YGGDRASH

Trust-based Multidimensional Blockchains
& Internet re-designed by blockchains

White paper (ver 0.22.2)

* 본 문서는 일반적인 정보 제공용으로 제작되었으며 본 백서의 어떠한 내용도 특정 회사 또는 개인과 거래 조건을 규정하는 것으로 해석되지 아니하며 AKASHIC FOUNDATION LTD.와 법률 관계를 형성하지 아니한 제 3자의 행위(제 3자간 거래 등)에 대하여 어떠한 책임도 지지 않습니다.
* 본 문서는 본사의 지적 재산권 이므로 무단 배포 및 도용시 법적 처벌을 당할 수 있습니다.
* 본 문서의 독자는 블록체인에 관한 기본적인 지식이 있다는 가정하에 작성되었음을 알려 드립니다.
* 궁금증이 있으시다면 info@yggdrash.io 로 문의 주시기 바랍니다.

머리말

우리가 생각하는 미래

우리의 미래는 점점 복잡해질 것이며, 점점 더 많은 거래와 데이터가 생성될 것이다.
현재와 다름없이 앞으로의 미래에서도 가장 중요한 요소로 손꼽히는 것은, 바로 데이터관리라고 말할 수 있다.
그런데 지금처럼 모든 데이터를 한곳에 모아 각각 연계된 모든 지점 역시 한곳에서 관리하는 체계가 계속된다면 어떻게 될까? 그것은 모든 리스크가 한곳에 밀집되는 것과 같다.
사람들이 자신의 자산을 이용하기 위하여, 혹은 자신의 생명을 지키기 위해서 신뢰해야 할 곳을 모든 데이터가 한 곳으로 모이는 지점으로만 선택해야 한다면, 그것은 과연 옳은 결정, 또는 최상의 선택지라고 말할 수 있을 것인가?
만약 그 한 지점이 어느 순간 동작을 하지 않는다면? 아니면 자신의 소중한 정보를 이용하는 사람들을 마주해야 하는 상황이 생겨난다면? 그 이후에도 여전히 그 체계 자체를 신뢰할 수 있을 것인가. 안전성이 보장되지 않는 체계를 계속 신뢰를 해야 하는지가 의문이다.

정보의 바다라고 불리는 인터넷의 모든 것을 블록체인으로 바꿀 수는 없어도, 우리 사회가 가진 많은 문제를 바꿀 수 있기에, 미래로 나가기 위한 한걸음의 시작으로 이러한 플랫폼의 필요성을 말할 수 있다.
모든 블록체인은 각각의 거버넌스를 가지고 있다. 비트코인과 이더리움이 다르듯 서로의 각 체인에는 추구하는 목표와 방향이 있으며, 해결하고자 하는 생각의 차이가 있다.

이그드라시는 그 생각 차이에 동의하며, 이를 해결하는 방법을 함께 제시해 나가는 플랫폼을 지향한다.

블록체인이 많은 이념을 바꾸었다. 그러나 이면에서 볼 때 아직은 각 블록체인이 문제를 해결하는 방식에는 어려움이 존재한다. 그 어려움은, 네트워크는 분산화되어 있으나 네트워크를 사용하는 이용자들이 각각의 네트워크를 사용하면서 하나의 블록체인에 집중되어 하나의 블록으로 모든 거래결과가 집중되어 있다.

이는 네트워크의 분산화 정보의 집중화를 초래하며, 블록체인의 성능의 한계점을 보여준다. 하나의 블록체인의 체결속도가 아무리 빨리 만들어도, 수많은 사람이 동시에 그 블록에 등록되기 위해서 노력한다면 반드시 병목현상이 생길 것이며 이는 p2p 네트워크가 풀어야 할 본질적인 과제이다.

많은 블록체인 프로젝트가 아직도 그 문제를 해결하려 노력해 가고 있으며 우리 역시 블록체인 월드에 이바지함으로써 이 문제를 해결해 나갈 것이다.

Team Yggdrash

1. 개요

1.1 Why, Another, Blockchain? (왜, 또 다른, 블록체인을?)

1.1.1 트랜잭션 처리 성능, 블록 검증 노드의 이기적인 경쟁 및 블록체인의 싱크 속도 문제

트랜잭션 속도(TPS) / 처리량(Throughput), 즉 트랜잭션 처리 성능은 무엇인가? 기본적으로 단위 시간당 얼마나 많은 트랜잭션을 처리할 수 있는가를 측정한 수치이다. 현재 블록체인은 급격한 거래 데이터와 DApp 데이터로 난항을 겪고 있다. 기존의 중앙화된 서버 방식이라면 트래픽 증가에 따라 서버를 증설하면 해결되는 문제지만, 블록체인은 분산화된 DB 환경과 처리 성능이 다른 P2P 네트워크 자원을 활용해 연산 작업을 함으로써 중앙화된 방식보다 느릴 수밖에 없는 태생적 한계를 가지고 있다. 또한, 노드 간의 합의 과정을 거쳐야 하는 절차가 더해지면서 문제 해결은 더욱 더디고 복잡하다.

