Version 1.0 (Korean)

Last Updated: January 31st, 2018

ICON Foundation

Contents

리좀은 시작하지도 않고 끝나지도 않는다. 리좀은 언제나 중간에 있으며 사물들 사이에 있고 사이-존재이고 간주곡이다. 나무는 혈통 관계이지만 리좀은 결연 관계이며 오직 결연 관계일 뿐이다. 나무는 "~이다(etre)"라는 동사를 부여하지만 리좀은 "그리고... 그리고... 그리고..."라는 접속사를 조직으로 갖는다. 이 접속사 안에는 <이다>라는 동사를 뒤흔들고 뿌리 뽑기에 충분한 힘이 있다. 어디로 가는가? 어디서 출발하는가? 어디를 향해 가려 하는가? 이런 물음은 정말 쓸데 없는 물음이다.

-『Mille Plateaux』, Gilles Deleuze & Felix Guattari

Abstract

블록체인 기술의 탄생은 우리로 하여금 탈중앙화된 세계에 대하여 눈뜨게 하였으며, 국가단위를 중심으로 이루어져 있는 화폐 시스템에 대하여 새로운 이슈를 제기하였다. 또한, 기술의 발달은 국가 간 경계를 허물고, 더욱 빠르게 교류할 수 있는 장을 만들었지만, 여전히 제공받을 수 없거나 불만족스러운 서비스들이 존재한다.

그러나, 수많은 블록체인 프로젝트는 이러한 요구와 별도로 블록체인의 탈중앙적 기술에만 초점이 맞춰져 있으며, 그로 인해 현실세계의 적용에 있어서 많은 한계를 드러내고 있다. ICON Project는 이런 한계를 극복하고 이를 통해 새로운 세상을 열어가고자 한다.

이 글에서 우리는 ICON이 그리는 세상에 대해서 설명할 것이며, 이것의 구체화를 가능하게 하는 loopchain과 loopchain을 활용하여 구축되고 있는 블록체인 세상에 대하여 설명할 것이다.

ICON은 질 들뢰즈와 펠릭스 가타리의 철학에 많은 영감을 받았으며, "중심화된 지점이 없는 세상, 어떠한 지점도 다른 지점들로 연결되는 과정일 뿐인 세상"을 꿈꾸고 있다. ICON은 블록체인별로 나눠져 있는 가상화폐세계를 연결시키며, 나아가 현실세계와 가상화폐세계를 연결시킨다. 또한, 이 과정에서 우리는 새로운 지점이 연결될 때마다 생겨나는 의미들에 주목하고, 새로운 의미들이 만들어내는 새로운 결정들에 대하여 의미 있게 받아들일 것이다.

1. Introduction

1.1. Vision

우리는 분산화된 세상을 실현하기 위해 공동체를 새롭게 정의 내리고, 정의된 공동체를 연결하며, 연결된 공동체를 통해 새로운 세상을 만들 것이다. ICON은 사회적·정치적 의미로만 존재하던 공동체(Community)에 경제적 관계를 결부시킴으로써 국가 단위로 정의되던 기존 경제시스템을 공동체 단위로 새롭게 정의하고, 정의된 각 공동체들을 이전보다 더욱 밀접하게 연결시킬 것이다. 또한, ICON은 현실세계(Real world)뿐만 아니라 가상화폐세계(Crypto-world)와도 연결되어 무한한 확장(Infinite scalability)을 가능케 할 것이다.

ICON 은 블록체인으로 구성된 다양한 독립적 Community 가 연결된 탈중앙화된 네트워크이다. ICON 세상에서는 누구나 새로운 블록체인 프로젝트를 만들 수 있으며, 새롭게 만들어진 프로젝트는 다른 프로젝트들과 연결되어 또 다른 세상을 만들어낼 것이다. ICON 은 그 자체로 살아 숨쉬는 하나의 유기체이며 생태계이다.

우리는 ICON 세상에서 국가의 경계를 넘어 전세계의 금융, 의료, 공공 등의 Community 와 접속할 수 있다. 그로 인해 한국에서 미국으로 더욱 빠르게 송금할 수 있게 되고, 인도 투자자들은 애플, 구글, 삼성 주식에 더욱 편리하게 투자할 수 있게 된다. 또한, 보험사와 병원은 자신의 고객을 위해 커뮤니티 내에서 더욱 빠르게 정보를 공유할 수 있게 되며, 대학교는 연구를 위해 다양한 데이터에 접속할 수 있게 된다. 우리는 미국 병원에서 연구목적으로 사용된 나의 의료 데이터로 인해 나의 Wallet 안으로 ICX 를 받을 수 있게 되는 세상을 실현하고자 한다.

우리는 ICON 을 통해 새롭게 정의되고, 새롭게 연결된, 새로운 세상 속으로 들어가게 된다.

1.2. Background

Overview

블록체인 기술의 탄생은 우리로 하여금 탈중앙화된 세계에 대하여 눈뜨게 하였으며, 국가 단위를 중심으로 이루어져 있는 화폐 시스템에 대하여 새로운 이슈를 제기하였다. 또한, 기술의 발달은 국가 간 경계를 허물고, 더욱 빠르게 교류할 수 있도록 만들었지만, 여전히 제공받을 수 없거나 불만족스러운 서비스들이 존재한다.

하지만 수많은 블록체인 프로젝트는 이러한 요구와 별도로 블록체인의 탈중앙적 기술에만 초점이 맞춰져 있으며, 그로 인해 현실세계의 적용에 있어서 많은 한계를 드러내고 있다.

Steem과 같이 하나의 블록체인 네트워크 속에서 새로운 세상을 만들어내는 프로젝트도 있지만, 현실세계와의 연결을 시도하는 프로젝트의 경우 대량의 거래량으로 인해 속도의 한계를 드러내고

있으며, 그로 인해 현실세계와의 연결을 위해서는 여전히 많은 연구가 필요한 상황이다. 또한, 이러한 문제점들을 포함한 프로젝트들은 가상화폐세계와 현실세계를 이원화시켜 새로운 세상을 만들고자 하거나, 해당 문제점에 대해서는 해결책을 제시하지 못하고 있다.

ICON 프로젝트는 이러한 배경 하에 시작되었다.

Ethereum[1]

이더리움은 블록체인 영역에 '스마트컨트랙트'라는 개념을 도입하여 중앙의 중개자 없는 분산 어플리케이션을 개발할 수 있는 환경을 구축하였다. 이는 비트코인처럼 단순한 거래 장부 공유를 통한 가상화폐 거래만을 지원하던 기존 블록체인 기술의 한계에서 벗어나 금융권을 비롯한 실제 업무에 블록체인 기술을 활용할 수 있는 단초를 마련한 것으로 블록체인 2.0 이라는 새로운 시대를 연 혁신적인 사건이었다.

이후 다양한 분산 어플리케이션이 등장했고 The DAO 프로젝트를 통해 탈중앙화된 자율적인 벤처캐피털을 구성하는 프로젝트에 약 2,000억원 규모의 자금이 유입되기도 했으나 취약점으로 인해 이더리움 자체가 이더리움 클래식과 분기되는 사건이 발생하였다. 현재도 PoS 도입 등이 비탈릭 부테린을 비롯한 주요 개발팀에 의해 논의되고 있지만 거대 채굴 그룹과의 대립구도가 형성되는 등 거버넌스 문제가 이슈가 되고 있다.

일부 한계점들에도 불구하고 이더리움은 ERC20 토큰을 기반으로 ICO 플랫폼으로서 인기를 얻고 있다. 그러나 역설적이게도 status.im 등 일부 ICO들의 인기는 이더리움 네트워크 전체에 과부하를 초래하는 등 확장성의 한계를 드러냈다.

Bancor[2]

뱅커는 이더리움 상에서의 준비금을 통해 적정가격을 도출하는 알고리즘을 기반으로 실시간으로 연결된 가상화폐를 거래할 수 있는 분산 거래소(DEX: Decentralized Exchange)를 제공한다. ICO 당시 $1.5억달러를 모집하여 큰 이슈가 되었고 곧이어 분산 거래소를 통해 이더와 뱅커 토큰 사이의 거래가 가능하게 되었다.

뱅커는 가상화폐 간에 준비금 기반의 전환이 가능하게 하여 ETF 등 다양한 비지니스 모델을 가능하게 하였으나, 이더리움을 기반으로 하고 있어 수수료가 높고 속도 또한 제한적이다. 이 때문에 뱅커 토큰으로 연결된 가상화폐간 실시간 전환은 구현해내기 쉽지 않을 것으로 보인다.

EOS[3]

EOS는 이더리움 확장성의 한계를 지적하며 등장한 플랫폼 블록체인이다. 특히 DPoS 방식의 합의 알고리즘으로 3초마다 블록이 생성되게 하고 거래 수수료를 제거하여 분산 어플리케이션의 활성화를 도모하고 있다.

EOS는 아직 개발 중인 플랫폼으로서 이더리움을 대체할 것이라는 기대를 받고 있지만 합의 알고리즘 외에는 별다른 특이점이 없고 스마트컨트랙트 플랫폼도 이더리움과 같은 가상머신 기반으로서 실제 대용량 거래에 대응할 수 있는지에 대해서는 검증이 필요하다. 따라서 실제 환경에서 EOS를 적용하기 까지는 앞으로 많은 시간이 필요할 것으로 예상된다.

2. ICON Overview

2.1. Hyperconnect the World

ICON Project는 '연결'을 통해 우리의 일상을 풍요롭게 만들기 위해 시작되었다. 인류가 이룩해온 기술혁신의 역사는 결국 '연결'의 역사이다. 문자의 발명은 직접 만나지 않아도 서로의 생각이 연결될 수 있게 했다. 전화는 서로 먼 곳에 있어도 실시간으로 연결될 수 있게 했고, 무선 통신은 이동 중에도 연결이 가능한 세상을 열었다. 그리고 인터넷의 등장으로 전세계 어디든 실시간 연결이 가능해졌다. 연결의 비약적 혁신에도 불구하고 현재의 연결은 여전히 완벽하지 않다. 우리는 ICON Project를 통해 보다 완벽한 연결에 한걸음 더 다가가고자 한다.

스타벅스에서 카페라떼 한 잔을 주문하고 신용카드를 건네는 행위만으로 간편하게 결제가 이루어지는 세상에 우리는 살고 있다. 그러나 실제로 이 과정은 겉으로 보이는 것보다는 복잡한 과정을 거친다. 스타벅스에 설치되어 있는 카드단말기를 통해 읽어들인 카드번호, 유효기간, 청구지 우편번호, CVC 번호 등의 정보는 FEP(Front-end processor) 회사 등 총 7개 중개기관의 DB에 저장되고 파이프라인을 거쳐 전달되는 과정을 거치게 된다. 이 과정에서 단계마다 다양한 수수료가 발생된다. 이는 기존의 연결이 중개자 또는 제3의 기관을 통해 신뢰성을 확보하는 중앙집중화된 시스템이기 때문이다.

ICON은 기존의 중앙집중화된 연결보다는 분산화된 연결을 지향한다. ICON Network의 트랜잭션은 중앙집중기관이 보장하는 신뢰가 아니라 커뮤니티 네트워크 자체의 신뢰를 바탕으로 한다. 이를 통해 불필요한 중앙집중기관의 개입은 최소화되고 여러 중개기관을 거치며 발생했던 수수료는 크게 절감될 것이다. 또한, 분산화된 연결은 커뮤니티의 자율성과 독립성을 보장할 수 있다. 중앙집중시스템을 통해 연결되기 위해서는 중앙집중기관이 정한 정책과 시스템을 수동적으로 수용할 수밖에 없다. VISA나 Master 카드를 결제에 활용하기 위해서는 그들이 지정하는 시스템을 사용하고 그들이 정하는 정책을 따를 수밖에 없었다. 그러나 ICON Network에서는 각각의 커뮤니티가 적합한 시스템과 정책을 내부에서 자율적으로 결정하면서도 다른 커뮤니티와 연결이 필요할 경우 신뢰성 있는 연결이 가능하다.

ICON Network를 통한 분산화된 연결은 중앙집중시스템에 존재했던 다양한 경계들을 넘어설 수 있게 해줄 것이다. 한국의 주식투자자는 미국의 주식투자자로부터 애플 주식을 실시간으로 매매하고, 한국 대학병원의 당뇨병 전문의는 시드니와 런던 병원의 당뇨병 환자 데이터를 함께 연구할 수 있게 된다. 경계를 넘어서는 연결은 자산과 권리의 토큰화(Tokenization)를 통해 가속화되고, 네트워크의 역동성은 극대화될 것이다. 토큰화는 점차 다양한 영역에서 광범위하게 일어날 것이다. 기존 화폐의 토큰화[4]는 물론이고, 부동산, 자동차 등의 유형자산, 특허권, 저작권, 상표권과 같은 무형자산, 투표권이나 시민권 등의 같은 법적 권리, 심지어는 DNA 분석 데이터나 혈액검사 결과 데이터들까지 토큰화가 이루어질 것이다. 이러한 토큰화는 시공간의 경계를 희미하게 하고 유형과 무형의 선 긋기를 무의미하게 한다. 아파트 0.2채와 자동차 0.8대의 교환이 가능해지며, SNS

에 올린 글 5개로 보험료를 납부할 수 있게 된다.

ICON은 경계를 넘어서는 실시간 트랜잭션과 자유로운 협업이 가능한 무한한 확장성을 가진 연결을 통해 인류의 연결을 한 걸음 더 발전시키고자 한다.

2.2. How to Design

ICON Project는 특정 블록체인 또는 커뮤니티 내 Node들의 연결 뿐만 아니라 커뮤니티와 커뮤니티 간 연결에 대한 연구이며, 가상화폐세계 뿐만 아니라 현실세계에 적용하는 것을 목적으로 시작되었다. 우리는 ICON Network를 설계하기 위해 다음 3가지 질문에 대하여 고민하였다. 첫째, 무엇을 연결할 것인가? 둘째, 어떻게 연결할 것인가? 셋째, 어떻게 작동해야 하는가? 이러한 질문에 답하기 위해, 우리는 ICON Network를 구성하는 요소들을 정의하고, 각 구성요소들이 연결되는 방식에 대하여 고민하였다. 그리고 연결된 네트워크들이 효과적으로 작동하기 위한 거버넌스를 연구하였다.

2.3. Components of the ICON Network

ICON Network의 구성요소: ① Community, ② C-Node(Community Node), ③ C-Rep(Community Representative), ④ ICON Republic, ⑤ Citizen Node

Community

동일한 거버넌스를 가지는 Node들로 구성된 네트워크이다. 금융, 정부, 학교, E-Commerce, Healthcare, BTC, ETH 등이 각각 Community가 될 수 있다. 각 Community는 각자의 특성 및 상황에 따라 Node의 구성 및 규모를 달리한다.

C-Node

C-Node(Community Node)는 Community의 구성단위로 Community 내의 합의 또는 거버넌스를 결정하는데 영향을 미친다. C-Node는 개인 또는 기관(은행, 증권사, 보험사, 학교, 정부 등) 모두 가능하며 Node에 대한 정책은 각 Community에서 결정한다.

C-Rep

C-Rep(Community Representative)은 Community를 대표(Representation)하는 단위이며, 동시에 ICON Republic의 거버넌스를 구성하는 단위로 ICON Republic 상에서 발생한 거래에 대한 검증과 거버넌스에 대한 투표권을 가진다. C-Rep은 각 Community 내부의 의사결정에 따라 선정되며, 특정한 C-Node가 지속적으로 C-Rep일 필요는 없다. 각 거버넌스의 상황 및 목적에 따라 C-Rep은

변경 가능하다. 또한, C-Rep은 ICON Republic을 유지하고 활성화하는 대가로 보상(Incentives)을 받게 된다.

