Version 1.0 (English)

Last Updated: January 31st, 2018

ICON Foundation

Contents

A rhizome has no beginning or end; it is always in the middle, between things, interbeing, intermezzo. The tree is filiation, but the rhizome is alliance, uniquely alliance. The tree imposes the verb "to be" but the fabric of the rhizome is the conjunction, "and ... and ...and..."This conjunction carries enough force to shake and uproot the verb "to be." Where are you going? Where are you coming from? What are you heading for? These are totally useless questions.

- 『Mille Plateaux』, Gilles Deleuze & Felix Guattari

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 use cases 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 redefine the meaning of communities, and in doing so, introduce an era of decentralization. We envision 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 nation states. 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 break the boundaries between countries, 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.

Apart from these demands, many blockchain projects place emphasis on the decentralization of the blockchain, but present a number of limitations in real-world applications.

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 facing 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.

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 Proof-of-Stake consensus, are still under discussion among Ethereum developers, including the founder Vitalik Buterin and other 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 was successful 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. Due to the reasons above, the real-time cryptocurrency conversion using Bancor tokens does not seem easy to implement.

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 counted on by many for its potential to replace Ethereum. But so far, it appears to have no substantial difference from Ethereum other than the consensus algorithm. Furthermore, its smart contract platform is based on Virtual Machines (VM) like Ethereum; therefore, we need to see if EOS is capable of handling massive, real-time transactions.

2. ICON Overview

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 each other. Telephones made it possible to connect each other in real-time regardless of the distance, and wireless communication added freedom of mobility. With the advent of the Internet, real-time connection to everything, not just people, has become possible anywhere in the world. Despite these breakthrough, 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 in and transmitted to the databases of seven (7) intermediaries such as a front-end processor (FEP) company, and transmitted to pipelines; 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 different from the existing centralized networks. 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 connect 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 required to use their designated system and follow their policies. However, the ICON Network allows each community to autonomously determine their systems and policies, while reliably connect to other communities when needed.

ICON aims to eradicate 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. Cross-border connections will be accelerated through the tokenization of assets and rights, and the dynamics of the network will be maximized. Currencies, tangible assets such as real estates and automobiles, intangible assets such as patents, copyrights, and trademarks, our legal rights such as suffrage and citizenship, and even DNA data or blood tests 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 pay insurance fee directly just by uploading 5 posts on our social media.

ICON brings the connection of humanities one step closer through real-time transactions beyond the boundary and infinite scalability that enables free collaborations.

2.2. 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.

2.3. 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 a representative unit of Community and a unit that comprises ICON Republic governance at the same time. It has the right to vote on transaction verifications and its governance 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-Reps are subject to change depending on the situation and purpose of each governance. Furthermore, C-Rep will receive incentives for its maintenance and activation of ICON Republic.

Only the node representatives that have highly contributed to ICON Network above a certain level are qualified as C-Reps. A node representative's contribution to ICON Network is scored by IISS (ICON Incentives Scoring System), the AI (Artificial Intelligence) based scoring system of ICON. The node representatives that maintain I_score(IISS Score) above a minimum requirement for a certain period can acquire the minimum requirements to qualify as a C-Rep. Finally, it will be decided whether the representative Node can be selected as a C-Rep or not through the process of consensus between incumbent C-Reps within Representation Channel. A specific cap of the C-Rep and the minimum requirements for C-Rep qualification both can be modified through the consensus between C-Reps.

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 votes of C-Rep, and hence, decentralized. ICON Republic functions as a communication channel between communities.

ICON Republic does not interfere in 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 but has only the right to generate a transaction. Citizen Node can also be a C-Rep with voting rights if certain conditions are met.

2.4. How to Connect

There are four types of connections in the ICON Network: 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 financial institutions, governments, schools, medical centers, Bitcoin, and Ethereum, can organize themselves into different blockchains and 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. Therefore, it adopted a consensus algorithm that allows processing of real-time transactions. 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

A Community and ICON Republic are connected in real-time via DEX (Decentralized Exchange). DEX provides exchange ratio in Community and ICON Republic by setting currency reserves and facilitates 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 cryptocurrencies), consensus within ICON Republic is suspended until the consensus of the Community is completed.

Connection between different Communities

Connection between different Communities is also 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.

2.5. How to Operate

Community

Each community operates independently based on its own governance according to the characteristics of its own blockchain. Communities can reach its own consensus and make decisions on consensus algorithm, operation of a cryptocurrency, participation of nodes independent to ICON Republic.

ICON Republic

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

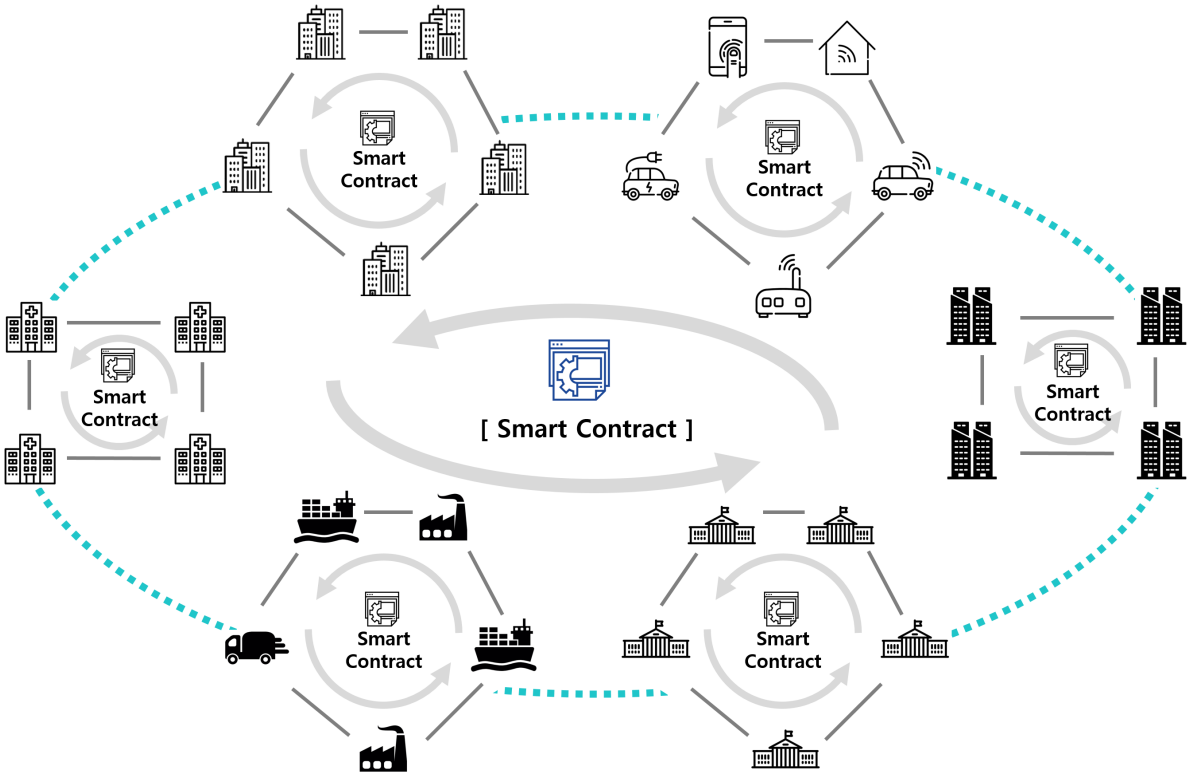
2.6. What to Expect

A wide variety of communities tailored to each business are formed around the world in various fields such as finance, public service, logistics, healthcare, IoT, energy, manufacture, and E-Commerce. With the development and spread of blockchain technology, these communities are expected to accelerate both in quantity and quality. In such an environment, most tasks will be handled through Smart Contracts within the community, and the role of many centralized agencies and intermediaries in each field will gradually shrink or disappear, accelerating the paradigm shift of business processing.

It is expected that changes to the community-centered work environment will not only affect the way the community works internally, but also fundamentally change the way works are handled between communities. In general, most communities initially begin with the goal of improving the work efficiency among the internal members of the community, but in many cases they evolve naturally in the direction of increasing transactions with the outside world. In this case, rather than handling external affairs through a separate centralized institution, the Smart Contract of each community will become the subject of the transaction and the works will be handled through the connection between the Smart Contracts.

In the megatrends that will result from the spread of blockchain technology, ICON aims to be in the lead by connecting communities to create an environment where all communities in ICON Republic can work in real time based on Smart Contracts.

As the number of communities connected through ICON increases, the transactions in ICON Republic will increase exponentially, resulting in maximum utility of each and every community members connected through ICON.