블록체인의 처리 성능과 불가분의 관계에 있는 것이 바로 블록 검증 노드, 즉 채굴자들의 경제적 인센티브이다. 블록체인의 시초인 비트코인은 수학적인 증명과 게임 이론에 따라 채굴자들의 자발적인 참여와 그에 상응하는 보상을 통해 투명하고 안정적인 생태계를 만들 수 있다고 믿었다. 하지만 선형적· 폭발적으로 증가하는 트랜잭션 환경이 발생하자 수익성을 기준으로 모든 거래와 DApp을 줄 세우기를 하는 이기적인 블록 검증인으로 변해가고 말았다. 또한, 높은 가치를 창출할 수 있는 트랜잭션이 있더라도 낮은 수수료를 지불할 경우 아주 늦게 실행되거나 영원히 실행되지 못하는 상황까지 치닫게 된 것이 오늘날의 블록체인 현실이다.

블록체인 세상에서 아직 크게 논의되지 않았던 것은 블록체인 용량 증가와 싱크 속도의 문제이다. 블록체인은 기본적으로 블록과 블록이 연결되는 구조로 트랜잭션이 늘어남에 따라 전체 블록들의 용량과 블록 싱크 시간이 지속해서 증가할 수밖에 없는 구조를 가진다. 비트코인은 2012년을 기점으로 블록체인 용량과 블록 싱크 시간이 매년 평균 2배씩 증가하고 있으며 2018년 2월, 현재 비트코인의 용량은 150GB, 블록 싱크 시간은 평균 14일 정도가 걸린다. 이는 일반인의 블록체인 참여를 저해하는 요소로 동작하며 분산화된 블록체인이 중앙화로 변해가는 잘못된 결과를 초래하고 있다. 현재 블록체인은 당장 눈앞에 처한 처리 성능의 이슈를 해결하기 고군분투하고 있으나 4차 산업의 하나인 소형 IoT 디바이스에 블록체인을 적용하기 위해서는 블록체인 용량 이슈와 싱크 속도 문제를 반드시 해결해야 한다.

1.1.2 비트코인의 한계점과 현 주소

블록체인 1.0세대인 비트코인이 처음 나왔을 때, 가장 많은 관심을 받았던 이유는 탈중앙화 기반의 보안성, 빠른 송금, 제로에 가까운 수수료였다. 그러나 현재는 어떠한가? '빠른 송금 속도'는 엄청난 거래지연과 미승인 문제로 이슈가 되었고, '제로에 가까운 수수료'는 최근 3개월 기준 평균 55달러, 즉 한화로 6만원을 넘어 일상에서 결제용으로 쓰거나 소액거래를 하기엔 불가능한 상황에 봉착하게 되었다. 이러한 문제들은 왜 발생할까? 모든 퍼블릭 블록체인이 가진 숙제인 1) 분산 DB의 처리 속도를 해결하지 못한 것과 2) 분산 DB를 생성/공유하는 노드들의 경제적 인센티브 설계에 실패했기 때문이다.

다음은 현재 비트코인이 겪고 있는 현 상황들을 여실히 보여주고 있다.

"51분"

최근 30일간 비트코인 거래가 성사되기까지 소요되는 평균 시간 (BlockchainInfo.com)

"55달러"

최근 3개월 기준, 1비트코인당 평균 거래 수수료 (blockchain.info/charts)

"214,817"

지금 현재 비트코인 네트워크에서 블록에 포함되지 못하고 떠돌고 있는 거래의 건수 (blockchain.info/charts)

"150GB & 14일"

현재 비트코인의 전체 블록 사이즈와 블록 싱크에 소요되는 시간 (bc.daniel.net.nz)

"30.14 테라와트"

비트코인이 1년 동안 소비하는 전력량 (가상화폐 전문 온라인매체 디지코노미스트)

30.15TW 는 아일랜드 전체 소비량*(*연간 *25TW)*을 넘어선 수치이다.

1.1.3 이더리움의 한계점과 현주소

블록체인 2.0세대인 이더리움은 단순한 화폐의 기능뿐 아니라 계약서, SNS, 전자투표 등 다양한 DApp을 운영할 수 있는 플랫폼을 제공한다. 하지만 이는 1) 이더리움의 블록체인상에서 모든 DApp을 기록하고 처리해야 하는 확장성 문제를 함께 야기시키며 2) 비트코인과 유사한 경제학적 인센티브의 한계점이 드러나고 있다.