ICON Network에 대한 기여도를 기준으로 상위 일정 범위에 포함되는 Community의 대표 Node만이 C-Rep이 될 수 있다. 여기에서 해당 대표 Node의 ICON Network에 대한 기여도는 ICON의 AI 기반 점수 시스템인 IISS(ICON Incentives Scoring System)를 통해 측정된다. 기준치 이상의 I_score(IISS 점수)를 일정 기간 이상 유지한 대표 Node는 C-Rep으로서의 최소 요건을 갖추게 되며, 최종적으로 Representation channel에서 기존 C-Rep 간 합의 과정을 거쳐 해당 대표 Node의 C-Rep 선정 여부가 결정된다. 구체적인 C-Rep 수의 상한과 C-Rep 자격 획득을 위한 최소 요건 등은 C-Rep 간 합의를 통해 조정될 수 있다.

ICON Republic

ICON Republic은 Community들이 연결되고 모이는 지점으로, 각 Community를 대표(Represent)하는 C-Rep과 Citizen Node들로 구성된다. ICON Republic의 거버넌스는 C-Rep의 투표로 결정된다. ICON Republic은 다양한 종류의 Community를 연결하는 탈중앙화된 네트워크이다. ICON Republic은 하나의 Community에서 다른 Community로 이동하는 통로로써 작동할 뿐, 다른 Community의 거버넌스에는 영향을 미치지 않는다.

Citizen Node

Citizen Node는 ICON Republic의 Node 중 하나로, 누구나 loopchian 기반의 DApp 생성을 통해 참여할 수 있다. 다만, Citizen Node는 ICON Republic의 거버넌스에 대한 직접 투표 권한은 없고, 거래 생성 권한만을 가진다.

2.4. How to Connect

ICON Network에서 연결의 종류: ① 단일 Community 내 Node 간 연결, ② ICON Republic 내 Node 간 연결, ③ Community와 ICON Republic의 연결, ④ Community와 Community의 연결

단일 Community 내 Node 간 연결

Community들은 각각의 특성에 맞는 종류의 블록체인을 선택할 수 있다. 그렇기 때문에, 금융, 정부, 학교, E-Commerce, Healthcare, BTC, ETH 등 각각 Community는 서로 다른 블록체인으로 구성될 수 있으며, 각기 다른 합의 알고리즘을 사용할 수 있다.

ICON Republic 내 Node 간 연결

ICON Republic은 loopchain을 기반으로 연결된다. ICON Republic은 가상세계(Crypto-world) 뿐만 아니라 현실세계(Real world)에 존재하는 다양한 커뮤니티들을 연결하는 것을 목표로 설계되어, 실시간 트랜잭션 처리가 가능한 합의 알고리즘을 적용하였다. ICON Republic은 각각의 Community와는 별개의 거버넌스를 갖고 있으며 독자적인 합의 알고리즘(LFT)으로 작동한다.

Community와 ICON Republic의 연결

Community와 ICON Republic은 DEX(Decentralized Exchange)를 통하여 실시간(Real-time)으로 연결된다. DEX는 Community와 ICON Republic에 Reserve를 설정함으로써 교환비율을 제공하고, 해당 교환비율을 통하여 실시간 가치 교환이 가능하다. 다만, 실시간으로 합의가 가능하지 않은 Community와의 연결의 경우(e.g. Bitcoin, Ethereum 및 Ethereum 기반 Cryptocurrency)에는 해당 Community에서 합의가 완료될 때까지 ICON Republic과의 합의가 완료되지 않는다.

Community와 Community의 연결

Community와 Community의 연결은 ICON Republic을 통해서 가능하다. ICON Republic은 DEX(Decentralized Exchange)를 통해 실시간(Real-time)으로 각 Community들과 연결되고, C-Node는 C-Rep과 ICON Republic을 통해 다른 Community에 속한 C-Node들과 실시간으로 연결된다.

2.5. How to Operate

Community

각 Community는 해당 Community에서 사용하는 블록체인의 특성에 따라 자체 거버넌스를 바탕으로 독립적으로 운영된다. 합의 알고리즘, 합의 참여 Node, Community 내 가상화폐 운영 등 모든 사항에 대하여 ICON Republic과는 독립적으로 합의하고 의사결정 할 수 있다.

ICON Republic

ICON Republic의 거버넌스는 C-Rep들의 합의과정을 통해 결정되고, 거버넌스의 범위는 ICON Republic으로 한정된다. ICON Republic은 다른 Community의 거버넌스에는 영향을 미치지 않는다.

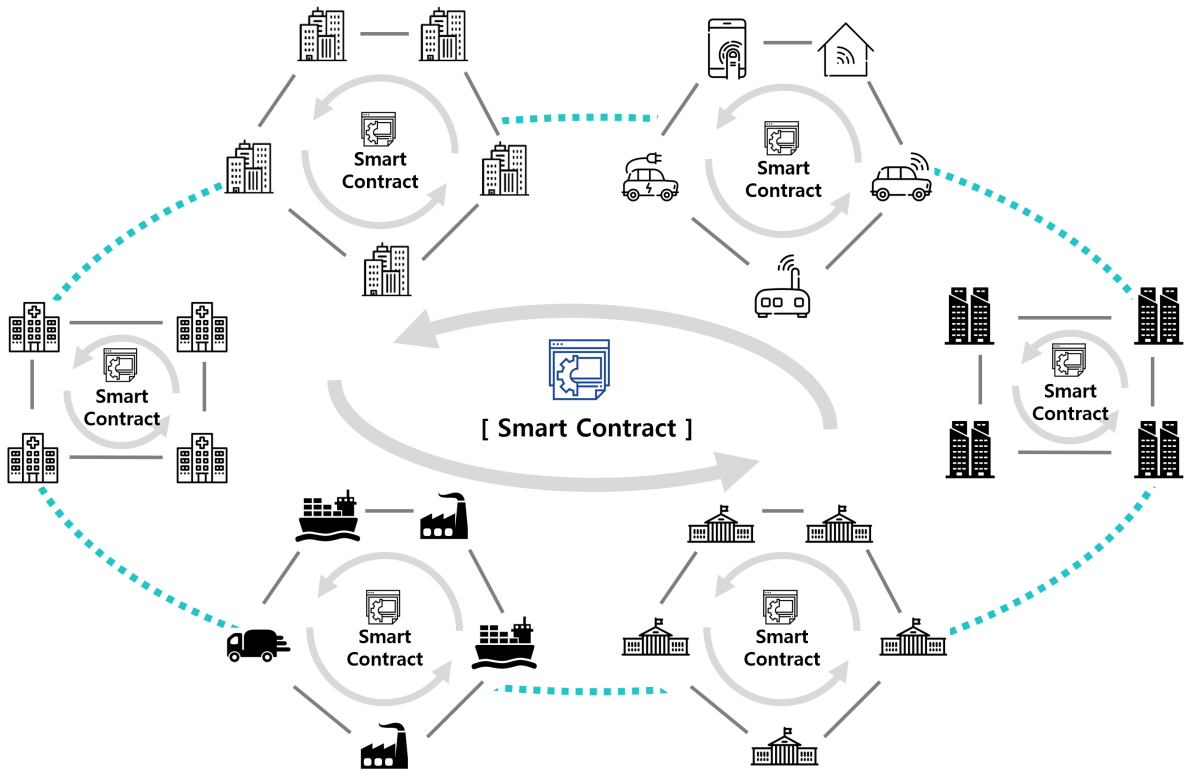
2.6. What to Expect

전세계적으로 금융, 공공, 물류, 헬스케어, IoT, 전력, 제조, E-Commerce 등 수많은 분야에서 각각의 업무 특성에 맞는 다양한 Community가 형성되고 있다. 블록체인 기술의 발전과 확산으로 이러한 Community는 양적으로나 질적으로 성장세가 가속화될 것으로 보인다. 이와 같은 환경에서

는 대부분의 업무들이 Community 내부에서 스마트컨트랙트를 통해 자체적으로 처리되고, 각 분야에 존재하던 수많은 중앙집중기관과 중개자들의 역할은 점차 축소되거나 사라지면서 업무처리의 패러다임 전환이 가속화될 것이다.

Community 중심 업무환경으로의 변화는 커뮤니티 내부의 업무처리 방식에만 영향을 미치는 것이 아니라, Community와 Community 간의 업무처리 방식에도 근본적인 변화를 가져올 것으로 예상된다. 일반적으로 대부분 Community가 초기에는 Community 내부 구성원 간의 업무처리 효율성 개선에 목표를 두고 시작하지만, 많은 경우에 점차 외부와의 트랜잭션이 증가하는 방향으로 자연스럽게 진화하게 된다. 이 경우 기존과 같이 중앙집중화된 별도의 기관을 거쳐 외부와의 업무를 처리하는 것이 아니라, 각 Community의 스마트컨트랙트가 트랜잭션의 주체가 되어 스마트컨트랙트와 스마트컨트랙트의 연결을 통해 업무 처리가 이루어지게 될 것이다.

블록체인 기술의 확산이 만들어낼 메가트렌드에서 ICON은 Community와 Community를 연결하여 ICON Republic 내의 모든 Community들이 스마트컨트랙트를 기반으로 실시간으로 업무를 처리할 수 있는 환경을 한 발 앞서 만들어 가고자 한다. ICON을 통해 연결되는 Community의 수가 증가할수록 ICON Republic에서의 트랜잭션은 기하급수적으로 증가하고, ICON을 통해 서로 연결된 각 Community 내부 구성원들의 효용은 극대화될 것이다.



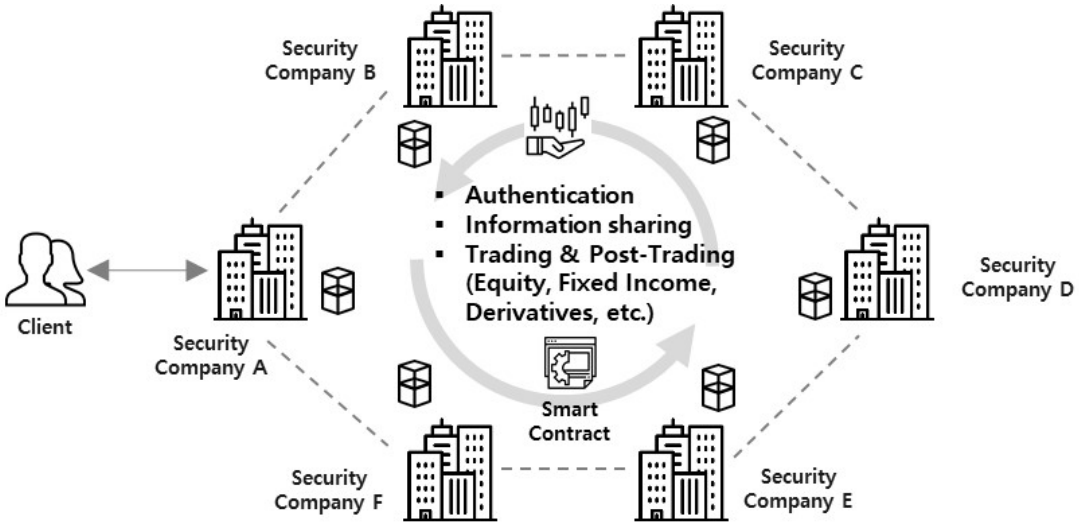
2.7. Implementation of loopchain

우리는 loopchain을 기반으로 자본시장, 보험, 대학교, 헬스케어 등 다양한 커뮤니티에서 실제 블록체인을 적용하는 사례를 만들어가고 있다. 각각의 커뮤니티는 각 커뮤니티 내부의 니즈로 블록체인을 도입하기 시작했으나, 다른 커뮤니티와의 연결을 통한 다양한 비즈니스 확장 아이디어를 만들어내며 스스로 진화해가고 있다. ICON Network는 이러한 커뮤니티들의 상호 연결 니즈를 지원하며 모든 블록체인 커뮤니티들을 서로 연결하게 될 것이다.

Capital Market

국내 주요 25개 증권사 및 금융투자협회가 참여하고 있는 '금융투자업권 블록체인 컨소시엄'은 더루프가 개발한 loopchain을 기반으로 자본시장의 블록체인 기반 혁신을 추진해 나가고 있다. 컨소시엄에서 추진하는 첫 번째 서비스인 블록체인 기반 공동인증서비스("Chain ID")는 BSI(Blockchain Signature Infrastructure) 기반으로 인증서를 발급하여 별도의 인증기관 없이 사용자와 금융기관간 직접적인 인증 및 전자서명 생성 및 검증이 가능한 서비스로 2017년 10월 말에 공식 오픈되었다. 본 컨소시엄은 loopchain의 스마트컨트랙트 구현환경인 SCORE를 통해 Authentication, Post-trading, Trading 등 자본시장 업무 프로세스 전반에 대하여 단계적으로 블록체인 적용 범위를 넓혀갈 계획이다.

자본시장에서는 전세계적으로 다양한 거래가 다수의 중개기관과 중앙집중기관을 통해 끊임없이 이루어지고 있다. 거래의 체결과 청산결제를 위해 여러 기관을 거치면서 결제 프로세스는 길어지고 후선(Back office) 업무는 복잡해진다. 그 결과 주식매매 후 청산결제 업무가 완결되기까지는 일반적으로 2일에서 3일이 소요되며, 미국 시장에서만 이와 같은 후선업무 처리를 위해 연간 90억 달러를 지출하고 있는 실정이다.

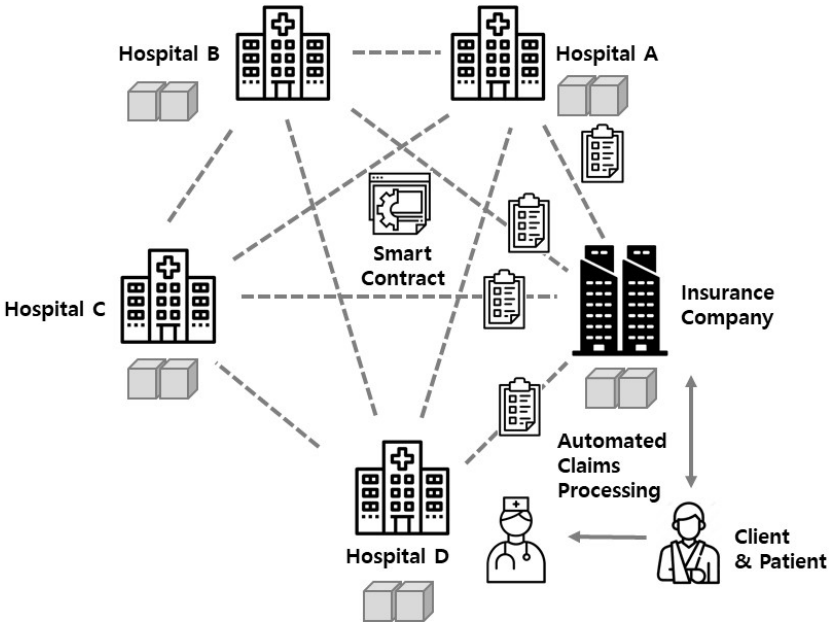


Insurance

국내 Top-tier 생명보험사는 더루프가 개발한 loopchain을 기반으로 메이저 대학병원 등과 함께 블록체인을 활용한 보험금 청구 및 지급에 대한 시범사업을 추진하고 있다. 실손보험 등 보험 가입자가 병원 치료를 받은 후에 진단서를 비롯한 보험금 청구에 필요한 개인정보를 보험사에 전달하는 것에 대한 동의 및 보험사 가입 정보를 기반으로 환자의 신원을 확인하는 등의 업무를 블록체인을 기반으로 중개자 없이 처리하여 보험금 청구가 자동적으로 이루어진다. 본 시범사업은 loopchain의 스마트컨트랙트 환경인 SCORE를 통해 구현되었으며, 2017년 12월 초부터 실손보험 등 일부 상품을 대상으로 시범사업을 시작했다. 본 사업은 2017년 4월 미래창조과학부 블록체인 지원사업에 선정되어 더 강력한 추진력을 확보하였고, 향후 타 보험사 및 타 상품으로의 확장에도 더욱 탄력을 받을 수 있을 것으로 보인다.

