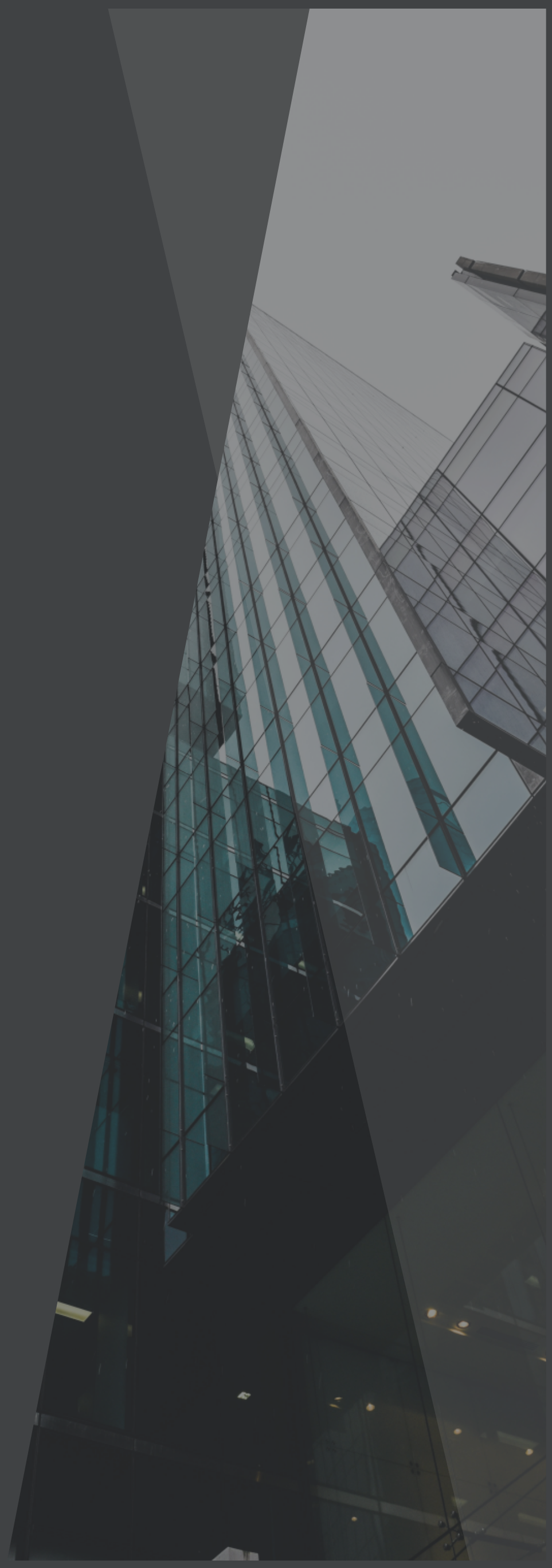
PROTOCON

A Window into the Protocol Economy

PROTOCON

Contents

Contents



01 Abstract

21세기를 관통하는 화두 중 하나는 사회 전반의 디지털 전환(Digital Transformation)이다. 디지털 전환이란 용어는 두가지 의미를 내포하고 있다. 하나는 아날로그 즉 종이를 기반으로 생산되고 처리되어 왔던 정보 전체를 디지털로 전환하는 것이고, 다른 하나는 디지털 인프라에 기반하여 정보를 생산하고 처리하는 전 과정을 자동화하는 것이다. 정보 생산 및 처리 과정이 자동화된다는 것은 사회 시스템 전반이 자동화된다는 것을 의미한다. 조만간 사회 시스템 전반의 대규모 자동화와 더불어 프로토콜로 작동하는 경제 시스템 즉 순수 디지털 경제가 본격화될 것이다. 이미 블록체인 기술을 기반으로 디지털 화폐뿐만 아니라 부동산이나 미술품, 음악 저작권 등 전통적인 아날로그 자산들의 디지털 전환이 시작되었고 디파이(DeFi)를 통해 프로토콜 이코노미가 현실화되었다. 경제와 사회 시스템이 자동화된다고 SF적인 우울하고 암울한 상상에 빠질 필요는 없다. 경제와 사회 시스템이 애초 합의되고 약속된 프로토콜대로 작동된다면 오히려 불리한 것은 의사결정 권한과 실행권을 독점하고 자의적으로 권력을 행사해왔던 이들이 될 터이니 말이다. 우리는 오히려 반대로, 프로토콜 사회에서 개인의 힘은 더 강해질 것이라고 믿는다. 그리고 블록체인은 개인들이 집합적으로 합의하고 계약하는 과정 상의 위변조 불가능성을 보장해주고, 합의된 사항들이 프로토콜로 구현되어 반드시 작동하도록 보장함으로써, 궁극적으로 독립적인 개인들의 힘을 더 강화할 것이다. 프로토콘넷 (ProtoconNet)[1] 은 디지털 시대에 신뢰 인프라 제공을 목표로 하는 메인넷 프로젝트다. 핵심 알고리즘인 ISAAC+는 실제 산업에 사용할 수 있도록 대규모 데이터 처리에 적합하게 설계되었으며, 블록체인 기술을 필요로 하는 모든 영역에 사용될 수 있도록 범용성을 확보했다. 또한 프로토콘넷은 FeeFi라는 사용자 참여형 금융 모델을 통해 블록체인의 사용성(UX)을 획기적으로 개선하고, 블록체인 네트워크가 만들어내는 부가가치를 생태계 전체에 분배한다. 또한 탈중앙화된 네트워크와 생태계 전체를 아우르는 거버넌스로 프로토콜 기반의 순수 디지털 경제를 촉진할 것이다. 그러나 미래는 한번에 오지 않는다. 오프라인의 데이터와 가치를 디지털로 전환하는 방법론은 아직 정답이 없다. 아날로그로 구축되어 있는 현실을 디지털로 전환하는 작업은 제법 오랜 시간이 걸리기 마련이며, 순수 디지털 경제의 선행 모델은 애초부터 순수 디지털 데이터로 구성된 게임산업과 메타버스에서 먼저 출현할 것이다. 이런 측면에서 우리는 게임 산업과 메타버스를 다가올 디지털 경제의 마중물이자 프로토콘넷 1.0의 출발점으로 삼는다.

02 Introduction

2008년 비트코인이 처음 출현한 이후 블록체인 산업은 부침과 발전을 거듭했다. 십수년에 걸친 검증 기간 동안 비트코인 그리고 블록체인 기술을 둘러싸고 수 많은 의문이 제기되었고 날카로운 것 같지만 무용한 비판들이 이어졌으며, 다른 한편에서는 강력한 규제와 통제로 비트코인과 탈중앙화 네트워크를 길들이려는 시도들이 있었다. 그럼에도 불구하고 비트코인은 블록체인 아키텍쳐의 견고함을 증명하며 결국은 금과 비견되는 글로벌 자산 레벨에 올라섰다. 2세대 블록체인인 이더리움 역시 DAO 사태와 하드포킹을 포함한 숱한 사고들을 겪으면서도, 디파이(DeFi)라는 새로운 산업 영역을 탄생시키며 토큰 발행 플랫폼에서 탈중앙화 자산관리 플랫폼으로 진화하는 중이다. 비트코인과 이더리움의 뒤를 잇는 3세대 블록체인들은 꾸준히 자신들이 정의한 문제를 풀기 위해 아직 존재하지 않는 길을 더듬어가는 중이다. 아쉽지만 이중 누군가가 블록체인 산업이 풀어야할 문제들에 대한 해답을 제시했다고 보기에는 아직 이르다.

그렇다고 한번 자신의 가치를 증명한 기술이 역사의 시간을 뒤로 돌리는 법은 없다. 블록체인 산업이 거품과 폭락을 거듭하며 바닥을 다지는 사이, 기술의 용도를 확장하려는 다양한 노력들이 진행되었다. 덕분에 블록체인은 디지털 토큰의 기반기술을 넘어 디지털 데이터의 존재 증명, 위변조 방지, 유일성 보장, 진본 확인 등을 위한 필수 기술로 자리잡아 가고 있다. '가치'를 가진 디지털 데이터를 보호하기 위해서는 반드시 블록체인 기술을 활용할 수 밖에 없기에 블록체인은 디지털 사회의 필수적인 신뢰 인프라로 활용될 것이다.

2017년 MakerDAO로부터 시작되어 2020년에 갑자기 폭발한 디파이(DeFi, Decentralized Financing)는, 대리인과 중개인의 개입이 최소화된 프로토콜 기반 자동화 금융이 가능하다는 것을 증명했다. 이른바 '스마트 컨트랙트'라는 방법론으로 구현된 디파이 프로토콜에는 약속 또는 계약이 담겨 있고 이 약속 또는 계약은 블록체인 상에서 위변조 없이 정해진 대로 반드시 작동한다. 아직은 어설프고 설익은 상태로 시행착오를 반복하고 있지만, 마치 비트코인이 위변조 불가능한 디지털 토큰이 가능하다는 것을 증명하며 블록체인을 하나의 산업으로 일구어낸 것처럼, 디파이는 위변조 불가능하고 대리인과 중개인의 개입이 최소화된 프로토콜 기반 자동화 경제 시스템 즉 프로토콜 경제(Protocol Economy)가 가능하다는 것을, 더 나아가 프로토콜 기반 사회시스템 구축이 불가능하지 않다는 것을 보여주고 있다.

사실 상당한 수준으로 자동화된 경제 시스템, 사회시스템은 블록체인 덕분이 아니라 디지털 기술 자체가 가지고 있는 본질적 속성이다. 전방위적인 사회의 디지털 전환(Digital Transformation) 속에서 우리는 이미 자율주행 자동차, 로봇, 드론, AI가 적용된 사물 등을 통해 일상에서 자동화된 디지털 시스템들을 만나고 있다. 더 나아가 조만한 사회 시스템 전반의 대규모 자동화가 진행될 예정이다. 그러나 기존의 디지털 기술로는 무한 복제 가능성과 해킹 및 위변조 가능성 때문에 '가치 있는 데이터'를 다루기가 어려웠다. 만약 자동화된 경제 시스템이 무한 복제되거나 해킹 또는 위변조 될 수 있다면, 자동화된 사회 시스템이 애초 공동체가 합의한 대로 작동하지 않는다면 그것은 단순한 사고 수준을 넘어 대규모 자연 재해에 맞먹는 재난 상황을 만들어낼 것이다. 블록체인은 일반적인 디지털 기술만으로는 확보할 수 없는 디지털 데이터의 위변조 불가능성, 계약 실행의 불가역성을 제공하기에 디지털 기술의 취약점을 보완하고

디지털 경제의 가능성과 잠재력을 폭발시킨다. 비트코인이 토큰으로부터 시작되어 블록체인 산업을 일구어냈다면, 디파이라는 맹아에서 성장한 프로토콜 경제는 점차 확대되고 확장되어 정치·사회·경제 전반을 프로토콜 기반의 디지털 시스템으로 재편할 것이고, 블록체인은 자동화된 프로토콜 경제, 프로토콜 사회 시스템이 안전하게 작동하도록 해주는 신뢰 인프라로 작동할 것이다. 우리는 겨우 그 초입의 근처에 들어서 있을 뿐이다.

아마도 제법 오랜 시간이 걸릴 것이다. 무엇보다 이를 위한 기술적 자원이 아직 충분하지 않다. 지금의 상태는 블록체인 기술에 대한 상상력과 의지와 수요는 넘치지만, 실제 구현된 기술은 그 기대치를 충족시키기에 역부족인 상황이다. 공동체를 구성하는 개인들 사이의 또는 개인과 권력기관 사이의 약속, 합의, 계약이 중개인과 대리인의 개입이 최소화된 형태로 작동하는 프로토콜 경제, 공동체가 합의한 대로 시스템이 작동하는 프로토콜 기반 사회를 구축하기 위해서는 다음과 같은 몇가지 사항들이 보완되어야 한다.

첫번째, 데이터 처리 성능 측면에서 현수준의 경제나 사회 시스템을 작동시키기에 부족하지 않은 정도 혹은 그에 근접하는 정도의 성능을 확보해야 한다.

두번째, 비용 측면에서 비교적 저렴하고 안정적인 수준으로 블록체인 서비스를 지속적으로 제공할 수 있어야 한다. 만약 블록체인 사용 비용이 급격하게 변동하며 널뛰기를 한다면 예측가능하고 지속가능한 서비스를 제공할 수 없다. 이러한 급격한 변동성 덕분에 블록체인은 더디게 확산되고 있다.

세번째, 다양한 디지털 데이터들을 안전하게 다룰 수 있고, 프로토콜의 확실한 작동을 보장하는 실행환경을 제공해야 한다. 통상 이것은 이더리움이 제안한 '스마트 컨트랙트'라는 방법론으로 구현되지만, 기간의 경험은 이더리움 방식의 스마트 컨트랙트가 가진 취약성을 반복적으로 확인해주었다. 따라서 스마트 컨트랙트의 보안 취약성을 보완할 수 있는 개선된 방법론이 필요하다.

네번째, 네트워크 운영권이 특정인 또는 소수에게 귀속될 수 없는 탈중앙화된 네트워크여야 한다. 한동안 정부와 기업들이 프라이빗 블록체인으로 다양한 프로젝트들을 진행해왔고 그것은 그것대로 의미를 가지고 있지만, 이미 시장은 프라이빗 블록체인이 탈중앙화 블록체인의 신뢰성을 뛰어넘을 수 없다고 평가하고 있다. 블록체인에서 탈중앙성은 이상론자들의 고매한 이상이나 도덕적인 우위, 멋있는 선전문구 수준이 아니라, 특정인 또는 생태계 내의 소수가 블록체인 네트워크를 장악하거나 독점적인 권력을 행사하지 못하게 함으로써 단일지점 장애(Single-Point Failure) 문제를 상당한 수준으로 극복해주는 구조적 장치다. 따라서 탈중앙성 확보는 블록체인의 존재 목적인 '신뢰'와 직결되어 있는 과제다.

그리고 마지막으로 다섯번째, 블록체인이 적용된 서비스들의 UI/UX 문제를 반드시 짚어야 한다. 이것은 크게 두가지로 정리할 수 있다. 하나는 블록체인을 사용할 때 각 개인들이 보안키 또는 개인키(Private Key)를 직접 관리하는 방법을 익히고 관리의 리스크를 떠안아야 한다는 점이다. 처음 접하는 사람에게는 굉장히 낯설고 번거로우며 부담스러운 일이다. 다른 하나는 dApp 서비스 토큰을 사용하는데 있어 메인넷 토큰을 수수료로 내야한다는 점이다. 이것은 비유하자면 원화를 지불하기 위해 어디선가 달러를 구해서 수수료로 입금해야 하는 것과 다르지 않다. 사소해 보이는 수수료 문제는 블록체인의 사용성을 어렵게 만들고 dApp 서비스 및 블록체인 생태계의 확장을 가로막는 가장 큰 걸림돌 중 하나다.

위 다섯 가지 문제들은 이미 블록체인 산업에서 오래전부터 풀어야 할 '숙제'로 제시되어 온 것들이다. 프로토콘넷에서 우리는 이 문제들을 종합적으로 풀어낼 것이다. 아울러 기술 개발과 사용성 확보 또는 좋은 기술을 보유한 것과 성공적인 블록체인 프로젝트로 성장하는 것은 사실상 별개의 과제다. 아무리 뛰어난 기술을 개발했다 하더라도 기술 그 자체가 광범위한 사용이나 사회적 채택을 보장하지 않는다. 따라서 블록체인의 사용성 확보 또는 사회적 채택을 위해서는 별도의 계획이 필요하다. 특히 이더리움이 토큰발행 플랫폼에서 자산관리 플랫폼으로 전환되며 그 입지를 공고화하고 있고 이더리움과 경쟁하려는 다수의 블록체인 프로젝트들이 존재하는 상황에서 신규 프로젝트는 어떻게 메인넷 시장에 진입할 것인가 하는 문제는 풀어야 한다.

이 문제의 해답으로 우리는 게임산업과 메타버스를 선택했다. 우리는 그 동안 블록체인 산업에서 쌓은 경험과 분석을 토대로 (온라인) 게임과 메타버스에 특화된 블록체인 서비스를 제공하고자 한다. 블록체인이 '가치를 가진 디지털 데이터'를 인증하고 보호해주는 기술이라는 측면에서 보자면, 게임이나 메타 버스에서 창출되는 다양한 유형의 데이터를 이야말로 '가치를 가진 디지털 데이터'의 전형이다. 적어도 게임과 메타버스에서는 블록체인에 데이터를 저장하기 위해 아날로그 데이터를 디지털로 전환하는 작업을 거치지 않아도 되고, 구현보다 규제를 검토하고 고민하는 헛된 시간을 쓰지 않아도 된다. 이미 시장에서는 디지털 아이템들을 거래하는 다소 불안하고 미성숙한 시장이 조성되어 있다. 또한 게임에 블록체인이 결합되면 게임 산업에서 발생하는 사기를 방지할 수 있고, 특정 게임이 종료되거나 혹은 해당 게임을 운영하던 게임업체가 사라져도 게임 내에서 획득한 아이템과 게임 이력들을 유지/보관할 수 있으며, 해당 아이템들을 또 다른 게임에서 재활용할 수 있다. 이로써 그동안 무시되고 유린되어 왔던 게임 유저들의 자산과 권리가 보호될 것이고, 나아가 게임이나 메타버스에서 생산된 다종다양한 디지털 아이템들이 신뢰를 기반으로 시장에 유통되는 새로운 디지털 경제 생태계가 활성화될 것이다. 이미 시장에서는 NFT를 비롯하여 게임과 블록체인을 결합하는 다양한 시도들이 진행되고 있다. 프로토콘넷은 다양한 게임 데이터들을 블록체인에 연동할 수 있는 방법론을 제시함으로써 게임 유저들의 자산과 권리를 증진시키고, 사용자 기반의 메타버스 생태계가 구축되도록 할 것이다.

03 Technology

프로토콘넷은 미텀(Mitum) 블록체인으로 작동하는 메인넷이다. 미텀은 ISAAC+ 컨센서스 프로토콜을 기반으로 하고 있으며, ISAAC+ 컨센서스 프로토콜은 PBFT[2] 구현체다. 미텀은 두번째 쓰여진 코드다. 우리팀은 보스코인(BOScoin) 프로젝트에서 세박(Sebak)[3]이라는 PBFT 기반의 블록체인 구현체를 개발 및 공개한 바 있다. 미텀은 Sebak 개발 및 운영 경험을 바탕으로 완전히 새롭게 쓰여졌으며, 세박이 그렇듯 미텀 역시 바닥부터 완전히 새롭게 개발되었다. 우리는 스텔라, 텐더민트, 하이퍼렛저, EOS 등 이전에 나온 많은 PBFT 구현체들의 알고리즘 및 소스코드들의 문제의식과 장단점을 면밀히 검토했으며, 이를 기반으로 산업에 적용 가능한 수준의 처리성능과 안정성을 확보할 수 있는 제품을 만들었다. 특히 PBFT 알고리즘을 기반으로 탈중앙화 목표에 보다 근접한 네트워크를 만들기 위해 많은 노력을 기울였다. 또한 블록체인 플랫폼의 스마트 컨트랙트에 대응하는 '모델(Model)' 개념을 도입했다. '모델(Model)'이란 미텀 블록체인 코어를 프레임워크로 활용하여 비즈니스 요구사항을 수용하고 감당할 수 있도록 다양한 데이터 형식 및 로직을 구현할 수 있는 미텀만의 개발 방법론이다. 모델의 목적과 기능은 타 블록체인 플랫폼들의 스마트 컨트랙트와 유사하지만, 보다 높은 안전성을 확보하는 동시에 구현에 있어서는 더 많은 자유도를 제공해 줄 수 있는 새로운 방법론이다.

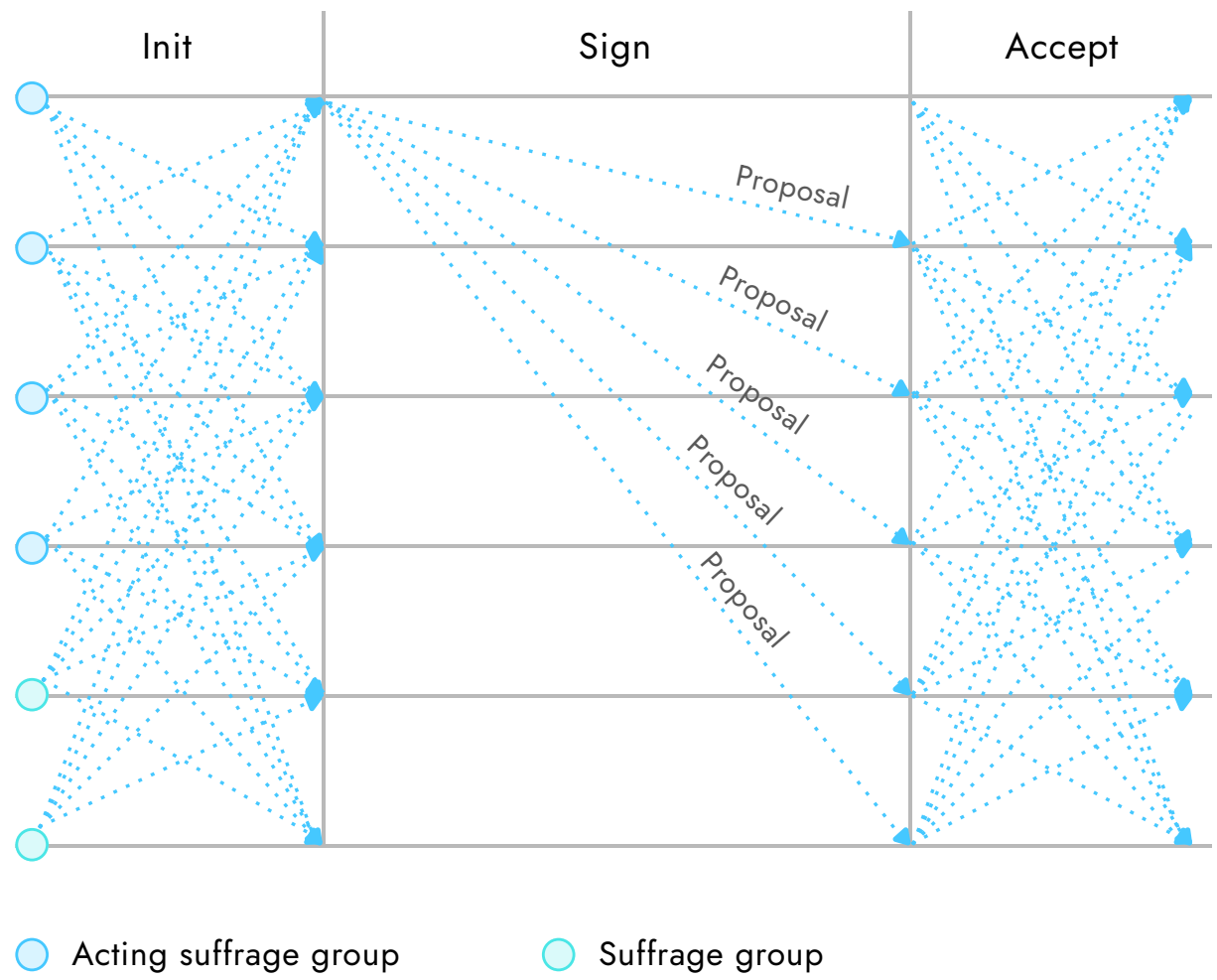
미텀에는 여러가지 새로운 기술과 기법들이 적용되었다. keccak 256, keccak 512 등 다양한 hash algorithm 지원, 비트코인, 이더리움, 스텔라 등이 사용하는 주소(프라이빗키와 퍼블릭키)를 그대로 사용할 수 있는 기능, 계좌와 주소를 퍼블릭키와 분리하여 계좌를 별도로 관리 가능하도록 한 계좌 관리 기능, 모든 유형의 데이터를 수용할 수 있는 데이터 구조, 용도에 따라 다양한 데이터베이스를 접목해서 사용할 수 있는 기능, 블록체인 내부 데이터 검색 속도를 증가시키기 위한 AVL Tree 도입, 탈중앙화 네트워크의 기술적 기반인 Acting Suffrage 그룹 개념 도입, 노드들이 투표를 통해 모델을 수용하거나 코드 및 정책 변경 사항을 블록체인에 반영할 수 있는 노드 투표 기능, 네트워크 환경과 구성요소들의 변화에도 최대한 중단 없이 네트워크를 가동시킬 수 있는 네트워크 디자이너 기능 등, 블록체인의 성능과 네트워크의 안정적인 운영을 보장하는 다수의 기능들을 보완했다. 특히 Acting Suffrage 그룹 개념은 PBFT의 특징인 finality를 보장하면서도, 네트워크 및 개별 노드들의 건강성을 감시하고 특정조건을 만족하는 노드들을 컨센서스 노드에서 자동으로 탈퇴시키거나 자동으로 가입시키기 위한 장치이다. 이는 PBFT 알고리즘 기반으로 Permissionless Network를 구현하기 위해 미텀이 새롭게 도입한 방법론이다. 또한 네트워크 디자이너라는 기능은 블록체인 네트워크의 항상성을 유지하기 위해 노드의 신규 가입과 탈퇴 처리, 블록 생성 속도 변경, 모델 업데이트 등 네트워크 관리와 관련된 주요 작업들을 네트워크 중단 없이 처리할 수 있도록 했다. 이 모든 기능들은 여러번에 걸친 최적화 작업을 거쳤으며, 최소한의 코드로 최대한의 성능을 낼 수 있도록 반복적으로 튜닝되었다.