아래는 현재 이더리움이 겪고 있는 현 상황을 기술하였다.

“Crypto Kitty"
11월 28일 가상의 고양이를 사고, 팔 수 있는 이더리움의 DApp인 크립토키티의 인기 때문에 이더리움 네트워크의 pending transaction 건수는 평균 6배 증가하면서 이더리움 네트워크의 마비 현상이 일어났다.

“이더리움 가스(gas, 수수료) 이슈”
이더리움은 튜링 완전성(Turing-Completeness), 보안 등의 이유로 사용자에게 가스비를 내도록 설계되었다. 전통적인 중앙화 서비스 이용자들이 받아들이기 힘든 수수료 정책이다. (EOS의 토큰 정책이 더 합리적임)

“DApp 간 상호연동 시, 수수료 지불 이슈"
이더리움 위에 수많은 DApp들이 런칭되고, 이 DApp들이 상호연동하여 하나의 서비스로 동작할 때, (각 DApp이 독립적인 수수료 정책 시행 시) 사용자는 하나의 서비스를 위해 사용자가 알지도 못하는 각각의 DApp들에게 매번 수수료를 지불해야 한다 (물론 모든 서비스가 상용화 수준까지 발전하면, 현존하는 대부분의 DApp들이 서로 통합되어 더 완결된 구조의 DApp이 태어날 것이다)

“낮은 수준의 DApp의 경우 실행되지 않거나 영원히 실행되지 못할 이슈”
이더리움은 수수료를 지불하는 측은 이용자나 해당 서비스를 실행하는 측은 검증인이다. 검증인은 오직 수익성이 높은 DApp들을 우선하여 검증하다보니, 수익성이 낮은 DApp들은 거의 실행되지 않거나 영원히 실행되지 않을 수 있는 이슈가 있다.

“공격자 비용과 사용자 비용 이슈”
공격자와 사용자를 구별할 수 없고, 공격자와 사용자가 같은 수수료 정책을 적용받기 때문에 발생하는 이슈다. 이용자들을 위해서는 수수료가 낮아야 하고, 공격자들을 막으려면 높아야 하는 것은 딜레마다.

“650GB & 8일”
현재 이더리움의 전체 블록 사이즈와 블록 싱크에 소요되는 시간 (bc.daniel.net.nz)

2. 이그드라시 소개

세계수의 의미를 담고 있는 이그드라시는 모든 블록체인을 연결하는 통로이다.

이그드라시 프로젝트는 신뢰를 기반으로 모든 블록체인을 연결(Trust-based Multidimensional Blockchains)하고 인터넷 상의 모든 서비스를 블록체인(Internet re-designed by blockchains)으로 재구성하는 것을 목표로 하고 있다.