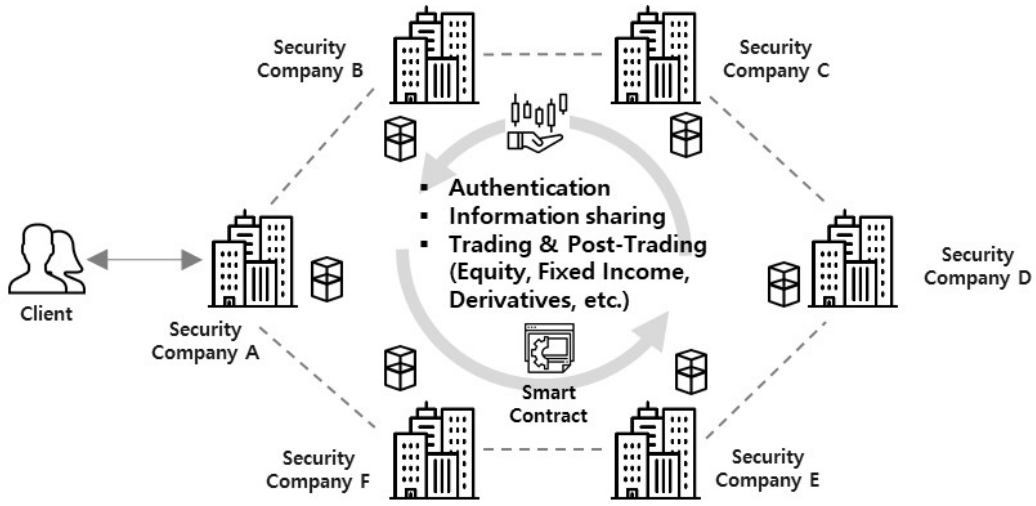
2.7. Implementation of loopchain

We have been continuously building use cases of blockchain with various communities made up of reputable institutions, including capital markets, insurance, university, and healthcare. Each community has started to embrace blockchain technology to solve existing inefficiencies and has begun 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. Chain ID, launched in October 2017, is the Consortium's first service. Based on Blockchain Signature Infrastructure (BSI) technology, Chain ID is capable of authentication as well as generating and verifying digital signatures in the absence of third party oversight. 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.

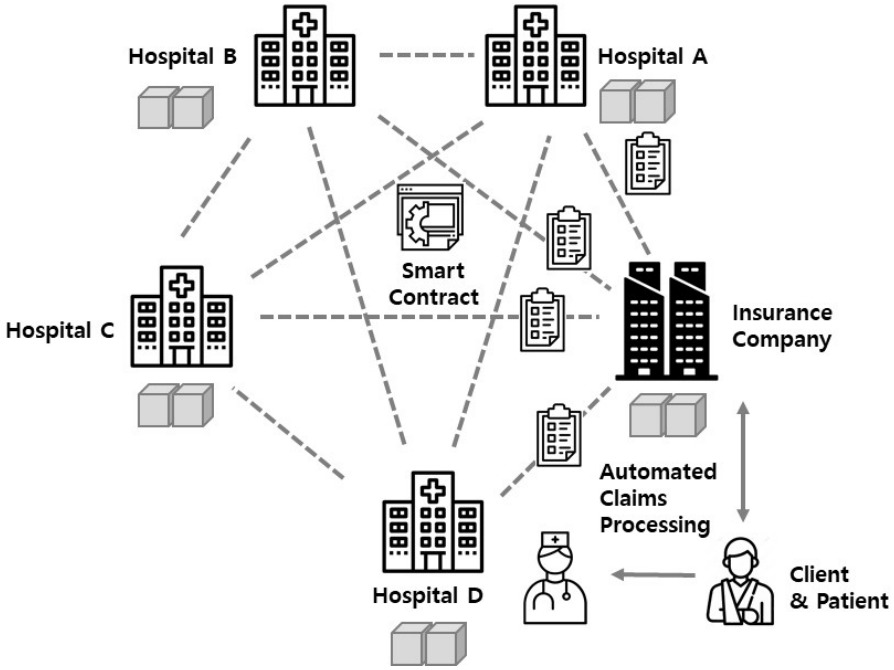
Throughout the global capital market, countless transactions are constantly being carried out through large group of intermediaries and centralized institutions. Because of these intermediaries, the transaction becomes lengthy and back-office work becomes complicated. In general, the clearing and settlement process (post-trading process) for stock transaction takes 2~3 days, and the United States alone spends over USD 9 billion dollars every year.



Insurance

Top tier insurers and hospitals in South Korea have launched a pilot to incorporate theloop's blockchain technology into their claims and payments processes. 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 has been implemented through SCORE and started since December first 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[5]. Innovation of claims and payment services not only can reduce the cost by improving the efficiency of the transaction process but also can greatly enhance consumer experience, thereby improving the overall satisfaction of the insurance industry.

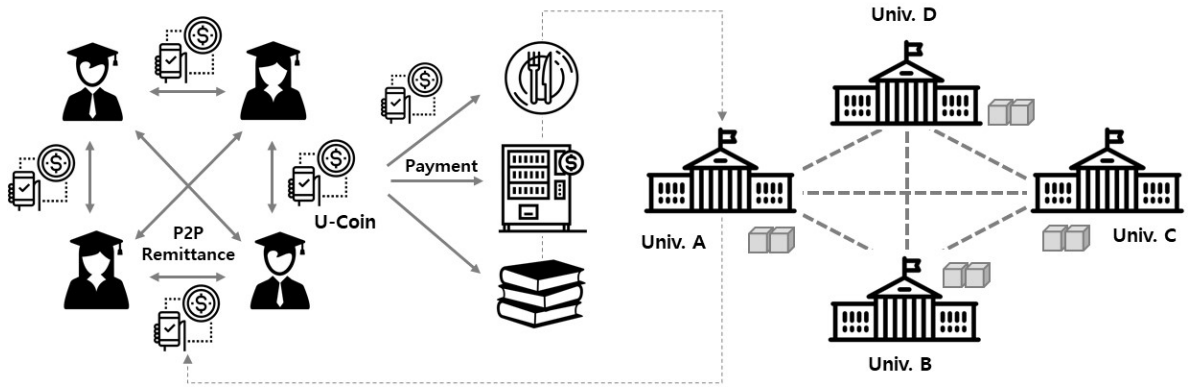


Compared to those of other financial industries, transactions within the insurance industry frequently involves external parties (both in terms of data and transfer of funds). However, these external organizations generally operate on isolated system infrastructures unique to each institution, which 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

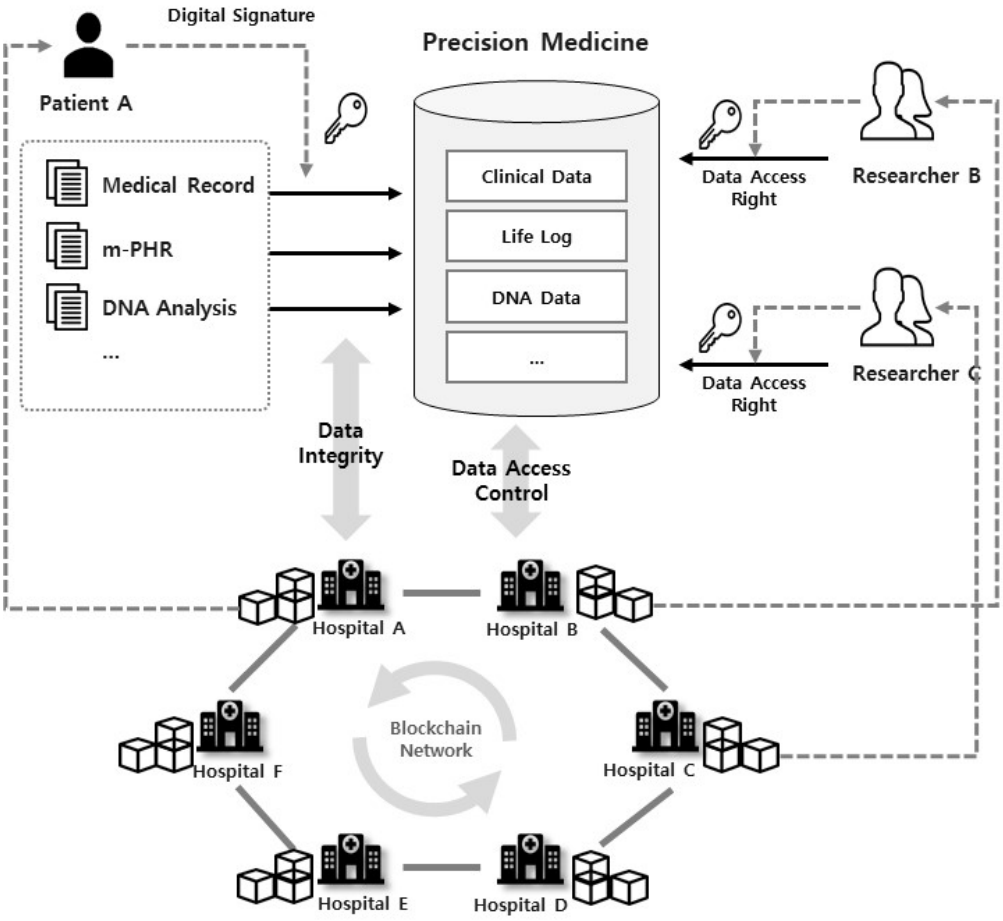
U-Coin (‘University-Coin’) is a cryptocurrency for university students in major universities in Korea and its pilot test has been launched since the end of 2017. U-Coin received a grant from the Ministry of Creation and Science in April 2017 and is expected to expand its services to other universities 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.[6]. 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 OHDSI (Observational Health Data Sciences and Informatics)[7]. 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 can 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.