위에서 기술한 내용들의 많은 부분이 이미 구현된 상태다. 미텀에서 새롭게 시도되는 기술에 대해서는 별도의 기술문서(Technical Paper)로 상세하게 설명할 것이다. 여기서는 미텀을 구성하는 핵심적인 요소들과 특징들을 개략적으로 기술하고자 한다.

01 합의 알고리즘

ISAAC+[4] 는 PBFT(Practical Byzantine Fault Tolerance) 알고리즘(이하 PBFT)을 수정 개선한 합의 프로토콜로, 블록의 Finality를 보장하고 제한된 Fault Tolerance 안에서 Liveness와 Safety를 보장한다.

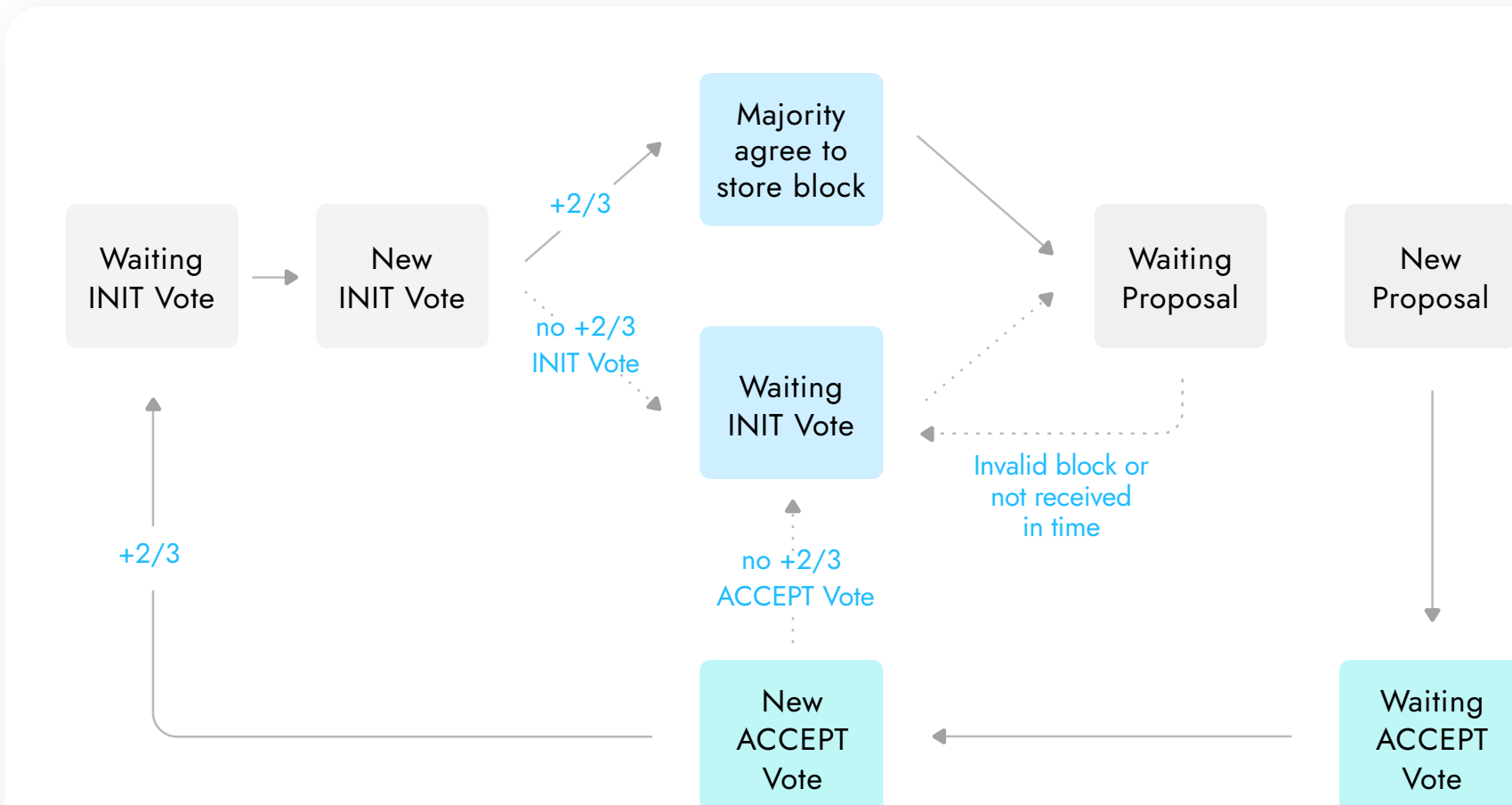
우리가 PBFT 기반 합의프로토콜을 선택한 이유는 블록체인을 산업에 적용하기 위해 빠른 처리 속도에 대용량 서비스를 제공할 수 있어야 하기 때문이다. 그리고 PoW는 데이터 확정을 위해 최소 수분에서 한시간까지 기다려야 하기 때문에, 최대한 실시간에 가깝게 데이터를 처리해야 하는 산업과 비즈니스 현장에서 적합하지 않다. 블록체인을 본격적으로 산업에 활용하기 위해서는 실시간에 가까운 Data Finality를 확보해야 하며, 이에 가장 적합한 알고리즘은 PBFT다. PBFT를 개선한 합의 프로토콜 ISAAC+ 역시 Data Finality를 보장하며, 제한된 장애허용범위(3f+1, f=faulty node수)안에서 liveness와 safety를 보장한다. 아래는 ISAAC+ 알고리즘에서 노드간의 메시지 전달과 합의 과정을 그래프로 표현한 것이다.



ISAAC+에서 합의 과정에 참여하는 노드 그룹을 Suffrage Group이라 부른다. Suffrage Group은 매 라운드마다 임의의 노드들로 구성되는 Acting Suffrage Group을 선출한다. 즉 매 합의 라운드마다 Suffrage Group에서 랜덤으로 일정 수의 Acting Suffrage Group을 선출하고, 이들 중에 새로운 블록을 제안하는 리더를 선출하는 방식으로 기존 PBFT의 합의 단계를 재구성했다. Acting Suffrage을 도입한 이유는 매 라운드마다 일정 수의 노드들의 활동을 검사하여 노드들의 건강성을 상시적으로 모니터링하기 위함이다. ISAAC+ 알고리즘의 합의는 Init -Sign - Accept이라는 3단계로 구성된다.

Init 단계에서는 합의에 참여하는 모든 노드(Suffrage Group)는 이전 Round에서 생성된 블록에 대한 합의를 검증하여 그 결과를 ballot에 담아 Suffrage Group에 전송한다. 합의에 이르지 못하면, 다음 Round의 Init 단계를 새롭게 시작하여 다시 한번 해당 블록에 대해 voting을 진행한다. 합의에 성공하면 이전 라운드에 생성된 블록을 블록체인에 기록하고 새로운 라운드를 시작한다. 이때 suffrage group은 합의된 블록을 블록체인에 기록하고 Sign 단계로 넘어간다. Sign 단계에서는 random 함수에 의해서 이번 라운드의 블록생성을 제안할 Proposer와 Acting Suffrage Group 멤버를 선택한다. Acting Suffrage Group은 Proposer의 Proposal에 대해서 검증하고 그 결과를 전체 Suffrage Group에 전송한다. Sign 단계에서 Acting Suffrage Group의 voting 결과에 상관없이, Suffrage 그룹은 Accept 단계의 voting을 진행하고 그 합의에 성공하면 INIT 단계로 넘어가게 된다.

위에서 설명한 Init-Sign-Accept 프로세스를 정리하면 아래와 같다.



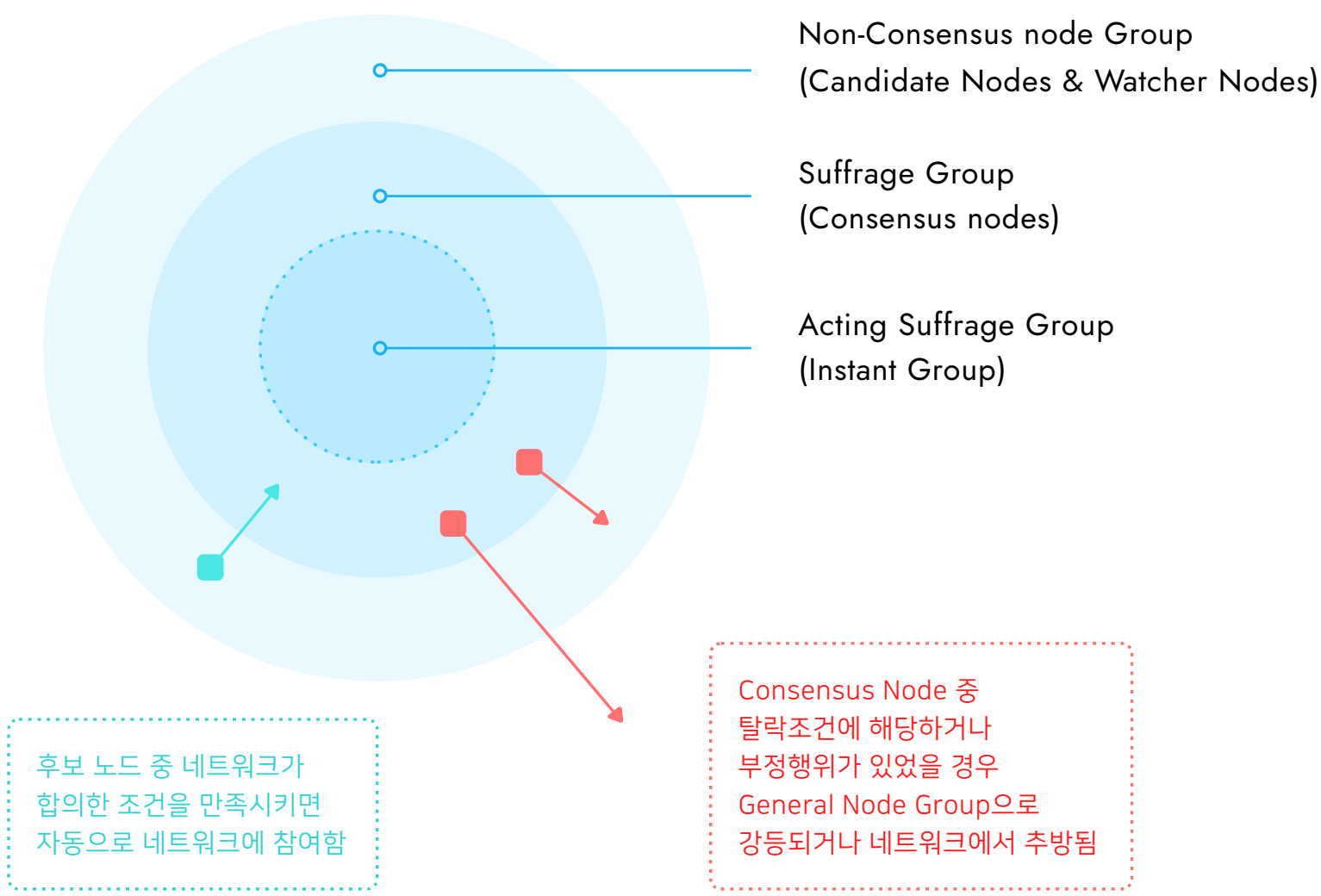
여기서 일정 수만큼의 Acting Suffrage Group을 선출하는 이유는 Proposer를 선택하는 과정에서 random하게 노드를 샘플링하여 faulty 노드 여부를 검증하기 위해서다. 만약 어떤 노드가 일정한 한계 이상으로 비정상적인 패턴을 보인다면 Suffrage Group에서 퇴출된다. 즉 컨센서스를 수행하는 Suffrage Group에 속한 노드들 중 문제가 발생한 노드들이나 건강하지 않은 노드들을 지속적으로 모니터링하고 임계치 이하의 노드들은 대기중인 건강한 노드로 교체함으로써 전체 네트워크가 건강한 상태를 유지할 수 있도록 하기 위함이다. 이러한 과정을 통해서 Suffrage Group에서 faulty node의 발생가능성을 줄일 수 있게 된다. 즉 프로토콜에서 정한 일정한 기준을 만족하는 노드들에게만 consensus 참여의 기회를 주어 네트워크의 안정성을 돕고, 나아가 임의의 참여노드들에게도 블록체인 네트워크안에 활동할 수 있는 기회를 주어 안정성을 보장하면서도 Permissionless한 Network를 확보하게 된다.

02 노드 운영 구조

프로토콘넷에는 3가지 유형의 노드가 존재한다. 첫번째는 블록체인에서 가장 중요한 '합의'를 만들어내는 역할을 담당하는 Suffrage Group 노드로, 우리는 이들을 일꾼(Worker)이라 부른다. PBFT 알고리즘의 특성상 Suffrage Group의 노드 숫자는 제한적일 수밖에 없을 것이다. PoW는 비록 노드수는 제한이 없지만 처리 성능 자체에 한계가 있고, 잘 구현된 PBFT 알고리즘은 최대 수천 tps까지 처리가 가능하지만 노드수를 무한대로 늘릴 수 없는 한계가 있다. 일반적으로 PBFT는 노드수와 성능이 반비례하기 때문에, 안정성, 경제성, 탈중앙성 등을 고려해 최적의 조합을 찾아내야 한다. 우리는 베타넷 단계에서 점진적으로 네트워크를 확대해 가면서 여러가지 테스트와 최적화 작업을 통해 적절한 수준의 노드수를 확보할 예정이다. 아울러 프로토콘넷은 산업에 적용할 수 있는 수준의 네트워크 성능을 제공하는 것을 목표로 하며, 따라서 Suffrage 노드를 운영하기 위해서는 일정 수준 이상의 처리 성능과 안정적인 네트워크 대역폭을 확보해야 한다. 즉 노드를 운영하려면 일정한 성능과 안정성 조건을 만족시켜야 한다. 노드 운영 관련 필요 조건에 대해서는 별도로 안내할 것이다.

프로토콘넷의 구조는 대략 다음과 같다.

프로토콘넷 노드 생태계 구조



Suffrage Group의 외곽에는 다수의 Non-Consensus Node Group이 존재한다. 이들은 합의된 블록을 백업하는 역할과 동시에 외부에서 데이터 조회 등의 요청이 올 경우 데이터를 제공하는 역할을 하게 되며, 이에 따라 Suffrage Group은 오롯이 합의와 모델 데이터 처리에만 집중함으로써 블록체인 전체의 처리 성능을 높일 수 있다. 우리는 향후 블록체인의 사용성이 증가할 경우 컨센서스에 대한 요청만이 아니라 데이터 조회에 대한 요청도 폭발적으로 증가할 것으로 예상하기에 Non-Consensus Node Group의 역할도 점차 중요해질 것으로 판단한다. Non-Consensus Node는 일반적으로 Suffrage Group보다 성능이 낮거나 다소 완화된 보안 환경, 덜 안정적인 네트워크 환경에서 다수의 Node들이 참여할 수 있다. 또한 컨센서스 과정에 참여하고 싶은 노드의 경우 Non-Consensus Node Group에서 대기 상태(Candidate Nodes)로 있다가 퇴출되는 노드가 발생하면 그 자리를 대신해 Suffrage Group에 참여할 수 있다, 노드를 내보내고 새로 들이는 과정은 초기에는 노드들의 투표에 의해 그리고 나중에는 자동화된 알고리즘에 의해 자동으로 진행될 예정이다.

그러나 이러한 이상적인 그림에 한번에 도달할 수는 없다. 성숙한 단계에 진입하기까지는 적지 않은 노력과 시간 그리고 축적된 운영 경험 등이 필요할 것이다. 이런 측면에서 우리는 프라이빗 블록체인에 가까운 네트워크로부터 시작해서 비즈니스 생태계를 구축하면서 단계적으로 탈중앙화 네트워크까지 나아가는 전략을 실행할 예정이다.

03 노드 그룹 운영 정책

프로토콘넷은 네트워크 중단 없이 노드의 출입이 가능하기 때문에, 이론적으로 일꾼들이 일을 제대로 하지 못할 때는 전체 노드수의 ⅓ 이내의 범위에서 언제든지 교체될 수 있다. 다소 비유적으로 표현하자면 프로토콘 생태계의 노드 운영 정책은 자발적으로 자원한 일꾼들 중에 튼튼하고 충직한 이들을 골라 네트워크 운영 관리 역할을 맡기고 이들에게 충분한 보상을 제공하는 것이다. 만약 누군가 일꾼으로 참여하려면 일꾼 목록에 신청서를 제출하고 대기상태에서 non-consensus node 역할을 수행해야 한다. Suffrage Node Group에 참여할 수 있을 정도로 준비가 완료되었다는 것이 확인된 노드들은 네트워크의 허가를 받아 대기 상태에 존재하게 되며, 대기상태의 노드들에게도 일정 수준의 노드 보상이 지급된다. 대기 노드(Candidate Nodes)들의 숫자는 Suffrage 노드 수의 ⅓ ~ ½ 까지 허용하는데, 이것은 어떠한 이유로 복수개 노드들의 활동이 중단되거나 네트워크에서 탈퇴했을 때 즉시 대기중인 후보군에서 새로운 노드를 충원하기 위함이다.

통상 많은 PBFT 알고리즘들이 PBFT 알고리즘에 지분 구조(Stake)를 결합한 PoS 또는 DPoS 구조를 채택해 왔다. 이 배경에는 지분을 많이 보유한 이들은 일반적으로 자신의 경제적 이득을 극대화하기 위해 다른 이들보다 더 네트워크를 운영에 주도적으로 참여할 수 있고 또한 네트워크의 발전에 저해되는 행동을 하지 않으리라는 가정이 존재한다. 그리고 PoS나 DPoS 구조에서 지분을 많이 보유한 이들이 지분량에 비례하여 블록을 생성할 수 있는 확률을 배정하고, 지분 비율에 근접하게 블록 생성 보상을 가져가게 함으로써 지분이 많은 이들의 경제적 이해관계를 충족시킨다. 그런데 이 구조에서 지분을 많이 보유한 이들이 담합하게 되면 네트워크 전체에 대한 통제권을 획득할 수 있다는 우려와 더불어, PoS 구조에서는 소수 거대 지분을 가진 이들의 경제적 이해관계가 과도하게 반영됨으로써 전체 생태계 발전이나 프로젝트의 장기전략에 반하게 된다는 비판도 존재한다. 또한 특정 노드가 과도하게 많은 지분을

경우에는 해당 노드를 타겟으로 공격할 경우 네트워크 전체가 영향을 받게 될 수도 있는 단점도 존재한다. PBFT 알고리즘의 본질적인 측면에서 보자면 블록 생성 확률을 최대한 랜덤하게 분포시키는 것이 보안상 더 유리하기에, 전체 네트워크의 안전성과 신뢰성이라는 측면에서 보자면 합의 알고리즘에 지분의 이해 관계를 결합시켜 블록 생성의 랜덤성을 훼손하는 PoS 또는 DPoS는 PBFT와 궁합이 잘 맞는 구조는 아니다. 이런 측면에서 우리는 PoS나 DPOS 구조가 아니라 순수하게 노드들의 처리 능력과 네트워크의 안전성을 중심으로 노드들을 선별하는 PoC(Proof of Capability) 구조를 채택했다.

PoS나 DPOS와 같은 블록체인의 알고리즘 구조는 단순히 블록 생성 및 블록 보상에만 영향을 미치는 것이 아니라 생태계 구성 방법 및 생태계 참여에 대한 보상 구조에까지 영향을 미친다. 즉 PoS나 DPOS 구조에서는 노드가 보유한 지분량이 중요하기 때문에 토큰 예치(Staking) 구조가 노드들을 중심으로 짜여지게 된다. 이러한 구조는 생태계 전체에서 토큰 보유자들이 노드 운영자들에게 의존하도록 함으로써 노드 운영자들의 권한을 더 강화시키는 경향이 있다. 그러나 우리는 모든 노드들이 동등한 권한과 책임 그리고 동등한 보상을 받을 수 있는 PoC 구조를 선택함으로써 노드들을 중심으로 한 토큰 예치 구조를 채택하지 않을 수 있게 되었다. 또한 노드 운영자들 중심의 거버넌스 구조를 만들지 않고 생태계 이해 관계자 전체가 참여하는 거버넌스 시스템을 구축할 수 있게 되었다. (이와 관련해 우리는 토큰 보유자들이 네트워크 전체의 사용성을 개선하는 작업에 기여하고 보상을 받아가는 FeeFi를 제안하며, 이에 대해서는 4장에서 자세하게 기술하였다.) 그럼에도 불구하고 노드들은 네트워크의 유지 및 관리를 담당한다는. 측면에서 생태계 내부에서 대단히 중요한 역할을 하기에 이들에게 충분한 경제적 보상을 제공할 것이다. 이러한 전제 하에 네트워크를 유지 및 관리하는 역할을 담당하는 Suffrage 노드 그룹 즉 일꾼 (Worker)들에 대한 운영 정책은 다음과 같다.

1. Suffrage 그룹에 참여하는 노드들은 동일한 금액을 예치하고, 동일하게 리워드를 받는다. 또한 이들은 거의 동일한 확률로 블록을 생성하게 된다.

2. Suffrage 노드의 초기 예치 금액은 500만 PEN으로 하되, 예치 금액은 PEN 토큰 가격의 변화에 따라 거버넌스에서 조정할 수 있다. Suffrage 노드 그룹에 참여하려는 대기 상태의 노드들 즉 후보 노드들 역시 500만 PEN을 예치하고 있어야 한다.

3. 우리는 장기적으로 노드들이 서비스를 제공하고 받는 수수료 그 자체로 노드 운영 비용을 보상 받을 수 있는 구조로 나아가는 것이 목표다. 그리고 이 단계에 도달하기 전까지는, 노드 운영비 충당을 위해 네트워크에서 노드들에게 일종의 보조금을 지급한다. 노드 보상은 네트워크 사용으로 발생되는 수수료 중 일부와 더불어 블록 생성 시 만들어지는 인플레이션 코인 중 일부로 지급된다. 노드 보상은 노드를 운영하기에 충분한 수준으로 지급한다.

4. 네트워크에서 노드를 선택하는 기준은 노드들의 안정성과 처리 능력(Capability)이다. 노드 운영자는 네트워크가 요구하는 최소한의 하드웨어 성능과 네트워크 성능을 만족시켜야 하고 충분한 노드 운영 능력을 증명해야 한다. 품질이 나쁘거나 네트워크가 일정 기준 대비 안정적이지 않다는 것이 반복적으로 확인될 경우 해당 노드는 노드 투표 또는 자동화된 알고리즘에 의해 퇴출될 수 있다. 품질이 나쁘다는 것은 대략 1) 하드웨어 성능이 기준에 못 미치는 경우, 2) 네트워크 성능이

기준을 만족시키지 못하거나 불안한 상태가 지속되는 경우, 3) 노드가 의도적으로 일을 게을리 하고 있다는 것이 확인되는 경우 등이다.

5. 노드가 이중 사인 등 악의적인 행위를 한 것으로 확인되는 경우 해당 노드는 페널티를 받는다. 페널티는 사안의 경중에 따라 예치 금액에서 벌금을 내는 방식, 예치금을 몰수 당하고 퇴출 당하는 방식 등이 존재하는데, 최대한 엄격하게 처벌하는 것을 원칙으로 한다. 기여에 대한 보상은 충분하게 하되 악의적인 행위에 대해서는 '일벌백계'로 처벌할 것이다. 이에 대해서는 별도의 노드 운영 가이드를 통해 상세하게 안내할 것이다.

6. 노드가 예치한 금액은 예치금 인출을 신청한 이후 대략 4주 후 락업이 해제된다. 이는 대량의 물량이 시장에 일시에 풀려 시장을 교란하는 행위를 막기 위함이다.