블록체인은 보험업 밸류체인[5] 전반에 걸쳐 혁신을 일으키고 있다. 특히 보험금 청구 및 지급 업무의 혁신은 보험사 관점에서 업무 프로세스 효율성 향상을 통한 비용 절감을 가능케 함은 물론이고 소비자의 편의성 또한 제고함으로써 보험업 전반에 대한 만족도 향상에 크게 기여할 것이다.

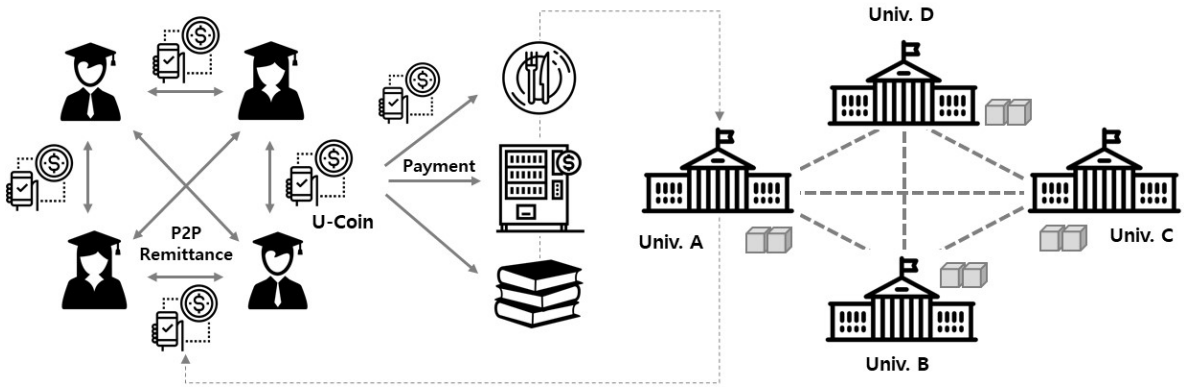
보험업은 타 금융업권에 비해 외부 기관과의 트랜잭션(데이터 및 자금 양 측면에서 모두)이 빈번하게 발생하고 그 중요성 또한 크다. 그러나 외부 기관들은 일반적으로 각 기관의 특성에 맞는 다양한 시스템을 기반으로 운영되고 있어 해당 기관들과의 트랜잭션이 효율적으로 운영되지 못하고 있다. 블록체인은 다양한 시스템 간의 상호운용성(Inter-operability)을 확보함과 동시에 상호 신뢰성을 확보함으로써 다양한 기관들 간 트랜잭션의 효율성을 극적으로 향상시킬 수 있다. 이러한 기대들로 인해 보험업 및 이를 둘러싼 생태계에서 블록체인의 활용은 가속화될 것으로 보인다.



University

U-Coin은 대학생을 주 사용계층으로 하는 가상화폐(U-Coin: University Coin)로 2017년 12월 말 국내 주요 대학을 대상으로 첫번째 파일럿 서비스를 시작했으며, 2018년 상반기 런칭 계획이다. U-Coin은 사업성과 기술력을 인정받아 2017년 4월 미래창조과학부의 블록체인 지원사업으로 선정되어 더욱 추진력 있게 진행되고 있으며, 대상 대학교 및 활용 범위는 점차 확대될 예정이다. 자동판매기를 포함하여 캠퍼스 및 인근 가맹점에서 쉽게 사용할 수 있는 가상화폐 기반 간편 결제·송금 시스템 구축을 시작으로 다른 커뮤니티와의 연계도 확대해 나갈 예정이다.

대학생들은 신기술에 대한 수용성이 가장 높은 계층 중 하나로 언제나 혁신 기술을 가장 먼저 경험하고 주변에 전파하는 역할을 해왔다. 특히, 혁신의 속도가 가속화되고 있는 상황에서는 세대별, 계층별 신기술 수용도의 격차가 더욱 확대될 수밖에 없다. 이러한 경향은 가상화폐 시장에서도 마찬가지이다. 궁극적으로 가상화폐가 현실세계 깊숙하게 보급 및 확산된다고 가정할 때, 대학생 커뮤니티는 그 어떤 세대나 계층보다 가장 먼저 가상화폐를 사용하고 전파하는 얼리어답터의 역할을 수행할 것이다.



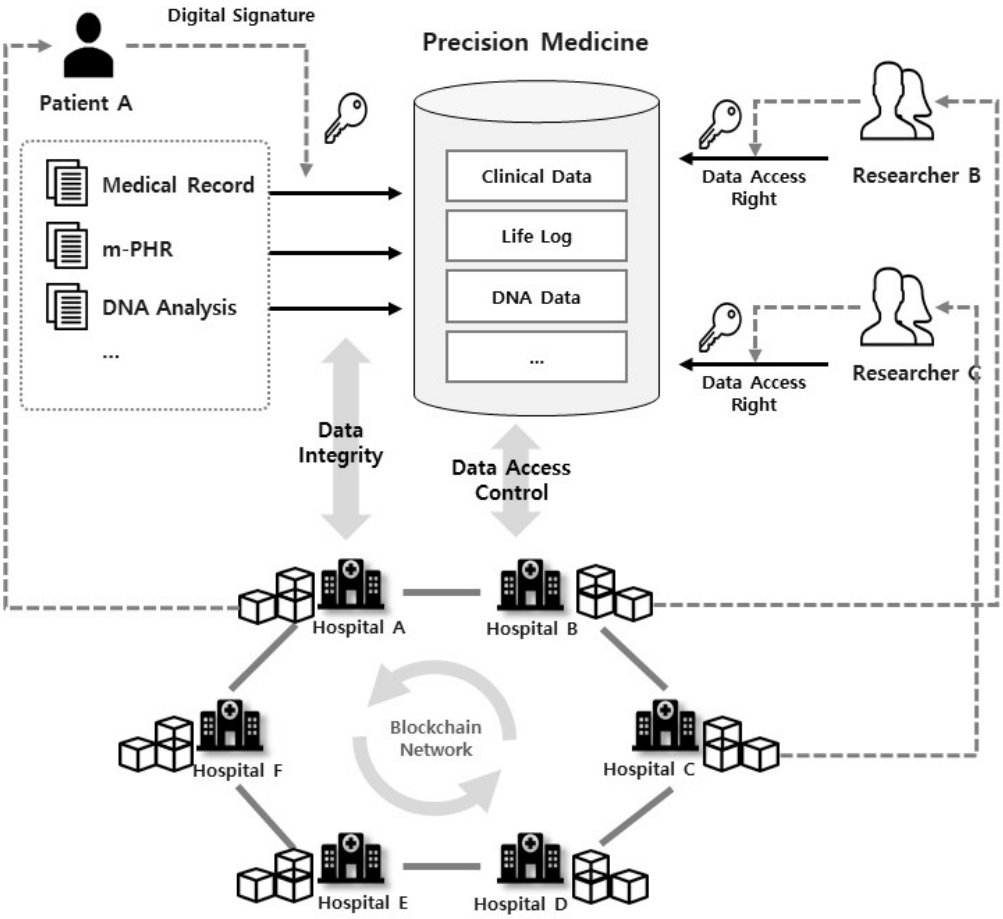
Healthcare

국내 주요 병원이 대부분 참여[6]하는 정밀의료병원정보시스템(P-HIS) 구축 프로젝트에는 더루프가 개발한 loopchain이 도입될 예정이며 OHDSI(Observational Health Data Sciences and Informatics)[7] 등 글로벌 네트워크를 기반으로 의료정보 유통의 범위를 전 세계로 확대할 계획이다. 본 컨소시엄에서는 블록체인을 기반으로 의료정보의 안전하고 투명한 공유 및 유통체계를 구축하고 관련 생태계 활성화를 위해 가상화폐 도입을 추진하고 있다.

의료정보는 예방, 진단, 치료, 연구 등 의료 서비스 전반의 효율성 향상 및 경쟁력 강화를 위해서 공유가 필수적인 반면, 가장 민감한 영역의 개인정보로 무분별하게 사용되거나 유출될 경우 큰 피해가 발생할 수 있다. 또한, 최근 진단(NGS 등) 및 IT 기술(웨어러블 기기 등)의 발달로 의료정

보의 범위와 양이 폭발적으로 증가함에 따라 다양한 레벨의 데이터 트랜잭션을 효율적으로 처리하면서도 보안성과 안정성을 확보하는 방법에 대한 논의가 활발하게 이루어 지고 있다.

블록체인은 의료정보를 둘러싼 복잡한 문제를 해결하고 관련 산업을 활성화 시킬 수 있는 대안으로 부상하고 있다. 블록체인을 활용하면 각기 다른 병원시스템 간의 상호운용성(Inter-operability)을 확보할 수 있고, 데이터에 대한 접근권한 관리 및 접근 기록을 신뢰성 있게 관리할 수 있다. 블록체인 기반의 투명한 의료정보 유통과 체계적이고 공정한 보상체계를 바탕으로 의료정보 유통 생태계는 더욱 활성화될 것으로 보인다.



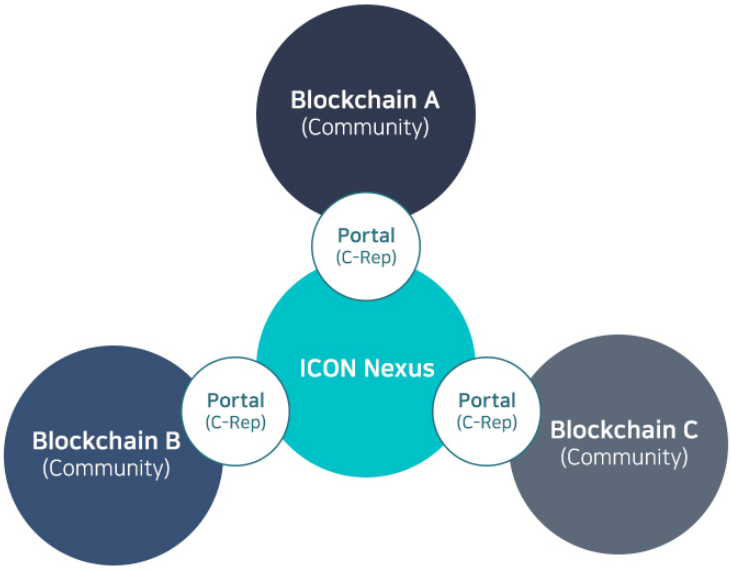
3. ICON Architecture

3.1. Introduction

ICON은 블록체인으로 구성된 다양한 독립적인 Community들을 각 Community를 대표하는 C-Rep(Community Representative)을 통해 연결하여 하나의 Republic과 같은 네트워크를 구성하는 프로토콜과 그 형상을 말한다. ICON에서 Republic을 구성하는 블록체인 네트워크를 Nexus라고 하고 C-Rep은 Portal로 구성하여 Nexus에 연결된 블록체인들은 Portal을 통해 토큰 이동 및 다양한 거래를 빠르고 신뢰할 수 있게 처리할 수 있다. 하나의 Nexus는 Nexus에 상응하는 또 다른 블록체인 네트워크와 연결이 가능하며 이를 통해 블록체인 네트워크가 다양하게 확대 가능하다.

3.2. Conceptual Model

ICON은 Nexus를 중심으로 다양한 블록체인이 Portal을 통해 연결된다. Nexus는 loopchain을 기반으로 구현된 블록체인으로서 다른 블록체인을 연결하는 Portal 및 여러 Node가 참여하여 탈중앙화된 거버넌스를 구현한다. Nexus에 연결된 블록체인은 Portal을 통해 BTP(Blockchain Transmission Protocol)을 기반으로 다양한 블록체인간 거래 연동이 가능하다. 이러한 구조는 하나의 거버넌스를 가지는 네트워크를 다른 네트워크에 연결하여 '네트워크의 네트워크'를 구현한 결과 모든 컴퓨터가 하나의 통신망 안에 연결된 인터넷과 같은 구조이다.



인터넷은 TCP/IP라는 표준 인터넷 프로토콜을 사용해 전 세계를 연결하는 지구 전체의 컴퓨터 네트워크 시스템이다. ICON도 BTP라는 표준 프로토콜을 사용해 거대한 블록체인 네트워크를 구축하고자 하며 하나의 블록체인으로 모든 구성원이 연결되는 방식이 아닌 여러 블록체인마다 독립적

인 거버넌스를 보장하면서 필요에 따라 연결되는 방식을 추구한다.

3.3. Nexus

Nexus는 연결된 블록체인 각각의 Light Client들로 구성된 Multi-channel 블록체인이다. 각각의 블록체인은 Portal을 통해 Nexus로 연결되며 기본적으로 Portal은 독립적인 블록체인 네트워크의 대표로서 Nexus 블록체인 네트워크에 Node로서 참여하게 된다. Nexus는 loopchain을 기반으로 구축되어 loopchain의 특성인 그룹화에 따라 LFT 기반 consensus가 이루어진다. Nexus에는 운영 정책을 제안하고 투표를 통해 적용할 정책을 선정하는 Representation channel이 포함되어 있으며 기본적으로 Portal은 자신의 커뮤니티를 대표하는 C-Rep으로써 Representation channel에 참여한다.

Nexus에는 기본적으로 ICX(ICON Exchange)라는 Token이 내재되어 있으며 연결된 블록체인들은 ICX를 통해 다양한 블록체인 간 가치 이동을 처리할 수 있다. Nexus 역시 하나의 블록체인으로서 또다른 Nexus에 연결될 수 있으며 이러한 결합을 통해 다채로운 거버넌스를 가지는 블록체인들이 연결되어 거래를 연동하거나 가치를 이동시킬 수 있다.

3.4. Portal

Portal은 독립적인 블록체인과 Nexus를 연결시키는 구성요소로서 Nexus와 BTP 기반의 통신을 통해 연동된다. Portal은 하나 혹은 복수의 Node로 구성될 수 있으며 필요에 따라 또 다른 합의 네트워크를 만들 수도 있는데 이는 오롯이 해당 블록체인의 정책에 따른다.