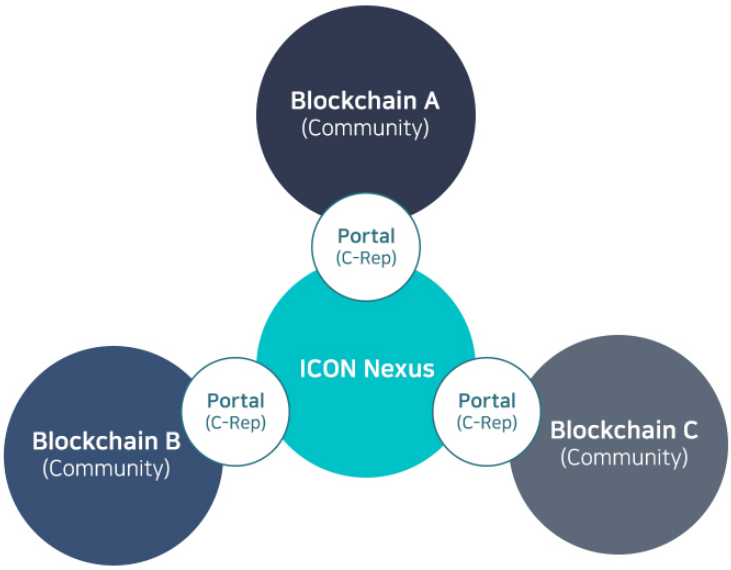
3. ICON Architecture

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 ICON, blockchain network constituting Republic is called Nexus, and C-Rep is configured as Portal, so that blockchains connected to Nexus can handle token transfers and various transactions quickly and reliably through Portal. A Nexus can connect to another Nexus-equivalent blockchain network, 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 facilitates 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, works as 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 achieved based on LFT consensus algorithm, one of the *loopchain* features with a unique function of grouping. 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. 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

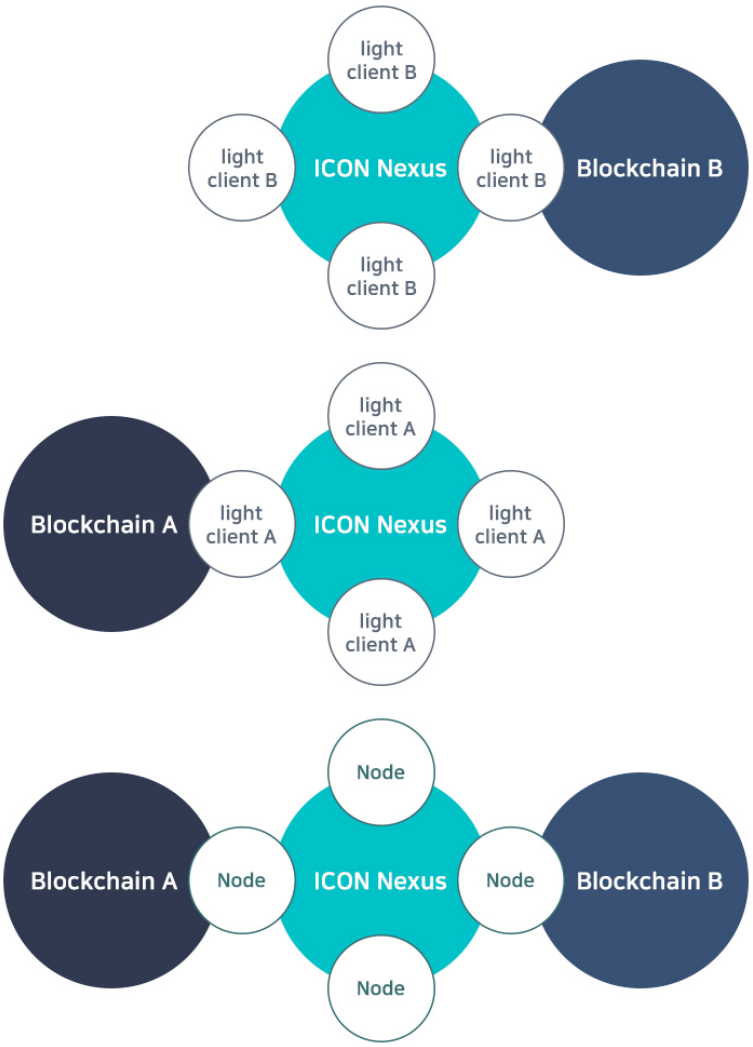
As a component that connects independent blockchain to Nexus, Portals are connected to Nexus through BTP. Depending on the policy of respective blockchains, Portal can be organized by a single node or multiple nodes, or it can make another form of consensus network to serve the different needs.

The Portal is best understood as an analog to the SWIFT[8] network in international banking, which facilitates communications between financial institutions with different currency systems. Likewise, the number of nodes in Nexus can also be single or plural. Nodes are managed in one group by *loopchain*'s grouping function. Portal represents its own blockchain as a C-Rep and suggests the policies and votes for it within Representation Channel to realize a decentralized governance.

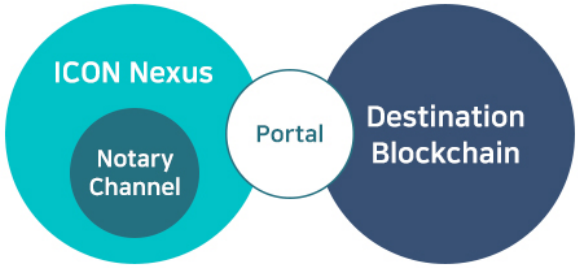
3.5. BTP (Blockchain Transmission Protocol)

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.

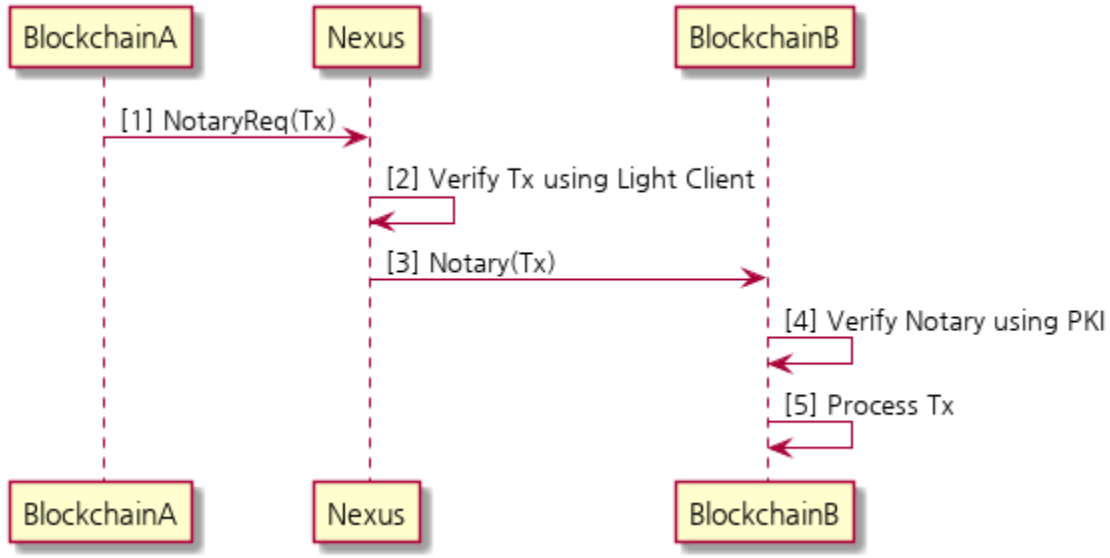
In this sense, Nexus nodes with voting rights to the Notary channels possess multiple channels, where the Light Client of each blockchain connected to Nexus is counted as one channel. A Notary channel is implemented based on Multi-Channel function of *loopchain*. It can identify the transactions confirmed by respective blockchains through the blockchain's Light Client connected to Nexus.



Multiple signatures of nodes with voting rights to request Notary registration are included in the blocks to form blockchains of the 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.



BTP consists of NotaryRequest(Tx) which confirms whether the transaction from the transmission blockchain is confirmed in Nexus and Notary(Tx) which transfers the transaction confirmed by Nexus to the receiving blockchain. Transactions initiated in the transmission blockchain are identified on the Nexus through the Light Client of the corresponding blockchain and registered in the Notary Channel. Transactions registered in the Notary Channel are delivered to the receiving blockchain, and the receiving blockchain verifies the signature of the delivered Notary block to verify the consensus in Nexus, and thereby processes the transaction.



3.6. DEX (Decentralized Exchange)

DEX[9] is a trading platform 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 security breach[10]. 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[11] and Bitshares[12] 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 shortfall.

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[13].

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[14] 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[15] 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.