7. 새로운 노드가 추가되는 경우는 1) 기존 노드가 (어떠한 이유로) 탈퇴해서 노드를 새로 충원하는 경우, 2) 네트워크 규모 확장으로 기존 노드들 이외에 신규 노드들이 추가되는 경우로 나눌 수 있다. 이 경우 노드 후보군 중에 가장 상태가 좋은 노드가 추가된다. 노드가 추가되는 방식은 초기에는 노드들의 투표에 의해서 추가되며, 이후 노드 관리 기술이 성숙되면 네트워크 자체의 판단에 따라 후보군 중에서 최적의 노드를 찾아 자동으로 추가하게 될 것이다.

8. 노드 운영자들은 프로토콘넷에 배포되는 컨센서스 알고리즘과 모델 등 각종 프로그램과 정책에 대해 투표를 통해 승인할 권한을 보유한다. 이중 네트워크 및 생태계에 큰 영향을 미치는 보안, 안전성, 성능과 관련된 사항에 대해서 노드들은 1차 관리자 역할을 수행한다. 그러나 모든 노드 운영자들은 '의회'가 의사결정한 사항에 따라야 한다.

위 운영 정책들은 테스트넷 및 메인넷 1단계에서 충분한 테스트를 거쳐 검증 및 보완될 예정이다. 특히 노드 운영 보조금은, 노드 운영자들이 수수료가 많지 않을 것으로 예상되는 초기에는 거의 절대적으로 보조금에 의존할 수밖에 없으며, 또한 수수료로 만들어내는 총가치가 늘어남에 따라 보조금의 량도 적절하게 조절되어야 하기 때문에 노드 운영 보조금 정책은 프로젝트의 발전에 따라 변경될 수밖에 없다. 이와 같은 변경 사항들은 노드 운영 보상과 관련된 가이드라인에 따라 수정안들이 마련되고 최종적으로 의회의 승인을 거쳐 확정될 예정이다.

04 모델

비트코인이 블록체인 개념을 제시하여 '암호화폐'라는 새로운 영역을 개척했다면, 이더리움은 '블록체인과 스마트 컨트랙트(Smart Contracts)를 통해 전세계에 걸친 탈중앙화된 컴퓨팅 인프라스트럭처 라는 개념을 제시하고 블록체인의 적용 영역을 확장했다는 평가를 받고 있다.[5] 이더리움으로부터 시작된 스마트 컨트랙트의 혁신성에 힘입어 대부분의 메인넷들은 이더리움과 유사한 구조의 스마트 컨트랙트를 구현하고 있다.

그런데 스마트 컨트랙트를 통해 '누구나' 수수료만 내면 블록체인 상의 트랜잭션을 일으키는 것이 타당한가 하는 문제가 있다. 기존의 스마트 컨트랙트 작동 구조에서는 적절하지 않거나 악의적인 스마트 컨트랙트라도 블록체인 네트워크에서 실행된 후에야 즉 사고나 문제가 발생한 후에야 알 수게 된다는 점에서, 잘못된 스마트 컨트랙트가 배포되는 경우 스마트 컨트랙트 작성자뿐만 아니라 노드 운영자, Dapp 운영자 그리고 사용자 등 생태계 전체 피해를 보게 되는 구조를 가지고 있다. 이와 같은 방식은 일견 자유도가 높은 것처럼 보이지만 불안정하거나 악의적인 프로젝트가 생태계 전체에 좋지 않은 영향을 끼치더라도 네트워크 차원에서 전혀 대응할 수 없다는 취약점을 가지고 있다. 이러한 문제 의식에 따라, 우리는 블록체인의 보안성을 높이고 전체 생태계를 보호하기 위해, 누구나 쉽게 배포할 수 있는 스마트 컨트랙트의 '배포 자유도'를 포기하고 노드 그룹 등을 중심으로 최소한의 품질 관리가 가능하도록 하면서, 또한 개발 그 자체와 관련해서는 블록체인 코어 기능을 직접 사용하여 보다 높은 수준의 '구현 자유도'를 확보할 수 있는 '모델(Model)' 개념을 제안한다. 우리가 제안하는 '모델(Model)'이란 <블록체인 코어가 제공하는 기능들을 활용하는 프레임워크를 통해 다양한 비즈니스에서 요구되는 오퍼레이션을 처리하는 프로그램>으로 정의할 수 있다. '모델(Model)'은 대략 다음과 같은 특징을 가지고 있다.

1. 프로토콘넷은 누구나 개발 가능하도록 '모델' 개발 프레임워크를 제공한다. 개발자라면 누구나 모델 관련 문서를 보고 독자적인 모델을 개발할 수 있다.

2. 하나의 네트워크에 여러 개의 모델을 동시에 운용할 수 있다.

3. 기존 스마트 컨트랙트에서 반복적으로 발생해왔던 보안 문제를 관리하기 위한 최소한의 장치로, '모델'의 채택, 운영, 보완 및 업데이트는 노드 운영자들의 승인을 통해서만 가능하도록 했다. 정책 역시 블록체인의 안정성 및 가치 전체에 영향을 미치는 경우에는 노드들의 검토 후 승인하는 것으로 정의했다.

4. 모델 내에 '기능'과 '정책'의 분리를 통해서 구현 자유도를 최대한 보장한다.

5.신규 모델 적용이나 기존 모델의 업데이트를 할 경우에도 미텀 메인넷은 중단없이 작동한다.

코인 발행 기능을 제공하는 미텀 커런시(currency) 모델을 기준으로 예를 들어 보자. 미텀 커런시 모델을 이용해서 신규 코인을 발행하고 싶을 때는 정책에 해당하는 파라미터 값(코인명, 수량, 수수료 등)을 설정하여 토큰발행 제안서를 제출하면, 노드들의 승인을 거쳐 신규 코인이 발행된다. 이때 노드들은 프로젝트 주체가 명확하고 신뢰할 수 있는지, 제출된 코드가 문제가 없는지, 장기적으로 생태계의 발전과 확장에 기여할 수 있는 프로젝트인지 등 신규 프로젝트들의 정책과 코드들을 검토한 후 네트워크에 업로드될 수 있도록 승인할 것이다.

여기서 블록체인은 데이터 무결성을 보장하는 특별한 유형의 데이터베이스로써 기능하며, 모델은 토큰을 포함해 다양한 유형의 데이터와 정책을 정의하고 처리할 수 있는 기능을 제공한다. 이와 같은 확장성 덕분에 프로토큰넷에서 토큰 거래나 데이터 관리 또는 기타 블록체인 기반의 응용서비스 등 블록체인이 필요한 모든 서비스를 개발할 수 있다. 향후 다양한 모델들이 개발될수록 더욱 풍부한 기능을 사용할 수 있게 될 것이다.

현재 우리는 미텀 블록체인을 사용하는데 있어 필수적이라고 생각하는 다음과 같은 모델을 개발 중이며, 이중 토큰 모델은 개발 완료되었다. 데이터 모델은 아래에 기술할 블록체인 기반의 디지털 문서 및 데이터 관리 서비스 '블록사인'과 연동되어 사용할 수 있는 프로토타입 버전을 개발 중이다. 그 외 수수료와 관련된 UX 문제를 해결하기 위해 특별하게 고안된 수수료 모델(FeeFi), 투표모델 등 다양한 모델들이 개발될 예정이다. 아래 모델들은 엄격한 보안검사를 거친 후, 노드들의 합의에 의해 블록체인 네트워크 위에 배포될 것이다. 우리가 초기에 구현하려는 모델의 유형은 대략 다음과 같다.

토큰모델

토큰 모델은 일반적으로 메인넷 위에서 토큰을 발행하고 전송하는 기능을 담고 있다. 현재는 이더리움의 ERC-20 유형에 해당하는 모델이 개발되어 있으며, 이후 다양한 특징을 가진 토큰 모델들을 순차적으로 개발할 예정이다. 토큰 모델을 포함한 모든 모델들은 수수료 모델을 통해 네트워크 사용료를 지불한다. 프로토콘넷은 네트워크가 자체 발행한 PEN 토큰을 프로토콘 생태계의 기축통화이자 거버넌스 토큰으로 사용하며 토큰 모델을 통해 작동한다. dApp 서비스 제공업자들 역시 토큰 모델을 활용해 각자의 토큰을 발행할 수 있다. 아래 그림과 같이 발행량, 수수료 정책, Currency ID 등의 몇몇 값을 정하여 Operation을 작동시키면 쉽게 dApp 토큰을 발행할 수 있다.

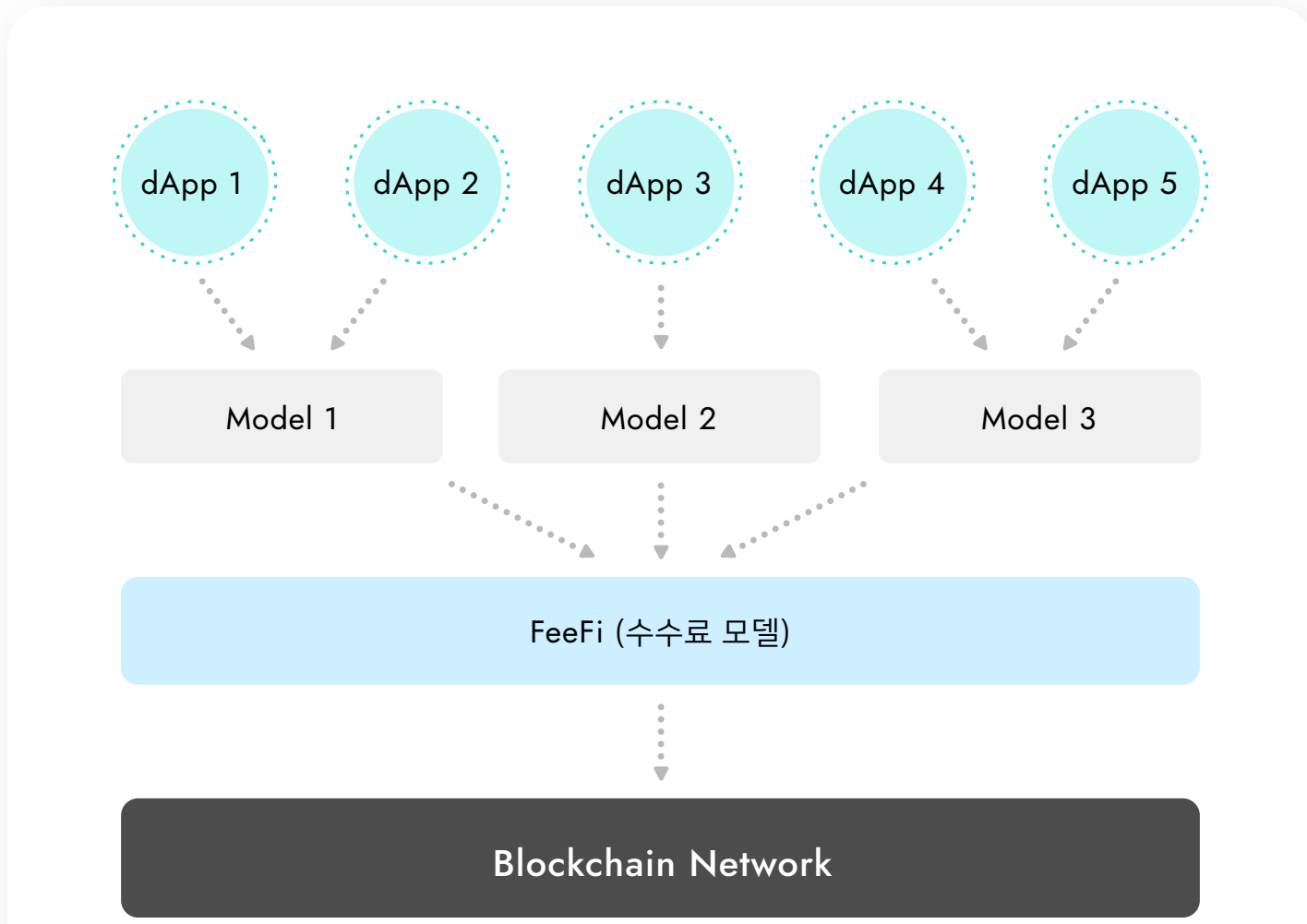
[dApp 토큰 생성 operation]


```
"operations": [
    {
        "hash": "98Qu7EytGVZMHW7ujDWbwPh1uYGhWS7RKQip7eEUyHvx",
        "fact": {
            "_hint": "a028:0.0.1",
            "hash": "25panwZiZ7KLLdjrRgZ6HW5YT4vW86NaHUSYtJN51utG",
            "token": "MjAyMS0wMy0yNlQxNTo0ODozOC42NTE2MyswOTowMA==",
            "currency": {
                "_hint": "a030:0.0.1",
                "amount": {
                    "_hint": "a022:0.0.1",
                    "amount": "99999999999999999999",
                    "currency": "PEN"
                },
                "genesis_account": "4UM4CN8MZNyv26TK84486CX5X8bu9EUYbsWz5ovRsp1M-a000:0.0.1",
                "policy": {
                    "_hint": "a036:0.0.1",
                    "new_account_min_balance": "10",
                    "feeer": {
                        "_hint": "a032:0.0.1",
                        "type": "fixed",
                        "receiver": "4UM4CN8MZNyv26TK84486CX5X8bu9EUYbsWz5ovRsp1M-a000:0.0.1",
                        "amount": "3"
                    }
                }
            }
        },
        "fact_signs": [
            {
                "_hint": "0150:0.0.1",
                "signer": "skRdC6GGufQ5YLwEipjtdaL2Zsgkxo3YCjp1B6w5V4bD-0113:0.0.1",
                "signature": "AN1rKvtJhUbbZAEtqQ7g7R8R1iyz64Yxq4GTQDrZZE2yDBJZ1Vc6xr1fKtxven7ZZraHr5BW8QvXVw6CD5SwKzM3JavTMszps",
                "signed_at": "2021-03-26T15:48:38.652382+09:00"
            },
            {
                "_hint": "0150:0.0.1",
                "signer": "ktJ4Lb6VcmjrbexhDdJBMnXPXfpGWnNijacdxD2SbvRM-0113:0.0.1",
                "signature": "381yXZL5jLng9CTHKLywBVdFegFNRaW12AE7wzsHpLphF28JZVuA1LzpVETy7ZDeBWFRv7sMP7wiSqvEHZVYwL7TAksgmpKe",
                "signed_at": "2021-03-26T15:48:39.12282+09:00"
            },
            {
                "_hint": "0150:0.0.1",
                "signer": "wfVsNvKaGbzB18hwix9L3CEyk5VM8GaogdRT4fD3Z6Zd-0113:0.0.1",
                "signature": "AN1rKvtX5DJGPjUG6NJwYviozrpfERfF1NemwH1SPWJ3Uqj5zbRM8zwcDLiWr9hYWPRcr6WAaDrpxnUXdZfcH4GTRjorjMkHi",
                "signed_at": "2021-03-26T15:48:39.265779+09:00"
            },
            {
                "_hint": "0150:0.0.1",
                "signer": "vAydAnFCHoYV6VDUhgToWaiVEtn5V4SXEFpSJVcTtRxb-0113:0.0.1",
                "signature": "AN1rKvtgkDFxZibobzNvqaARiVNikbXh56XyjqZZJLMsJmJQ61fBz2Y25jVUQLBXRgueZa7efHHWP4AJNgy4wSHkroSqB2u9X",
                "signed_at": "2021-03-26T15:48:39.279463+09:00"
            }
        ],
        "memo": "",
        "_hint": "a029:0.0.1"
    }
]
```


수수료 모델

우리는 블록체인의 사용성 개선을 위해 수수료와 관련된 UX 문제를 반드시 풀어야할 문제라고 생각한다. 통상적인 메인넷이라면 사용자들은 dApp 토큰을 사용하기 위해 메인넷 토큰을 구매하던지 아니면 사용을 포기해야 한다. 그리고 실제로 많은 잠재적 사용자들이 이 단계에서 블록체인 서비스 사용을 포기하고 만다. 물론 일부 수수료를 대납하거나 또는 시스템 자원을 선구매하는 방식 또는 한정된 기간 동안 무료로 서비스를 제공하는 경우도 있지만 우리는 이것이 문제를 근본적으로 해결해주지 못한다고 생각한다. 수수료 대납이나 무료 정책은 DDOS 공격을 유도할 수 있고, 시스템 자원을 선구매하는 방식은 자원을 두고 무한경쟁을 유도하여 네트워크 사용 비용이 급격하게 변동하도록 만들기 때문이다.

이 문제를 해결하기 위해 우리는 토큰 홀더들이 참여하여 수수료 사용성을 개선하는 모델을 제시하고, 이에 대한 대가를 나누어 갖는 수수료 마켓 모델, 즉 FeeFi(Fee Financing)을 구현할 예정이다. 프로토콘넷에서 사용자가 수수료를 지불하는 방식은 두가지가 있다. 하나는 PEN으로 수수료를 지불하는 것이고 다른 하나는 dApp 토큰으로 수수료를 지불하는 것이다. 즉 프로토콘넷에서는 메인넷의 기축 토큰 PEN이 아닌 dApp 토큰으로 네트워크 수수료를 지불할 수 있다. 첫번째 방식은 별도의 dApp 토큰 없이 프로토콘넷을 사용할 때 수수료를 지불하는 방식이고, 두번째 방식은 사용자가 dApp 토큰을 사용하는 경우에 해당한다. 이에 대해서는 '4장 토큰이코노미와 수수료''에서 보다 자세하게 기술할 것이다. 아래 그림은 일반 모델과 수수료 모델의 관계를 도식화한 것이다.



DID 모델

블록체인의 활용도와 관련하여 중요하게 부상하고 있는 영역 중 하나가 바로 DID 영역이다. DID는 탈중앙화 네트워크 또는 개별 국가의 경계를 뛰어넘는 글로벌 경제활동에서 개인의 Identity와 유일성을 확보해주고 나아가 블록체인에 저장되는 각종 자산과 인증 기록, 저작물 등의 소유권과 처분권을 관리해주는 인프라 서비스다. 우리는 프로토콘넷 기반, 글로벌 표준을 준수하는 DID 모델을 구축하여 보다 편리한 사용성을 제공할 것이다.

데이터 모델

블록체인의 중요한 기능 중 하나는 디지털 데이터의 원형 또는 hash값을 위변조 불가능한 방식으로 보관함으로써, 데이터나 문서의 원본 확인 및 부인방지, 문서 변경 이력 관리 등 디지털 데이터의 원본, 고유성, 유일성을 보장해 주는 것이다. 또한 해당 값을 외부에서 조회하고 검증할 수 있기 때문에 문서 발행 이력 및 문서의 진본 여부 등을 공개적으로 검증할 수 있도록 한다. 데이터 모델은 이처럼 디지털 데이터나 문서를 관리하는데 필요한 여러가지 기능들을 구현한 모델이다. 본 모델은 블록사인(https://blocksign.ai) 서비스에 직접적으로 사용될 예정이며 서비스 및 사용자들의 요구에 따라 지속적으로 개선될 예정이다.

디지털 자산 모델

최근 NFT 토큰처럼 블록체인 기반으로 디지털 자산(Asset)을 관리하려는 시도들이 본격화되고 있다. 사회 전반이 디지털 전환됨에 따라 현실의 자산을 기반으로 현실 자산에 대응하는 고유한 디지털 자산을 생성한다던지, 애초부터 디지털로 존재하는 디지털 자산을 다루는 일들이 이제 막 시작되었다. NFT는 디지털 자산을 정의해주는 아주 초보적인 모델일 뿐이며, 우리는 블록체인으로 디지털 자산을 관리하는 방법을 하나씩 찾아내야 하는 상황이다. 우리는 내부에서 이와 관련된 여러가지 아이디어들을 발전시키고 있으며, 준비되는 시점에 하나씩 시장에 공개할 것이다. 사전적으로 블록시티를 통해 게임 내에서 필요한 다양한 디지털 자산을 블록체인으로 관리하는 여러가지 방법론들을 정식화할 예정이다.

투표 모델

투표 모델은 일반적인 온라인 투표에 범용적으로 사용될 수 있는 모델로, 블록체인 상에서 기명투표 및 무기명 투표를 가능하게 한다. 우리는 이 모델을 프로토콘 네트워크 거버넌스의 의사결정에 참여하는 투표툴로 사용할 예정이다. 또한 이 모델은 커뮤니티, 지자체, 정부 기관, 협동조합 및 커뮤니티 등에서 블록체인 기반의 투표 시스템으로 사용할 수 있으며, 또한 게임 내에서 사용자 의사결정 기반의 게임을 만드는 방법론에 의사결정툴로도 사용할 예정이다. 프로토콘 네트워크는 충분한 성능을 확보하고 있기 때문에, 소규모 커뮤니티에서 수행하는 투표뿐만 아니라 지자체와 국가 단위 국민투표 등에서 문제없이 사용될 수 있을 것이다.

이외에도 훨씬 더 많은 모델들이 필요할 것이다. 블록체인 산업은 아직 초기이기에, 우리는 아직 산업 현장과 비즈니스에 필요한 구체적인 요구사항들을 다 알지 못한다. 우리는 지속적으로 산업 및 생태계와 교류하여 최대한 많은 이들이 블록체인 기술을 광범위하게 활용할 수 있도록 안전하고 편리한 모델들을 지속적으로 업데이트할 예정이다. 또한 우리는 기술 문서에서 블록체인을 활용하여 모델을 개발하는 자세한 방법론을 제공할 것이기에, 따라서 개발자라면 누구든 자신만의 모델을 만들 수 있다. 다만 프로토콘 네트워크는 임의의 소스를 업데이트해서 운영할 수 있는 구조가 아니기 때문에, 해당 모델을 프로토콘 네트워크에서 작동시키려면 엄격한 보안 테스트와 더불어 프로토콘 네트워크 거버넌스의 의사결정을 거쳐야 한다.

04 탈중앙화 전략과 거버넌스 구조

비탈릭 부테린은 '탈중앙화의 의미'(The Meaning of Decentralization)[6]라는 글에서 탈중앙화의 여러가지 측면을 검토한 바 있다. 이 논지와 더불어 탈중앙화와 관련된 여러가지 논쟁과 주장들을 요약하면 탈중앙화란 '특정 개인 또는 소수 집단이 네트워크를 장악하거나 통제할 수 없는 상태'로 정의할 수 있다. 그리고 블록체인 네트워크는 고정된 상태로 존재하는 것이 아니라 살아움직이는 것이기에 보다 현실적이고 실질적인 의미에서 탈중앙화 네트워크는 '특정 개인 또는 소수 집단이 네트워크를 장악하거나 통제할 수 없는 상태로 지속적으로 유지 및 관리되며 스스로 개선, 확장할 수 있는 네트워크'라고 재정의할 수 있다. 그렇다면 어떻게 탈중앙화된 상태에서도 지속적으로 유지, 발전할 수 있는 네트워크와 생태계를 구축할 수 있을까?

앞에서 이야기했듯이, ISAAC+에서 탈중앙화를 위한 기술적 장치를 마련했지만 탈중앙화는 기술적 요소만으로 확보되지 않는다. 탈중앙화 네트워크를 구축하기 위해서는 기술적 요소, 경제적 요소, 거버넌스 구조 등을 복합적으로 구성해야 한다. 일반적으로 탈중앙화 되었다고 평가받는 PoW 알고리즘조차도 51% 공격이라는 논리적이고 치명적인 단점이 존재하며 실제로 51% 공격이 성공한 프로젝트도 몇개 있다. 비트코인이나 이더리움은 시나브로 막대한 공격 비용이 필요한 수준까지 성장함으로써 쉽게 공격 당하지 않는 방식으로 탈중앙성을 확보한 것이다. 즉 PoW에서는 기술적 장치 이외에 경제적 장치가 탈중앙화를 유지하는 하나의 요소로 작동하고 있다. 따라서 노드들의 출입이 PoW 만큼 자유롭지 않은 PBFT에서는 탈중앙화 상태를 유지하기 위해서는 기술적 장치와 더불어 경제적 이해관계를 다루는 토큰 이코노미 그리고 특정 개인, 집단 또는 세력의 독점을 제어할 수 있는 거버넌스 구조 등이 동시에 고려되어야 한다. 이런 측면에서 먼저 블록체인 생태계 참여자들의 유형, 특징, 권한, 참여자들이 고유하게 가지고 있는 위험요소 또는 관리요소 등을 구분해볼 필요가 있다.