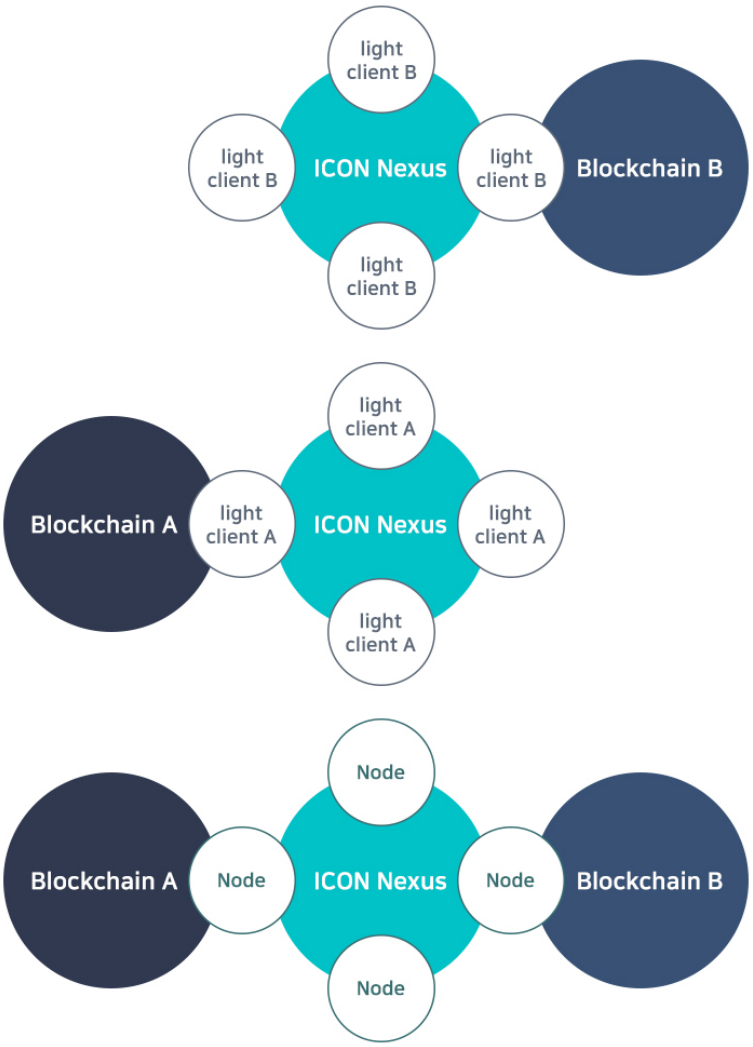
이는 나라별로 독립적인 통화체계를 갖추고 SWIFT[8]를 통해 은행들이 연결된 현재 구조와 비교하면 한 나라에서 SWIFT를 이용할 수 있는 은행이 여러 개인 것과 같은 구조이다. Nexus에 참여한 Portal의 Node 수 역시 하나 혹은 복수가 될 수 있으며 이는 loopchain의 그룹화 기능을 통해 하나의 그룹으로 관리된다. 한 블록체인의 Portal은 C-Rep으로서 해당 블록체인을 대표하여 Representation Channel에서 정책을 제안하고 투표를 함으로써 탈중앙화된 거버넌스를 수행하게 된다.

3.5. BTP(Blockchain Transmission Protocol)

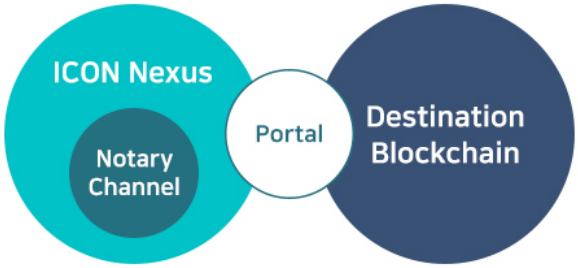
BTP는 Nexus와 연결된 블록체인 간 거래를 연계하기 위한 프로토콜이다. Nexus에 구성된 Notary channel을 통해 송신 블록체인의 거래가 수신 블록체인으로 전달되게 된다.

이를 위해 Nexus 구성 Node 중 Notary channel의 투표권한이 있는 Node는 Nexus에 연결된 각 블록체인의 Light Client를 하나의 채널로 한 다수의 채널을 보유하고 있다. Notary channel은

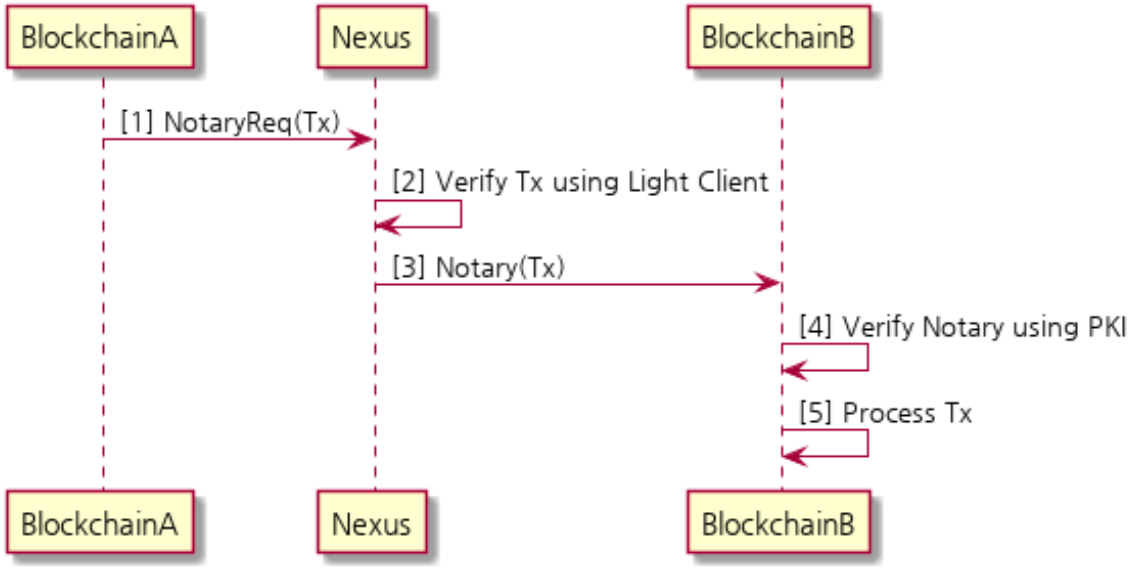
loopchain의 Multi-channel 지원 기능을 기반으로 구현되며 Nexus에 연결된 블록체인의 Light Client를 통해 해당 블록체인에서 합의된 거래를 Nexus에서 확인할 수 있다.



Notary 등록 요청 거래에 대해 투표권이 있는 Node들의 복수의 서명이 블록에 포함되어 Notary channel의 블록체인을 이루게 된다. Notary channel에 등록된 거래가 포함된 블록 데이터는 Portal을 통해 수신 블록체인으로 전달된다. 이후 수신 블록체인에서 해당 블록 데이터를 검증할 때는 Nexus의 Notary channel을 구성하는 Node들의 인증서를 기반으로 각 Node의 서명을 검증하고 LFT 기반의 합의를 따르는 Notary channel 규격에 따라 2/3 이상의 서명이 확인되면 해당 거래의 합의 여부가 확인되어 거래를 진행한다.



BTP는 송신 블록체인에서 발생한 거래의 합의 여부를 Nexus에서 확인하는 NotaryRequest(Tx)와 Nexus에서 확인한 거래를 수신 블록체인으로 전달하는 Notary(Tx)로 구성된다. 송신 블록체인에서 시작된 거래는 Nexus에서 해당 블록체인의 Light Client을 통해 확인되고 Notary channel에 등록된다. Notary channel에 등록된 거래는 수신 블록체인으로 전달되고 수신 블록체인은 전달된 Notary 블록의 서명을 검증하여 Nexus에서의 합의 여부를 검증한 후 해당 거래를 처리한다.



3.6. DEX(Decentralized Exchange)

DEX[9]는 일반적인 가상화폐 거래소처럼 Third party를 통해 거래하는 Centralized exchange가 아닌 블록체인 상에서 자동으로 거래를 처리해주는 시장이다. Centralized exchange는 사용이 쉽고 예약 거래 및 마진 거래 등 다양한 거래가 가능한 장점이 있지만 사용자가 거래소를 완전히 신뢰해야만 하며 회원가입 후 이용하기 때문에 익명거래가 어렵다. 특히 Mt.Gox 사태[10] 처럼 해킹 등의 사고 발생시 피해가 사용자에게 전가되는 문제점들이 있다. 이에 반해 DEX는 특정한 거래소를 신뢰

할 필요없이 자동화된 거래가 가능하고 완전한 익명거래를 지원하며 거래소 다운이나 해킹 이슈가 없다. 대표적인 DEX로는 Bitsquare[11], Bitshares[12] 등이 있으나 사용자가 거래시에 항상 온라인이어야 한다거나 유동성이 쉽게 부족해지는 등의 문제가 있었다.

ICON은 자체적인 거버넌스를 가지는 여러 블록체인들을 연결하는 블록체인 네트워크로서 ICX 기반의 DEX를 제공한다. Bancor Protocol[13] 을 기반으로 Reserve를 통한 거래 가격을 산정하여 가상화폐 간 거래를 제공한다.

ETH와 ICX간 거래의 경우 Ethereum내에 Reserve 스마트컨트랙트와 ICON내 Reserve 스마트컨트랙트에 투표권이 있는 Node로 DEX를 구성할 수 있으며 이 경우 아래와 같은 형태로 ICX의 가격이 형성된다.

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

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

DEX를 통해 ETH로 ICX를 구매할 경우 ETH로 구성된 Reserve Balance가 늘어나고 ICX Volume은 줄어들어 결과적으로 ICX Price가 올라간다. 반대로 ICX로 ETH를 구매하게 되면 Reserve Balance가 줄어들고 ICX Volume이 늘어나게 되어 ICX Price가 떨어지게 된다. 자세한 구매가격 및 ICX 토큰 수 계산은 Formulas for Bancor system[14] 을 참고한다.

ICX가 다른 거래소에 상장되어 거래될 경우 해당 거래소에서의 가치와 ICON DEX에서의 가치가 다를 수 있다. 이경우 Arbitrage 거래가 발생하게 되고 ETH 유입 및 환전이 이루어져 가격이 비슷해지게 된다.

이러한 ICX 기반 DEX 체계를 통해 ICON에 연결된 다양한 독립 블록체인의 자체 가상화폐와 거래가 가능하다. 특히 loopchain과 같은 BFT[15] 계열의 합의 알고리즘을 사용하는 블록체인의 경우 환전이 실시간으로 이루어진다. 예를 들어 Nexus에 연결된 금융기관용 블록체인이 있고 해당 금융기관끼리만 사용하는 Fcoin 이라는 가상화폐가 있을 경우, Fcoin과 ICX로 구성된 Reserve를 기반으로 Fcoin DEX 서비스가 제공되며 Fcoin과 ICX는 실시간으로 거래가 가능하다. 또한 이렇게 변환된 ICX를 이용해 ICON에 연결된 다른 가상화폐와 교환이 되므로 결과적으로 서로 다른 가상화폐 간 거래가 실현된다.

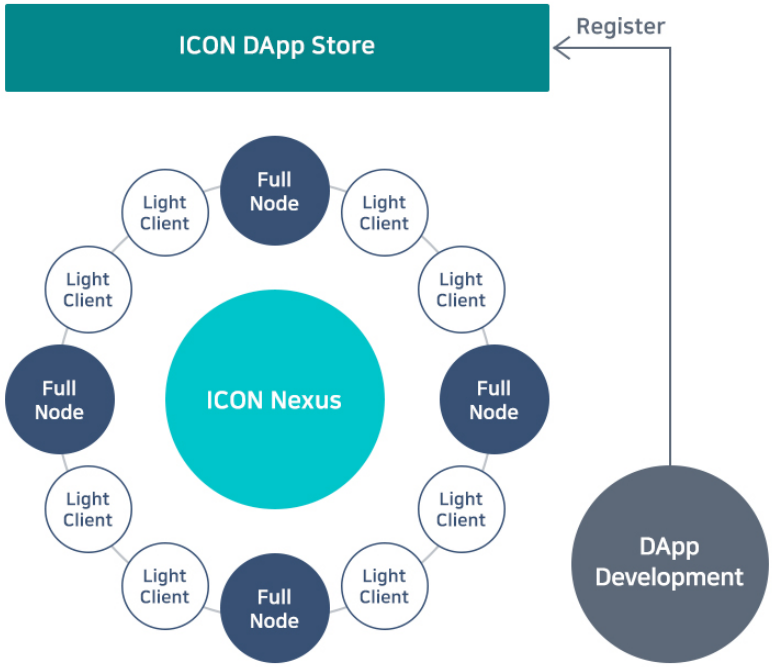
ICON DEX의 또다른 주요한 특징은 가상화폐 간 거래에 있어 전체 통화량, 거래 빈도 및 가격 등의 누적된 데이터를 기반으로 A.I. 분석 모델[16] 수립이 가능하다는 점이다. 이러한 데이터를 통해 Reserve Rate과 각 가상화폐의 Reserve 구성 비율 등 다양한 조절이 가능하게 되어 실생활에서 사용 가능한 안정감 있는 가상화폐를 구현할 수 있다.

3.7. Nexus Public Channel

Nexus에는 모든 사람에게 공개된 Public channel이 포함되어 있다. 이는 loopchain의 Multi-channel 지원 기능을 통해 Nexus에 구현되며 이름 그대로 이더리움이나 비트코인처럼 누구나 Public channel에 참여할 수 있다. Public channel에 참여한 사용자는 ICX 거래뿐 아니라 다양한 DApp[17]을 만들고 이용할 수 있다. Public channel에서의 DApp의 개념은 이더리움과 비슷하나 배포 및 실행하는 방법에는 차이가 있다. 이더리움은 거래 데이터에 컴파일한 코드를 포함시키고 VM(Virtual Machine)으로 해당 코드를 실행시키는 방식을 사용하는데 반해 Public channel에서는 사전에 DApp을 개발하여 DApp Store에 등록하고 해당 거래에 참여할 Node는 DApp Store로부터 DApp을 받아서 설치한 후 이용하게 된다.

Public channel에 참여하는 Node는 거래를 등록하고 확인할 수 있는 Light Client 기반의 Node와 거래에 대한 합의를 이루는 Full Node로 나뉘어진다. Full Node의 경우 ICX 거래, 스마트 컨트랙트 운영, DApp 운영 등에 있어 핵심적인 역할을 담당하는 만큼 일정한 자격 조건이 요구된다. ICON Republic 내에서 규정된 자격 조건을 갖춘 Node만이 개별 C-Rep의 선정을 거쳐 Full Node가 될 수 있다.

거래 참여자들의 Transaction fee로 수취된 ICX는 Full Node와 Light Client에게 지급되며, 이는 각 참여 주체에게 블록 생성과 거래 정보 검증에 대한 인센티브로서 작용하게 된다.



3.8. Governance

ICON은 기본적으로 탈중앙화된 거버넌스를 지향한다. Nexus에 연결된 각각의 블록체인은 자체적인 거버넌스를 가지고 있으며 Nexus는 일종의 간접민주주의[18]처럼 각 블록체인의 대표들이 원칙에 따라 공정하게 배분된 투표권을 가지고 협의를 진행하게 된다. 이를 위해 Nexus에는 BTP 처리를 위한 Notary channel 외에 정책 제안 및 투표를 위한 Representation channel이 포함되어 있다.

Representation channel

Nexus의 Node 중 C-Rep으로 참가하여 투표 권한이 있는 Node로 구성된 블록체인 채널로서 Nexus에서 발생하는 모든 이슈에 대한 규칙을 결정하는 협의시스템이다. Nexus에 연결된 블록체인은 기본적으로 C-Rep을 통해 투표권을 보유하고 있다. 이 외에도 ICX 거래소, 은행 등 off-chain 거래[19]를 지원하는 Node 등 다양한 Node들이 Representation channel에 참여할 수 있다. Representation channel에서는 Nexus에 신규 Node를 추가하거나 기존 Node 제거 등 Node 관리에 대한 정책을 포함하여 ICX 거래 수수료를 조정하거나 Notary, Representation channel 등 각 채널에 포함된 Node의 선정 및 제거를 관리할 수 있다.

투표권은 ICON 네트워크의 활성화에 대한 해당 커뮤니티의 기여도, 즉 I_score에 따라 배분된다. C-Rep이 아닌 참여자의 경우 I_score의 위임 계약을 통해 계약의 상대방이 되는 C-Rep의 투표권 할당량을 증가시킬 수 있다. 이를 통해 작은 규모의 커뮤니티라고 할지라도 네트워크 내 지지자 확보를 통해 Representation channel에서의 영향력을 강화시킬 수 있다.