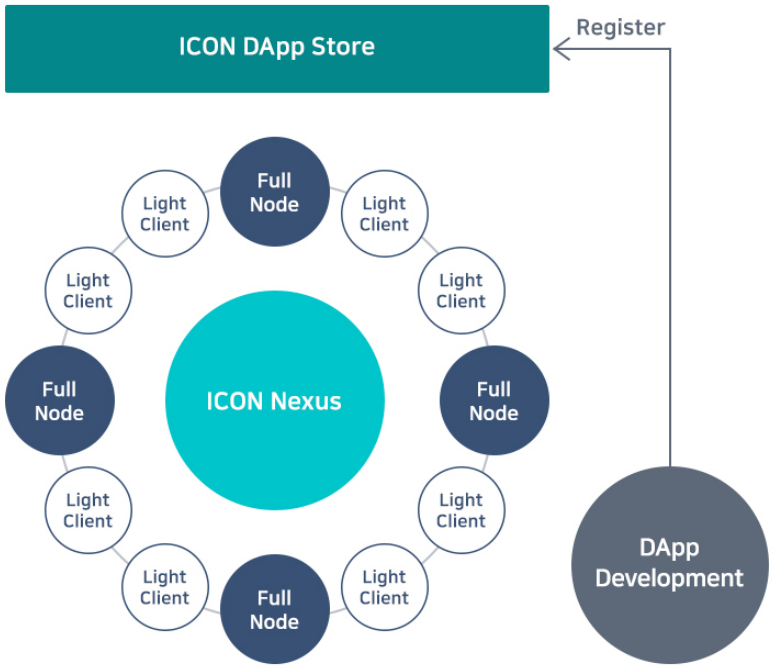
Another key feature of ICON DEX is that it can establish an A.I. Analysis Model[16] based on the accumulated data such as total call volume, transaction frequency, and price involved in transactions among different cryptocurrencies. Such data enable various adjustments of features such as the Reserve 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[17]. 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. In the case of Full Node, certain qualifications are required as it plays a key role in ICX transaction, smart contract operation, and DApp operation. Only the nodes that satisfy specified qualifications within ICON Republic can become the Full Node through the selection of each C-Rep.

ICX collected as transaction fees from transaction participants will be provided to Full Node and Light Client, thereby acting as incentives to each principal for block generation and transaction validation.



3.8. Governance

ICON essentially aims for a decentralized governance. Each blockchain connected to the Nexus has its own governance structure. The Nexus functions as a form of indirect democracy, where the representatives of each blockchain reach consensus by exercising a systematically and fairly allocated vote[18]. To this end, Nexus also includes Representation channels to propose policies and cast votes, 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[19] 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 and Representation channel.

The voting rights are distributed to the community based on I_score, which is the contribution level of corresponding community towards the invigoration of ICON Network. Participant which is not a C-Rep can increase the quota of voting rights of C-Rep through the I_score delegation contract. Therefore, even though the size of community is small, it can increase its own influence within Representation channel by securing supporters in network.

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[20], most synonymously used for virtual currency, is a distributed ledger that effectively 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[21] and the concept of Smart Contract[22], 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 execute 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)[23] 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 participate in the transaction emerged. Hyperledger Fabric[24] and R3 Corda[25] 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)[26]-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[27] 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

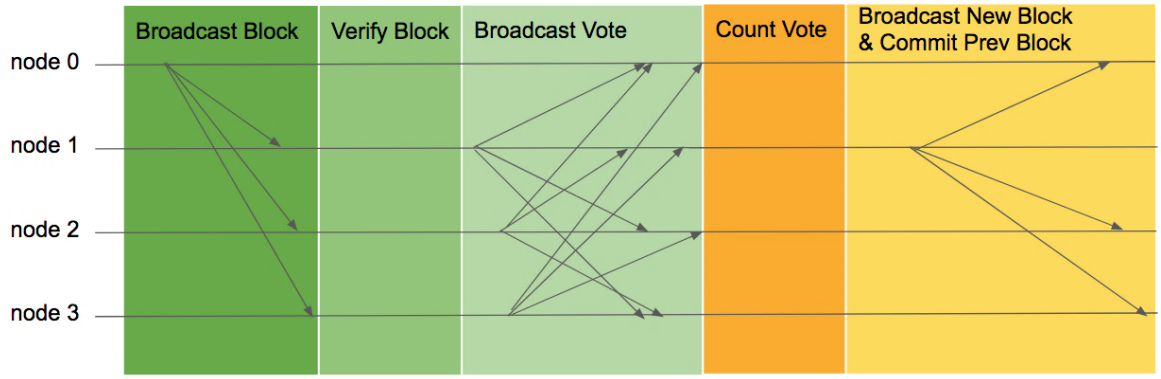
Background

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[28]. However, Bitcoin's Proof-of-Work algorithm had several shortfalls that limited its use in environments requiring efficiency and speed. The algorithm was extremely slow, inefficient in its use of energy, and underwent partial network forks.

To resolve this type of the problem, we started to use BFT (Byzantine Fault Tolerance)[29] 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)[30]), make consensus by voting for validation of data and sharing the results. Tendermint[31] 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[32] algorithm, one of the State machine replication[33] 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 validator 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 validator 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, validator 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[34] 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 Tangaroa[35].

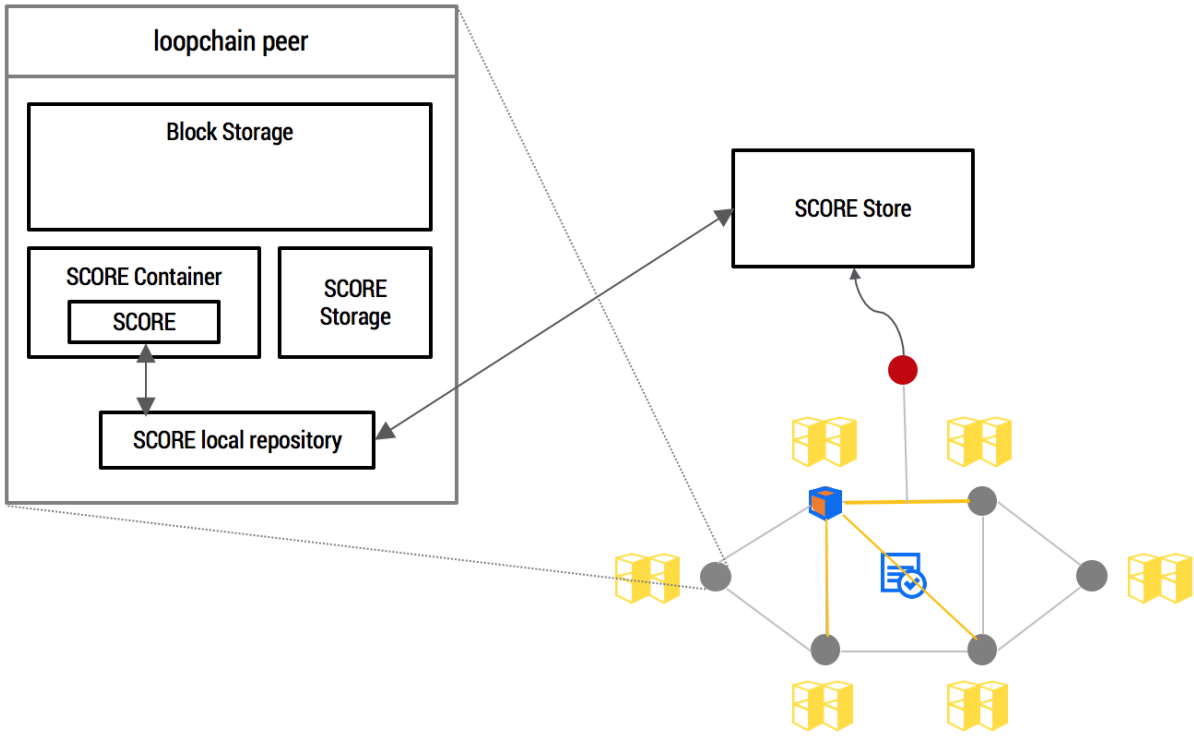
LFT is a distributed consensus algorithm for permissioned blockchain. We improved the existing BFT algorithm for the blockchain and simplified the process using block data. Details of the consensus process can be found in LFT white paper[36].