블록체인 생태계 참여자들

블록체인 생태계는 재단을 중심으로 하는 프로젝트 리더 그룹, 블록체인 네트워크를 운영 및 관리하는 노드 운영자들, 오픈소스 개발에 참여하는 개발자 커뮤니티, 토큰 보유자를 중심으로 한 커뮤니티, dApp 서비스 파트너 등 다양한 참여자들이 존재하며, 이들은 생태계 내에서 각각 서로 다른 역할을 담당하는 여러 참여자들이 명시적으로 또는 암묵적으로 협력하고 경쟁하고 견제하면서 작동한다. 탈중앙화 네트워크에서 암호화폐를 매개로 만들어진 개인들의 모임을 크립토 커뮤니티(Crypto Community)라고 명명할 수 있는데, 크립토 커뮤니티는 프로젝트가 제시하는 비전에 대한 믿음과 기술에 대한 신뢰를 바탕으로 자발적으로 작동하는 글로벌 경제공동체다. 크립토 커뮤니티에 참여하는 이들은 각각 역할이 구분되어 있고 권한과 책임의 경중이 다르지만, 생태계가 건전하게 작동하기 위해서는 이들 모두가 서로 협력하고 또한 견제하면서 생태계 전체의 성장에 일조할 수 있도록 구조가 만들어져야 한다. 장기적으로 지속적으로 성장하는 블록체인 생태계를 설계하기 위해서는 이들 참여자들의 역할과 책임을 보다 깊이 있게 살펴볼 필요가 있다.

01 리더그룹

거의 모든 블록체인 프로젝트들은 프로젝트 리더그룹이 존재한다. 최초 개발자가 사라진 비트코인의 경우에도 초기에는 사토시 나카모토를 축으로 하는 프로젝트 리더 그룹이 존재했다. 이들은 프로젝트를 처음 고안하고 발의하고 프로젝트에 필요한 필요한 자금을 만들고 기술을 개발하고 생태계 활성화를 적극적으로 추동하는 역할을 맡는다. 또한 리더그룹은 노드 운영자들이나 토큰 보유자들을 포함한 생태계 전반의 지지를 받으며 프로젝트를 주도하고, 프로젝트가 어느 정도 성장한 이후에도 기술 개발을 주관하고 프로젝트 전반의 방향을 설정하는 역할을 한다. 이들이 없으면 프로젝트 자체가 존재하거나 존속하기 어려우며, 특히 프로젝트 초기에 이들의 역할과 책임은 절대적이다. 이들은 프로젝트의 시작과 존속에 필수적인 존재이기에, 생태계 안에서 다소 특별한 지위를 갖는다. 이런 이유로 현재 대부분의 프로젝트들에서 프로젝트 리더 그룹이 절대적인 권력을 보유하게 되는 경우가 많다. 이는 어떤 측면에서는 피할 수 없는 일이기도 하지만, 권력 집중이 지나쳐 의사결정 권한을 독점하게 되는 경우 간혹 이기적이고 독단적인 결정과 일방적인 집행으로 생태계 활성화에 역효과를 내기도 한다. 또한 이러한 구조는 이들이 손쉽게 자산을 사유화하거나 탈취하는 등 범죄를 저지르도록 유도하는 경향도 없지 않다. 즉 프로젝트 리더 그룹이 중앙화 권력의 가장 큰 문제로 지적되어 왔던 Single Point Failure의 근원이 될 위험성이 존재하는 것이다. 따라서 이들이 생태계에서 차지하는 비중과 역할이 충분히 인정되면서도 이들의 권력은 어느 정도 제어되고 감시받아야할 필요성이 있다.

02 노드 운영자

블록체인 생태계는 살아 있는 노드들의 집합에 기반해서 존재한다. 노드는 노드 운영자들에 의해 유지되고 관리된다. 대부분의 경우 노드 운영자들은 자신의 컴퓨팅 리소스를 제공하고 노드 운영에 따른 보상을 받는다. 이들 역시 생태계 내에서 특별한 지위를 가지고 있는데, 그것은 이들이 노드를 작동시키는 하드웨어 및 소프트웨어에 대한 통제 권한을 보유하고 있기 때문이다. 이 권한은 전체 네트워크에 대한 권한이 아니라 오로지 자신이 운영하는 노드(컴퓨터)에만 행사되는 권한이지만, 만약 노드 운영자들 다수가 특정 사안을 두고 담합한다면 네트워크와 생태계 전체에 대해 강력한 영향력을 행사할 가능성이 있고, 심지어 네트워크 전체를 통제할 수 있게 되는 경우도 발생한다. 익명성을 활용하여 한명이 다수의 노드를 장악하는 것도 불가능한 일은 아니다. 블록체인 네트워크는 탈중앙화된 상태를 유지하기 위해 각 노드에 대한 소유권과 통제권을 최대한 분산시켜야 하지만, 이렇게 분산된 상태에서도 노드 운영자들이 자신들 공동의 이익을 위해 인적으로 담합하는 것을 막기는 쉽지 않다. 이런 이유로 비트코인 전송 수수료를 낮추려던 시도가 비트코인 노드 운영자들의 반대로 무산되었던 사례와 같이, 그리고 파일코인에서 노드 운영자들이 파업을 해서 네트워크를 중단시켰던 사례와 같이, 종종 생태계 전체의 이득과 발전이나 장단기적인 정책이 노드 운영자들의 이해관계와 충돌할 때, 생태계 참여자 전체의 입장보다 노드 운영자들의 입장이 강하게 또는 일방적으로 반영되는 사례들이 있었다. 따라서 구조적으로 이들의 담합을 제어할 수 있는 기술적, 정책적 장치들이 필요하다.

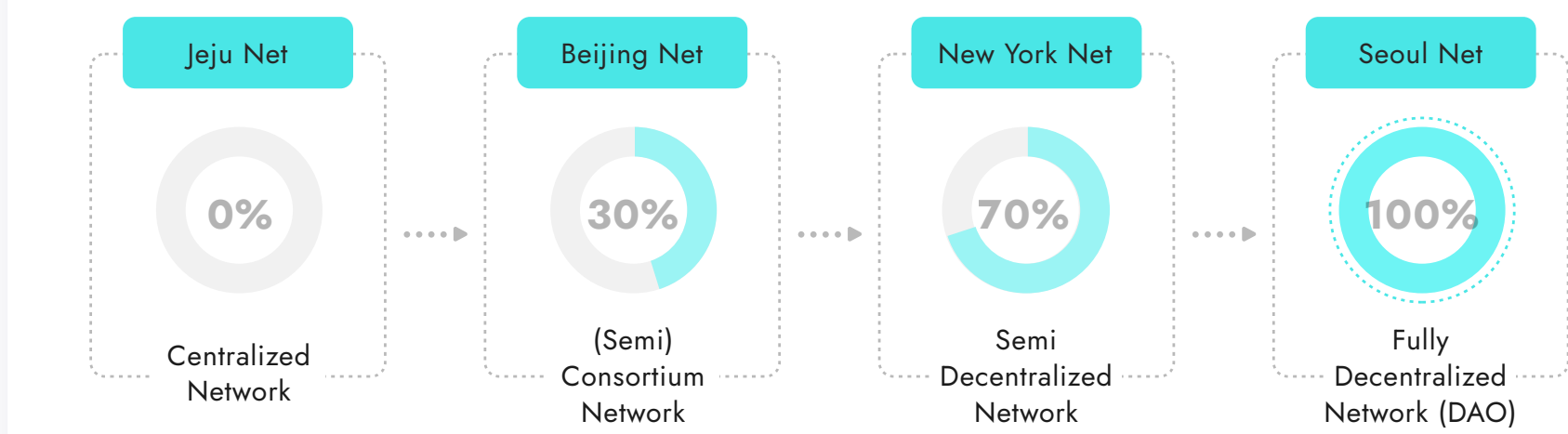
03 커뮤니티

프로젝트 리더그룹, 노드 운영 그룹 이외에 토큰 보유자 집단 즉 토큰 커뮤니티 또한 중요한 이해관계자들 중 하나다. 이들은 토큰을 보유하고 자발적인 지지자로 활동하면서 프로젝트에 활기를 불어넣고 프로젝트를 홍보하는 역할을 담당한다. 이 외에도 오픈소스 개발자 커뮤니티, dApp 서비스 파트너 등 다양한 참여자들이 존재하는데 통상 이들은 '토큰 보유자' 또는 광범위한 의미의 '커뮤니티'로 묶일 수 있다. 초기 블록체인 프로젝트들에서 이들은 단순히 토큰을 구매해주고 토큰을 보유하며 경제적 이득을 기대하는 수동적인 존재였다. 이들은 가장 많은 수로 구성되어 있지만 실제 프로젝트에 대한 의사결정에서 종종 배제되었었다. 그러나 최근 프로젝트들은 토큰 보유자들에게 거버넌스에 참여할 권한을 주고, 토큰 유동량을 조절하기 위해 토큰을 스테이킹(Staking) 하도록 하는 등 적극적인 참여를 유도하고 있다. 또한 이들에게 직접적인 의사결정 권한을 부여하기도 하며 보다 적극적으로 거버넌스에 참여할 수 있도록 유도하려는 시도들도 늘어나고 있다. 생태계의 다양한 구성원들의 수가 많을수록 그리고 많은 이들이 적극적으로 참여할수록 생태계 전체의 가치가 커지기 때문이다.

이들 참여자들 모두는 공통의 이해관계를 가지고 있는데, 그것은 바로 네트워크와 생태계 성장에 따른 경제적 이득을 나누어 갖는 것이다. 그리고 프로젝트가 성장하고 발전할수록 나눌 수 있는 파이는 급격하게 커지는 경향이 있다. 만약 이들 생태계 참여자들이 장기적인 비전을 보고 프로젝트의 성장을 위해 협력한다면 해당 프로젝트는 급격하게 성장할 수 있다. 그러나 만약 이들이 각자 자신들의 단기적인 이득에만 집중한다면 해당 프로젝트는 성장이 지체되거나 어떤 경우에는 중단되게 된다. 따라서 탈중앙화된 상태를 유지하면서도 각 참여자들이 서로 공동의 목적을 위해 협력할 수 있는 거버넌스 구조를 구축하는 것이 무엇보다 중요하다. 또한 통상 이러한 거버넌스는 강제적인 참여를 유도하기 쉽지 않고 프로젝트의 흥망성쇄에 따라 참여도가 급격하게 변화하기도 한다. 따라서 거버넌스를 유지하고 발전시키는 행위에 지속적으로 참여를 독려하는 인센티브 장치 등 여러가지 보완 장치들도 필요하다. 우리는 이와 같은 암호화폐 생태계의 실험과 노력과 시행착오들을 십분 반영하여 탈중앙화 거버넌스 구조를 설계하고자 한다.

탈중앙화 단계

탈중앙화 전략과 거버넌스 구조는 노드 탈중앙화와 밀접한 연관성을 가지고 있다. 초기 우리는 프라이빗 네트워크에 가까운 형태로 메인넷을 오픈할 예정이며, 이 시점엔 소수의 파트너들이 노드 운영에 참여하게 될 것이다. 즉 대부분의 노드를 운영하는 재단이 거버넌스에 대한 통제권을 가지게 될 것이다. 우리는 이미 내부적으로 알파넷을 운영하고 있으며, 베타넷 단계에서 블록사인 서비스와 블록시티 게임 서비스를 연동하여 관련 기능의 개발 및 테스트를 진행할 예정이다. 이후 FeeFi를 비롯한 토큰 이코노미 구축 작업이 완료되는 시점에 메인넷 1.0인 Jeju Net을 공식 오픈할 것이다. Jeju Net 단계에서는 어쩔 수 없이 재단이 의사결정에 주도적인 역할을 하게 되며, 이후 여러 단계를 거쳐 점차 거버넌스를 탈중앙화 하면서 마침내 탈중앙화 조직(DAO, Decentralized Autonomous Organization)으로 나아갈 것이다. 이를 위해 다음과 같은 4단계 전략을 수행하고자 한다.



1단계: Jeju Net

1단계에서 재단 중심으로 노드들을 관리하는 방식으로 프로토콘넷을 시작하게 된다. 또한 생태계 초기 파트너들이 Suffrage 노드 운영에 참여하게 될 것이다. 이미 Suffrage 노드 운영에 참여할 두개 이상의 초기 파트너들을 확보했다. 또한 지속적으로 비즈니스 파트너 등을 참여시키는 방식으로 단계적으로 네트워크를 확장하면서 파트너 노드수를 늘려나가서 재단 이외의 노드 운영수가 전체 노드수의, ⅓+1이 넘어서면 2단계로 넘어가게 된다. 이론적으로 전체 노드수의 ⅓+1까지 파트너 노드수가 늘어나면 재단 단독으로 네트워크를 통제하는 것이 불가능해진다. 1단계에서 중요한 작업은 네트워크 안정화 작업, 필수 모델 기능 개발과 더불어 노드 및 전체 네트워크 운영 경험을 축적하는 것이다. 1단계 네트워크 가동 시 첫번째 응용 서비스로 블록사인(Blocksign)과 블록시티(Blockcity)을 연동하여 서비스를 제공할 예정이다. 또한 몇몇 초기 파트너들과 함께 준비하고 있는 서비스들도 준비가 되는대로 연동될 예정이다. 파트너들의 준비 정도에 따라 일부 서비스들은 베타넷 단계부터 실서비스를 제공할 수도 있다.

1단계에서 우리는 여기서 사회 전반의 디지털 전환 및 프로토콜 이코노미 구현을 위해 필요한 응용 기술의 표준 모델들을 상당부분 개발하게 될 것이다. 특히 개발 중인 블록사인과 블록시티는 블록체인을 실제 서비스에 적용하는 사례를 구축하는 Living Lab의 역할을 하게 된다. 이런 면에서 블록사인과 블록시티는 프로토콘넷의 우수성을 검증하는 실험실인 동시에 기술 쇼룸(Showroom) 역할도 동시에 하게 될 것이다. 1단계에서 우리는 많은 실험을 진행하게 될 것이다. 예컨대 최적의 수수료 구조를 찾기 위해 네트워크 운영비용과 부대비용 등을 산정하고, 노드 운영 비용과 수수료가 창출하는 가치가 장기적인 비즈니스가 가능한 수준의 합리적인 값이 나오는 지 직접 확인하는 과정을 거칠 것이다. 이런 과정을 거쳐 네트워크 운영 및 경제 시스템과 관련된 세부적인 모델이 정립될 것이다. 기술적으로 이 단계에서 새로운 노드가 네트워크에 참여하는 방식은 현재 노드로 참여하는 이들의 투표를 통과해야 하는데, 일정 기간 동안 프라이빗 네트워크로 운영될 예정이기에 1단계에서는 어쩔 수 없이 초기 프로젝트 제안자인 프로토콘넷 재단이 선량한 감독자로서 생태계 내부의 의견을 수렴하여 의사결정을 주도하게 될 것이다. 즉 1단계에서 재단은 프로젝트 개발 및 비즈니스 개발 전반을 주관하고, 프로토콘에 올라올 dApp 서비스들을 선별하고 결정하면서 생태계를 확장하는 역할을 하게 될 것이다.

2단계: Beijing Net

2단계의 목표는 노드 운영 참여자들을 확대해서 재단이 운영하는 노드수를 점차 줄이고 전체 노드수의 ⅔+1까지 외부 노드 운영자들이 참여하도록 하여 탈중앙화 전단계까지 네트워크를 확장하는 것이다. 재단이 운영하는 노드가 아닌 외부 참여 노드수가 ⅔+1 이상이 되면 재단은 더 이상 네트워크에 대한 어떠한 통제권도 행사할 수 없게 된다. 이 단계에 이르러 1단계에서 실험한 내용들을 반영하여 생태계와 커뮤니티가 보다 단단하게 구축되고, 실질적으로 탈중앙화된 거버넌스 구조의 초기 모델이 시작된다. 실질적으로 분권화된 노드 네트워크가 작동함에 따라 노드 보상 구조가 본격적으로 작동하게 되고, 또한 Suffrage Group 이외에 다수의 Non-Consensus Node들이 네트워크 운영에 참여할 수 있도록 함으로써 네트워크를 더욱 안정화시키고, 탈중앙화로 나아가는 기본적인 틀을 마련할 것이다. 거버넌스 역시 이에 맞게 탈중앙화될 예정이다. 이 단계에서 새로운 노드가 네트워크에 참여하는 경우 조건을 만족하는 노드들이 자동으로 네트워크에 참여하는 기능을 테스트할 예정이다.

2단계에서 우리는 충분히 정교하지 않지만 어느 정도 제도화된 거버넌스를 가동할 예정이다. 프로토콘 거버넌스는 두개의 의사결정기구를 갖게 된다. 하나는 Suffrage Node Group만의 의사결정 기구인 Node Committee이고 다른 하나는 투표모델을 활용하여 토큰 홀더들이 의사결정 권한을 행사하는 의회(Congress)다. 다만 프로토콘넷에 대한 '최종적인' 의사결정 권한은 토큰 홀더들의 의사결정기구인 의회가 갖는다.

1. 2단계에서 재단은 의사결정 권한을 내려놓고, 생태계 의사결정 권한을 토큰 홀더들의 거버넌스 기구인 의회에 이양한다. 즉 프로토콘넷의 최종 의사결정은 토큰 홀더들의 투표로 결정된다. 단 효율적인 의사결정을 위해 안건들을 분류하여 일부 안건들, 특히 생태계 전체와 직접적인 연관이 없거나 토큰 홀더들 대부분의 경제적인 이해관계와 크게 관련 없고 주로 노드 운영과 관련된 사안들은 Node Committee에서 결정할 수 있도록 한다. 또한 일상적이고 지속적인 업무 수행을 위해 재단 및 개발팀은 의회에 연단위 Proposal을 제출하여 의회의 승인을 얻은 후 해당 내역안에서 일상적인 사업을 집행한다.

2. Suffrage Node Group이 멤버로 참여하는 Node Committee는 버그 수정이나 기능 개선 같은 네트워크 업데이트, 모델 업데이트 등 노드 운영 및 개선과 관련된 일상적인 투표 권한을 갖는다. 또한 노드 자동 업데이트 기능이 도입되기 전까지 신규 노드의 진입 허용이나 Faulty 노드를 퇴출시키는 권한도 보유한다. Node Committee의 투표 통과 기준은 PBFT의 룰을 따라 전체노드의 ⅔ 이상의 동의로 진행한다. 다만 생태계 전체의 이해관계가 걸린 사안에 대해서 이견이 있는 경우 Suffrage Node Group은 의회의 의사결정을 따라야 한다.

3. 의회는 토큰 홀더들의 모임으로 프로토콘넷에 대한 최종적인 의사결정 권한을 갖는다. 여기서 토큰 홀더란 시스템에 토큰을 예치(Staking)한 사람들의 집합으로 정의된다. 토큰 예치는 두가지 자금, 노드들이 담보로 예치한 자금과 토큰 홀더들이 FeeFi에 예치한 자금이 존재한다. 토큰 홀더들은 두 곳에 예치된 토큰 총량을 기준으로 1토큰 1표를 행사하게 되며, Suffrage 노드 운영자들도 담보로 맡긴 토큰량에 비례하여 투표권을 갖는다. 그런데 1토큰 1표는 종종 고래들의

관계를 관철시키는 데 악용되어 왔다. 그래서 의회는 두개의 의사결정 룰을 갖는다. 첨예한 이해 대립이 없는 사안인 경우 총 예치수량 기준으로 투표 찬성수가 과반수를 넘으면 승인된다. 첨예한 이해 대립이 있거나 또는 민감한 사안인 경우 총 예치수량의 80% 이상의 찬성표를 얻어야 통과된다. 첨예한 이해 대립이 있는 경우란 1) 특정 노드가 생태계 전체에 반하는 행동을 하여 의회에서 퇴출시킬 경우, 2) Node Committee의 의사결정에 대해 다수의 토큰 홀더들이 반대하는 경우, 3) 그 외 어떤 사안에 대해 예치된 토큰량 대비의 1/5 이상이 서명을 하여 첨예한 이해관계로 다룰 것을 의회에 청원한 경우다. 이와 관련된 보다 세부적인 운영안은 1단계 네트워크 운영 시기에 마련되어 첫 의회 투표에 올려질 예정이다.

4. 만약 의회에서 Node Committee의 의사결정에 반하는 결정을 한 경우, Node Committee는 이를 따라야 하며, 이를 따르지 않는 경우 의회는 추가적인 투표를 통해 이에 반대하는 노드를 퇴출시킬 권한을 갖는다. 이 경우 투표 통과 즉시 해당 노드는 자동으로 네트워크에서 퇴출된다. 이렇게 강력한 권한을 두는 이유는 노드 운영자들과 전체 토큰 홀더들의 이해관계가 충돌되는 사례가 종종 발생하는데 이 경우 대부분은 노드 운영자들의 입장이 관철되어 왔기 때문이다. 이를 방지하기 위해 강력한 통제 장치를 두어 Node Committee들의 이해관계와 의사결정이 최종적으로 전체 토큰 홀더 및 생태계의 이해관계에 부합되도록 한다.

5. Node Committee와 Congress 투표에 참여하는 경우 참여자에게 일정량의 투표 리워드를 제공하며, 이 리워드는 공공자금(Commons Budget)에서 지출한다. 이는 통상 이와 같은 거버넌스 시스템을 운영할 때 나타나는 참여율 하락 현상을 방지하기 위함이며, 또한 원칙적으로 전체 생태계 발전에 참여하는 행위에 대해 보상을 제공하는 것은 논리적으로 타당하기 때문이다. 리워드 정책 역시 1단계에서 세부안이 확정될 예정이다.

80% 정족수란 아이디어는 테조스[7] 거버넌스의 아이디어를 참고했다. 1토큰 1표 구조는 다량의 토큰을 보유한 이들이 보다 많은 의사결정 권한을 행사하도록 만드는 단점을 가지고 있다. 즉 소수의 이해를 대변하는 금권정치 수단으로 악용될 가능성이 항존한다. 이에 대한 대안 중 하나는 1인 1표를 시행하는 것인데, 우리의 경험상 1인 1표는 참여와 운영 과정이 상당히 복잡하고 비용이 많이 든다. 반면 80% 정족수 룰은 생태계 전체의 압도적인 찬성을 기반으로 하는 것이기에 그 결과값은 사실상 1인 1표와 다르지 않게 된다. 즉 1토큰 1표라는 제도에 80% 정족수라는 비교적 간단한 장치를 부가함으로써 1인 1표와 비슷한 직접민주제 효과를 낼 수 있는 것이다.

위에서 제시한 원칙은 의회에 대한 대략적인 가이드라인이며, 의사결정기구를 보다 원활하고 빈틈없이 운영하기 위해서는 보다 정교한 디자인 작업이 필요할 것이다. 예컨대 의회에 청원하는 경우에는 무분별한 청원을 막는 장치가 필요하다. 통상 이런 시스템을 운영하는 경우 장난이나 악의적인 행위들이 일정 비율로 발생하기 때문이다. 이런 이유로 청원에 참여하는 경우에는 투표 리워드 보상을 주지 않고, 경우에 따라서는 청원인의 진정성을 확보하기 위해 공탁금을 걸도록 하는 장치를 둘 수도 있다. 이것은 하나의 사례일 뿐이며, 우리는 2단계에서 얻은 운영 경험을 토대로 3단계에서 보다 정교하고 빈틈없는 의회 모델을 구현할 것이다.

3단계: Ney York Net

3단계는 탈중앙화된 네트워크의 초기 단계로 진입하는 것이다. 이 단계에서 재단은 상징적인 수준의 노드를 운영하고, 대다수의 노드들을 외부 참여자들이 운영하도록 유도할 것이다. 11페이지의 프로토콘 노드 생태계 구조 그림에서 볼 수 있듯이 맨 바깥쪽에 다수의 Non-Consensus Node Group이 존재하고, 그들 중 Consensus Node로 전환되기에 충분한 조건을 만족하는 이들이 Suffrage Group을 형성하여 데이터를 처리한다. 만약 Suffrage Group에 있던 노드가 어떤 이유로 반복적으로 문제를 야기하거나 의도적으로 네트워크의 정상적인 운영을 방해하는 경우, 이 노드는 사전에 정의된 알고리즘에 따라 Suffrage Group에서 자동으로 방출되어 일반 노드에 속하게 될 것이다. 사안이 심각한 경우에는 모든 담보 자산이 몰수되고 네트워크에서 영원히 퇴출될 수도 있다. 또한 Non-Consensus Node 중 Consensus Node에 참여하고 싶은 노드는 대기 중에 있다가 기존 Consensus Node가 퇴출되는 시점에 Consensus Node에 참여할 기회를 얻게 된다.

4단계: Seoul Net

4단계는 노드 운영 및 거버넌스 구조가 완전히 탈중앙화된 DAO를 구축하게 된다. 이 단계에서 재단의 개입은 최소화되며, 탈중앙화된 글로벌 커뮤니티가 네트워크를 운영하게 된다. 4단계에서는 기간의 실험과 경험을 바탕으로 정교한 거버넌스 룰이 수립되며 보다 정교하고 체계적인 거버넌스 구조가 작동하게 될 것이다. 이상 단계별 목표 일정 및 의사결정 주체, 생태계의 주요 계획들을 도식화하면 다음과 같다. 아래의 예상 일정은 개발 진척도 및 비즈니스 현황에 따라 다소 조정될 수 있다.

