action

⑧ Saves block in the blockchain

## A.3. Integration of loopchain and Legacy Systems

It is accessible to the blockchain peer in REST API through *loopchain* proxy. A task-specific *loopchain* Application SDK, which is "wrapped" so that it can be easily used according to legacy environment and different tasks, is provided as well. This enables business development just by calling API.
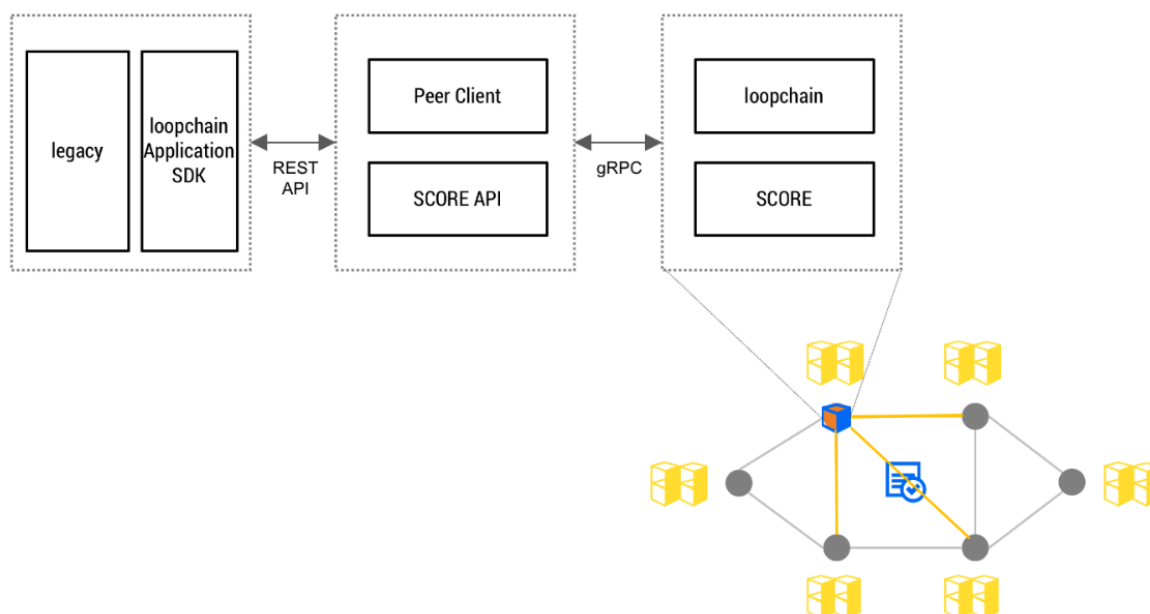
A.4. loopchain Multi-channel

It is accessible to the blockchain peer in REST API through *loopchain* proxy. A task-specific *loopchain* Application SDK, which is "wrapped" so that it can be easily used according to legacy environment and different tasks, is provided as well. This enables business development just by calling API.
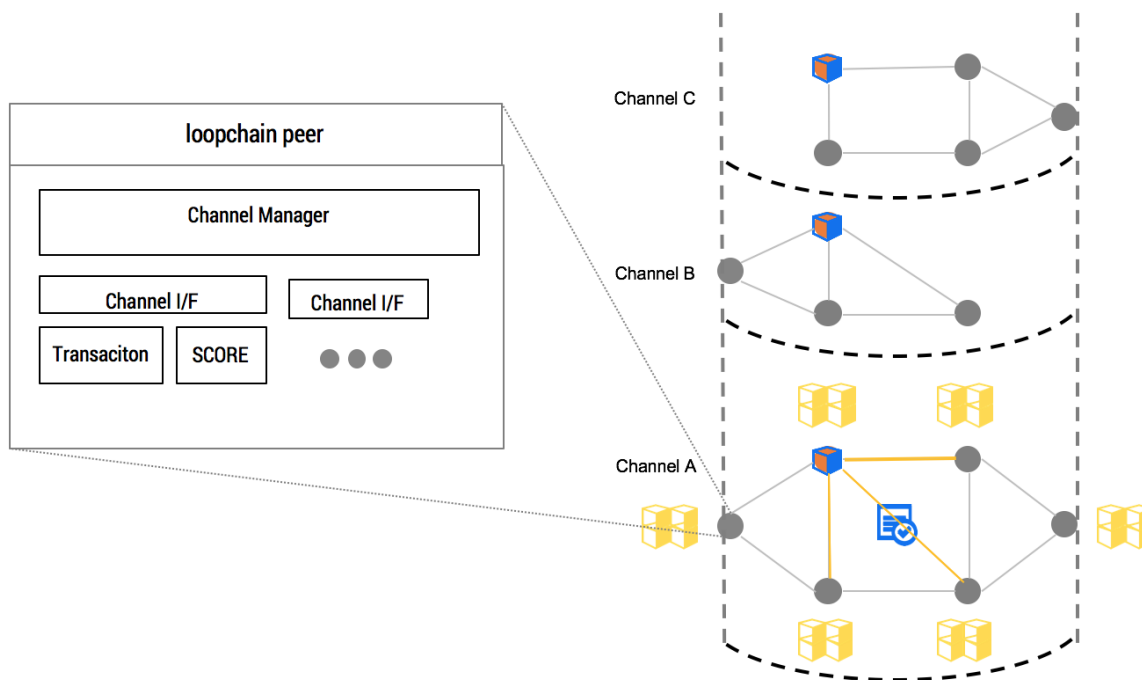
A.5. AI-driven Policy

In the present economic system, centralized institutions make most of the decisions. A small group of experts (e.g. FOMC) of the central bank judges the prices and the economy, and then decides the standard interest rate. The government coordinates the formation and distribution of wealth based on various policies. Government policies in other various fields are also led by a small number of government officials belonging to each department. The data that serve as the basis for such a series of decisions and adjustments are often data with low accuracy that was collected in the past. Therefore, the economic judgment in the existing economic system often produces adverse effects since it is slow, inaccurate, and the consequent action either inappropriate or belated. In addition, since it relies on human analysis and judgment, the personality or characteristics of a person is inevitably reflected to the analysis or decision the person makes, which leads to a lack of consistency, yielding different decision-makings from the same set of data.