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[37], 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. ICX Token

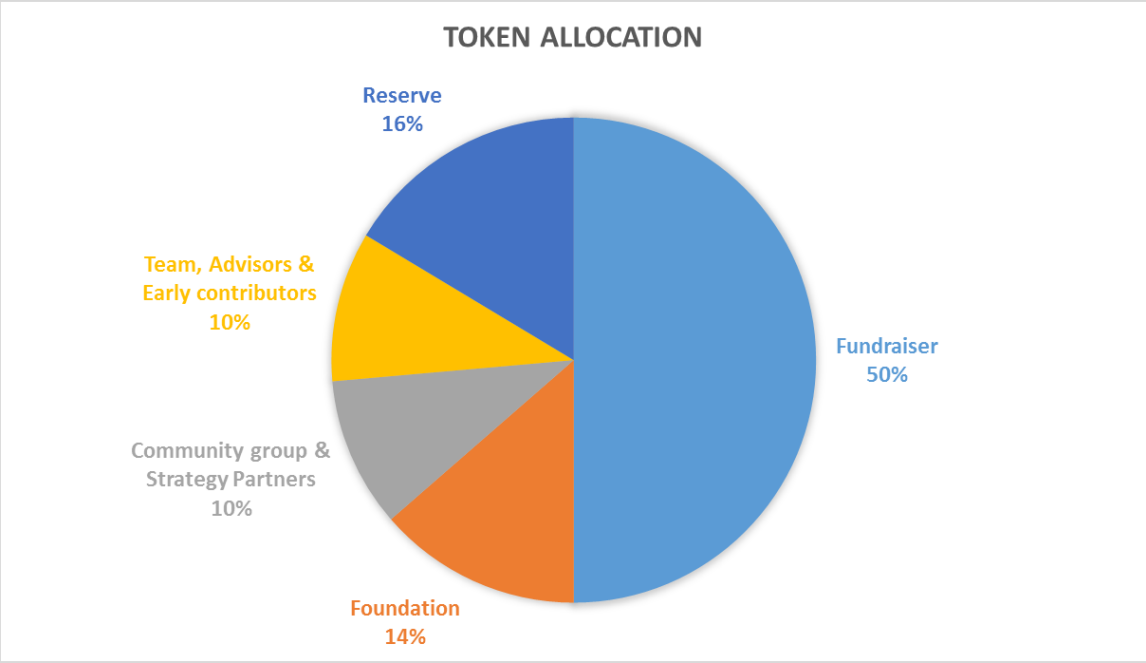
5.1. Token Sale

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)
- Offering Summary

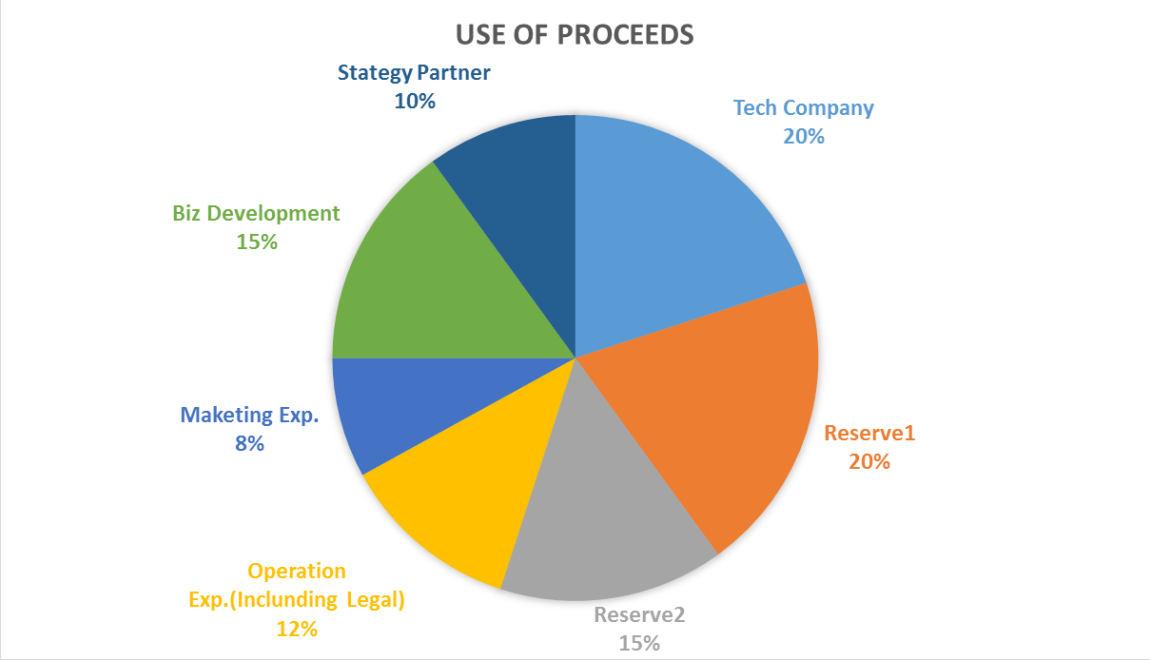
Topic	Description
ICX Token	• ICX is a *loopchain*-based smart contract digital protocol that facilitates, verifies, and enacts a negotiated agreement between consenting parties within ICON
The Issuer	• ICON Foundation, a Swiss nonprofit organization
Rights	• ICX represents limited license to validate 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

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%.

Use of Proceeds



- Use of Proceeds: Tech Company, Reserve, Foundation Operating Expenses, Business Development, Strategic Partnerships..
- Tech Company: Development expense for blockchain engine, DAPPs, artificial intelligence, etc.

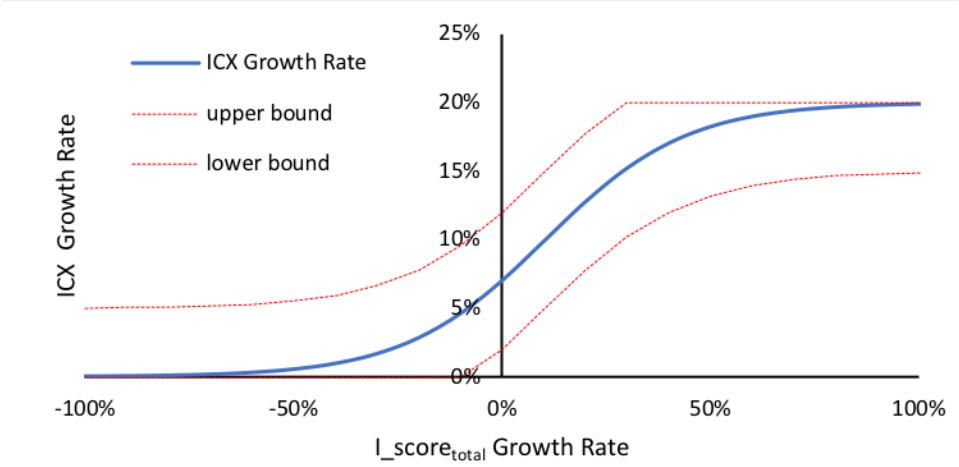
- Reserve: Required for real-time DEX with other blockchain network. Reserve is divided into Reserve1 (ETH Reserve) and Reserve2 (Other Reserve) Reserve1 is required for DEX with Ethereum-based networks. Reserve2 is allocated to DEX with other non-Ethereum based networks.
- Foundation expense: Covers operating expenses, marketing fees, legal & accounting 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 Partnerships: Costs associated with ICON Network expansion, which are provided to the global business partners

5.2. Issuance

Additional issuance of ICX is determined by a cycle of 15,552,000 blocks (approximately 1 year). The amount of newly issued ICX is an increment function of the growth rate in the ICON Network activity. In practice, the amount can be further adjusted within a certain range through the consensus among C-Reps. The purpose of taking into account the activity levels in determining quantity of issue is to check ICX against volatility driven by spikes in demand. The activity level of the ICON Republic is measured by the sum of monthly IISS scores of individual participants during the period of time that it takes to generate 15,552,000 blocks (Approximately 1 year).

$$I\_score_{total} = \sum_{m=1}^{12} \sum_{j} I\_score_{jm}$$

The annual rate of additional ICX issuances will be determined by the logistic function value of increase rate regarding I_score_{total} . The parameter is set so that the maximum rate of additional ICX issuances does not exceed 20%. For example, when the increase rate of I_score_{total} is 0%, additional issuing rate is 7%. The graph shows that the maximum parameter of 20% has been set as well.



Additional ICX issuance rate will be confirmed through the consensus of the C-Rep within the Representation channel. Further adjustments can be made in the range of ±5%p only If more than 2/3 of the C-rep oppose to the calculated figure. Such mechanism will allow the network to be stable and to deal flexibly with unexpected situations, including external financial shocks.

From the point of time when reliable figures are presentable and meaningful consensus can be reached from the accumulation of IISS-related data and the increase in the number of C-Rep, the above method will be the basis for determining the amount of additional ICX into the ecosystem. However, until then, the amount is scheduled to be at a fixed rate.

6. Incentives

6.1. Incentives

Any ICX newly issued, as well as ICX allocated to be distributed as transaction fees, is first held in the Public Treasury. The Public Treasury is the account from which Incentives are distributed. Any ICX not allocated or distributed to a particular party due to reasons including but not limited to the elimination of incumbent C-Reps will be held in the Public Treasury and held as source of incentives to be distributed at a later date.

Newly issued and deferred ICX are distributed to Full nodes and Light Clients according to the I_score. From this segregation of incentive system, the transaction fees generated from transactions will be distributed only to those who have contributed directly. As a result, a direct incentive to participate in the transaction is generated and the incentives are given out stably to the Full Node and Light Client irrespective of additional amount issued or potential change in IISS policy.

I_score will be released every 1,296,000 blocks and these scores will be the guidelines for additional issuance and the ICX deferred to be distributed accordingly. Transaction fees will be distributed every 1,296,000 blocks generated (Approximately 1 month).