단계	예상 일정	의사 결정 주체	노드 운영 주체	노드 신규 참여 및 퇴출 방식	응용 서비스 및 주요 이벤트	FeeFi
알파넷	작동중	재단	재단	노드 투표	블록사인 테스트 버전	X
베타넷	2021년 4분기	재단	재단 + 파트너	노드 투표 (재단 의사결정)	블록사인, 블록시티, 기타 dApp 서비스 연동 및 시범운영	X
Jeju Net	2022년 상반기	재단	재단 + 파트너			
Beijing Net	2023년 상반기	의회	재단 + 파트너 + 임의의 참여자	노드 투표 (노드 의사결정)	PEN 코인 발행 및 다양한 dApp 서비스 운영	FeeFi 적용
New York Net	2024년 상반기	의회	재단 + 파트너 + 임의의 참여자	프로토콜 기반 자동화 (시범 운영)		
Seoul Net	2025년 상반기	의회 (DAO)	재단 + 파트너 + 임의의 참여자	프로토콜 기반 자동화		

05 토큰 이코노미와 수수료

비트코인 네트워크가 시작된 지난 10여년간 암호화폐 산업은 참으로 과격한 변화를 겪었다. 어떤 사람들은 아직도 퍼블릭 블록체인 산업이 실체가 없다고 주장하지만, 이는 암호화폐 산업의 실상을 모르고 하는 이야기다. 이미 비트코인 수수료 총액은 법정화폐로 환산했을 때 2020년 기준 연 $1B을 훌쩍 넘었다. 2021년 3월 기준 이더리움 수수료는 약 $698M의 가치에 상응하는데, 이를 연단위로 환산하면 $9B가 훨씬 넘는다. 시나브로 블록체인 산업은 본격적인 비즈니스 단계로 접어들고 있다.

블록체인 경제 시스템

블록체인 메인넷의 경제 시스템은 크게 두 가지를 축으로 작동한다. 하나는 시장에서 형성된 토큰 가격이고 다른 하나는 해당 네트워크가 서비스를 제공하고 받는 수수료다. 현재 대부분의 블록체인 프로젝트들은 프로젝트가 경제적으로 존속하는 자원을 확보하는데 있어 이 두가지를 혼용해서 사용하고 있는데, 이 두가지는 긴밀하면서도 명확하게 구분되는 특징들을 가지고 있다. 먼저 토큰 가격이 가지는 특징을 살펴보자. 거의 대부분의 프로젝트들은 블록 생성 시 새로운 코인을 추가 발행하고 이를 네트워크 참여자들에게 배분해줌으로써 네트워크 운영 비용을 지급하고 생태계 참여를 유도한다. 토큰 가격이 높은 경우에는 추가 발행된 토큰만으로도 상당한 경제적 보상이 되기에, 이 자체로 네트워크 유지에 필요한 경비가 충당되기도 한다. 그리고 토큰의 시장가격은 해당 프로젝트의 리더 또는 팀의 인지도, 시장에 알려진 프로젝트 팀의 기술력, 네트워크 실 사용 트래픽, 기술적 비전의 타당성과 아름다움, 마케팅 능력, 해당 프로젝트를 지지하는 커뮤니티의 크기, 때로는 사기에 가까운 포장과 과장 능력까지 다양한 요인들이 복합적으로 작용하여 결정된다. 두번째, 블록체인 네트워크가 서비스를 제공하고 받는 수수료는 해당 블록체인 네트워크를 사용하는 Operation 수(ops) 또는 Transaction 수(tps)를 기준으로 하기 때문에 비교적 실질적이고 명확하다. 즉 실제 블록체인의 사용성이 어느 정도인지에 따라 측정되는 것이다. 그리고 어떤 블록체인이 의미 있는 수준으로 데이터 처리 용량을 달성하는 순간 해당 프로젝트의 토큰 가격은 급격히 상승한다.

극소수를 제외한 대부분의 코인들은 아직 시장에서 그 쓰임새를 명확하게 인정받지 못했기 때문에, 실제적인 사용가치보다는 오히려 이 기술이 미래에 창출해낼 것으로 기대되는 가치 즉 미래가치가 더 크게 작용하고 있다. 많은 프로젝트들이 실제적인 사용가치를 만들기 위해 노력해왔고 어마어마한 자금을 쏟아붇기도 했지만, 뚜렷한 성공 사례는 극히 드문 것이 사실이다.그러나 최근 디파이 서비스들의 성장에 따라 이더리움 네트워크의 사용량이 급증하면서 이더리움은 그 존재 가치를 입증한 바 있으며, 한국발 프로젝트인 테라(Terra)[8] 는 단기간에 블록체인 처리량이 급증하면서 이와 같은 성과를 기반으로 단기간에 코인 마켓캡 40위권에서 10위권으로 급상승했다. 이와 같은 현상은 고무적이라고 말할 수 있는데, 이제 블록체인도 미래가치보다는 실사용성으로 평가받게 되는 시점이 점차 다가오고 있기 때문이다.

[2021년 3월 18일 기준 각 메인넷 프로젝트들의 수수료 가치 현황]

Project	24H Revenue	7D Revenue	30D Revenue	1 Year Revenue (Estimated)
Ethereum	$26,835,163	$184,533,658	$698,045,626	$8,376,547,512
Bitcoin	$6,206,822	$50,124,904	$196,436,318	$2,357,235,816
Terra	$19,214	$182,472	$776,554	$9,318,648
Filecoin	$5,396	$45,722	$152,722	$1,832,664
Polkadot	$4,247	$35,449	$125,899	$1,510,788
Tezos	$412	$3,648	$13,316	$159,792

Source : https://www.tokenterminal.com/

위 표는 2021년 3월 18일 기준으로 각 메인넷 프로젝트들이 하루, 한주, 30일(1개월), 1년 동안 만든 수수료를 법정화폐 기준으로 환산한 추정치다. 이 표에 의하면 이더리움은 월간 약 $698M(연 기준 약 $1B 이상)의 가치에 상응하는 수수료를 만들고 있으며 비트코인은 연간 약 $2.3B에 해당하는 수수료 가치를 만들어내고 있다는 사실을 알 수 있다. 최근 급성장한 테라는 연간 약 $9.3M 정도의 수수료 가치를 만들고 있다. 블록체인 메인넷 전체가 만들어내는 수수료 가치를 합치면 약 $15B 가까이 된다. 이를 통해 우리가 확인할 수 있는 것은, 이제는 블록체인 산업은 실제 의미 있는 수준의 사용가치를 만들어내며 작동하는 의미 있는 인터넷 비즈니스 중 하나로 자리매김하고 있다는 사실이다. 즉 퍼블릭 블록체인 산업이 불안정한 미래 가치나 탈중앙화 가치와 같은 추상적인 논의나 구호 수준을 넘어 비즈니스적으로 주목할만한 수준으로 성장하고 있는 것이다. 이것은 의미 있는 수준의 Transaction을 확보할 경우 수수료가 만들어내는 가치만으로도 네트워크가 충분히 운영되면서, 이것이 토큰 이코노미를 활성화시킬 수 있는 촉매제로 작동할 수 있다는 것을 의미한다. 예컨대 수수료를 $0.03으로 잡고 초당 평균 처리 건수를 1000건으로 잡으면 연간 수수료 총 가치는 약 $1B에 가깝게 된다. 프로토콘넷의 데이터 처리 속도는 최적 상태에서 최대 5,000ops로 평균적으로 초당 1000 ~ 2000건 이상을 충분히 처리할 수 있기 때문에, 프로토콘넷은 수수료를 지불하는 거래 건수만 충분히 만들 수 있다면 수수료 그 자체로 네트워크와 블록체인 생태계를 유지하는 것이 가능할 것이다.

그런데 수수료 문제는 단지 비즈니스에만 국한된 것이 아니다. 그것은 비즈니스와 서비스 접근성과 블록체인의 대중적 확산(Mass Adoption)과 관련된 문제에 폭넓게 연결되어 있는 핵심 논제다.

수수료 문제

블록체인의 사용성을 나쁘게 만들고 소위 대중적 확산(Mass Adoption)을 가로막는 큰 이유를 꼽자면 다음과 같은 3가지, 1) 프라이빗 키 관리의 까다로움, 2) dApp 토큰 사용 시 메인넷 토큰을 구매해야 하는 불편함, 3) 수수료 자체의 높은 변동성을 들 수 있다. 이 중 프라이빗 키 관리와 관련된 문제는 최근 지갑 기술의 발달과 지문, 안면인식과 같은 생체인식 기술의 발달 및 스마트폰의 보급화로 보안키(Secret Key 또는 Private Key)를 유실하는 등의 사고 발생률은 확연하게 줄어든 것으로 보인다. 그럼에도 불구하고 여전히 키 분실 시 모든 권한과 자산의 상실이라는 근본적인 문제는 남아 있는데, 우리는 이 문제에 대해서는 탁월한 누군가가 해법을 기다리고자 한다. 블록체인 사용성과 관련해 우리가 집중하고자 하는 문제는 바로 수수료와 관련된 것이다. 블록체인 산업에서 수수료 문제는 결코 단순하지 않은 것이, 그것은 단지 경제적인 비용의 문제만이 아니라 사용자들의 사용성(Usability) 또는 사용자 경험(User Experience)와 직결되어 있기 때문이다. 수수료를 둘러싼 블록체인 업계의 현안들을 요약해보면 대략 다음과 같다.

1. 블록체인 수수료의 적정성 문제
2. 블록체인 수수료의 변동성 문제
3. 블록체인 수수료 지급 방식의 까다로움 (수수료 UX 문제)

첫번째 문제는 블록체인을 사용하는 비용으로 과연 얼마를 내는 것이 적당한가 하는 문제다. 최근 디파이가 성장하면서 이더리움 수수료가 200달러까지 치솟은 적이 있다. 비트코인 송금 수수료보다 훨씬 높은 수준이다. 이더리움을 비롯한 대부분의 메인넷 수수료는 한정된 자원을 경쟁입찰 방식으로 사용하도록 설계되어 있기 때문에 블록체인 수요가 늘어날수록 수수료가 높아지는 특성을 가지고 있다.

이 때문에 두번째 문제가 발생한다. 예컨대 어떤 사업자가 수수료로 최대 $0.1을 예상하고 블록체인을 사용하고 있었는데 이것이 어느 순간 수십달러로 급등한다면 해당 사업자는 더 이상 블록체인을 사용할 수 없게 된다. 만약 해당 서비스가 블록체인에 크게 의존하고 있는 서비스라면 곧바로 서비스 중단으로 이어질 수밖에 없다. 이것은 이더리움 기반의 수 많은 dApp 서비스들이 실제로 겪고 있는 문제이기도 하다. 그리고 서비스 도중에 수수료 급등이 예상된다면 애초부터 블록체인을 활용하여 안정적이고 지속적인 서비스를 설계하는 것 자체가 불가능해진다. 즉 블록체인을 사용한 범용적인 서비스를 시도할 수 없게 되는 것이다.

만약 블록체인을 매우 특수한 용도로 극소수만 사용하거나 또는 값비싼 자산만을 다룬다고 가정한다면 블록체인 사용 비용이 비싸지거나 급등하는 것은 큰 문제가 아닐 수 있다. 실제로 지금도 사람들은 비싼 금융비용(수수료)를 지불하고 비트코인과 이더리움 네트워크로 자산거래를 하고 있기 때문이다. 그러나 블록체인의 대중적 확산(Mass Adoption)을 추구한다면 비싼 수수료와 과격한 변동성은 블록체인의 대중적 확산을 가로막는 장벽으로 작용한다. 특히 사회의 전방위적인 디지털 전환 시대를 고려한다면 비싼 수수료는 블록체인 산업의 성장을 방해하는 커다란 장애요소로 작동할 것이다.

수수료의 적정성과 변동성 문제가 경제적인 것과 관련된 문제라면 3번, 지급방식의 까다로움은 서비스 사용성 즉 UI/UX와 관련된 문제다. 메인넷 토큰은 해당 메인넷의 내부 결제 시스템으로 반드시

필요하다. 그러나 현재 지배적으로 사용되고 있는 수수료 구조는 dApp 서비스 또는 dApp 토큰 사용자들에게 메인넷 토큰으로 수수료를 지불하라고 사용자들에게 강요하는 구조다. 토큰 이코노미에 익숙한 사람이라면 거래소에서 메인넷 토큰을 구매해서 수수료로 지급하는 것이 가능하겠지만, 토큰을 처음 접하는 사람들은 메인넷 토큰을 구하는 일 자체가 대단히 어려운 일이다. 이와 같은 구조는 특히 블록체인을 활용해 대중적인 서비스를 제공하려는 dApp 서비스 사업자들에게 심각한 장벽으로 작용한다. 이 문제는 대부분의 메인넷들에게 공통적으로 존재하는데, 그것은 메인넷 프로젝트들이 거의 대부분 이더리움의 수수료 구조를 똑같이 따라하거나 혹은 그 근본 전제를 그대로 두고 약간 변형하거나 개선하려는 시도만을 했기 때문이다.

수수료와 관련된 UI/UX 문제의 핵심은 사용자들이 dApp 서비스와 토큰을 사용하기 위해서는 반드시 메인넷 토큰을 어디선가 구해야 한다는 것이다. 이더리움을 예로 들어보자면, 이더를 구하는 방법은 크게 3가지가 존재한다: 1) 채굴하기, 2) 타인에게 전송 받기, 3) 거래소에서 구매하기. 그런데 블록체인과 암호화폐에 익숙한 사람들을 제외하고, 이 3가지 방법 모두 대다수의 잠재적 사용자들에게는 결코 쉽지 않은 일이다. 이더를 구하는 행위 자체가 어려운데, 어떻게 그것에 기반한 서비스들이 활성화 되기를 기대할 수 있겠는가? 참고로 디파이의 성장은 이에 대한 변명이 되지 못한다. 디파이는 암호화폐에 익숙한 이들이 암호화폐만을 가지고 참여하는 서비스이기 때문이다.

이 문제와 관련해 EOS와 같은 프로젝트들이 몇가지 실험을 진행한 바 있다. EOS는 자원을 경매 방식으로 선구매하는 로직을 구현했다. 즉 EOS 토큰을 예치하는 것으로 자원을 선구매한 이들에게 시스템의 일정 용량을 할당해줌으로써 사용자들이 직접 수수료를 내지 않아도 되는 구조를 만들었다. 이것은 사용자들이 메인넷 토큰을 구매하지 않고도 블록체인 서비스를 사용할 수 있게 했다는 측면에서 분명히 진일보한 방식이다. 그러나 각 서비스 제공자들은 한정된 시스템 자원을 두고 경쟁하게 되기 때문에, 경쟁이 심화되는 경우 네트워크 사용 비용이 급격하게 상승하게 된다. 게다가 EOS는 자원 경쟁 구조이기 때문에, 내가 먼저 자원을 일정 확보했다고 하더라도 다른 사업자가 더 많은 EOS 예치하면 그만큼 이전에 확보해 둔 자원이 줄어든다. 즉 다른 사업자가 더 많은 토큰을 예치해서 자원을 빼앗아 간다면 기존 사업자는 이전과 같은 양의 자원을 확보하기 위해 추가로 EOS 물량을 시스템에 예치해야 하는 것이다. 따라서 사업자 부담은 급격하게 올라갈 수 밖에 없다.

이러한 문제가 발생하는 근본적인 원인 중 하나는 대부분의 메인넷들이 '자원 경쟁 모델'을 채택했기 때문이다. 특히 EOS는 비록 사용자들이 수수료를 내지 않아도 되는 방식을 제안함으로써 블록체인 사용성 개선을 시도했지만, 서비스 제공자들이 자원을 두고 직접적으로 무한경쟁을 해야하는 구조를 만들었다. 이런 방식이면 언제 갑자기 폭등할지도 모르는 수수료를 기꺼이 감당할 수 있는 서비스 사업자들만 블록체인 네트워크를 사용할 수 있게 되는데, 이런 부담을 감당할 수 있는 사업 영역과 사업자는 극히 극소수다. 따라서 메인넷의 사용 용도가 아주 제한적일 수밖에 없다.

한편 이러한 장벽을 우회하는 방법으로 블록체인 서비스를 아예 무료로 제공하거나 또는 수수료를 대납해주는 시도들도 있다. 그러나 이것은 한시적인 마케팅 정책이나 서비스 초기의 촉진 정책 정도로 가능한 것이지, 지속적으로 수수료를 대납해주거나 무료로 제공하는 것은 불가능하다. 블록체인 네트워크는 실제 해당 네트워크를 작동시키기 위해 막대한 비용이 들어가기 때문에, 정당한 보상구조 없이 네트워크가 지속될 수 있으리라고 가정하는 것은 합리적이지 않다. 또한 수수료를 무료로 제공하거나

순전히 대납에 의존하게 되면 어느 순간 DDOS 공격에 노출될 위험성이 존재한다.

우리는 비용 측면에서나 UX 측면에서나 dApp 사용자들이 메인넷을 쉽게 사용할 수 있도록 해야 블록체인의 대중적 확산이 가능하리라 본다. 따라서 이 문제는 선택의 문제가 아니라 블록체인의 대중적 확산을 위해 반드시 풀어야 하는 문제다. 다행스럽게도 ISAAC+의 탁월한 성능 덕분에 우리는 사용자들이 적절한 수수료를 내게 하면서 더 많은 이들이 블록체인 서비스를 사용하도록 하는 전략을 채택할 수 있게 되었다. 이미 앞에서 고찰한 바, 블록체인 수수료만으로도 상당한 규모의 토큰 이코노미를 구축할 수 있기에, 우리는 블록체인 네트워크가 만들어낸 부가가치 즉 수수료로 작동하는 토큰 이코노미를 구축하는 FeeFi(Fee Financing), 일종의 수수료 마켓이라는 새로운 개념을 제안한다.

FeeFi (Fee Financing)

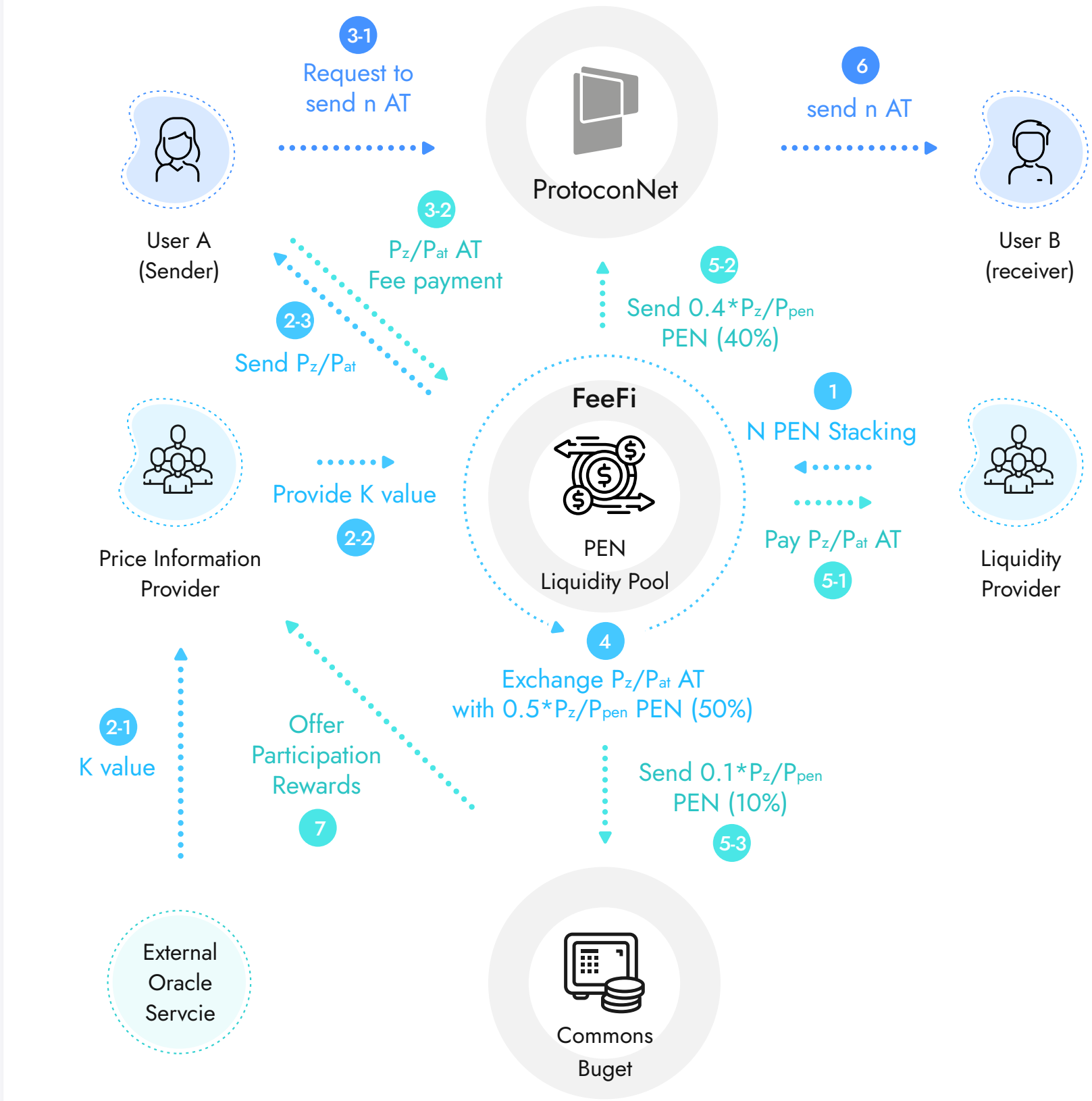
Fee Financing, 일명 피파이(FeeFi)는 수수료에 디파이 금융기법을 적용하여 수수료를 둘러싼 여러 문제들을 풀어내는 새로운 방법론이다. 프로토콘넷에서 FeeFi는 두가지 역할을 한다. 하나는 사용자들이 수수료와 관련된 제반 숙제들을 해결하는데 참여하면서 네트워크가 만들어낸 부가가치를 나누어 갖는 것이다. 다른 하나는 사용자들이 토큰을 예치함으로써 시장 조절 기능에 참여하는 것이다. 다만 프로젝트 초기에는 수수료로 얻게 되는 가치가 미미할 것이기에 사용자들의 참여를 유도하기 위해 인플레이션으로 발행된 토큰이 인센티브로 제공될 것이다. FeeFi를 통해 우리는 블록체인 산업에서 그동안 이슈로 제기되어 온 수수료와 관련된 세가지 숙제, 수수료의 적정성, 변동성, 수수료 지급 사용성(UX) 문제에 대한 해결 방안을 제시하고자 한다.

해결방안 1 : FeeFi

dApp 서비스를 사용하거나 또는 dApp 토큰을 전송하기 위해 메인넷 토큰을 구해서 수수료로 지급하는 것은 블록체인의 대중적 확산을 막는 가장 좋지 않은 UX 중 하나다. 핵심은 dApp 토큰 보유자들이 dApp 토큰 그 자체로 수수료를 지급할 수 있도록 하는 것인데, 우리는 이 문제를 FeeFi를 통해 해결하고자 한다.

예를 들어 살펴보자. 우선, 편의상 A라는 dApp 서비스의 토큰을 AT로 부르기로 하자. 프로토콘넷에서 작동하는 dApp 토큰의 일종인 AT 사용자 중에는 PEN 토큰을 보유하고 PEN으로 수수료를 지불할 줄 아는 사용자도 있지만 PEN을 보유하지 않고 AT만을 보유하고 있는 사람들이 훨씬 많을 것이다. 제대로 된 사용성을 제공하는 서비스라면 AT 사용자는 AT 자체만으로 블록체인 사용 수수료를 지급할 수 있어야 한다. 이 문제를 해결하기 위해 우리는 토큰 보유자들이 참여하며 수수료로 지급한 dApp 토큰과 PEN을 교환하는 내부 거래소, 일종의 DEX인 FeeFi(Fee Financing)을 제안한다. FeeFi의 구조는 다음과 같다.

[수수료마켓 구조]



Market Price	Exchange Rate	FeeFi Fee	Fee Correction Value
1 PEN = P_{pen} (USD) 1 AT = P_{at} (USD)	PEN:AT = P_{pen}:P_{at} AT = P_{at}/P_{pen} PEN	Constant price P_z (USD) (P_z/P_{at} AT or P_z/P_{pen} PEN)	K = $f(c,t)$

우선, 예시를 위해 수수료 분배 비율과 토큰의 시장가격 및 송금 수수료를 다음과 같이 정의하였다.