4. Inside ICON

ICON의 코어는 loopchain이며 효율적인 스마트컨트랙트를 기반으로 실시간 거래를 지원할 수 있는 고성능 블록체인이다.

4.1. loopchain

가상화폐의 대명사처럼 일컬어지는 비트코인[20]은 분산원장으로서 블록체인 기술의 신뢰성을 실질적으로 증명하고 있다. 초기 블록체인 기술은 비트코인과 같은 가상화폐에 주력하여 다양한 가상화폐가 출현하게 되었으나 실제 금융기관에서는 도입하지 않는 등 널리 사용되지 못하고 사설 거래소를 통한 투자 수단으로 이용되고 있다. 그러던 중 이더리움[21]이 블록체인 기술을 기반으로 스마트컨트랙트[22]라는 실행 환경을 제공하게 되면서 블록체인 기술은 제도권의 폭발적인 관심을 받게 되었다. 스마트컨트랙트를 통해 중개자 없는 거래가 가능하게 되어 단순한 거래 원장 수준에 머물던 블록체인 기술은 어플리케이션 플랫폼으로 확대되었다.

금융권을 중심으로 이더리움과 같은 퍼블릭 블록체인 플랫폼을 기반으로 중개자 없는 거래를 구현하고자 하는 다양한 시도가 있었으나 초당 거래 건수가 7~15건[23]에 불과하고 거래 내역이 모든 Node에 공개되는 등의 문제로 금융과 같은 규제가 필요한 영역에 적용하는 데는 한계가 있었다. 이러한 퍼블릭 블록체인의 한계를 극복하기 위해 금융권을 중심으로 인증된 Node만 참여하는 엔터프라이즈 블록체인 기술이 대두되었다. Hyperledger Fabric[24], R3 Corda[25] 등이 대표적인 엔터프라이즈 블록체인으로 금융, 공공, 공급망 관리 등 다양한 분야에서 도입을 진행하고 있다.

엔터프라이즈 블록체인이 적용되는 도메인은 다양한 업무에 따른 요구사항과 거버넌스가 필요하기 때문에 다양한 특징을 가진 블록체인 기술이 필요하다. loopchain은 이러한 배경에서 출발하였다. loopchain은 스마트컨트랙트를 지원하는 고성능 엔터프라이즈 블록체인을 목표로 개발되었으며 업무에 따라 다양한 커스터마이징을 지원하고 특히 다른 독립적인 블록체인과의 연계를 통해 블록체인 네트워크를 확장할 수 있도록 한다.

4.2. Features

Consensus

loopchain은 BFT[26](Byzantine Fault Tolerance)를 지원하는 LFT(Loop Fault Tolerance)를 통해 분기가 없는 빠른 합의를 지원한다. 또한 LFT를 기반으로 신뢰 관계가 있는 복수의 Node를 하나의 그룹으로 묶어 좀더 빠른 합의를 이뤄낼 수 있으며 이러한 그룹 및 Node에게 투표권 수를 자유롭게 설정할 수 있어 다양한 합의 체계 구축이 가능하다.

SCORE(Smart Contract On Reliable Environment)

SCORE는 loopchain에서 지원하는 스마트컨트랙트를 지칭하는 것으로서 별도의 VM(Virtual Machine)없이 Node 운영환경에서 직접적으로 실행되는 고성능 스마트컨트랙트 지원 기능이다. SCORE는 쉽게 작성할 수 있어 높은 생산성을 가진 스마트컨트랙트이며 블록체인 프로세스와 별도의 프로세스로 동작하면서 다양한 업무를 개발할 수 있도록 지원한다.

Multi-channel

Multi-channel[27]은 하나의 독립적인 블록체인 네트워크 내에서 업무별로 채널이라는 가상의 네트워크를 구성하여 채널별로 거래 요청, 합의 및 스마트컨트랙트를 수행할 수 있는 기능이다. 하나의 Node에 여러 업무별로 해당 업무 당사자들만 연결된 다양한 채널을 형성하기 때문에 채널별로 무결성 보장 및 합의가 이루어지며 거래 데이터를 실제 거래 당사자들만 보유하게 되어 다양한 규제에 대응할 수 있다.

Tiered System

블록체인 네트워크 참여를 위한 인증과 함께 거래별로 PKI 기반 인증을 통해 거래내역 검증 및 보안이 이루어진다. 또한 거래에 참여하지 않지만 필요에 따라 거래 내역에 대한 감사를 수행할 수 있는 기능을 특정 Node에 부여하는 기능도 지원한다.

4.3. Consensus

Background

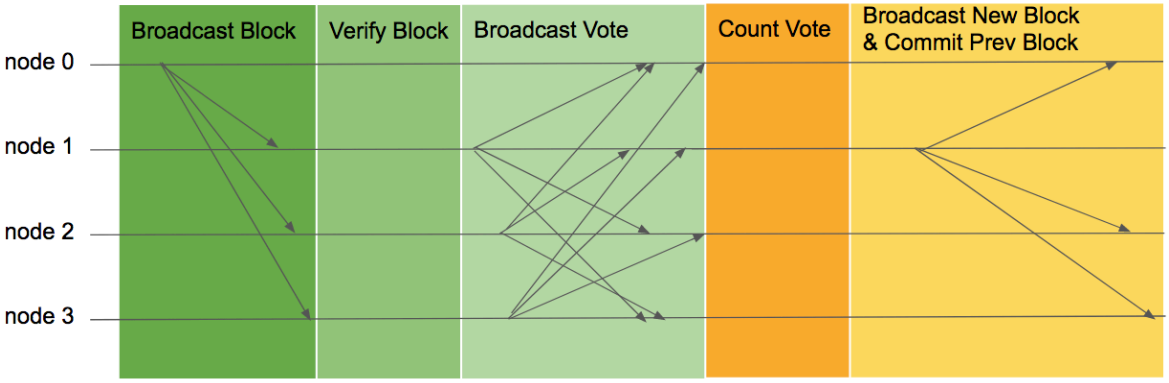
최초의 블록체인 구현 서비스인 비트코인은 작업증명[28](Proof of Work) 알고리즘을 이용하여 Global Scale의 네트워크에서 모든 비트코인 Node의 거래장부에 대한 합의를 이루었다. 그러나 비트코인에서 사용한 작업증명 알고리즘은 지나치게 낮은 속도와, 비효율적인 에너지 사용, 부분적인 네트워크 분기가 생기는 문제 때문에 효율성과, 즉각적인 결제 완료를 요구하는 환경에서 사용하지 못했다.

이러한 기존 블록체인 합의 알고리즘이 가진 문제를 해결하기 위하여 전통적 분산 상태머신 복제에 활용하는 BFT(Byzantine Fault Tolerance)계열의 합의 알고리즘이 활용되기 시작했다. PBFT[29](Practical Byzantine Fault Tolerance)로 대표되는 BFT계열 합의 알고리즘은 데이터 합의를 위해 데이터의 유효성에 대하여 투표하고 투표한 결과를 공유하는 방식으로 합의를 수행한다. Tendermint[30]는 PBFT 알고리즘을 DPOS(Delegated Proof Of Stake) 형태로 변형시킨 블록체인 합의 알고리즘을 발표하였다. 또한 엔터프라이즈용 프라이빗 블록체인 프로젝트인 IBM Fabric은 0.6버전에서 PBFT를 합의 알고리즘으로 채택하였으며 1.0버전에서는 Orderer 서비스를 위한 합의

알고리즘으로 PBFT를 단순화 시킨 합의 알고리즘인 SBFT(Simple Byzantine Fault Tolerance)를 활용하려 하고 있다.

LFT(Loop Fault Tolerance)

LFT는 전통적인 BFT 방식의 합의 알고리즘으로서 기존 분산 환경에서의 Fault Tolerance 방법으로 많이 사용하는 상태 머신 복제(State machine replication[31]) 알고리즘 중 하나인 Raft[32]알고리즘을 비잔틴 Node의 공격에도 방어할 수 있고(Byzantine Fault Tolerance) 블록체인 네트워크 특성에 최적화 되도록 개선한 합의 알고리즘이다.



블록체인 네트워크를 구성하는 객체를 Node라 칭한다. 이러한 Node들은 블록 생성, 검증, 보유의 의무를 가지며 각각의 Node는 자신의 메세지를 식별할 수 있는 서명을 생성할 수 있다. BFT 계열 합의 알고리즘을 사용하는 대부분의 네트워크의 경우 리더 Node와, 검증 Node 두 가지로 Node의 종류를 구분한다. 리더 Node의 경우 블록을 생성하고 전파하는 역할을 수행하고, 검증 Node의 경우 리더가 생성한 블록의 내용을 검증하여 블록의 유효성을 투표하는 역할을 수행한다. LFT 또한 BFT 계열 합의 알고리즘으로서 리더 Node와 검증 Node로 구성된다.

LFT가 동작하는 방식은 다음과 같다. 네트워크가 시작되면 검증 Node들은 리더 Node에게 처리하기 원하는 트랜잭션을 전송한다. 리더 Node는 수집한 트랜잭션을 이용하여 블록을 생성하고 자신의 서명과 함께 다른 모든 검증 Node에게 전송한다. 각 검증 Node들은 블록을 받으면 1)현 리더가 블록을 생성했는지 확인하고, 2)블록의 높이와 이전 블록 해시가 올바른 지 확인하고, 3)블록의 데이터가 올바른 지 확인한다. 검증 Node는 1~3번이 옳다면 Vote 데이터를 생성하여 네트워크의 모든 Node들에게 전파한다. Vote 데이터를 전체 Node에게 전파하는 것은 매우 중요하다. 리더 Node가 비잔틴일 경우 정족 수 이상의 Node들에게만 블록을 전파하여 특정 Node들을 네트워크로부터 분리하도록 시도할 수 있다. 이러한 문제를 방지하기 위해 모든 피어에게 Vote 데이터를 전파한다. 블록을 못 받은 Node는 블록이 생성되었는지에 대한 정보를 알 수 있고 다른 Node에게 블록을 요청할 수 있다.

리더는 블록을 생성하기 위하여 정족수 이상의 Node에게 Vote 데이터를 받는다. 리더는 새롭게

만들 블록에 Vote 데이터를 포함하여 블록을 생성하고 모든 피어들에게 전파한다. 이는 PBFT 처럼 정족수 이상의 피어가 같은 Vote를 했다는 것을 보장하기 위해 한번 더 모든 데이터를 전송할 필요가 없게 하며 새로운 블록의 Vote 확인을 통해 블록을 확정 지을 수 있게 한다. 전파받은 블록이 최초 블록이 아닌 경우 검증 Node는 블록을 검증할 때 정족수 이상의 Vote 데이터 검증을 같이 수행한다. 이 때 모든 Node들은 이전 블록을 최종 Commit 한다.

블록체인은 신뢰가 부족한 Node들이 모여 데이터 분산 합의를 통해 신뢰 네트워크를 구축하는 기술이다. 기존 상태 머신 복제 시스템처럼 모든 상태머신이 응답을 보장하는 것이 아닌 각 Node가 서비스를 제공하고 트랜잭션을 생성한다. 리더 Node는 블록 생성시 특정 Node의 트랜잭션을 거부 할 수 있다. 이러한 문제를 최소화하기 위해 Spinning[33] 기법을 사용하여 매 블록 생성 시마다 리더를 교체하여 비잔틴 리더에 의해 발생할 수 있는 서비스 장애 요소를 줄였다. 또한 기존 Tangaroa[34] 등의 알고리즘에서 사용하는 복잡한 리더 장애 복구 알고리즘을 피하여 장애 리더를 바로 Tolerance 할 수 있는 방법을 만들었다.

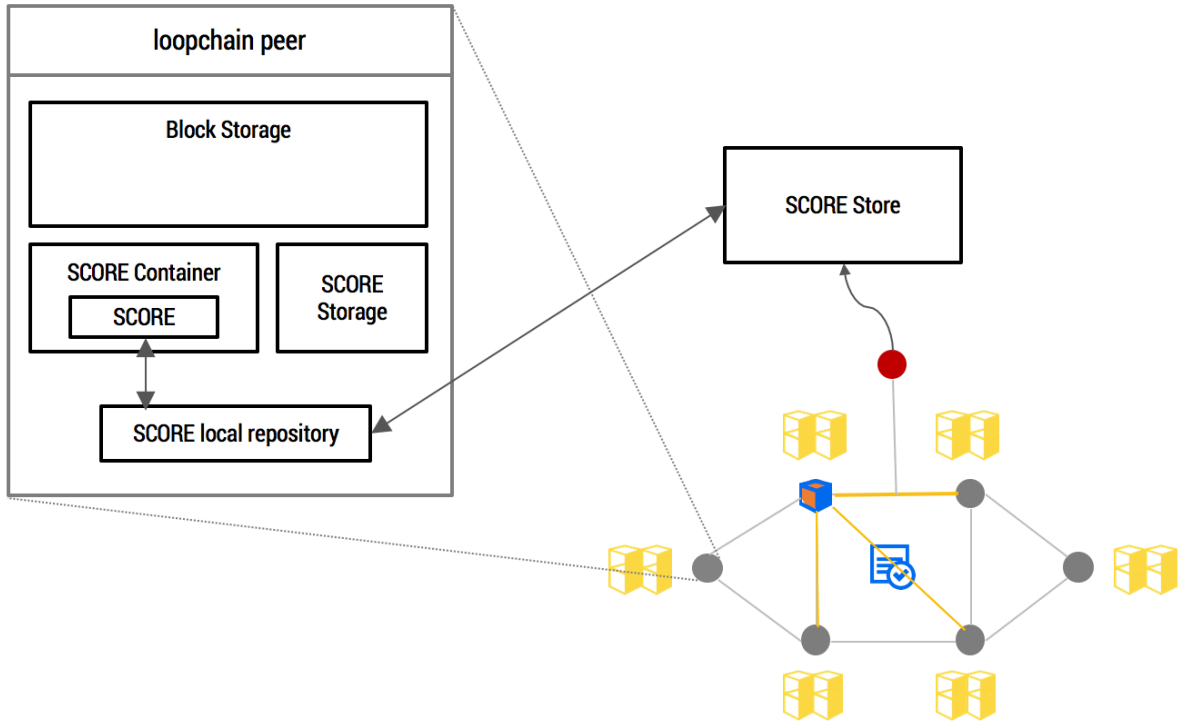
LFT는 허가형 블록체인을 위한 분산합의 알고리즘이다. 기존 BFT 알고리즘을 블록체인에 맞게 개선하고 블록 데이터를 이용하여 프로세스를 단순화 시켰다. 합의 과정에 대한 자세한 내용은 LFT white paper[35]에서 확인 할 수 있다.

4.4. SCORE(Smart Contract on Reliable Environment)

SCORE는 loopchain에서 실행되는 높은 생산성의 스마트컨트랙트 구현환경이다. 별도의 VM(Virtual Machine)이 아닌 실제 런타임에서 바로 실행되어 고성능 스마트컨트랙트 구현이 가능하며 기본 블록체인 프로세스와 별도의 컨테이너 기반 런타임에서 실행되어 스마트컨트랙트에 문제가 생기더라도 기본 블록체인 프로세스는 정상적으로 작동한다.

SCORE는 Repository 기반의 Versioning을 지원하는 것이 특징인데 일반적으로 스마트컨트랙트의 변경이 필요한 경우 새로운 스마트컨트랙트를 생성하고 기존 스마트컨트랙트의 State을 모두 이관해야 하는데 비해 Versioning을 이용하면 새로운 버전의 스마트컨트랙트에서 예전 버전의 State에 접근할 수 있어 별도의 State 이관 작업 없이 간편하고 신속하게 스마트컨트랙트를 업데이트 할 수 있다.