IISS (ICON Incentives Scoring System)

IISS is an AI-based evaluation system for an effective ICX allocation. The purpose of IISS is to explore the optimal incentive scheme to vitalize the ICON Republic.

IISS is based on AI, however, the system will need to accumulate data during the initial stages of its implementation. During the preparation period, the I_score of a participant j is calculated by the following equation:

$$\text{I\_score}_j = \sum_{i=1}^{m} C_{ij}(1 + g_i)w_i\alpha_i$$

The score of participant j is the weighted sum of participant j's level of contribution for 'm' number of evaluation items. The categories include ICX transaction amount, DEX transaction amount, participation in the voting of policies, DEX Freezing volume, and DApp generation & usage. C_{ij} indicates the contribution level of participant j with regards to the category 'i'. For example, when the evaluation category is in regards to ICX transaction amount, the formula will be $C_{ij} = \frac{ICX\ transaction\ amount\ of\ Node\ j}{Total\ amount\ of\ ICX\ transactions}$, and this represents the level of participant j's contribution to the network with respect to the total ICX transactions ($\sum_j C_{ij} = 1$). g_i indicates the increase rate of category 'i'. This will administer higher scores to the categories that are faster at reaching greater activeness. w_i is defined by (1 – Gini coefficient) and functions as the weight that can mitigate the 'Degree of inequality' regarding the distribution of incentives. In the case of some categories, small number of participants may monopolize most of the contribution level and the incentives they bring. w_i lowers the weight for the categories that suffer extreme inequality and mitigates the unfair distribution of incentives. This will lead to the participants with greater level of contribution to encourage more participation from the greater number of participants with low level of contribution to receive higher scores. The whole process will result in more activities within the ICON Republic. α_i indicates the weight imposed on each category. The appropriate level of α_i can be determined and modified through the consensus of the Representation channel. During the initial stages of implementation, the initial weight will be fixed at 0 for those categories that are deemed difficult for ordinary participants to participate and those that have not been fully activated, including 'DEX transaction amount' and 'DApp generation & usages'.

For the actual incentive distribution, the network will use the previous 3 periods weighted average

I_scores ($I\_score_{j\tau}^{avg}$).

$$I\_score_{j\tau}^{avg} = \frac{1}{1+\rho+\rho^2} I\_score_{j\tau} + \frac{\rho}{1+\rho+\rho^2} I\_score_{j\tau-1} + \frac{\rho^2}{1+\rho+\rho^2} I\_score_{j\tau-2}$$

If the data is accumulated enough for a period of time (1~t), the set of information available at time t is as follows:

$$\Omega_t = \{I\_score_1, X_1, I\_score_2, X_2, \dots, I\_score_t, X_t\}$$

I_score_t refers to the entire I_score information of all participants at the end of period 't'. X_t indicates the rest of the accumulated data except I_score that have been generated during the period 't'. The accumulated I_score information will be adjusted after evaluating the scores against factors, including the efficiency of IISS, fairness of distribution, prevention of IISS misusage, and others. The adjusted score ($I\_score_t^{adj}$) and its relationship with other variables will be learned with Deep Learning. The network will utilize data points, including the accumulated data Ω_t, the newly obtained data X_{t+1}, and the relationship of variables learned to predict the optimal level of $I\_score_{t+1}^{adj}$ for the future period.

$$\mathrm{E}(I\_score_{t+1}^{adj} | \Omega_t, X_{t+1})$$

All measurable variables can be presented by the C-Rep to be taken into consideration when calculating the I_score. When the variable satisfies certain criteria, it may be included to the data set which determines the I_score.

Incentives

I_score functions as incentives in the ICON Network in two ways.

First, the additionally issued ICX and the deferred ICX from previous periods will be distributed according to the equation shown below:

$$ICX\ Earnings_j = (Issued\ ICX + Deferred\ ICX) \times \frac{I\_score_j}{\sum_k I\_score_k}$$

$ICX\ Earnings_j$ indicates the ICX distribution to the participant j and I_score_j refers to the I_score of participant j.

However, participants with insignificant participation may be excluded from the distributions to prevent excessive load on the network. Please refer to ***Incentives Distribution*** for more details.

Second, the voting rights in the Representation Channel are distributed in a similar way. The voting rights are granted only to the C-Rep and the delegated I_score is considered when distributing the voting rights. In other words, the voting rights are allocated proportionate to 'the total sum of I_score for the individual C-Rep and the I_score delegated to the C-Rep.'

$$Vote_j = \frac{I\_score_j + D.I\_score_j}{\sum_k (I\_score_k + D.I\_score_k)}$$

$Vote_j$ represents the voting rights granted to the C-Rep 'j'. I_score_j refers to the I_score of C-Rep and $D.I\_score_j$ refers to the total sum of the I_score delegated to C-Rep 'j'.

Delegation

The participant, except C-Rep, does not have the right to vote directly in the Representation Channel.

Instead, all participants can freely delegate their I_score to the C-Rep they wish to support. Every participant can increase the voting right of the C-Rep by delegating its I-score, so that each participant can contribute to extending the influence of corresponding C-Rep in Representation channel.

Dormant account

The account that does not make any transaction and maintains its balance below a certain level for a certain period will be considered as Dormant account and excluded from I_score calculation.

Incentives Distribution

In principle, incentives are provided to every account except for Dormant accounts. However, if the number of accounts that deserve receiving ICX as incentives is more than several million, a significant amount of time will be required to generate blocks and process the distribution. Thus, it may negatively affect the ICON Network. Therefore, the actual incentives payable will need to be limited to accounts that receive a meaningful level of incentives.

As such, the ICX distribution will be limited by the following recipients. Active group that has high I_score receives ICX based on calculated I_score. The Inactive group determines the number of accounts payable (C) by dividing the unpaid ICX (A) by the ICX paid to the lowest account in the Active group (B), and (A)/(B) is rounded up to the nearest ones. Then the total ICX of (A)/(C) will be distributed in the order of descending I_score order. For instance, if payable ICX incentives are 1,000,000 ICX and Active group includes top 100,000 I_scores, 50.93 ICX will be equally distributed to 100,001 ~ 100,589 I_scorers as below.

Category	Allocated ICX	I_score ranking	ICX_{calc}	ICX_{actual}	
Active group	970,000	1	95,000	95,000	
		2	72,000	72,000	
		3	47,000	47,000	
		⋮	⋮	⋮	
		100,000	51**(B)**	51	
Inactive group	30,000**(A)**	100,001	49	50.93	30000/51=588.235 **(A)**/**(B)** = **(C)** → 589 participants will receive ICX incentives.
		100,002	48	50.93	
		⋮	⋮	⋮	
		100,588	38	50.93	
		100,589	**37**	**50.93**	30000/589=50.93 ICX **(A)**/**(C)** = 50.93 ICX
		100,590	**35**	**0**	
		100,591	33	0	
		⋮	⋮	⋮	

Transaction Fee

Even though the transaction fee is currently set to 0.01 ICX per transaction, it will be charged according to a fee structure that reflects the degree of complexity of each transaction. This change will compensate for an increase in processing costs caused by increasing number of complex tasks requested from smart contract or DApp.

Transaction fees are paid in ICX, but other tokens will also be available by converting them into ICX

through DEX.

Newly generated Transaction fees are reserved in Public Treasury and it will be provided to Full Node and Light Client participating in concluding transactions. A certain proportion of the total amount of paid transaction fee will be provided to Full Node and the rest will be assigned to Light Client. Each Full Node will equally receive distributed amount divided among the number of Full Nodes and Each Light Client will equally receive distributed amount divided among the number of Light Clients as well.

Elements such as the amount of transaction fee or the respective fee ratios of Full Nodes and Light Clients can be modified through consensus in Representation channel. An optimal level of transaction fee will be proposed by AI analysis prior to the consensus so that C-Reps can take it into account during the consensus. The AI model will derive the optimal fee level for smooth operation of the ICON Network with the specific goals of attracting enough number of Full Nodes and Light Clients and maintaining the appropriate transaction size.

6.2. Penalty

Penalties are given to malicious activities of Full Nodes participating in LFT algorithm. By malicious activities it refers to leaders proposing invalid blocks and validators voting for invalid blocks or voting against the rules.

Similar to Ethereum's Casper, the ICON Network will require all nodes to deposit a minimum amount of ICX required. Malicious nodes will be penalized by burning their ICX deposits, thereby resolving any 'nothing at stake' issues caused by moral hazards.

Appendix

A.1. Definitions

Transaction(Tx)

- Fundamental unit of data in a blockchain.

Block

- Unit of consensus between peers. Consists of one or more transactions.

Peer

- Represents one peer in a P2P network. Executes most blockchain activities.
- Generates transactions.
- Transfers blocks and transactions in a P2P network.

Leader Peer

- Peer with permission to generate blocks.
- Collects transactions periodically to generate blocks and broadcast them to the network.
- Transactions generated by each peer are gathered at leader peer.

RadioStation

- Generates groups and connects peers to groups.
- All active peers can connect to RadioStation in case they need to check the status of other peers in the same group.
- Monitors status of each peer.