노드 운영자 40%, 유동성 공급자 50%, 공공 자금 10%

P_z (USD) := x USD (x는 수수료) (1.1)

P_{pen} (USD) := 1PEN (1.2)

P_{at} (USD) := 1 AT (1.3)

$Fee_{at} = P_z/P_{at}$ (AT) (1.4)

$Fee_{pen} = P_z/P_{pen}$ (PEN) (1.5)

(P_{pen} :1 PEN의 USD 가격,P_{at} : 1 AT의 USD 가격, P_z:수수료의 USD 가격)

그림은 FeeFi 아키텍처의 작동 흐름을 단계적으로 나타낸 것이다. 가장 먼저, 유동성 공급자들은 FeeFi에 **N PEN**을 예치한다. 이후 **AT** 사용자로 인해 거래가 발생하면 유동성 공급자들은 **AT** 사용자가 지불한 수수료 중 일부를 보상으로 지급받을 수 있다. 이때 **AT**와 **PEN**의 시장 가격이 움직임에 따라 **AT** 사용자가 지불해야 하는 실질적인 수수료 값에 큰 변동이 생길 수 있다. FeeFi 아키텍처에서는 이러한 수수료 변동성 문제를 해결하기 위해 외부 오라클인 **K**를 도입하였다. **K**에 대한 내용은 아래에서 별도로 다루기로 하고 여기서는 설명을 생략한다.

AT 사용자는 거래의 규모와 상관없이 P_z/P_{at}만큼의 **AT** 토큰을 FeeFi에 수수료로 지불한다. 이후 사용자가 **AT**로 지불한 수수료는 FeeFi에서 **PEN**과 교환된다. 두 토큰은 서로 같은 가치의 양만큼 교환되어야 한다.

Fee_{at}(AT) = Fee_{pen}(PEN)=P_z(USD) (1.6)

그러나 FeeFi에서는 Fee_{at}는 0.5*Fee_{pen}(PEN)과 교환이 이루어진다. 원래대로라면 Fee_{at}(AT)는 같은 가치를 갖는 Fee_{pen}(PEN)과 교환되어야 하지만 50%의 가치와 교환함으로써 PEN을 예치한 유동성 공급자들에게 수수료의 절반 0.5*Fee_{pen}(PEN)을 지급하는 효과를 낸다. 이렇게 교환된 50%p의Fee_{pen} 중에서 10%p는 공공자금으로 저축하고 40%p는 노드 운영자들에게 지급한다. 마지막으로 0.5*Fee_{pen}(PEN)과 교환한 Fee_{at}(AT)는 FeeFi에 **PEN**을 제공한 유동성 공급자에게 예치 지분에 따라 분배한다. 이로써 유동성 공급자들은 0.5*Fee_{pen}(PEN)을 제공하고 2배 가치인 Fee_{at}(AT)를 얻게 되며 결과적으로 50%의 할인된 가격으로 **AT**를 구매할 수 있게 된다. 우리는 이러한 아키텍처의 작동과정과 그 결과를 일컬어 '수수료 농사' 또는 FeeFi(Fee Financing : 수수료 금융)이라고 부르고자 한다.

아울러 dApp 토큰은 거래소 등에 상장되어 공개적인 시장가를 가진 토큰과 아직 시장가가 없는 토큰으로 구분할 수 있다. 시장가가 있는 경우에는 위와 같은 수수료 마켓이 작동하지만 시장가가 없는 토큰의 경우, 다음과 같은 두가지 방법이 가능하다. 하나는 수수료 전용 계정을 두고 트랜잭션이 발생할 때마다 해당 계정에서 수수료를 대납하는 것이다. 단 이 경우 DDOS 공격을 막기 위해 사용자들이 소액이라도 dApp 토큰으로 수수료를 지급하도록 하는 것을 권고할 것이다. 또 다른 방법은, 예컨대 아직 상장되지 않은 스테이블 코인과 같은 경우 공개시장가는 없지만 일정한 가격이 존재하고 또는 존재할 것으로 예상되고 또 이 가격을 수수료마켓 참여자들이 인정한다면 수수료 마켓을 형성할 수 있다.

즉 당장 시장가격이 없는 경우에도 수수료 마켓은 사용자들에 의해 자율적으로 만들어질 수 있다.

이더리움이 이미 연 $8.3B(약 10조)이 이르는 블록체인 수수료 시장을 증명했기 때문에, 만약 우리가 충분한 거래량만 확보할 수 있다면 수수료 마켓은 하나의 독립된 금융시스템으로 작동할 수 있다. 이런 의미에서 우리는 이것을 FeeFi(Fee Financing)이라고 명명했다. 이와 같은 구조는 생태계와 관련해 여러가지 이점을 갖는다. 프로토콘넷에 참여하는 dApp 서비스 사업자들은 PEN토큰 보유자풀에 해당 토큰을 배분하게 됨으로써 그만큼 초기 사용자를 쉽게 확보할 수 있다. 즉 dApp 서비스는 이미 존재하는 PEN 토큰 유동성 공급자 풀을 공유하게 되어 자연스럽게 초기 생태계 참여자를 확보할 수 있다. 또한 사용자들이 받는 수수료에 dApp 서비스만의 독자적인 인센티브 모델을 추가로 제공함으로써 dApp 생태계 참여를 촉진할 수도 있을 것이다. PEN 토큰 유동성 공급자 입장에서는 보다 좋은 블록체인 UI/UX를 제공하는 작업에 참여하여 프로토콘넷의 성장에 직접적인 기여를 하면서 이에 대한 보상으로 dApp 토큰을 획득할 수 있다. 만약 프로토콘넷 위에서 작동하는 dApp 토큰들이 크게 성장한다면 PEN 토큰 유동성 공급자들은 그 성과를 함께 향유할 수 있게 된다. 이처럼 PEN 토큰 보유자들과 dApp 서비스 사업자들은 FeeFi를 통해 프로젝트 성장에 따른 성과를 공유하는 경제적 공생 관계가 성립됨으로써, PEN 토큰 보유자들은 PEN 토큰만이 아니라 프로토넷과 관련된 모든 프로젝트들의 후원자(Supporters)가 된다.

또한 우리는 'PEN 토큰 예치'라는 과정을 통해 생태계 발전 기여자들을 명확하게 특정할 수 있기 때문에, 이들에게 거버넌스 투표에 참여할 권한을 부여할 수 있다. 나아가 FeeFi가 자리잡을 경우, 예치된 PEN 토큰과 추가적으로 생성되는 안정적인 수수료 보상을 기반으로 더욱 다양한 금융 모델들을 개발하게 될 것이다. 또한 PEN 기반의 dApp 프로젝트들 초기 펀딩에 참여할 수 있는 권한을 부여받게 된다. 이를 통해 우리 메인넷 내부에서부터 프로토콜 이코노미가 작동하는 모습을 보여줄 것이다. FeeFi 참여자의 최소 예치 금액은 초기 10,000PEN으로 하되, 구체적인 가이드는 FeeFi가 가동되는 시점과 당시 PEN 가격을 고려해 거버넌스에서 결정할 것이다.

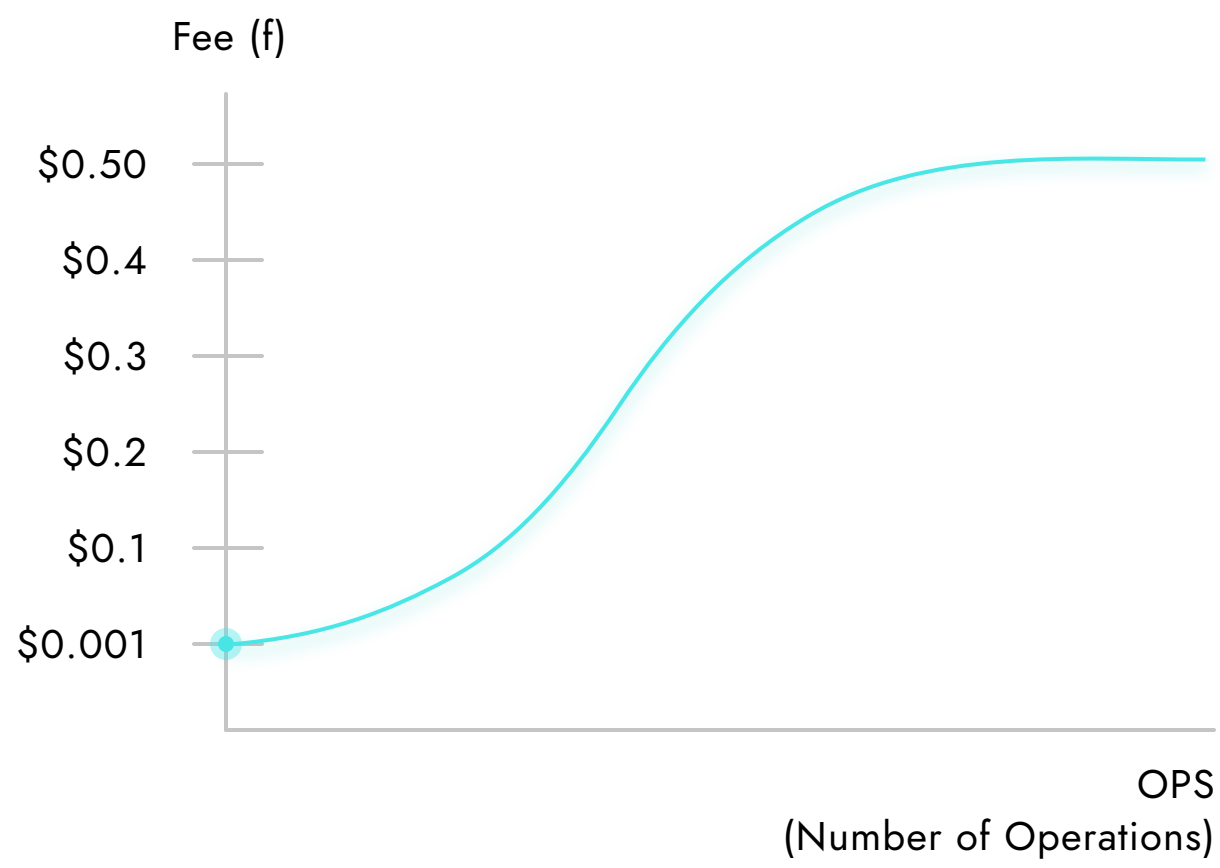
해결방안 2 : 수수료 변동성 제어

수수료와 관련된 또 다른 이슈를 요약하면 블록체인 네트워크 사용 수수료가 합리적인 수준이어야 하고, 또한 변동성이 크지 않아야 한다는 것이다. 그런데 이 문제 역시 그렇게 간단하지 않다. 무엇보다 퍼블릭 블록체인 산업은 수수료를 중심으로 한 네트워크 운영을 고민해본 사례가 많지 않다. 그래서 우리에게는 블록체인 서비스를 사용하는데 있어 어느 정도가 적정 수준인지 또는 합리적인 수준인지에 대한 근거자료가 불충분하다. 다만 다음과 같은 세가지 고려사항을 기반으로 추정할 수는 있을 것이다: 첫번째 코인 추가발행 등 별도의 인센티브 없이 수수료만으로 작동하는 블록체인 네트워크를 작동시키기 위한 총경비 또는 비용, 두번째 블록체인의 대중적 확산(Mass Adoption)이라는 관점에서 블록체인 사용자가 블록체인에 데이터 하나를 저장할 때 낼 수 있는 적정한 또는 심리적으로 허용가능한 최대치의 비용의 범위, 세번째 블록체인 네트워크에 대한 DDOS 공격을 방지하기 위해 필요한 최소한의 장벽으로서의 수수료.

이러한 요소들을 고려하여 우리는 단위 Operation 또는 단위 Transaction 당 처리 수수료 가격($\mathbf{P_z}$)의 최소치와 최대치를 $0.001에서 $0.5로 가정한다. 하나의 데이터를 처리하기 위해 복수개(N)의 Operation 또는 Transaction을 처리하는 경우에는 보다 많은 비용($\mathbf{P_z * N}$)이 필요할 것이다. $0.001은 네트워크 첫 부팅 시점 시장진입을 고려한 다소 전략적인 가격이라면, $0.5는 가치 있는 데이터를 보호하기 위해 대중적인 인터넷 서비스가 지불할 수 있는 또는 허용할 수 있는 최대치를 기준으로 추정한 값이다. 반면 만약 개별 operation 처리 비용이 일정 한도를 넘을 경우, 블록체인 사용 비용이 너무 비싸 비트코인이나 이더리움처럼 값비싼 금융 Transaction만을 처리할 수밖에 없을 것이다. 즉 비싼 수수료 때문에 블록체인의 사용성 확장에 제한을 받게 되는 것이다. 그렇다고 수수료가 마냥 낮은 것이 꼭 좋은 것만은 아닌 것이, 수수료가 너무 싼 경우 DDOS 공격 여지를 주기 때문이다.

프로토콘넷은 저렴하고 합리적인 비용으로 값비싼 금융 Operation도 처리하겠지만, 값비싼 Operation이 아닌 데이터의 고유성 확보, 문서의 진본 증명, 부인방지 기능 제공, 등기부 등본 정보 등록 및 증명 등 블록체인 기술이 일상생활과 산업 전반에 사용될 수 있도록 하기 위해서는 수수료가 일정 수준을 넘어서는 안된다고 생각한다. '서비스'로서의 블록체인 입장에서 보자면 네트워크 사용량이 증가한다고 이에 비례하여 경쟁적으로 수수료가 상승하는 구조는 서비스 지속성을 심각하게 저해할 것이다. 이런 이유로 우리는 초기에는 $0.001에서 시작해서 네트워크 사용량이 많아질 경우 수수료가 점차 상승해 적정 수준에 이르도록 관리 메커니즘을 구현할 예정이다. 물론 현재 최소치와 최대치를 $0.001에서 $0.5로 가정할 뿐, 아직 수수료의 적정값과 블록체인 이용자들이 감내할 수 있는 수수료의 상한선이 어디까지인지 추정할 수 있는 정보가 충분치 않다. 최소 $0.001에서 최대 $0.5라는 가정치 역시 그 동안의 경험과 타 블록체인들의 수수료 현황에 기반한 추정치이기 때문에 메인넷 1단계에서 실제 네트워크 가동을 통해 비용과 한계 효용 등을 확인하여 조정될 예정이다.

아울러 수수료의 높은 변동성 역시 '서비스'로서 블록체인의 품질을 저하시키는 요인 중 하나다. 만약 수수료의 최소치와 최대치를 각각 $0.001와 $0.5로 잡았는데 수수료가 어떤 때는 $0.001이고 어떤 때는 $0.5이라면 통상적인 인터넷 서비스 사업자들은 서비스를 제공하기 대단히 어렵다. 블록체인 사용 비용을 예측할 수 없기 때문이다. 이런 측면에서 우리는 Fiat Money 기준 '수수료 기준가격제'를 도입하고자 한다. 그리고 이 기준 가격은 블록체인 사용성이 증대됨에 따라 아래 그래프와 같이 조금씩 증가하게 될 것이다.



수수료 기준가격은 초기에는 재단이 그리고 Beijing Net 단계부터는 의회에서 결정하게 된다. 그리고 시장에서 토큰 가격은 끊임없이 변동하기에 수수료를 기준가격에 고정시키기 위한 별도의 장치들을 마련해야 한다.

수수료와 관련된 정책 결정은 다음과 같이 진행될 예정이다. 특정 시점, 프로토콘넷 생태계는 분기 별로 의회에서 달러 단위의 적정 수수료 값 또는 기준 가격($P_{z}0$)을 결정한다. 이때 **PEN** 토큰과 dApp 토큰(이하 **AT**)의 시장 가격은 변동성을 갖기 때문에 수수료 지불 시점(**t**)에 따라 dApp 토큰 사용자가 지불해야하는 **AT**의 양 또한 지속적으로 바뀌게 된다. 여기서 우리는 수수료로 지급하는 Fee_{at}**(AT)**와 이와 교환하는 Fee_{pen}**(PEN)**의 교환 가치가 의회에서 정한 기준가격을 최대한 근접하게 반영하도록 유도해야 한다. 이를 위해서는 수수료 지불 시의 **PEN** 시장 가격과 **AT** 시장 가격 그리고 **PEN**과 **AT**의 교환비율을 알아야 하는데, 시장 가격을 얻는 시점이 실시간에 근접할 수록 그리고 시장의 평균가격을 잘 반영할 수록 기준 가격에 가까운 수수료를 계산할 수 있게 된다.

먼저, 앞으로의 설명을 위해 아래와 같이 정의한다.

P_{z0}**:= Base Price.** (2.1)

$P_{z,\,t}$**(USD) :=fee in USD at time t,** $0 \le t$**.** (2.2)

(t=0 is the time when the market created)

AT 사용자가 어떤 시점 **t**에 **n AT**를 송금하려 한다고 생각해보자. 그렇다면 이때의 정확한 **PEN**과 **AT**의 시장 가격은 각각 $P_{exact\ pen,\ t}(USD)$와 $P_{exact\ at,\ t}(USD)$가 될 것이다. 우리가 **PEN**과 **AT**의 정확한 가격을 아는 경우 $Fee_{at,\ t}(AT)$와 $Fee_{pen,\ t}(PEN)$은 다음과 같이 교환된다.

$$Fee_{at,\ t}(AT) = P_{z0} / P_{exact\ at,\ t}(AT) = P_{z0}(USD) \quad (2.3)$$

$$Fee_{pen,\ t}(PEN) = P_{z0} / P_{exact\ pen,\ t}(PEN) = P_{z0}(USD) \quad (2.4)$$

$$1(AT) = P_{exact\ at,\ t} / P_{exact\ pen,\ t}(PEN) \quad (2.5)$$

하지만 사용자가 얻을 수 있는 시장 가격의 업데이트가 실시간으로 이루어지지 않을 경우 사용자가 얻게 되는 **PEN**과 **AT**의 가격이 $P_{exact\ pen,\ t}(USD)$, $P_{exact\ at,\ t}(USD)$ 값과는 오차가 있을 것이다. 혹은 외부에서 가져오는 시장 가격 자체가 부정확할 가능성도 있다. 정확한 시장 가격 값과 오차가 있는 가격을 구분하기 위해 다음과 같이 표기하겠다.

$$P_{der\ x,\ t} := \text{Externally derived } P_{x,\ t} \text{ at time t, } 0 \le t \quad (2.6)$$

$$P_{der\ y,\ t} := \text{Externally derived } P_{y,\ t} \text{ at time t, } 0 \le t \quad (2.7)$$

$$Fee_{at,\ t} = P_{z0} / P_{der\ at,\ t}(AT) = P_{z,\ t}(USD) \approx P_{z0}(USD) \quad (2.8)$$

$$Fee_{pen,\ t} = P_{z0}/P_{der\ pen,\ t}(PEN) = P_{z,\ t}(USD) \approx P_{z0}(USD) \quad (2.9)$$

위와 같이 실제 상황에서는 기준가격과 비슷한 가치의 수수료를 계산하기가 쉽지 않다. 우리는 이를 보정하는 값 **K**를 도입하여 **AT**와 **PEN**과의 교환중에 생기는 기준 가치와의 오차를 줄이려 한다. (K_t =**K** at time t, $0 \le t$)

$$c_t := \text{Externally derived state at time t, } 0 \le t \quad (2.10)$$

$$K_t := f(c_t, t) \text{ at time t, } 0 \le t \text{ s.t f is a correction function.} \quad (2.11)$$

$$1\ (AT) = K_t * P_{der\ at,\ t} / P_{der\ pen,\ t}(PEN) \quad (2.12)$$

앞서 FeeFi의 아키텍처를 설명할 때 서술된 내용과 결부시키자면 시점 t에서 PEN으로 환산된 수수료는 다음과 같다.

$$Fee_{pen,\ t} = (P_{z0}/P_{der\ at,\ t}) * (K_t * P_{der\ at,\ t}/P_{der\ pen,\ t})(PEN) \quad (2.13)$$

결국 우리는 K_t를 통해서 $P_{der\ at,\ t}$와 $P_{der\ pen,\ t}$의 교환비율을 보정하므로 더 정확한 수수료를 계산할 수 있게 된다.

각 $P_{z,t}$가 고정 기준 가격 P_{z0}에 근사하면 좋지만 모든 t에서 항상 P_{z0}와 같을 필요는 없으며 일정 범위의 t구간에서 평균해보았을 때 P_{z0}에 수렴하거나 수렴에 가까운 값이면 무난할 것이다. 교환 비율 보정값인 오라클 데이터 K_t (=f(c_t, t))를 적절하게 구현한다면 시점 t에서 AT와 PEN과의 수수료 교환가치가 같아지도록 조정할 수 있다.

오라클 데이터를 위해 우리는 2가지 메커니즘을 사용할 수 있는데 첫 번째는 체인링크(Chainlink)나 밴드 프로토콜(Band Protocol) 등의 오라클 데이터 서비스를 통해 외부 시장 가격을 가져오는 것이고, 두 번째는 Flare Network에서 사용하는 FTSO와 같이 수수료를 특정 기준치에 수렴시키는 탈중앙화된 내부 오라클 생산 시스템을 작동시키는 것이다. 그러나 오라클 데이터를 활용하는데 있어 여러가지 변수들이 존재하며 첫 번째나 두 번째 방법 하나에만 완전히 의존할 수 없기에, 우리는 첫 번째 방법을 통해 어느 정도 신뢰성 있는 외부 오라클 데이터를 가져오고(데이터 획득), 두 번째 내부 오라클 생산 시스템을 통해서(보정) 보다 정교한 데이터를 만들어내는 탈중앙화 오라클 생산 시스템을 검토하고 있다. 이렇게 함으로써 우리는 더욱 안정적이고 정교한 수수료 시스템을 구축할 수 있을 것이다.

ISAAC+는 최적화된 상태에서 안정적으로 최대 5,000ops까지 처리할 수 있는 고성능 알고리즘이다. ISAAC+는 현존 블록체인 대비 최고의 안정성과 속도를 확보했기 때문에, 만약 프로토콘넷이 포화 상태에 도달하면 이를 통해 프로토콘넷이 수수료로 만들어내게 되는 부가가치는 막대할 것으로 예상한다. 우리는 프로토콘넷 생태계에 참여하는 이들 모두가 네트워크 운영으로 창출되는 혜택을 볼 수 있도록 토큰 이코노미를 설계했으며, 이를 집약한 FeeFi라는 방법론으로 블록체인 네트워크가 만들어내는 부가가치를 생태계 전체가 공유하도록 구현할 것이다. 그리고 네트워크가 초당 평균 수천 건의 데이터를 처리하면서 포화 상태에 이르기 전에 더 많은 트래픽을 수용할 수 있는 대안들을 충분히 마련할 예정이다.

수수료 배분 및 인센티브 정책

우리는 수수료를 블록체인 네트워크를 작동시키는 근본적인 경제적 자원으로 간주하며, 블록체인 수수료를 중심으로 프로토콘넷의 토큰 이코노미를 설계했다. 단 네트워크가 충분히 성장하기까지 일정한 시간이 필요하기에 우리는 초기 노드운영 Incentive를 제공하여 노드 운영을 지원할 예정이며, 인센티브는 매 블록마다 추가 발행되는 토큰으로 지급한다.

수수료 수입과 추가 발행된 인센티브 토큰을 바탕으로, 초기 프로토콘넷에서 수수료 및 인센티브는 A) 노드 운영 보상금, B) FeeFi 보상금, C) 공공자금 충당금에 각각 배정될 수 있다. (A+B+C=100%) (A) 노드 운영 보상금은 노드 운영자들에게 노드 운영 보상으로 제공되는 자금이다. (B) FeeFi 보상금이란 FeeFi에 참여하여 블록체인 네트워크 전체의 사용성을 개선하는 역할을 한 FeeFi 예치자들에게 주어지는 보상이다. (C) 공공자금 충당금이란 생태계 전체의 발전을 위해 사용되는 자금을 비축해두는 일종의 예비비다. 우리는 어떤 비율로 배분하는 것이 기여에 대해 공정하게 보상하는 것 인지는 아직 알 수 없다. 또한 토큰 값이 변화함에 따라 공정하게 배분하는 비율도 점차 변화하게 될 것이다. 이런 이유로, A/B/C에 대한 배분 비율은 베타넷 단계에서 실제 노드 운영에 따라 여러가지 테스트와 실험을 거친 후 적절한 금액

수준을 재단에서 그리고 이후에는 의회에서 결정하게 될 것이다.

공공자금 (Commons Budget)

공공자금은 생태계 전체의 발전을 위해 사용될 수 있도록 블록체인 상에 비축해놓은 자금이다. 공공자금은 초기 토큰 할당 정책에 의해 150,000,000개가 초기자금으로 할당되고, 메인넷 피파이 가동 이후에는 수수료의 일정 비율(예컨대 10%)을 지속적으로 누적하여 공공자금을 구축할 예정이다. 공공자금은 투표 보상금, 마케팅 활동 지원, 생태계 파트너 지원, 개발 지원 등 생태계 전체의 발전을 위해 다양한 용도로 사용될 수 있다. 공공자금은 의회의 투표를 통해 지출되며, 상세한 계획은 별도로 발표할 것이다.