Blockchain is an economic platform that enables reliable transactions among participants without a separate intermediary or a trusted third party. The numerous transactions that take place within this platform reflect various economic motives and behaviors of the participants. All transactions on a blockchain are recorded and synchronized in real time with guaranteed integrity. If it is possible to analyze these big data precisely and delicately, a breakthrough can be achieved in the way economic problems are managed now.

DAVinCI LABS: Automatic modeling

DAVinCI LABS: Automatic Clustering

Over the past two years, with A.I. big data analysis we have produced results that outperform the models traditional financial institutions have developed over decades with hundreds of experts. Many financial institutions including the world's largest insurance group, major commercial banks, credit card companies, credit finance companies and savings banks have already begun adopting DAVinCI LABS, a machine-learning-based A.I. solution we have created. DAVinCI LABS are used in various tasks such

as loss ratio forecast, credit risk assessment, conversion rate prediction, price sensitivity measurement, FDS (Fraud Detection System) and EWS (Early Warning System).

The process based on traditional statistics requires user input at every step. During this process, the user's intuition and background knowledge may be applied to the methodology of analysis and the criteria of decision-making, which in turn cause misjudgments. Also, due to the nature of this technique, only a limited amount of data is made of use, which makes it unsuitable for analyzing the effects of different variables. On the other hand, more efficient and sophisticated data analysis is possible by automating analysis process with machine learning algorithm. The possibility of misjudgment caused by personal opinions is minimized by making human intervention as less as possible during the analysis. In addition, as the technique itself allows all data available to be utilized for analysis, it can make a synthetic analysis of the effects of different variables.

We will use AI solution DAVinCI, which is already verified by a number of major financial institutions, to analyze the data derived from the ICON Network and to optimize its reward scheme. By constantly monitoring and analyzing the transactions and the participants' behavioral data with DAVinCI in the ICON Network, the reward scheme will always remain optimized so that the two goals – incentives to participants and growth of the ICON Network – are always kept aligned.

Most of the reward and incentive policies of the existing blockchain networks operate in a rigid manner, failing to adequately address different market conditions. The ICON Network can maintain the growth level as it can flexibly respond to market situation by using AI.

References

[1] https://github.com/ethereum/wiki/wiki/White-Paper

[2] https://www.bancor.network/static/Bancor_Protocol_Whitepaper_en.pdf

[3] https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md

[4] http://www.coindesk.com/tokenized-dollars-singapores-central-bank-details-new-blockchain-trial/

[5] http://www.itu.int/en/mediacentre/Pages/2016-PR53.aspx

[6] https://en.wikipedia.org/wiki/List_of_countries_by_GDP_(nominal)

[7] https://e27.co/korea-stands-out-in-asia-as-a-key-test-market-for-global-tech-companies-including-facebook/

[8] http://www.investopedia.com/news/why-south-korean-bitcoin-price-1000-over-global-price/?lgl=rira-baseline-vertical

[9] https://exchangewar.info/

[10] product development and distribution, pricing and underwriting, payment and collections, claims, policy & administration and back offices, risk capital and investment management

[11] 7 of 10 state-designated research hospitals joined the Consortium

[12] https://www.ohdsi.org

[13] https://www.swift.com/

[14] https://www.cryptocompare.com/exchanges/guides/what-is-a-decentralized-exchange

[15] https://www.wired.com/2014/03/bitcoin-exchange/

[16] https://bitsquare.io/

[17] https://bitshares.org/

[18] https://bancor.network/static/Bancor_Protocol_Whitepaper_en.pdf

[19] https://goo.gl/HXQBUr

[20] https://en.wikipedia.org/wiki/Byzantine_fault_tolerance

[21] https://davincilabs.ai

[22] http://www.coindesk.com/information/what-is-a-decentralized-application-DAPP/

[23] https://en.wikipedia.org/wiki/Representation_(politics)

[24] https://en.bitcoin.it/wiki/Off-Chain_Transactions

[25] To *Section A.5. A.I. driven policy*

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

[27] https://github.com/ethereum/wiki/wiki/White-Paper

[28] https://en.wikipedia.org/wiki/Smart_contract

[29] https://github.com/ethereum/wiki/wiki/Sharding-FA

[30] https://www.hyperledger.org/projects/fabric

[31] https://www.corda.net

[32] https://en.wikipedia.org/wiki/Byzantine_fault_tolerance

[33] To *Section A.4. loopchain Multi-channel*

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

[35] https://en.wikipedia.org/wiki/Byzantine_fault_tolerance

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

[37] https://tendermint.com/static/docs/tendermint.pdf

[38] https://raft.github.io/raft.pdf

[39] https://en.wikipedia.org/wiki/State_machine_replication

[40] http://ieeexplore.ieee.org/document/5283369/

[41] http://www.scs.stanford.edu/14au-cs244b/labs/projects/copeland_zhong.pdf

[42] http://icon.foundation/whitepaper/_static/LFT.pdf

[43] htps://github.com/ethereum/wiki/wiki/Light-client-protocol