SCORE

- Smart contract supported by loopchain engine.
- Functions that change the state values by given transaction execution.
- Executed after verification and addition of a new block.

Service System

- An application system that uses blockchain technology. Can be either a legacy system that has been used previously or a new service.

C-Rep

- A representative unit of Community which comprises ICON Republic's governance.
- Holds voting rights on making decisions pertaining to operating governance in order to maintain and promote ICON network.
- Serves as Portal to Nexus. Manages token transfers and transactions between different blockchain networks.

Citizen Node

- All non-C-Rep nodes under ICON Republic.
- Does not hold rights to verify transactions or vote on governance issues. Only allowed to generate new transactions.

ICON Republic

- Refers to the entire ICON Network consists of C-Rep and Citizen Node.
- A decentralized network that connects Communities and DApps but does not interfere in the governance of independent Communities.
- Made up of blockchain networks called the Nexus.

Nexus

- Blockchain networks that comprises ICON Republic.

Representation Channel

- A consultation system, which only consists of C-Reps, that determines all rules for issue arising in ICON Republic.
- Voting right of each C-Rep is allocated by IISS score as a measure of contribution of the community C-Rep represents. Citizen Nodes, which do not have voting rights, can delegate their IISS scores to a particular C-Rep to participate in reallocating voting rights.

Notary Channel

- Channel for sending and receiving transaction between blockchains connected by Nexus.
- Nodes with voting rights to this channel have multiple channels of Light Clients in different blockchains on Nexus. This is implemented based on loopchain's multi-channel feature.

Node

- Physical unit which has computing power. Joins different kinds of channel to execute required activities.
- C-Reps select one or more Full Nodes which are able to execute transactions, consensus, and smart contract operations in Public Channel. Candidates for Full Nodes must meet certain requirements.
- Light Clients only play the role specifically assigned. Light Clients in Public Channels generate new transactions. Light Clients in Notary Channels facilitate consensus.
- Nodes are eligible to receive fees depending on the nature and importance of their roles.

A.2. SCORE

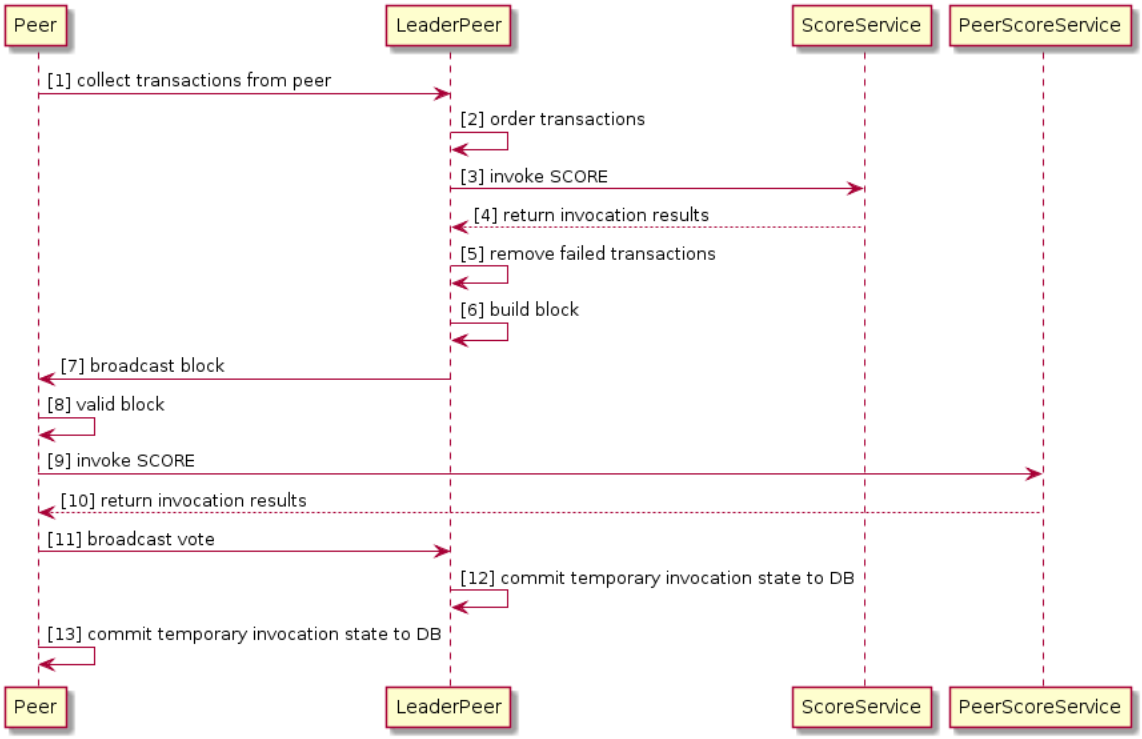
SCORE Code

```python
#!/usr/bin/env python

from loopchain.blockchain import ScoreBase

class UserScore(ScoreBase):
    """ Basic SCORE code
        boilerplate template code
    """

    def invoke(self, transaction, block):
        pass

    def query(self, **kargs):
        pass
```

The purpose of each function is as follows:

- invoke() : Add verified block data to a separate built-in database.
- query(): Search internal data.

SCORE Process Flow



Sequence

① Collect transactions from peers

② Order transactions

③ Invoke SCORE

④ Return invocation results

⑤ Remove failed transactions

⑥ Build block

⑦ Broadcast block

⑧ Validate block

⑨ Invoke SCORE

⑩ Return invocation results

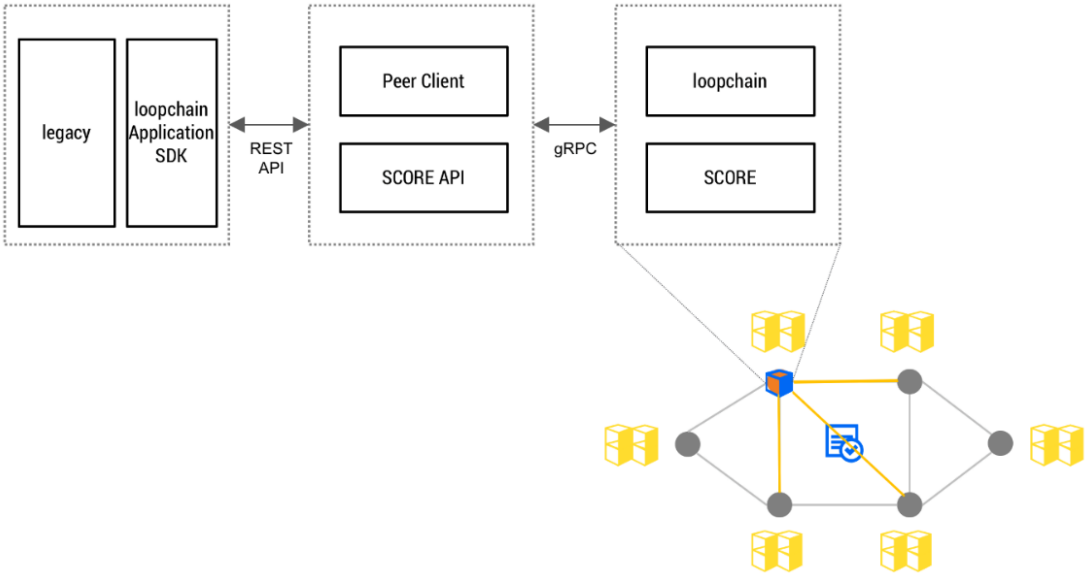
⑪ Broadcast votes

⑫ Commit temporary invocation state to DB (Leader Peer)

⑬ Commit temporary invocation state to DB (Peer)

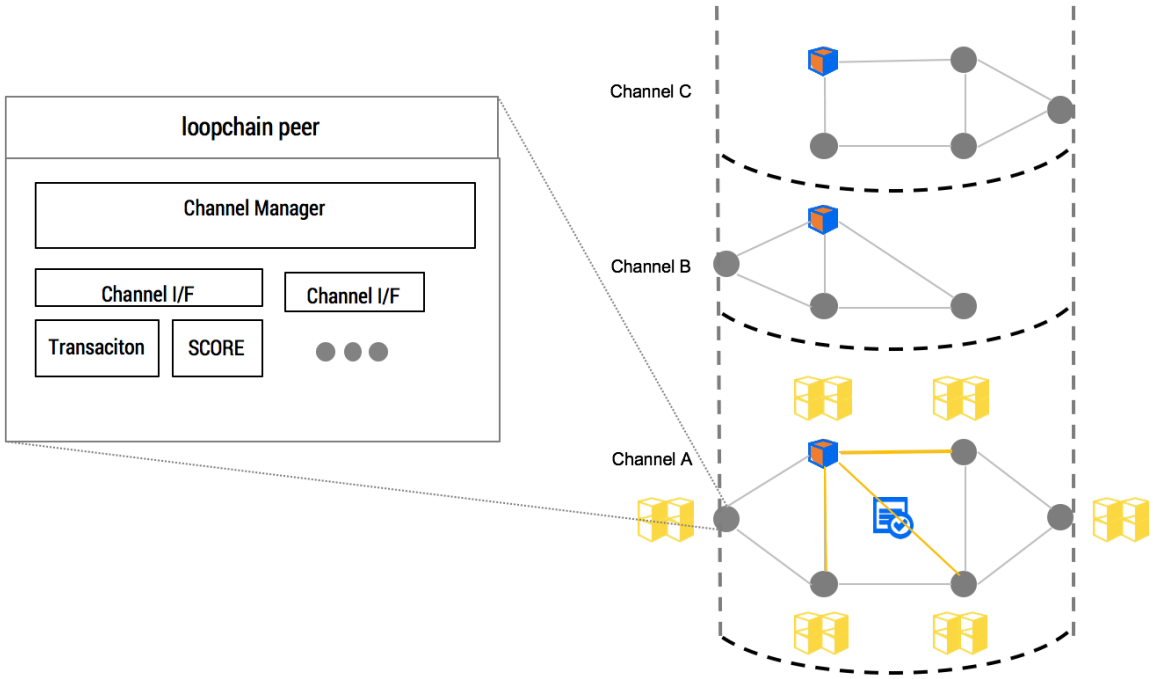
A.3. Integration of loopchain and Legacy Systems

loopchain Proxy allows access to blockchain Peers through REST API. The API is provided with loopchain Application SDK, wrapped for easy use in legacy systems and tasks so that product development is available with a simple API call.