SCORE 배포를 위해 기본적으로 Local repository를 제공하며 SCORE Store라는 Remote repository를 이용하면 편리하게 스마트컨트랙트를 배포하고 업데이트할 수 있다.



4.5. BSI (Blockchain Signature Infrastructure)

BSI는 블록체인 스마트컨트랙트를 기반으로 PKI와 같은 전자서명 Infrastructure를 구성할 수 있도록 한 것이다. 기존 PKI에서는 인증서 발급 키를 안전하게 관리하고 해당 키로 정책에 따라 인증서를 발급, 관리하는 역할을 담당하는 거래와 상관없는 별도의 TTP(Trusted Third Party)가 꼭 필요하다.

BSI는 Merkle tree 기반의 Proof of existence를 수행할 수 있는 정보를 기반으로 전자서명 정보를 생성하여 X.509 형식의 인증서를 발급하여 별도의 인증서 발급 키 관리가 필요 없다. loopchain에서는 검증 및 합의에 참여하는 일반 Node 외에 Light Client[36]로 참여하는 Node에게 BSI 기반의 인증서를 발급하여 loopchain 네트워크 참여 시 해당 Node의 인증 및 거래의 전자서명에 사용하게 된다.

구성요소

- 사용자: PKI기반 키 쌍을 생성하고 발급된 인증서를 관리
- RA(Registration Authority): 사용자를 확인하고 인증서 발급을 요청
- CA(Certificate Authority) SCORE: 별도의 기관이 아닌 loopchain 상에서 스마트컨트랙트로 인증서 발급 관련 서비스 제공

5. ICX Token

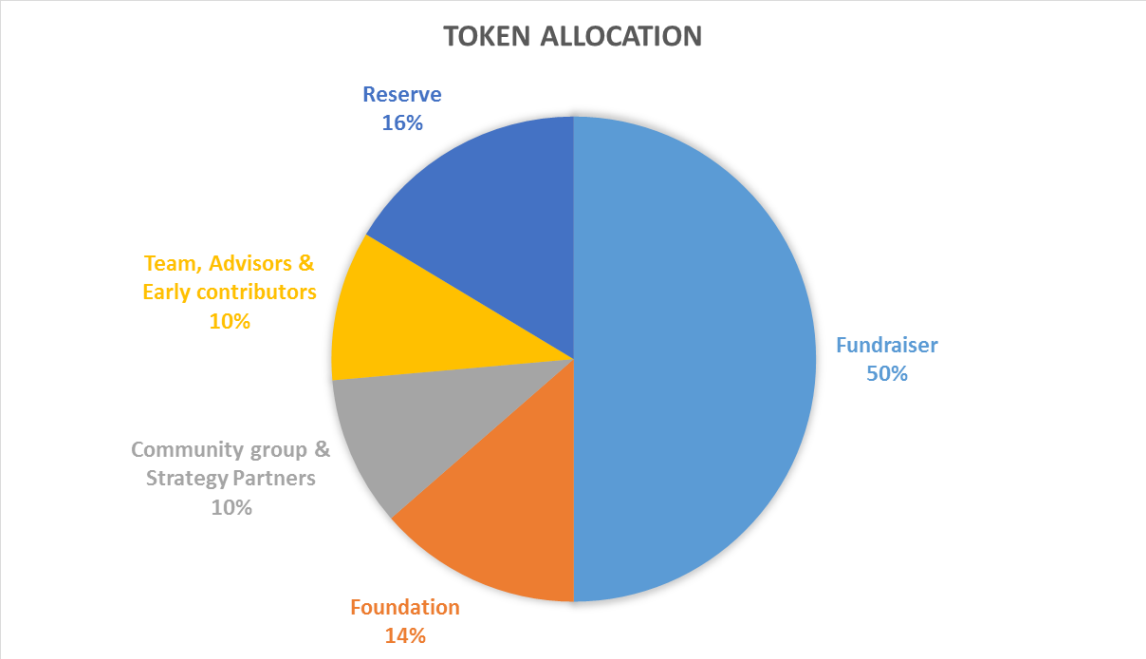
5.1. Token Sale

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

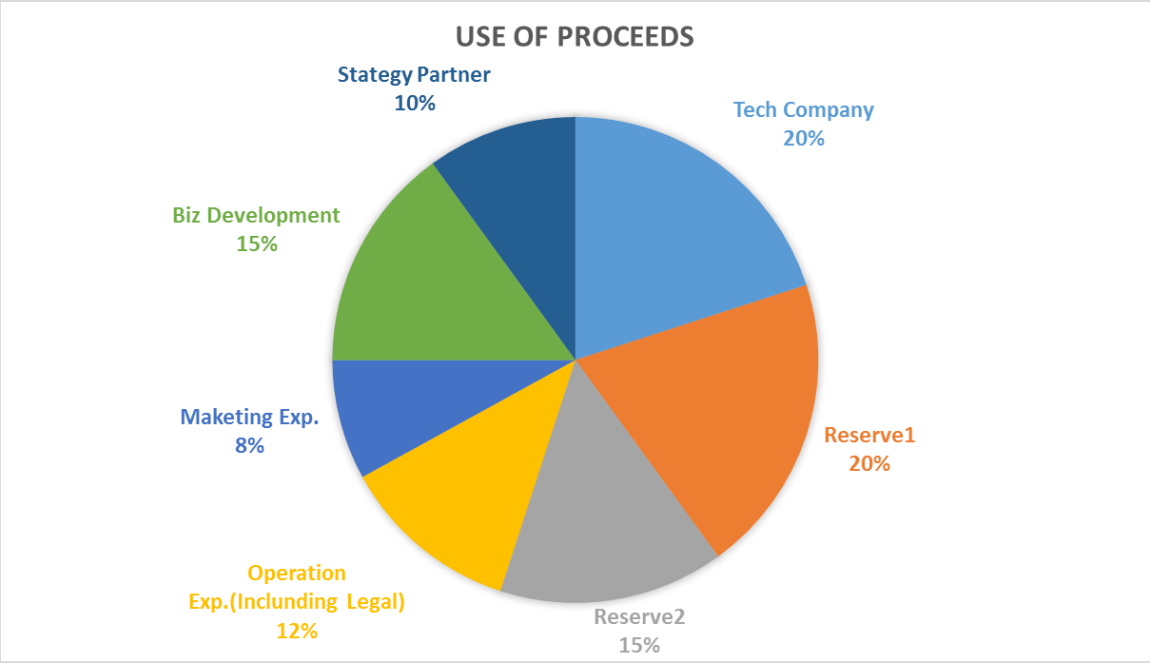
Topic	Description
ICX Token	• ICX is a loopchain-based smart contract digital protocol that facilitates, verifies, and enacts a negotiated agreement between consenting parties within ICON
The Issuer	• ICON Foundation, a Swiss nonprofit organization
Rights	• ICX represents limited license to validate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



- ICX Token은 50%는 Fundraiser, 14%는 Foundation, 16%는 ICX Reserve, 10%는 Community Group & Strategy Partner, 10%는 Team, Advisors & Early Donors에게 분배될 예정이다.

Use of proceeds



- Proceeds는 Tech Company, Reserve, Foundation Operating, Business development, Strategy Partner 등에 사용될 예정이다.

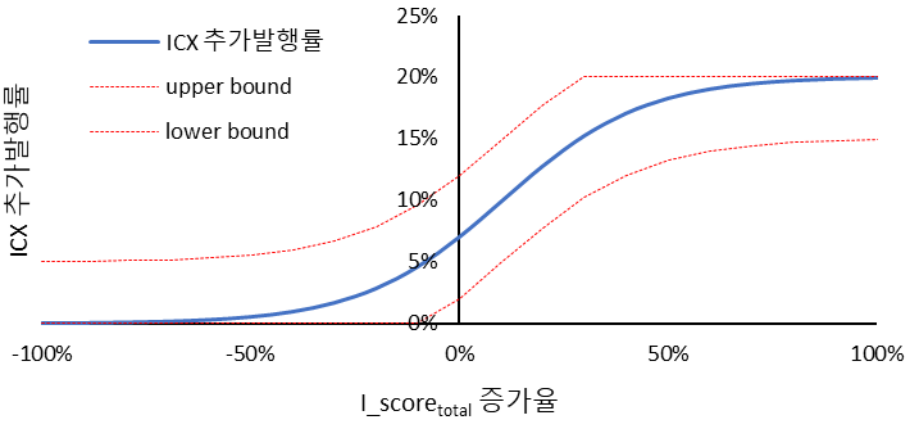
- Tech Company는 블록체인 엔진 개발 및 DAPP개발, 인공지능 개발 등에 사용되는 비용이다.
- Reserve는 타 블록체인 네트워크와의 실시간 DEX 구현을 위해 필요하다. Reserve는 Reserve1(ETH Reserve)와 Reserve2(Other Reserve)로 구분된다. Reserve1(ETH Reserve)은 Ethereum Network와의 DEX 구현을 위해 필요하며, Reserve2(Other Reserve)는 Ethereum 이외의 블록체인 네트워크와의 DEX 구현을 위해 필요하다.
- Foundation expense는 향후 Foundation 운영에 필요한 비용으로, Operating expense, Marketing fee, Legal & Accounting fee 등 이다.
- Business development fee는 ICON Foundation의 Global 확장을 위해 사용되는 비용으로, 전세계 주요 거점 지역에 오피스 설립 및 비즈니스 개발 등에 사용된다.
- Strategy Partner는 ICX 사용의 확장을 위해 사용되는 비용으로, Global Business Partner에게 지급되는 비용이다.

5.2. Issuance

ICX의 추가 발행량은 15,552,000개 블록(대략 1년)을 주기로 하여 결정된다. ICX의 추가 발행량은 ICON Network 활성화 정도의 증가함수값으로 결정되며, 실제 ICX 추가 발행률은 산출된 값 주변 일정 범위 내에서 C-Rep 간 합의에 의해 조정될 수 있다. ICX 추가 발행량 결정에 있어 ICON Network의 활성화 정도를 반영하는 것은 ICON Network의 활성화에 따른 ICX 수요 증가가 ICX 가치 불안정을 유발하지 않도록 하기 위함이다. 여기서 ICON Republic의 활성화 정도는 IISS(ICON Incentives Scoring System)에 의해 산출된 15,552,000개 블록(대략 1년) 간 개별 참여자들의 월별 IISS 점수 총합(I_score_{total})에 의해 측정된다.

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

연간 ICX 추가 발행률은 I_score_{total} 증가율의 로지스틱 함수값으로 결정될 것이다. 해당 함수에서는 ICX 추가 발행률의 최대값이 20% 이내에서 결정되도록 Parameter가 설정될 것이다. 아래는 한 가지 예시로서 I_score_{total}의 증가율이 0%일 때 ICX 추가 발행률이 7%가 되고 그 최대값은 20% 이내에서 결정되도록 Parameter를 설정한 로지스틱 함수의 그래프이다.



산출된 ICX 추가 발행률은 Representation channel에서의 C-Rep 간 합의를 거쳐 최종 확정될 것이며, 산출된 추가 발행률에 대해 2/3 이상의 C-Rep이 반대하는 경우에 한해 ±5%p 범위 내에서 합의를 통한 조정이 이루어질 것이다. 외부의 경제적 충격과 같이 특수한 상황이 발생하는 경우 이러한 조정 과정을 통해 유연한 대처가 가능할 것이다.

IISS 관련 데이터의 축적과 C-Rep 수의 증가에 따라 신뢰할 만한 수치 제시 및 유의미한 합의가 가능해지는 시점부터는 위와 같은 과정을 통해 ICX 추가 발행률을 결정할 것이다. 하지만 그 시점 이전까지는 ICX 추가 발행률이 고정된 수치로 유지될 것이다.

6. Incentives

6.1. Incentives

ICX 추가 발행분과 Transaction fee는 Public treasury에 보관되어 Incentives의 지급 재원으로 사용된다. 그리고 C-Rep의 퇴출 등의 이유로 Incentives로 지출되지 않은 ICX는 다음 기 Incentives의 재원으로 이월되어 사용된다.

추가 발행 및 이월된 ICX는 I_score에 따라 차등 배분되며, 수취된 Transaction fee는 거래 체결에 기여한 Full Node와 Light Client에게 지급된다. 이러한 Incentives 체계의 분리에 따라, 거래 체결로 발생한 Transaction fee는 거래에 직접적으로 기여한 주체에게만 Incentives로 지급된다. 결과적으로 거래 체결에 참여할 직접적인 유인이 발생하며, ICX 추가 발행량 변화 및 IISS 정책 변경 등과 무관하게 Full Node와 Light Client는 안정적인 Incentives를 제공받게 된다.

1,296,000개 블록(대략 1개월)이 생성될 때마다 해당 기간 동안의 활동 결과에 따라 산출된 I_score가 발표되며, 이 점수를 기준으로 추가 발행 및 이월된 ICX가 차등 배분된다. Transaction fee의 배분 또한 1,296,000개 블록(대략 1개월)이 생성될 때마다 이루어지게 된다.

IISS(ICON Incentives Scoring System)

IISS는 효과적인 ICX 배분을 위한 인공지능(AI) 기반 평가시스템이다. IISS는 ICON Republic 활성화를 위한 최적의 Incentive scheme을 탐색하는 것을 목표로 한다.

IISS는 인공지능을 기반으로 운영될 예정이다. 다만, 이를 위해서는 초기 데이터를 축적하는 기간이 필요하기 때문에 일정한 준비기간을 가지고, 그 기간 동안 축적된 데이터를 활용하여 인공지능을 구현한다. 준비기간 동안은 참여자 j의 IISS 점수, 즉 I_score를 아래와 같은 방식으로 측정한다.

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

참여자 j의 점수는 m개의 평가항목에 대하여 참여자 j의 기여도를 가중합한 형태이며, 평가항목은 ICX 거래량, DEX 거래량, 정책 투표 참여도, DEX Freezing volume, DApp 생성 및 이용량 등이다. C_{ij}는 평가항목 i에서 참여자 j의 기여도를 나타낸다. 예를 들어, 평가항목이 ICX거래량인 경우 $C_{ij} = \frac{Node\ j의\ ICX거래량}{전체\ ICX거래량}$ 으로 계산되며 전체 ICX거래량 중 j의 ICX거래 비중을 의미한다($\sum_j C_{ij} = 1$). g_i는 평가항목 i의 증가율로, 빠르게 활성화되는 평가항목에 더 높은 점수가 부여된다. w_i는 평가항목별로 Incentives 배분의 불균등도(Degree of inequality)를 완화하기 위한 가중치로 (1 – Gini coefficient)로 정의된다. 일부 평가항목의 경우 소수의 참여자가 대부분의 기여도를 차지할 수 있으며 이는 Incentives가 일부 참여자에 의해 독식될 수 있음을 의미한다. w_i는 불균등이 심한 평

가항목의 가중치를 낮춤으로써 Incentives 배분의 불균등을 완화하는 기능을 한다. 활동 규모가 큰 참여자들은 불균등 완화를 통한 점수 상승이 가능할 것이며, 이를 위해 기여도가 낮은 다수 참여자의 활발한 참여를 유도할 것이다. 이는 결국 ICON Republic의 활성화로 이어지게 될 것이다. α_i는 각 평가항목의 중요도에 대한 가중치로 Representation channel에서의 합의에 의해 결정 및 수정을 거쳐 적정값이 탐색될 수 있다. 초기에 'DEX 거래량', 'DApp생성 및 이용량' 등 아직 구현되지 않았거나 일반 참여자의 참여가 힘들 것으로 예상되는 항목에 대해서는 가중치를 0으로 설정할 예정이다.