06 시장 진입 전략

블록체인을 실제 사회 시스템이 적용하는 작업은 그다지 속도가 빠른 것은 아니다. 2016년부터 각국 정부와 기업들이 블록체인을 활용하려는 프로젝트들을 진행해왔지만[9] 여러가지 이유로 아직까지는 뚜렷한 성과라고 할만한 것이 많지 않다. 여기에는 크게 네가지 이유가 존재한다 : 첫번째는 기술 부족, 두번째는 경험 부족, 세번째는 아직 덜 진행된 디지털 전환, 네번째 아날로그 사회에 형성된 각종 규제와 사회 관리기술들. 이 네가지가 어느 것이 우세하다고 할 것 없이 복합적으로 작용하며 본격적인 디지털 전환을 가로막고 있다. 이 걸림돌들은 앞으로도 상당 기간 존재할 것이다.

이 문제와 관련해 우리는 기술적인 부분과 관련된 문제의 실마리들을 어느 정도 풀었다고 자부한다. 그러나 블록체인 기술을 실제 산업에 적용하는 일은 결국 수많은 시행착오를 겪을 수 밖에 없다. 현재 블록체인 업계가 쌓은 경험을 큰 틀에서 평가하자면, 어떤 것에는 블록체인을 적용해도 소용이 없고 또 적용해서도 안된다는 교훈을 겨우 얻은 정도로 보인다. 마치 모든 것이 다 될 것처럼 생각하고 접근했었는데, 이제 겨우 하면 안되는 일과 해도 소용이 없는 일 정도를 구분하는 단계에 온 것이다. 블록체인을 특정 산업이나 비즈니스에 구체적으로 적용하는데 있어서 '어떻게' 해야하는지에 대한 방법론은 아직 많이 개발되지 않았다. 그도 그럴 것이, 이제 겨우 블록체인 기반 암호화폐Cryptocurrency) 또는 디지털 자산(Digital Asset)이 제도권 내에 진입했고, NFT로 대표되는 자산의 디지털화가 아주 초보적인 형태로 진행되고 있기 때문이다. 따라서 앞으로 해야할 일들 중 대부분은 아직 누구도 해보지 않은 일들이기에 우리가 직접 실행해 보면서 경험을 쌓고 해답을 찾을 수밖에 없다.

아직 덜 진행된 디지털 전환 그리고 아날로그 시대의 규제와 사회관리 기술들이 만들어놓은 장벽도 엄청나다. 블록체인 기술을 제대로 적용하려면 대상 데이터가 디지털로 존재해야 하는데, 실제 존재하는 데이터들은 대부분 아날로그 형태다. 따라서 어떤 것에 블록체인을 적용하고자 시도할 때 먼저 디지털 전환을 어떻게 해야할지에 관한 문제부터 풀어야 한다. 블록체인 적용은 그 이후의 문제인데, 대부분의 프로젝트들이 성급하게 블록체인의 적용과 동시에 디지털 전환을 시도함으로써 어려움이 배가되었다. 이 과정에서 블록체인 기술을 어떻게 사용하는 것이 맞는 것인지에 대해 무지했던 것도 큰 역할을 했다. 게다가 현실 데이터에 걸려 있는 각종 규제 이슈도 실제 프로젝트를 하는데 엄청난 장벽으로 작용한다. 뭔가 시도를 하기 전에 하면 안되는 것들이 잔뜩 쌓여있기에, 원래 해야하는 일에 집중하기보다는 규제를 어떻게 회피할지, 어떤 일을 감행할 경우 예상되는 규제 리스크는 어느 정도인지 사전 검토하는 작업 때문에 막대한 자원을 소비하고 오랜 시간 고민할 수밖에 없기 때문이다.

From Game to Reality

이런 이유로 우리는 현재의 여러가지 장벽들을 슬기롭게 돌파하고 블록체인 기술의 현실화를 보다 가속화시킬 수 있는 시장 진입 전략이 필요하다고 판단하며, 이것을 위한 가장 적절하고 효율적인 방안은 게임과 메타버스에 적용하는 것이라고 판단한다. 적어도 게임이나 메타버스 공간에서 우리는 규제를 고민하거나 데이터를 어떻게 디지털로 전환해야 할지를 고민하지 않아도 되기 때문이다. 온라인 게임이나

메타버스라면 우리는 위에서 언급한 세번째와 네번째 이슈를 뒤로 하고 오롯이 첫번째와 두번째 문제만을 가지고 씨름하면 된다. 더구나 게임 내에서 다루는 데이터들도 모두 디지털이기 때문에 우리는 게임 내에서 구현되어 작동하는 검증된 대부분 기술들을 거의 그대로 현실에 가져다 쓸 수 있다. 우리는 게임에 블록체인 기술을 적용함으로써 블록체인 네트워크 사용성을 늘려나가면서 실질적으로 FeeFi가 작동할 수 있는 수준까지 수수료 수익을 늘려나가고자 한다. 그리고 여기서 구축된 기술을 경제 및 사회 시스템에까지 확장할 것이다. 그래서 프로토콘넷의 시장 진출 전략은 'From Game to Reality'로 요약된다.

게임과 블록체인을 결합하는 것은 새로운 것은 아니다. 당장 시장에서 시도하고 있는 것만으로도 NFT를 활용한 아이템 소유권 보장 및 거래 촉진, 디지털 부동산 소유권 증명, 거래 이력 증명 등 다양한 시도들이 진행되고 있다. 이미 엔진코인(Engine Coin), 디센트럴랜드(Decentral Land), 플로우(Flow) 등 몇 개의 프로젝트들이 게임과 블록체인을 결합하는 작업을 수년째 진행 중인데, 블록체인 상에 게임 관련 데이터들이 축적되면 자연스럽게 게임 아이템 또는 디지털 자산 거래라는 새로운 산업 영역이 촉발될 것이다. 게임 산업은 여전히 아이템 탈취, 아이템 도용, 아이템 해킹 및 복제 등 디지털 기술에서 전형적으로 발생하는 문제들을 겪고 있다. 바로 이 부분에서 블록체인은 디지털 자산의 관리 및 거래라는 새로운 산업 영역을 선도적으로 추동할 것으로 기대한다. 최근 급격하게 부상하고 있는 메타버스 역시 블록체인을 논외로 하고는 제대로 작동할 수 없다.

만약 완전히 디지털화된 경제의 구체적인 모습을 확인할 수 있는 가장 가까운 선행 모델이 무엇이냐고 묻는다면 그것은 아마도 게임산업일 것이다. 이런 측면에서 온라인 게임 산업은 단순한 수단을 넘어서 전략적으로 파고들어 적극적으로 실험하고 새로운 모델들을 발굴해야할 공간이다. 그러나 이더리움 네트워크를 중심으로 하는 이러한 시도들은 이더리움의 느린 속도와 비싼 수수료 때문에 의미 있는 산업을 추동해내기 쉽지 않을 것으로 예상한다. 이런 측면에서 우리는 메인넷 수준에서 게임에 필요한 온갖 기능들을 전략적으로 지원하는 것이 필요하고 가능하다고 판단한다. 그래서 우리는 게임을 중심으로 다음과 같이 네트워크의 성장전략을 실행할 것이다.

로드맵

1. Phase 1 : Model House(Blockcity) 구축
2. Phase 2 : Game Data Platform 구현
3. Phase 3 : From Game to Reality

우리는 Phase 1에서 블록시티를 통해 게임 데이터에 블록체인을 적용하는 다양한 방법론들을 개발하고자 한다. 여기서 마인크래프트를 이용한 블록시티 게임을 직접 구현하고, 아이템 소유권 보장, 디지털 부동산 소유권 증명, 거래 이력 증명, 게임 경험치 증명, 디지털 뱃지 발행 및 유통, 디지털 저작권 관리를 위한 다양한 모듈들을 실제로 구현해서 블록시티 게임에 적용할 예정이다. 또한 블록시티에서 구현된 기능들을 전체 마인크래프트 생태계가 사용할 수 있도록 블록체인 전용 플러그인이나 모드를 개발할 예정이다. 블록시티를 통해 만들어진 게임 관련 기능들은 활용성이 검증되고 데이터 모델이 확정되면 게임 산업 전체가 사용할 수 있도록 모듈화된 기능으로 시장에 제공될 것이다. 이어 Phase 2에서는 블록체인을 매개로 한 일종의 Game Data Platform을 구축함으로써 다종다양한 게임들이 자신들에게 필요한 블록체인 기능을 자유롭게 가져다 쓸 수 있도록 게임에 특화된 블록체인 기능들을 제공할 예정이다.

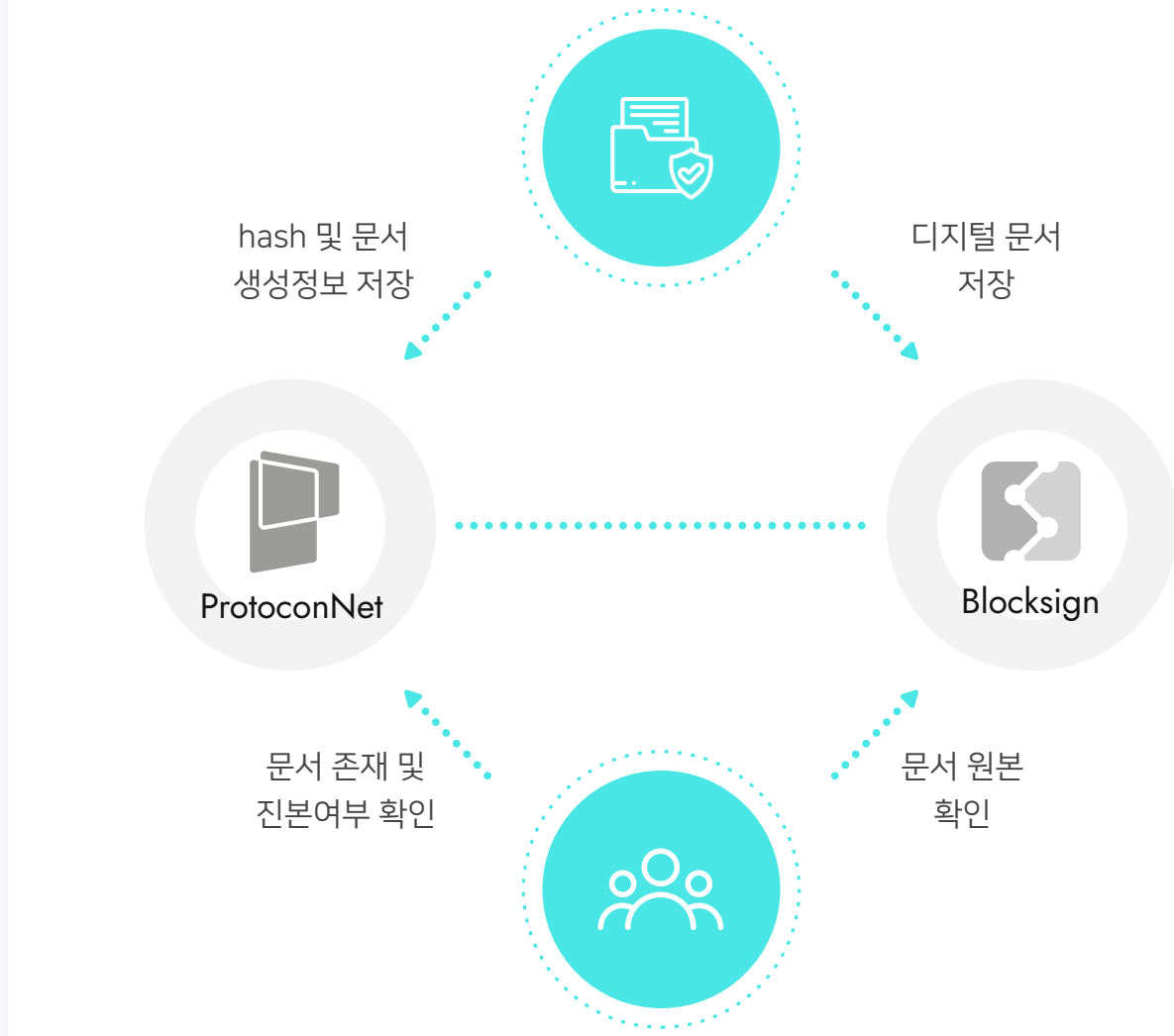
07 응용 서비스

우리는 블록체인 기술을 어떻게 산업에 적용할 수 있을지 많은 고민을 했다. 블록체인은 아직 다루기 까다로운 기술이고 이제 막 산업이 제시한 숙제들을 한창 풀고 있는 상황이기에 기술 자체를 활용하는 것이 쉽지 않다는 것을 확인했다. 블록체인 응용 사례가 가장 간단한 어플리케이션인 토큰에만 집중되어 있는 이유가 이것이다. 또한 블록체인은 초기 기술이기에 결국은 원천기술을 개발한 팀이 충분한 응용 사례들을 구축하지 않으면 다른 팀이 결과물을 가져다 쓰기가 쉽지 않다.

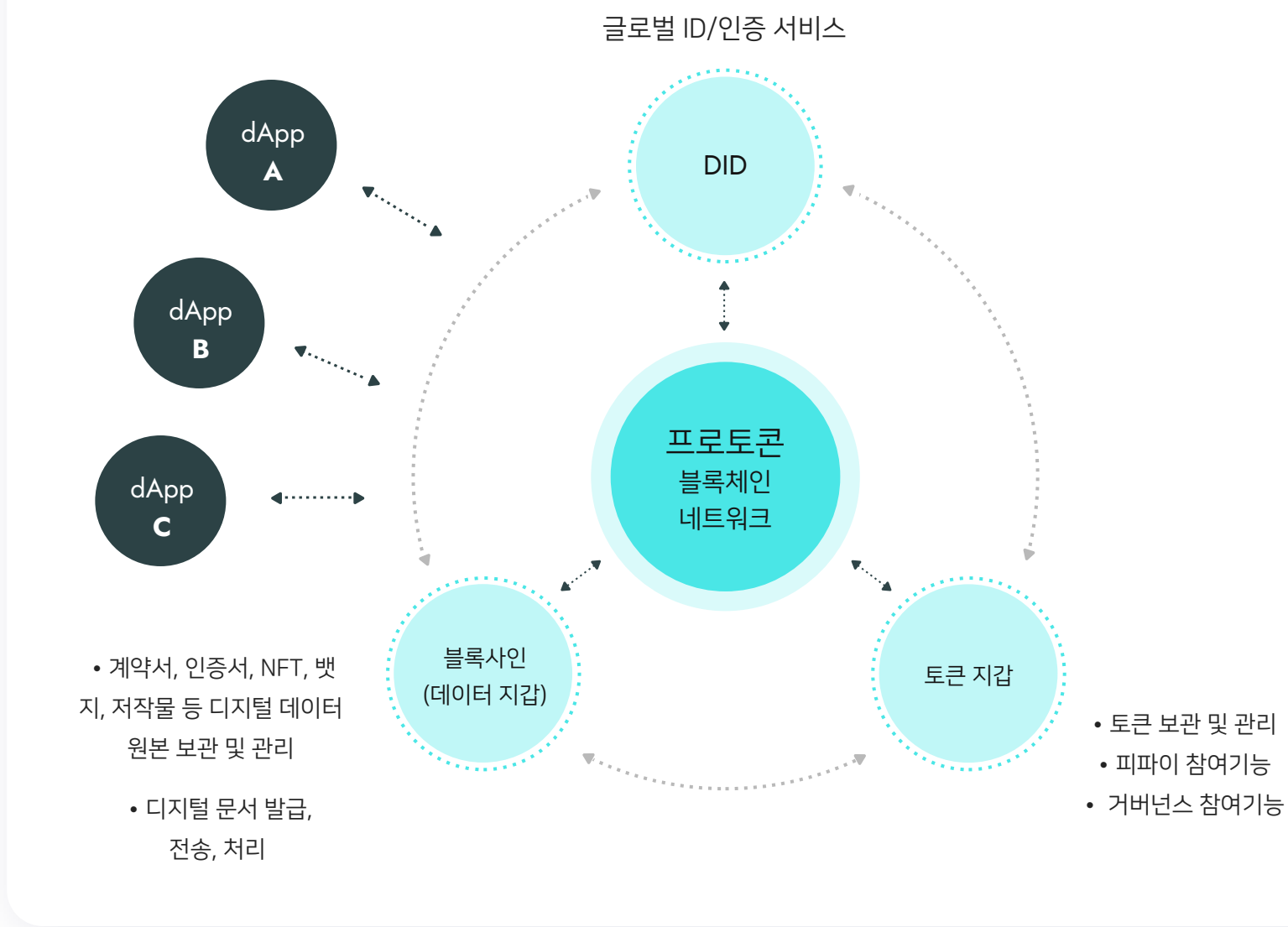
또한 블록체인 단독으로 디지털 전환에 필요한 모든 서비스들을 제공할 수 없다. 블록체인은 디지털 데이터의 신뢰를 보장하기 위해 필요한, 그 자체로 대단히 비싼 솔루션이다. 따라서 블록체인은 신뢰를 보장하기 위한 방법론으로 최적화되고 최소화되어 사용되어야 하며, 기존에 IT 서비스를 제공하는 방법론들과 적절하게 융합시켜 사용해야 한다. 이것이 우리가 원천기술과 더불어 블록체인과 연동된 문서 및 데이터 관리 시스템 '블록사인'과 블록체인 기술의 모델하우스이자 데이터 생산 공장인 '블록시티'를 자체적으로 구현하고 운영하는 이유다. 우리가 이런 작업을 직접 하지 않으면 우리 블록체인의 활용성을 만들기도 어렵고, 또한 블록체인 기술이 실제 산업에 유용하게 쓰이는 제대로 된 사례를 만들기도 쉽지 않다고 생각한다.

01 블록사인

이미 우리에게 익숙해진 디지털 토큰 이외에 블록체인 기반의 데이터나 문서를 본격적으로 다루기 위해서는 블록체인 네트워크와 더불어 데이터나 문서를 저장하고 프로세스에 따라 처리해주는 클라우드 서비스가 필요하다. 즉 블록체인을 산업적으로 다루기 위해서 지금까지는 단지 블록체인 그 자체에만 집중해왔지만, 이것만으로는 다양한 디지털 데이터들을 다룰 수 없다. 그렇기 때문에 우리는 프로토콘넷과 더불어, 블록사인(Blocksign)이라는 데이터 클라우드 서비스를 동시에 구현했다. 프로토콘넷 입장에서 블록사인은 블록체인을 접목한 응용 어플리케이션이지만, 디지털 데이터를 관리하는 측면에서 보자면 일종의 인프라 성격을 가진 서비스다.



특히 향후 블록체인의 산업적 활용이 확대되고, 개인들의 NFT 등에 기반한 저작물, 졸업증명서나 백신접종 증명서와 같은 인증서, 뱃지 등의 데이터들이 본격적으로 생산되기 시작하면 해당 데이터의 원본을 관리해야할 필요성이 증대된다. 그런 측면에서 우리는 토큰을 담는 지갑을 토큰 지갑이라고 한다면 블록사인은 일종의 데이터 지갑 성격을 가지고 있다. 이를 도식화하면 다음과 같다.



문서 관리와 관련해서는, 엄청나게 발전된 디지털 기술과 비교하자면 문서의 디지털화 정도는 심각할 정도로 지체되고 있다. 문서가 활발하게 디지털로 전환되지 못했던 또 다른 이유는 문서가 단지 종이에 인쇄된 문자로 구성된 것이 아니라 1) 문서는 특정한 프로세스를 거쳐 생성되며, 2) 특정한 프로세스를 거쳐 처리(수정/변경/폐기)되고, 3) 종이에 기록된 문장이나 숫자가 현실에 실질적인 힘을 행사하는 물리적 힘을 가지고 있는데, 이런 문서의 고유한 특징들을 디지털 방식으로 어떻게 처리할 수 있는지에 대한 적절한 방법론이 만들어지지 않았기 때문이다. 즉 지금까지 아날로그 방식으로 처리하던 문서를 디지털로 전환하고 디지털에 적합한 방식으로 처리하는 방법론들이 충분히 개발되지 않은 상황이다. 우리는 문서를 포함한 다양한 유형의 디지털 데이터들을 효과적이고 효율적으로 관리할 수 있도록 블록사인을 개발하고 있다. 특히 게임에서 생산된 아이템들과 소유권 확인 문서 등의 디지털 원본을 보관하는 저장소로 사용될 것이다.

블록사인은 총 4단계에 걸쳐서 개발될 예정이며 현재 1단계 개발을 완료하고 2단계 개발을 진행 중이다.

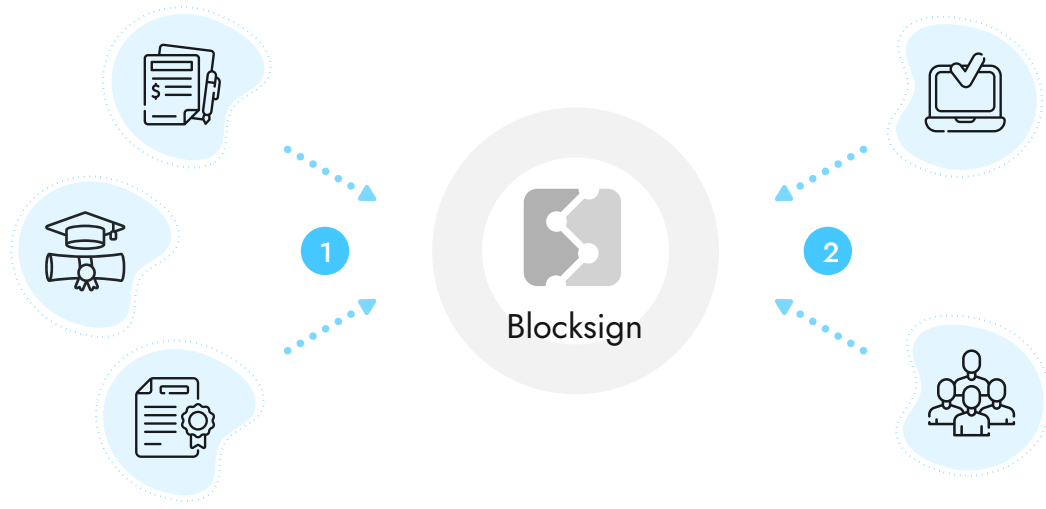
[블록사인 서비스 단계별 구현 계획]

1단계 (개발 완료)

블록체인 기반 My Data 관리 기본 기능

개인 데이터 저장, 상호 서명, 공유,
문서 원본 검증 기능 구현

1. 표창장, 졸업장, 계약서 등 블록사인에 저장
2. 제 3자가 블록사인에서 문서 유효성 확인

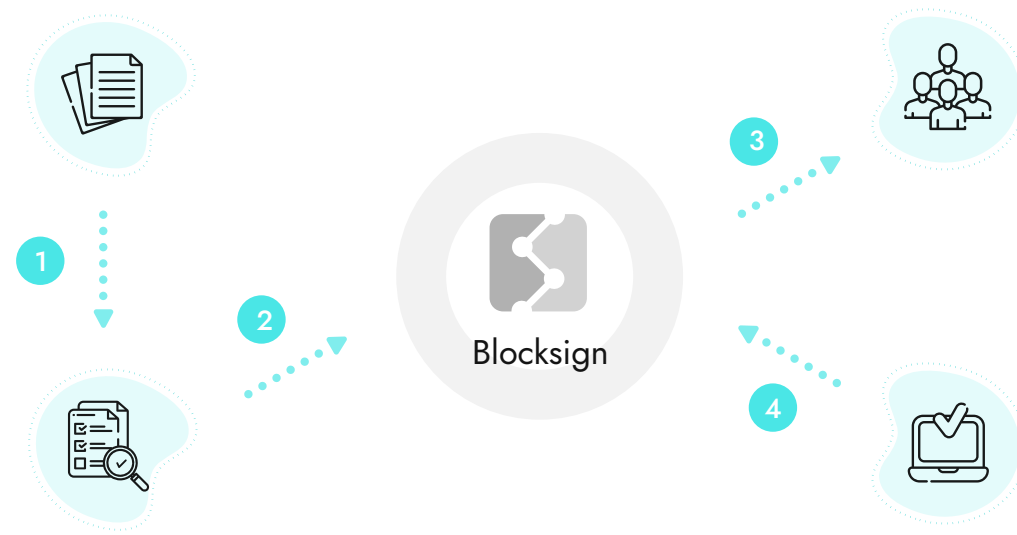


2단계 (개발 진행중)