A.4. loopchain Multi-channel

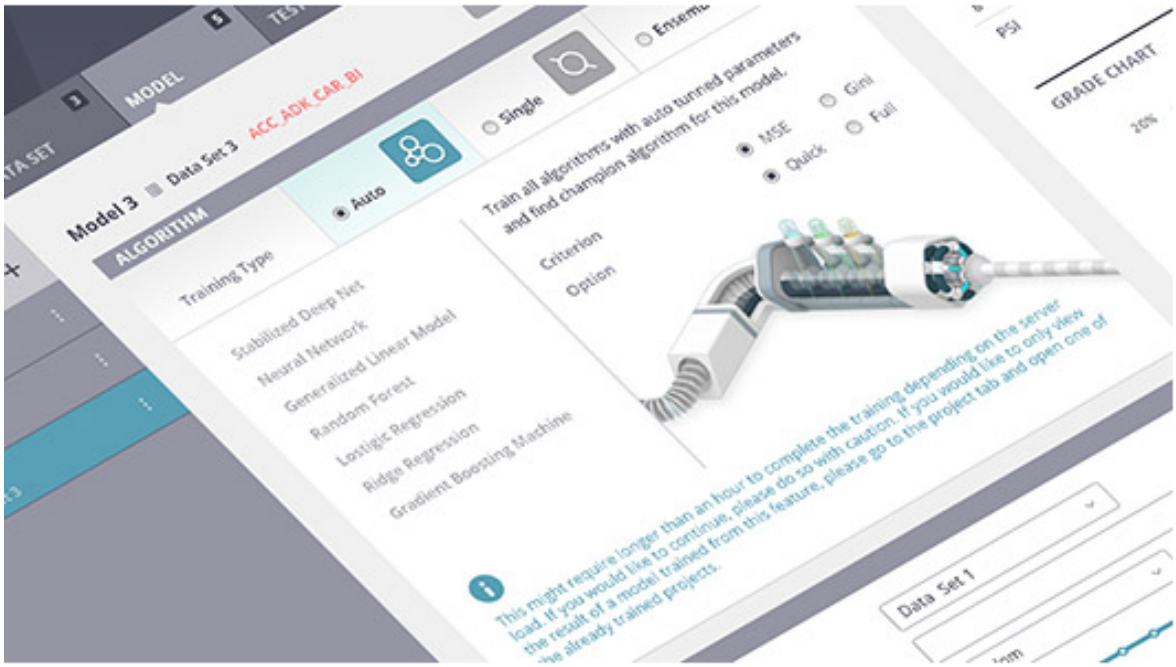
The multi-channel feature pools transaction and SCORE data by channel. It is possible to construct separate channels by each task only for related parties within a single blockchain network.



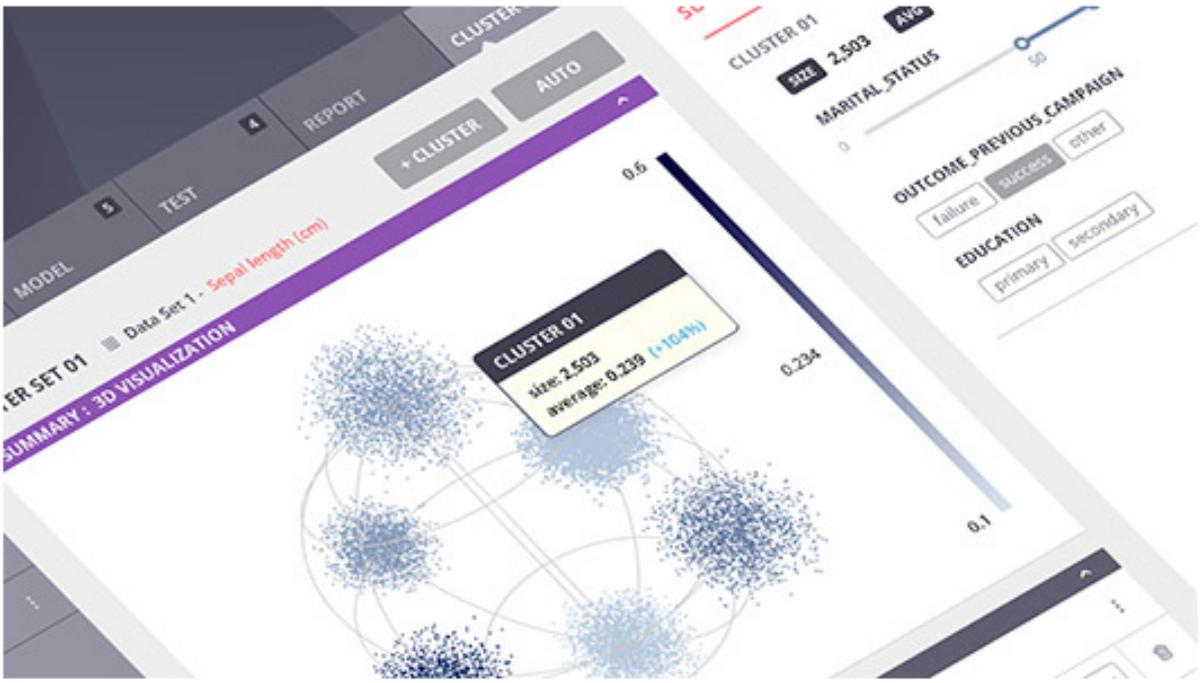
A.5. AI-driven Policy

Economic decision-making has historically been managed by centralized institutions. Central banks set reserve interest rates based on their own analysis of the economy. Governments use policy to manage accumulation and allocation of wealth. Much of the decision making surrounding consumer prices, macroeconomics, and reserve rates is done by small professional groups (e.g. FOMC) within central banks. Policies, too, are managed by small government groups. The decisions of these elites are often based on old and unreliable data. Economic decision-making and implementation is inherently slow and inaccurate, often leading to unexpected side effects. Decisions depend on the subjective analysis of a small number of people.

Blockchain is an economic platform to facilitate reliable transactions between parties in the absence of a central broker or mediator. Transactions are the product of each party's economic motivations and actions. The integrity of blockchain transactions are guaranteed and synchronized in real-time. In-depth analysis of blockchain data would allow for a far more efficient economic system.



DAVinCI LABS: Automatic modeling



DAVinCI LABS: Automatic Clustering

Over the last two years, we have used AI technology to create models that surpass those developed by in-house professionals at leading financial institutions. Global insurers, commercial banks, card issuers, savings banks, and other financial services providers use our DAVinCI LABS to predict insurance loss ratios, credit risks, conversion rates, and price sensitivities. Our solutions have also been employed in Fraud Detection Systems (FDS) and Early Warning Systems (EWS).

Existing statistical methods have required user input at each stage. The user's own subjective reasoning and background knowledge have been the main determinant of analytical success; in addition, the limited processing capability of statistical applications has often left out large sums of data for technical reasons. Machine learning algorithms, by contrast, automate much of the subjective selections process and analyze larger data sets than permitted by conventional statistical analysis.

We plan to implement DAVinCI on the ICON Network to analyze its data on optimize compensations. Transactions and other activity produced on the ICON Network will be continuously analyzed to align the Network's growth with individual compensation. Most other blockchain networks have been inflexible, failing to respond to market movements. The ICON Network advantage is in being able to maintain a sustainable basis for growth by responding quickly to market change.

References

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

[2] https://about.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] product development and distribution, pricing and underwriting, payment and collections, claims, policy & administration and back offices, risk capital and investment management

[6] 7 of 10 state-designated research hospitals joined the Consortium

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

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

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

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

[11] https://bitsquare.io/

[12] https://bitshares.org/

[13] https://about.bancor.network/static/bancor_protocol_whitepaper_en.pdf

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

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

[16] https://davincilabs.ai

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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