실제 Incentives 배분을 위해서는 아래와 같이 직전 3개 기간 I_score의 가중평균값($I\_score_{j\tau}^{avg}$)이 활용될 것이다.

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

데이터가 일정 기간 동안(1~t기) 충분히 축적이 되면 t시점에 가용한 정보집합은 아래와 같다.

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

I_score_t는 t기 말에 측정되는 모든 참여자들의 I_score 정보를 의미하며, X_t는 t기 동안 생성된 I_score 이외의 모든 축적된 정보를 의미한다. 축적된 점수 정보는 IISS의 효율성, 배분의 공평성, IISS의 악용 방지 등을 기준으로 한 사후적 평가를 통해 조정되고, 조정된 점수($I\_score_t^{adj}$)와 그 외 변수들과의 관계가 Deep Learning 기반의 방법론을 바탕으로 학습될 것이다. 이후 인공지능 모형은 매 기마다 다음 기의 점수 $I_score_{t+1}^{adj}$를 추정하기 위해 최근까지 축적된 정보 Ω_t, 이번 기에 추가로 입수된 정보 X_{t+1}, 학습된 변수들 간의 관계를 이용할 것이며, 이를 통해 최적의 점수를 예측할 것이다.

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

측정 가능한 모든 변수는 C-Rep에 의해 I_score 측정에 반영되도록 제시될 수 있으며, 해당 변수가 분석 결과 일정 요건을 충족시키는 경우 I_score 의 평가항목으로 포함될 수 있다.

Incentives

I_score의 획득은 두 가지 방식을 통해 ICON Network 참여자의 Incentives로 작용하게 된다.

첫째, 아래와 같이 참여자의 I_score에 비례하여 추가 발행 및 이월된 ICX가 배분된다.

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

$ICX\ Earnings_j$는 참여자 j에게 주어지는 ICX 지급분을 가리키며, I_score_j는 참여자 j의 I_score를 가리킨다.

다만 네트워크의 과도한 부하를 막기 위해 활동량이 미미한 참여자들의 경우 이러한 배분에서 배

제될 수 있다. 구체적인 내용은 아래의 ***Incentives 지급 대상*** 항목을 참고하기 바란다.

둘째, Representation channel 내에서의 투표권 또한 유사한 방식으로 배분된다. 다만 투표권은 오직 C-Rep에게만 배분되며, 그 배분에 있어서는 위임된 I_score가 반영된다. 즉 아래와 같이 투표권은 'C-Rep 자체의 I_score와 위임받은 I_score 합계'에 비례하여 배분된다.

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

$Vote_j$는 C-Rep인 참여자 j에게 주어지는 투표권을 가리키며, I_score_j와 $D.I_score_j$는 각각 'C-Rep j 자체의 I_score'와 'C-Rep j가 위임받은(Delegated) I_score 총계'를 가리킨다.

Delegation

C-Rep을 제외한 참여자는 직접적으로 Representation channel 내에서 투표권을 행사할 수 없다. 대신 모든 참여자는 자신의 I_score를 원하는 C-Rep에게 자유롭게 위임할 수 있다. 모든 참여자는 I_score의 위임을 통해 대상 C-Rep의 투표권을 증가시킬 수 있으며, 이를 통해 지지하는 C-Rep의 Representation channel 내 영향력 확대에 기여할 수 있다.

Dormant account

일정 기간 이상 ICX 거래내역이 존재하지 않고, 잔고가 일정 수준 이하로 유지된 경우에는 해당 계좌를 휴면계좌(Dormant account)로 인식하고 I_score 산출 대상에서 제외한다.

Incentives 지급 대상

기본적으로 Incentives는 휴면계좌를 제외한 모든 계좌에 지급하는 것을 원칙으로 한다. 다만 ICX 형태로 Incentives를 지급해야 할 계좌가 수백만 이상이 될 경우 이를 위한 블록 생성에만 상당한 시간이 소요될 것이며, 이에 따라 ICON Network의 정상적인 작동에 악영향을 미칠 수 있다. 따라서 실제 Incentives의 지급대상은 유의미한 수준의 Incentives를 지급받는 계좌로 한정할 필요가 있다.

따라서 다음과 같은 방법을 통해 ICX 배분의 범위를 제한한다. I_score가 높은 상위 그룹(Active group)은 산출된 I_score에 따라 ICX를 지급받으며, 하위 그룹(Inactive group)은 미지급된 ICX(A)를 상위 그룹 내 최하위 계좌에 지급된 ICX(B)로 나누어 지급대상건수(C)를 결정하고(A/B를 소수점 첫째자리에서 올림한 수) I_score가 높은 순으로 A/C만큼의 ICX를 지급한다. 예를 들어, 지급대상 ICX가 1,000,000 ICX이고, 상위그룹(Active group)이 I_score 기준 100,000번째까지인 경우 아래와 같이 100,001번부터 100,589번까지는 균일하게 50.93ICX가 배분된다.

구분	지급대상 ICX	I_score 순위	ICX_{calc}	ICX_{actual}
	970,000	1	95,000	95,000

활동그룹 (Active group)		2	72,000	72,000	
		3	47,000	47,000	
		⋮	⋮	⋮	
		100,000	51	51	
비활동그룹 (Inactive group)	30,000	100,001	49	50.93	30000/51=588.235
		100,002	48	50.93	
		⋮	⋮	⋮	→ 589개의 참여자
		100,588	38	50.93	들에게 지급
		100,589	**37**	**50.93**	30000/589=50.93
		100,590	**35**	**0**	ICX
		100,591	33	0	
		⋮	⋮	⋮	

Transaction Fee

Transaction fee는 현재 거래 당 0.01 ICX의 단일 액수로 설정되어 있지만, 향후에는 각 거래의 상이한 복잡성 정도를 반영한 차등 수수료 체계에 따라 부과될 예정이다. 이는 스마트 컨트랙트나 DApp과 같이 복잡한 작업 요청이 증가함에 따라 나타나는 Full Node의 정보 처리 비용 상승을 보상하기 위함이다.

Transaction fee는 ICX로 납부되며, DEX가 활성화됨에 따라 다른 종류의 토큰으로도 ICX 변환을 통한 Transaction fee 납부가 가능해질 것이다.

발생한 Transaction fee는 Public Treasury에 보관되어 거래 체결에 참여하는 Full Node와 Light Client에게 배분된다. 납부된 Transaction fee 총액 가운데 일정한 비율이 Full Node에 대한 지급분으로, 그 나머지가 Light Client에 대한 지급분으로 할당될 것이다. 개별 Full Node는 Full Node에게 할당된 지급분을 동등한 액수로 나눠서 수취하게 될 것이며, 개별 Light Client 또한 Light Client에게 할당된 지급분을 동등한 액수로 나눠서 수취하게 될 것이다.

Transaction fee 납부 액수나 Full Node와 Light Client 간 지급액 할당 비율과 같은 요소들은 Representation channel에서의 합의를 통해 조정될 수 있다. 합의에 앞서 인공지능 분석에 따른 적정 수수료 수준이 제시될 것이며, 이 수준을 참조하여 C-Rep 간 합의 과정이 진행될 것이다. 인공지능 모형은 적정 수의 Full Node, Light Client 유치와 적정 거래 규모 유지 등을 세부 목표로 하여 ICON Network의 원활한 작동을 위한 최적 수수료 수준을 도출해 낼 것이다.

6.2. Penalty

LFT 알고리즘에 참여하는 Full Node 가운데 잘못된 행동을 하는 Node에게는 Penalty가 부여된다. 여기에서 잘못된 행동이라 함은 리더 Node의 경우 유효하지 않은 Block을 Propose하는 것 등을, 검증 Node의 경우 유효하지 않은 Block에 동의하는 Voting을 하거나 원칙에 어긋나는 방식으로 Voting하는 것 등을 가리킨다.

ICON Network에서는 Ethereum에서 도입 예정인 Casper와 마찬가지로 Block 생성 과정에 참여하는 Node들로 하여금 Reserve Pool에 최소 기준치 이상의 ICX를 예치하도록 할 것이다. 잘못된 행동을 하는 Node의 경우 예치 ICX를 소각하는 Penalty를 통해 Nothing at stake 문제에 따른 참여 Node의 도덕적 해이를 방지할 것이다.

Appendix

A.1. Definitions

Transaction(Tx)

- 블록체인에 정보를 저장하는 기본 단위.

Block

- 한 개 이상의 Transaction을 담고 있으며 Peer들 사이의 합의 대상 단위.

Peer

- P2P 네트워크 상의 Peer 하나를 대표하며, 대부분의 블록체인 업무를 수행.
- Transaction 생성.
- P2P 네트워크 상에서 Block, Transaction 교환.

Leader Peer

- P2P내의 Peer들 중 Block을 만들 수 있는 Peer.
- Transaction을 일정 시간마다 모아서 Block을 만들고 이를 Network 상에 배포.
- 각 Peer들이 만든 Transaction은 Leader Peer에 집결.

RadioStation

- Group을 생성하고 Peer들을 Group과 연결.
- 모든 실행 중인 Peer들이 자신의 Group에 속한 이웃 Peer들의 접속 정보를 얻기 위해 필요 시 접속할 수 있음.
- 각 Peer 들의 상태 모니터링.

SCORE

- loopchain에서 지원하는 스마트컨트랙트.
- Transaction 데이터 처리에 따라 State 값을 변경하는 함수들.
- Block 인증이 끝나고 새롭게 Block이 추가된 후 실행.

Service System

- 블록체인을 이용하는 응용 시스템. 기존에 사용하던 Legacy system이 될 수도 있고 새롭게 만드는 Service가 될 수도 있음.

C-Rep

- Community를 대표하는 단위이자 ICON Republic의 Governance를 구성하는 단위.
- ICON Network을 유지하고 활성화하기 위해 Governance 운영 과정에서 발생하는 의사결정 사항에 대한 투표권을 가짐.
- ICON Republic의 블록체인 네트워크인 Nexus에서 Portal 역할을 수행하는 Node로서 여러 블록체인 사이의 토큰 이동과 거래를 연동함.

Citizen Node

- ICON Republic에 포함된 노드 중 C-Rep이 아닌 노드는 모두 Citizen Node.
- 거래 검증 및 Governance에 대한 투표 권한은 없고 거래 생성 권한만 가짐.

ICON Republic

- C-Rep과 Citizen Node로 구성된 ICON Network 전체를 의미.
- 다양한 Community와 다양한 DApp을 연결하는 탈중앙 네트워크이지만, 개별 Community의 Governance에는 개입하지 않음.

Nexus

- ICON Republic을 구성하는 블록체인 네트워크.

Representation Channel

- ICON Republic에 있는 노드 중 투표권한이 있는 C-Rep으로만 구성된, ICON Republic에서 발생하는 모든 이슈에 대해 규칙을 결정하는 협의시스템.
- C-Rep별 투표권의 크기는 각 C-Rep이 소속된 커뮤니티의 기여도, 즉 IISS 점수에 따라 차등 배분되며, 직접 투표권이 없는 Citizen Node는 자신의 IISS 점수를 특정 C-Rep에 위임하여 투표권 재분배에 관여할 수 있음.

Notary Channel

- Nexus를 통해 연결된 블록체인 간의 거래 송수신을 위한 채널.

- 이 채널에 투표 권한이 있는 노드들은, Nexus 상의 다른 블록체인의 Light Client들로 구성된 다수의 채널 보유. 이는 loopchain의 Multi-channel 지원 기능을 기반으로 구현됨.

Node

- 컴퓨팅 파워를 갖춘 물리적인 단위이며 각종 채널에 합류해서 필요한 작업을 수행.
- Public Channel에서 거래, 합의, 스마트 컨트랙트 수행에 이르는 모든 작업이 가능한 Full Node는 C-Rep이 하나 이상 선정하며, 규정된 자격 조건을 갖춰야 함.
- Public Channel에서는 거래를 생성하고 Notary Channel에서는 합의를 이끌어내는 Light Client는 목적에 맞춰 정해진 기능만 수행함.
- Node는 각자 맡은 역할과 중요도에 따라 수수료를 배분받을 수 있음.

A.2. SCORE

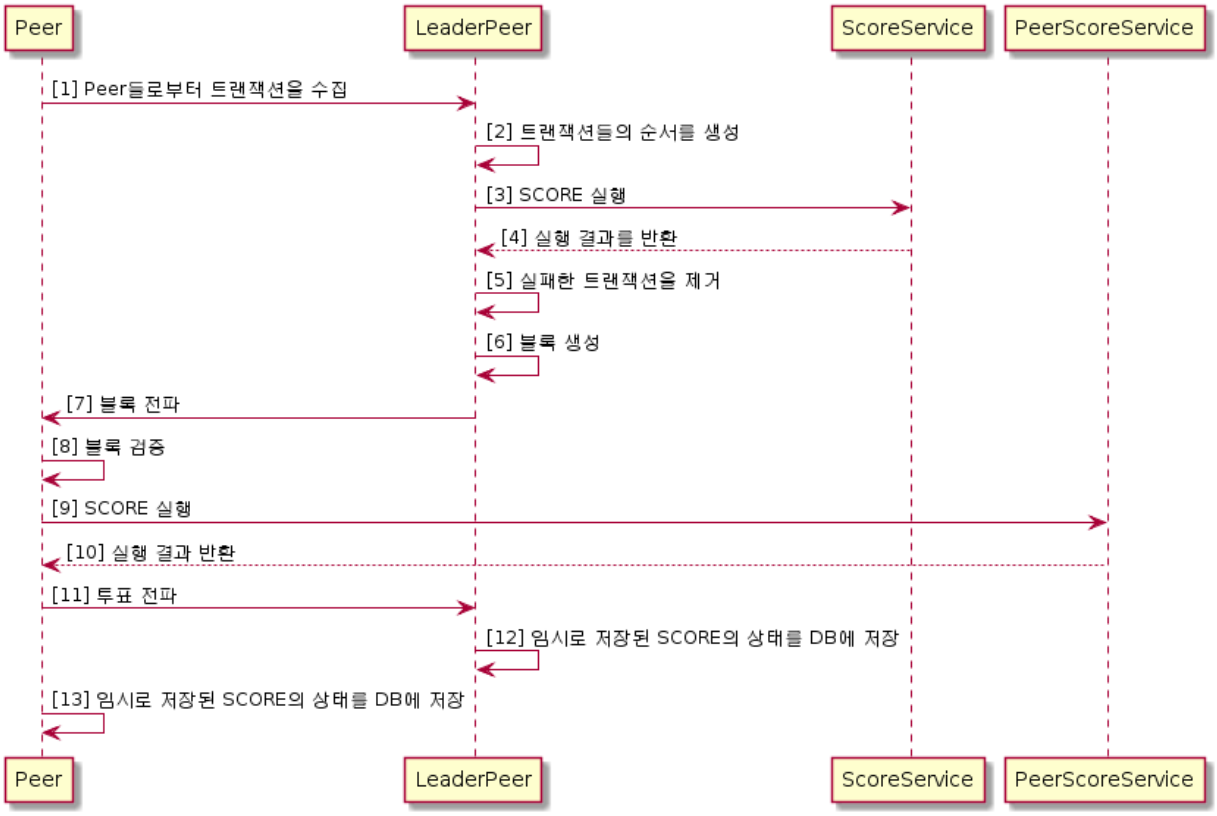
SCORE 코드 구성

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

from loopchain.blockchain import ScoreBase

class UserScore(ScoreBase):
    """ 기본 SCORE 코드
        기본 SCORE 코드는 아무런 역할을 하지 않는다
    """

    def invoke(self, transaction, block):
        pass

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

각 함수의 기능은 아래와 같다.

- invoke() : 검증이 완료된 Block의 data를 내장된 별도의 database에 추가한다.
- query(): 내부 data를 조회한다.