디지털 원본문서 발급 및 공유 기능

디지털 원본 문서 발급,
문서 상호인증 및 공유 기능 구현

1. 문서 생성자 문서발급 및 수신자 인증 요청
2. 문서 수신자 인증 및 블록사인 저장 완료
3. 제 3자에게 블록사인에 저장된 문서(이력) 전송
4. 제 3자가 블록사인에서 문서 유효성 확인



3단계 (개발 예정)

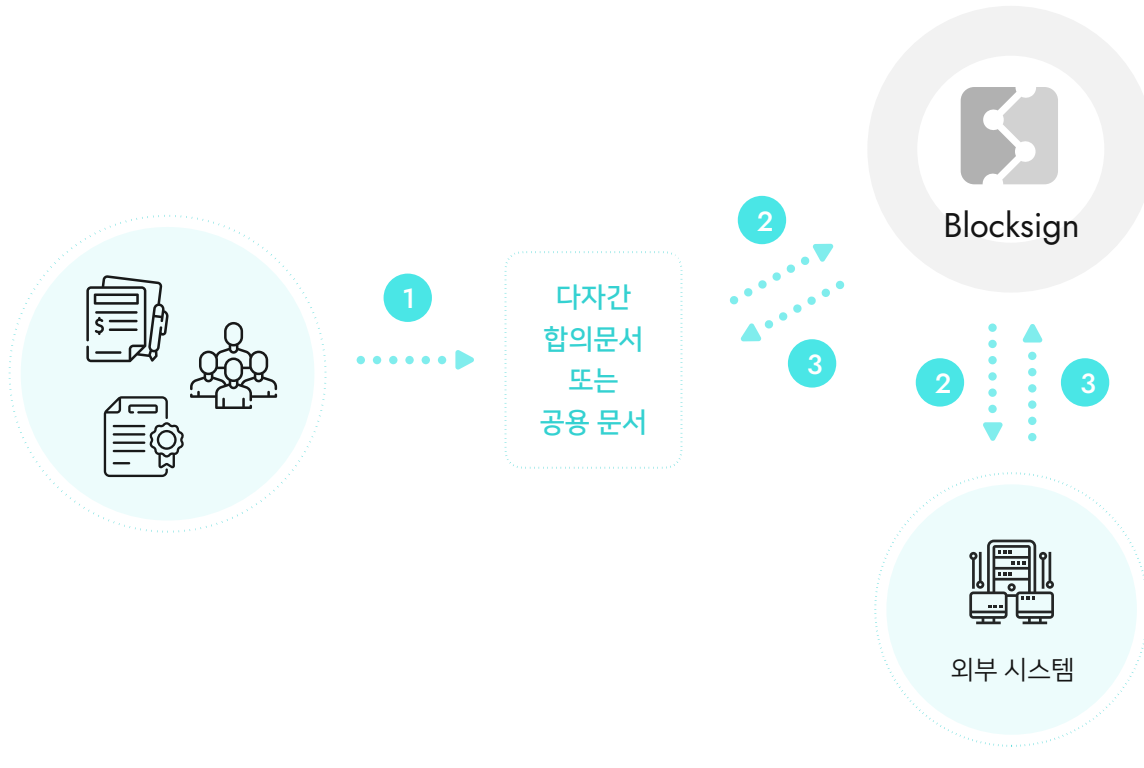
다자간 합의문서 생성 및 관리기능

공동 규약, 정관 등 다수 개인들의
합의/약속을 담은 합의문서 관리기능 구현

1. 다수 개인들이 규약, 정관, 약관 생성 및
수정 내용에 합의 (디지털 서명 혹은 투표)
2. 합의된 문서 및 합의에 참여한
개인정보 블록체인에 기록

4단계 (개발 예정)

외부 시스템 연동 문서 관리 기능

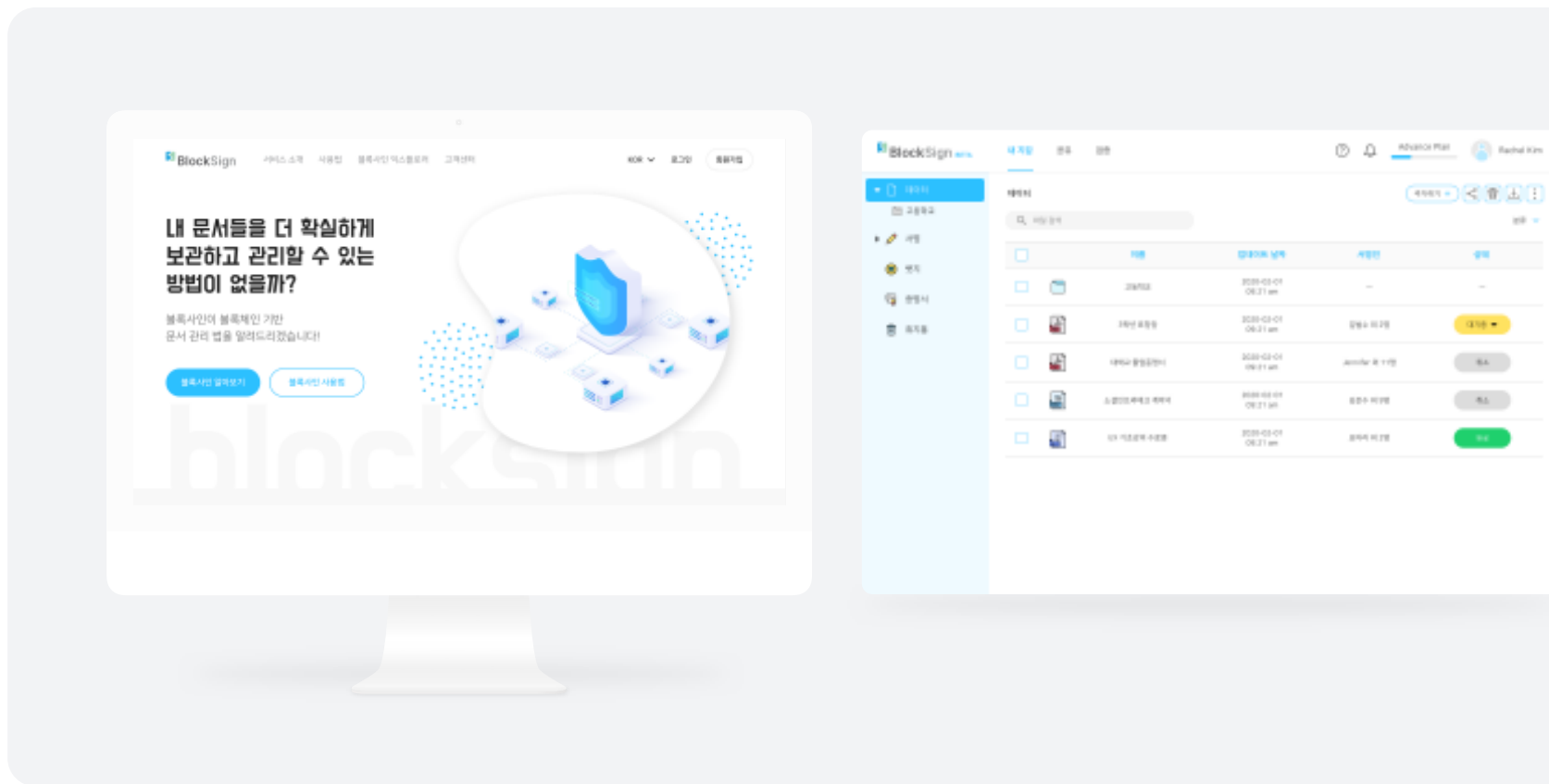


다수 개인들의 합의 사항이
외부 시스템 통제하는 기능 구현

1. 다자간 협의 문서 또는 공용문서 공동 관리
2. 합의된 문서 및 개인정보를 블록사인에 기록하고, 기록된 내용이 외부 시스템을 통제
3. 외부 이벤트가 블록사인을 통해 합의 문서 또는 공용문서의 내용을 시스템적으로 변경

블록사인 1단계는 문서 관리를 디지털화는 단계로, 개인 Mydata를 관리하는 클라우드 저장소 기능을 구현했다. 개인들은 블록사인에 본인이 보관하거나 원본을 증명해야할 문서들을 저장해놓고 본인 서명을 통해 블록체인에 hash값을 저장함으로써 문서 원본과 사인 이력 등을 증명할 수 있다. 즉 졸업 증명서, 표창장, 수료증 등 증빙이 필요한 문서들을 간편하게 저장 및 관리할 수 있으며 상호 서명을 통해 간단한 개인간 계약서 등도 처리할 수 있다. 현재 서비스 오픈을 위한 개선 작업을 진행 중이며, 2021년 상반기 서비스화될 예정이다.

[블록사인 1단계 서비스 화면]



블록사인 2단계는 문서 생성 및 발급의 디지털화하는 단계로, 학교, 기관 등에서 발급하는 문서를 디지털 원본으로 발급하고 수신, 공유, 검증할 수 있는 서비스다. 2022년 상반기 2단계 서비스 개발 완료

및 출시를 목표로 하고 있으며, 베타넷에 연동될 예정이다. 3단계에서는 다수 개인들의 합의에 의해 생성 및 수정되는 법률, 법인이나 협동조합의 정관, 자치 공동체들이 스스로 합의한 조례나 규약, 기업이나 단체의 이사회 결의서 등 다수의 합의에 기반한 또는 다수의 합의에 의해 생성되는 문서를 디지털로 관리하는 방법을 구현하고, 4단계는 최종적으로 합의에 기반해 생성된 디지털 문서의 내용이 현실의 디지털 인프라를 제어 내지 통제할 수 있도록 하는 기능 구현하는 것이다. 예컨대 주민자치 지역에서 스쿨존 제한속도를 30Km에서 20Km로 변경하기로 합의했을 때, 도로교통 관제시스템의 기준 속도를 공동체가 합의된 내용에 따라 실시간으로 또는 약속된 시점에 자동으로 변경하는 것과 같은 기능들을 구현하는 것이다. 우리는 블록사인의 사용성을 보여주기 위해 블록시티에서 사용자들이 구매한 토지소유 등기부 등본, 아이템 소유권, 뱃지 등을 문서화해서 블록사인에 저장하고 이를 공유할 수 있도록 할 예정이다. 또한 게임 내에서 합의에 의한 규칙 제정 및 제정된 규칙의 자동 적용 등을 통해 실제 작동하는 블록사인 3단계와 4단계 컨셉을 구현할 예정이다.

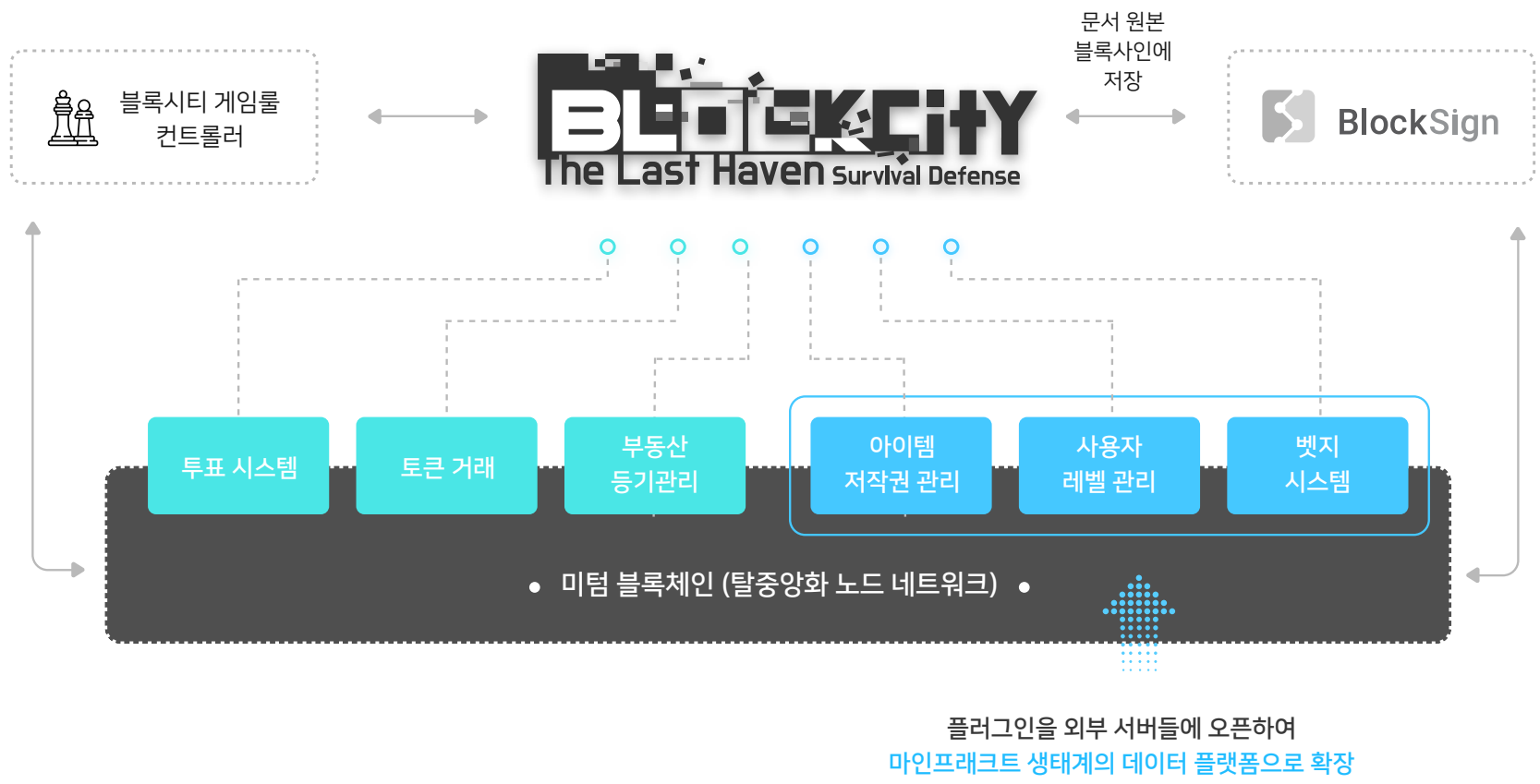
장기적인 관점에서 보자면, IPFS와 같이 탈중앙화 클라우드 저장 기술이 충분히 발전한 시점에 우리는 블록사인의 데이터들을 탈중앙화 저장소와 연결하는 작업 등을 염두해두고 있다. 그러나 아직까지 탈중앙화 저장소란 실험적인 수준에서는 시도해볼 수 있지만 산업적으로 안정적으로 사용하기에는 많은 시간이 필요하며, 더구나 데이터 및 문서 처리에 필요한 프로세스와 운영기능까지 포괄하기에는 요원한 것으로 보인다. 특히 IPFS의 프라이빗 키를 잃어버리는 경우 사용자는 IPFS에 저장된 모든 자료를 분실하게 된다. 즉 사용자 입장에서 대체불가능한 손실(Non-fungible loss)이 발생할 수 있다. 그래서 우리는 상용 클라우드 기반으로 블록사인 서비스를 구현하고, 장기적으로 IPFS와 연동하는 방향으로 나아갈 것이다.

블록시티

우리는 프로토콘넷의 산업적 활용 가능성을 증명하고, 또한 수익성 있는 메인넷 비즈니스 모델을 구축하기 위해 마인크래프트 게임에 블록체인 기술을 접목한 '블록시티'를 구현하고 있다. 또한 블록시티와 블록사인을 연결, 토지 등기 문서, 소유권 및 저작권 관련 문서, 뱃지 등의 원본을 저장함으로써 블록사인 서비스의 필요성과 유용성을 증명하고 사용성을 창출하고자 한다.

마인크래프트는 마르쿠스 알렉세이 페르손이 개발하고 마이크로소프트 스튜디오가 인수하여 배급하는 오픈 월드 인디게임으로, 전세계적으로 2억명 넘게 판매되었고 월 1억2천만명이 게임 서버에 접속하고 있다. 최초의 샌드박스형 게임으로 사용자들이 다양한 모드와 플러그인을 개발하여 게임을 자유롭게 변형할 수 있으며 임의로 독립적인 게임 서버를 구축하여 다양한 장르의 게임을 즐길 수 있다. 우리는 글로벌 팬덤을 보유한 마인크래프트를 활용하여 블록체인 기술이 적용된 블록시티 게임을 서비스화할 예정이다.

[프로토콘 네트워크, 블록사인, 블록시티 관계도]



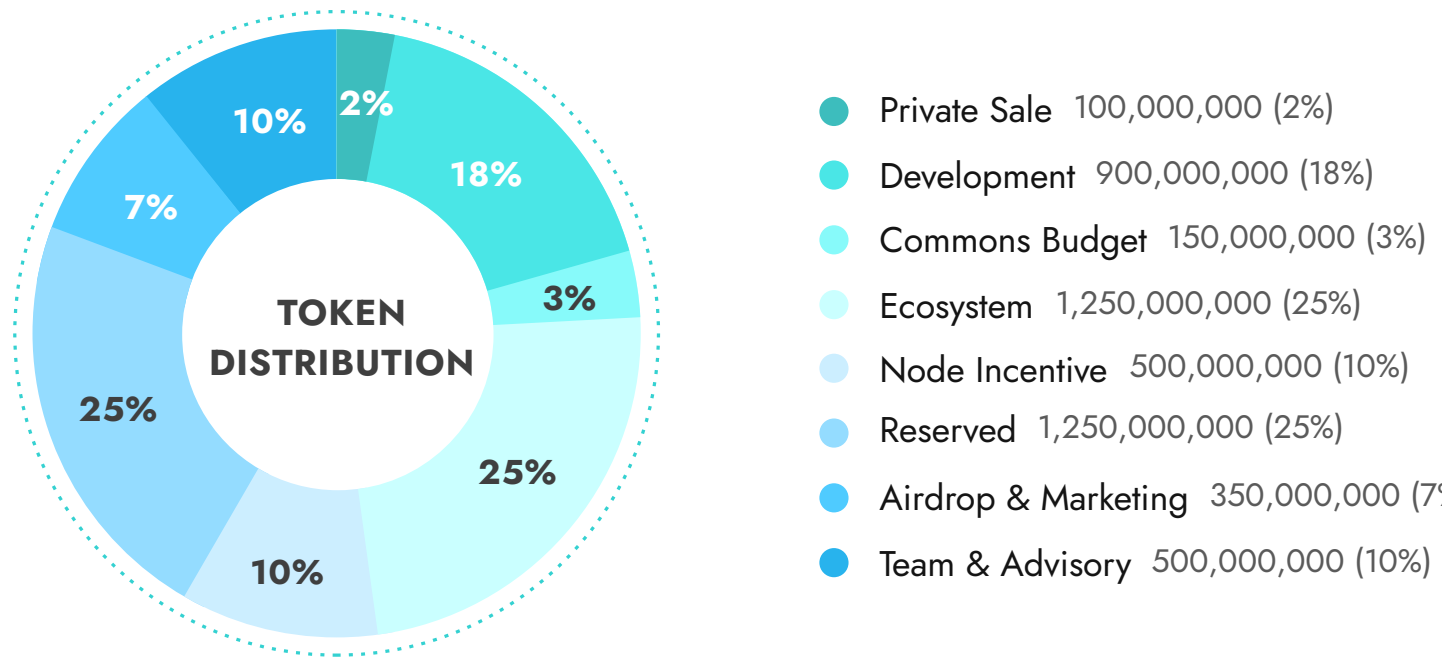
우리가 블록시티와 같은 게임들에서 구현할 블록체인 기술들은 대략 다음과 같다.

1. 투표 시스템 (블록시티 시민권자들이 투표를 통해 게임룰 제정에 참여하고 이를 블록체인 기반 코드로 구현하여 게임에 반영함, 블록사인 3/4단계 모델 연동)
2. 블록체인 기반 게임 내 포인트(게임 머니) 운영
3. 가상 토지에 대한 소유권 부여, 부동산 등기 등록 및 부동산 거래 내역 관리
4. 아이템 소유권/저작권 및 거래 내역 등록 및 관리 (블록사인 1단계 연동)
5. 게임 이력, 레벨, 경험치 등 게임포트폴리오 관리 (블록사인 2단계 연동)

우리는 블록시티를 통해 구현된 블록체인 기술들을 바탕으로 여러 게임에 확장적용하여 장기적으로 블록체인 기반 게임 생태계를 구축할 예정이다. 또한 위 게임에 접목되어 증명된 블록체인 기술은 그대로 공공 및 산업 영역에 적용하고자 한다.

08 토큰 배분 계획

PEN 토큰은 총 50억개가 발행되며, 개발 지속성 확보, 메인넷 작동과 에코시스템 구축 등을 고려하여 다음과 같이 할당된다.



위 50억개의 토큰은 총 15년에 걸쳐 순차적으로 할당되며, 초기 연도별 할당 계획은 다음과 같다. (단위, 100만개)

Items	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
Private Sale	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Development	0	100	100	90	80	70	60	50	50	50	50	50	50	50	50
Commons Budget	0	10	20	10	10	10	10	10	10	10	10	10	10	10	10
Ecosystem	0	100	200	150	150	120	100	90	80	70	50	50	30	30	30
Node Incentive	0	50	50	50	40	40	40	40	30	30	30	30	30	20	20
Reserved	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Airdrop & Marketing	30	30	25	25	25	25	25	25	20	20	20	20	20	20	20
Team & Advisory	100	30	30	30	30	30	30	30	30	30	30	30	30	20	20

위 계획은 프로토콘넷이 안정적으로 시장에 안착하고 토큰 가격이 급격하게 변동하지 않도록 하는 것에 최우선을 두고 설계되었다. Reserved 물량은 현재 용도를 특정하지 못했으나 향후 추가될 수 있는 영역 또는 초기 계획 대비 부족한 부분, 또는 2035년 이후에 필요한 토큰 사용처에 할당하기 위한 것이다. Reserved 물량을 사용할 경우에는 반드시 의회의 승인을 거쳐야 한다. 또한, 각 연도별 할당 물량은 토큰이 한번에 시장에 유통되는 것을 방지하기 위해 각 항목별로 별도의 락업 정책이 적용된다. 예컨대 멤버 물량은 2021년에 할당되더라도 락업이 해제되는 시점은 토큰 첫 상장 후 1년 반 이후로 하는 등 핵심 개발진들의 도덕적 해이를 막기 위한 장치들을 도입했다. 그러므로 위 표에서 연도별로 할당되는 토큰수와 실제 시장의 유통량은 반드시 일치하지 않는다. 또한, 이 중 일부 물량은 FeeFi를 통해 Commons Budgets에 지속적으로 쌓이게 되며, Commons Budgets에 축적된 물량은 의회의 승인을 거쳐 메인넷 유지와 생태계 지속성을 확보하는 용도로 사용될 것이다. 더불어 실제 메인넷이 가동되고 에코시스템이 작동하기 시작하면 애초 계획과 실제 현실은 차이가 나게 마련이다. 우리는 메인넷과 의회가 공식 가동하는 시점 이후, 의회에 연단위 계획을 제출하고 의회의 승인을 통해 토큰 유통 계획을 시장 환경에 맞게 조절할 예정이다.

Conclusion

이 백서에는 그 동안 우리의 경험과 보유 기술을 토대로 상당 부분 구현 했거나 근간에 구현할 내용들을 담았다. 현재 버젼에서 빠진 부분들은 세부안이 확정되는대로 업데이트할 것이다. 우리는 탈중앙화와 블록체인의 실생활 적용이라는 목표로 나아가기 위해 새로운 방법론과 길을 기꺼이 여행할 것이며, 이에 따라 백서는 지속적으로 업데이트될 예정이다.

09 References

[1] ProtoconNet은 Protocol Economy Network의 줄임말이다.

[2] Miguel Castro and Babara Liskov at 1999, [Practical Byzantine Fault Tolerance](http://pmg.csail.mit.edu/papers/osdi99.pdf)

[3] https://github.com/bosnet/sebak

[4] ISAAC+는 기존 ISAAC 합의프로토콜을 업그레이드했다는 의미로 +를 붙여 명칭을 정했다. ISAAC 합의프로토콜은 합의단계를 Init - Sign - Accept - All Confirm이라는 4단계로 구분하였으며 이는 PBFT의 4단계와 유사하며, 각 단계의 첫 글자를 따서 I-S-A-AC을 붙여 만든 명칭이다.

[5] Andreas M. Antonopoulos, Gavin Wood, Mastering Ethereum: Building Smart Contracts and DApps', O'Reilly Media, 2018

[6] https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

[7] https://tezos.com/

[8] https://terra.money/

[9] Myungsan Jun, 'Blockchain Government: A next form of infrastructure for the twenty-first century', CreateSpace Independent Publishing Platform, 2018