SCORE 처리 흐름



Sequence

① Peer들로부터 트랜잭션을 수집

② 트랜잭션들의 순서를 생성

③ SCORE 실행

④ 실행 결과를 반환

⑤ 실패한 트랜잭션을 제거

⑥ 블록 생성

⑦ 블록 전파

⑧ 블록 검증

⑨ SCORE 실행

⑩ 실행 결과 반환

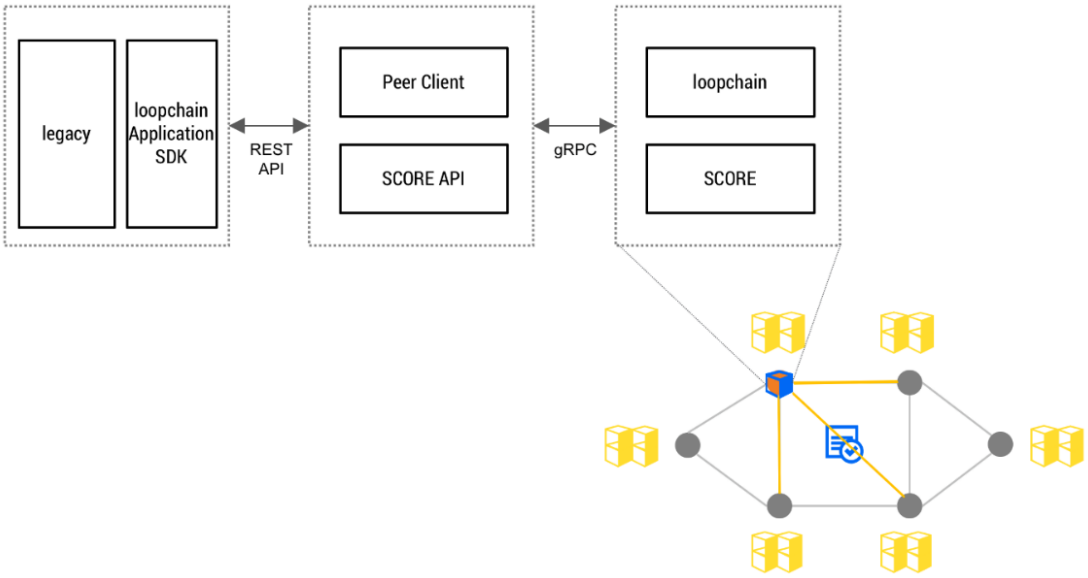
⑪ 투표 전파

⑫ 임시로 저장된 SCORE의 상태를 DB에 저장 (Leader Peer)

⑬ 임시로 저장된 SCORE의 상태를 DB에 저장 (Peer)

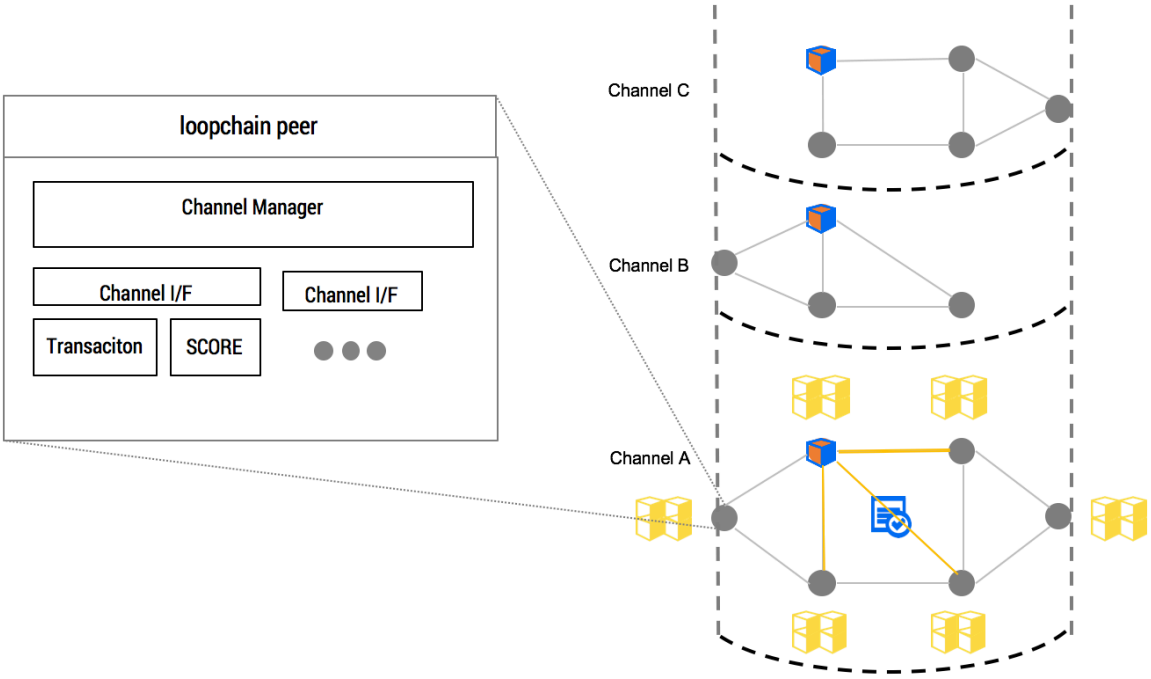
A.3. Integration of loopchain and Legacy Systems

loopchain Proxy를 통해 블록체인 Peer에 REST API로 접근이 가능하며 이를 Legacy 환경 및 업무에 따라 간편하게 사용할 수 있도록 wrapping한 업무별 loopchain Application SDK를 함께 제공하여 API 호출만으로 업무 개발이 가능하다.



A.4. loopchain Multi-channel

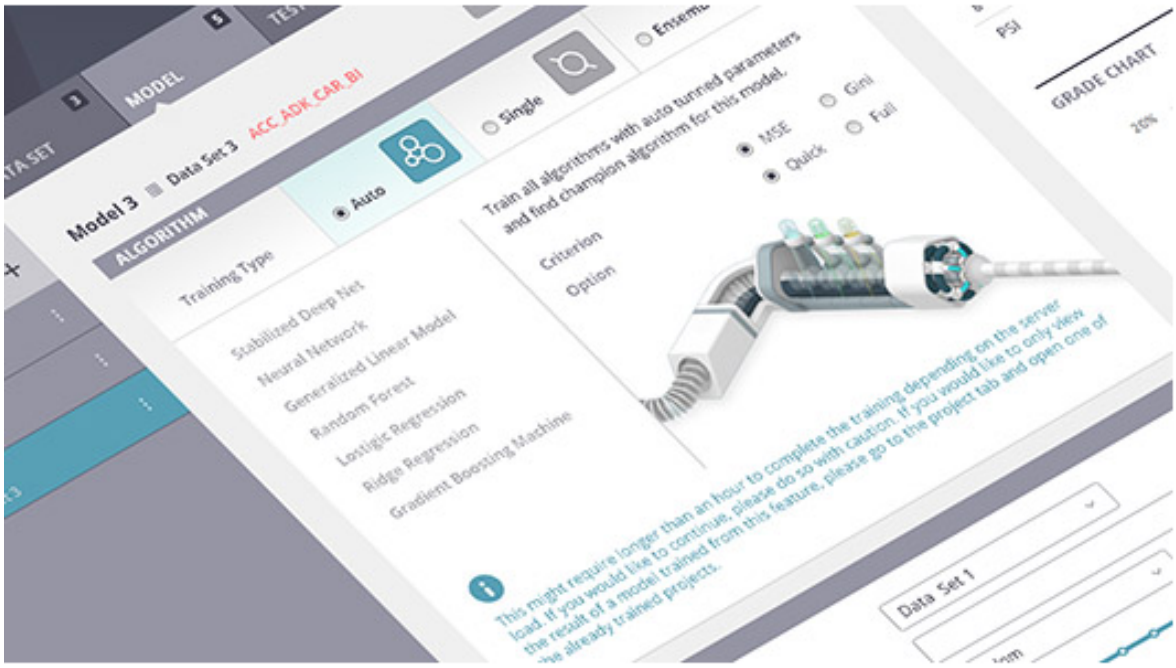
loopchain Peer 내에 채널 별로 거래 및 SCORE 분리를 제공하여 하나의 블록체인 네트워크에서 거래 당사자만 참여하는 업무별 채널 구성이 가능하다.



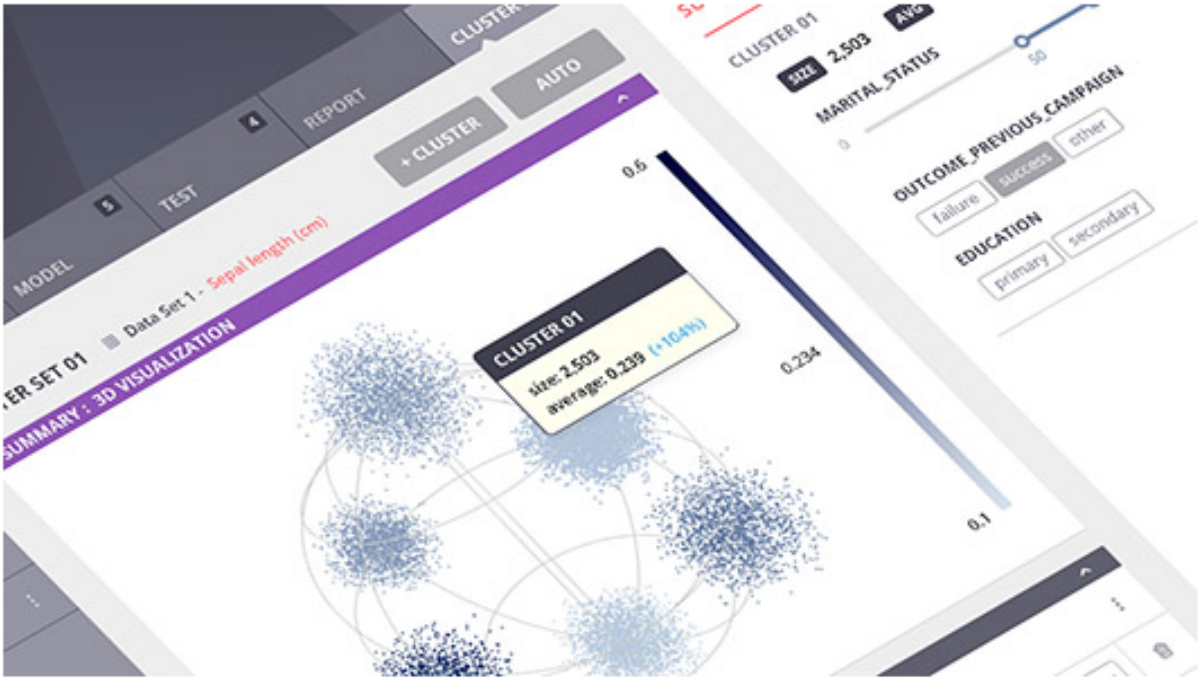
A.5. AI-driven Policy

기존의 경제시스템에서는 많은 부분이 중앙집중화된 기관들에 의해서 판단되고, 결정되고, 조정되었다. 중앙은행은 물가와 경기에 대하여 판단하고 기준금리를 결정한다. 정부는 다양한 정책들을 바탕으로 부의 형성과 분배를 조정한다. 이러한 중앙은행의 물가와 경기에 대한 판단과 기준금리 결정은 소수의 전문가집단(e.g. FOMC)에 의해 이루어진다. 다양한 분야의 정부 정책 역시 각 부처에 속한 소수의 공무원 조직이 주도한다. 이와 같은 일련의 판단, 결정, 조정의 근거가 되는 데이터는 일반적으로 과거 시점에 수집된 정확도가 낮은 데이터인 경우가 대부분이다. 이에 따라 기존 경제 시스템에서의 경기 판단은 매우 느리고 부정확하며 이에 따른 정책 대응은 부적절하거나 정책 시차로 인해 당초 정책의도와는 다른 역효과를 발생시키는 경우가 비일비재하다. 결국 사람의 분석과 판단에 의존하기 때문에 사람의 성향이나 특성이 반영될 수 밖에 없다. 동일한 데이터를 기반으로 이루어진 의사결정도 동일하지 않게 되어 일관된 의사결정이 이루어지기 어렵다.

블록체인은 별도의 중개기관이나 신뢰기관 없이 참여자들 간의 신뢰성이 있는 거래를 가능하게 하는 하나의 경제 플랫폼이다. 그 안에서 발생하는 수많은 트랜잭션에는 참여자들의 다양한 경제적 동기와 행동이 반영된다. 블록체인 상의 모든 트랜잭션은 무결성이 보장된 상태로 실시간으로 기록 및 동기화된다. 블록체인 상의 빅데이터를 정교하게 분석한다면 기존 체제 보다 비약적으로 개선된 경제운용체계를 구축할 수 있을 것이다.



DAVinCI LABS: Automatic modeling



DAVinCI LABS: Automatic Clustering

지난 2년간 우리는 인공지능을 활용한 빅데이터 분석을 통해 기존 금융기관들의 수많은 전문가들이 수십년간 고도화 시켜온 모델을 훨씬 뛰어넘는 결과를 만들어 냈다. 세계 최대 보험그룹, 메이저 시중은행, 카드사, 캐피탈사, 저축은행 등 많은 금융기관들이 이미 우리가 만든 머신러닝 기반 인공지능 솔루션 DAVinCI LABS를 도입하여 손해율 예측, 신용리스크 평가, 전환율 예측, 가격 민감도 분석, FDS(Fraud Detection System), EWS(Early Warning System) 등 다양한 업무에 활용하고 있다.

기존 통계 기반 프로세스는 모든 단계에서 사용자의 인풋을 필요로 한다. 이 과정에서 사용자의 직관 및 배경 지식이 분석 방법 및 결과를 판단하는 척도가 되어 주관의 개입에 의한 오판 가능성이 존재한다. 또한, 분석 기법의 특성상 일반적으로 제한된 양의 데이터만 활용할 수 있어 다양한 변수들의 영향을 종합적으로 분석하기에는 부적합하다. 반면, 머신러닝 알고리즘에 기반한 분석 프로세스 자동화를 통해 더욱 효율적이고 정교한 데이터 분석이 가능하고, 분석 과정에서 사용자의 주관 개입에 따른 오판 가능성이 최소화된다. 또한, 기법 특성상 사용 가능한 모든 데이터를 분석에 활용할 수 있어 다양한 변수의 영향을 종합적으로 분석할 수 있다.

우리는 이미 다수의 메이저 금융기관을 통해 검증된 인공지능 DAVinCI를 ICON Network에서 발생하는 데이터의 분석 및 보상 정책의 최적화에 사용할 것이다. ICON Network 상의 트랜잭션과 참여자들의 행동데이터들은 DAVinCI를 통해 지속적으로 모니터링 및 분석될 것이며, ICON Network의 성장과 참여자들의 인센티브가 일치되도록 항상 최적화된 보상 정책이 유지될 것이다.

기존 블록체인 네트워크들의 보상 및 인센티브 정책은 대부분 경직된 방식으로 작동하여 다양한 시장상황에 적절히 대응하지 못하고 있다. ICON Network은 인공지능을 통해 시장상황에 유연하게 대응함으로써 지속적인 성장동력을 유지할 수 있다.

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] 국가 지정 10개 연구중심병원 중 7개가 본 컨소시엄에 참여

[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] A.4. loopchain Multi-channel

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

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

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

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

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

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

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

[35] https://loopchain.files.wordpress.com/2017/07/lft-e18487e185a2e186a8e18489e185a5.pdf

[36] https://github.com/ethereum/wiki/wiki/Light-client-protocol