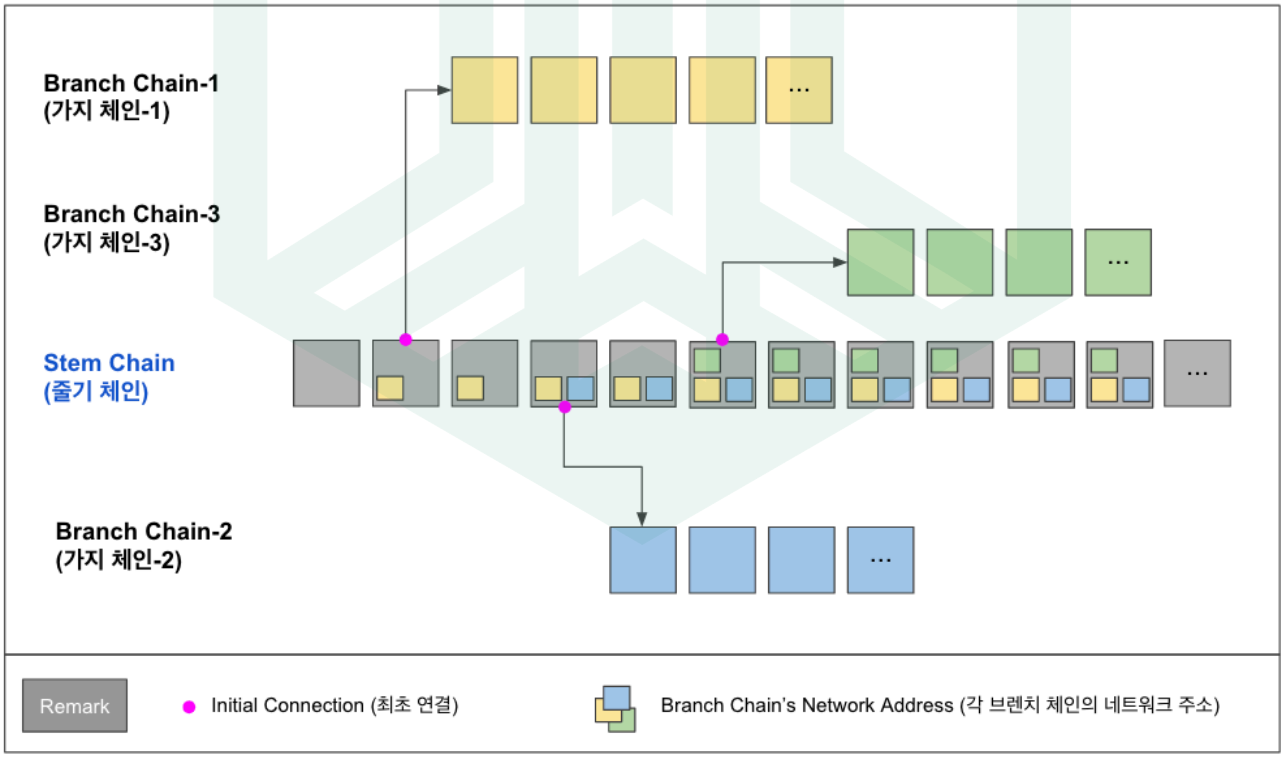
이그드라시 (Yggdrash) 어원

Yggdrash = Yggdrasil + Hash

*Yggdrasil*은 태초의 나무, 세계수, 신단수 등 신화에 나오는 전설의 나무로 인간 세상과 하늘의 세상, 지하의 세상 모두를 연결하는 통로의 역할을 하는 세계수이다.

2.1 이그드라시의 구성 요소

이그드라시는 크게 줄기 체인(Stem Chain)과 가지 체인(Branch Chain)으로 구성되며, 줄기 체인은 모든 가지 체인을 서로 통신하고 융복합할 수 있는 환경을 만들어 준다.



2.1.1 줄기 체인 (Stem Chain)

줄기 체인은 이그드라시의 근본이 되는 체인으로 모든 가지 체인의 정보를 담고 있는 정보의 집합체이자, 통로이다. 줄기 체인은 각 가지 체인의 주소 정보 등 최소한의 정보만을 저장함으로써 트랜잭션 처리 성능과 확장성에 최적화되어 있다. 또한, 각 가지 체인의 주소를 보유함으로써 각 가지 체인을 상호 연결할 수 있는 구조를 가지며 각 가지 체인의 Life-Cycle(생성/변경/파기)을 관리할 수 있다.

2.1.2 가지 체인 (Branch Chain)

가지 체인은 하나의 DApp인 동시에 하나의 블록체인이다. 가지 체인 자체가 블록체인이기에 당연히 자신들이 원하는 합의 알고리즘을 선택할 수 있으며 자신들만의 블록체인을 구성할 수 있다. 우리는 결국 하나의 가지 체인이 DAO(Decentralized Autonomous Organization) 레벨이 된다.

가지 체인을 사이드 체인과 비슷하게 볼 수 있다. 이 부분은 굉장히 중요한 개념으로 기존의 체인 간 연결은 Atomic Swap과 같은 인위적인 기술로 연결해야 했지만, 이그드라시는 가지 체인이 줄기 체인에 연결됨과 동시에 자연스럽게 다른 가지 체인을 참조 · 연결할 수 있어 각 체인 간 자산을 손쉽게 거래할 수 있는 환경이 만들어진다.
더불어 가지 체인은 각자 독자적인 블록체인으로 운영하기 때문에 특정 가지 체인의 트랜잭션 과부하, 장애 시에도 전혀 영향을 받지 않는다.

다음은 가지 체인의 유형을 소개한다.

1. 불멸 브랜치 체인 (Immunity Branch Chain)
이그드라시에서 사용되는 가지 체인이며, 이드를 소모하지 않고 목록에서 제거되지 않음

2. 소모성 브랜치 체인 (Mutable Branch Chain)
사용자가 생성하는 가지 체인이며, 일정시간마다 이드를 소모

3. 인스턴트 브랜치 체인 (Instant Branch Chain)
사용자가 생성하는 가지 체인이며, 이드를 소모하지 않고, 일정시간만 존재하는 가지 체인
(일정 수준의 신뢰도가 있는 사용자만 생성 가능)

4. 테스트, 프라이빗 브랜치 체인 (Test, Private Branch Chain)
이그드라시에 연결되어 있지 않은 가지이며, 테스트 및 프라이빗용 가지 체인
(줄기 체인은 이 체인을 알 수 없으며, 이 가지 체인의 정보를 알고 있는 사용자끼리만 공유 또는 자기 자신만 보유하는 체인)

2.1.3 주요 가지 체인 (Important Branch Chain)

1) 내부 화폐 체인 : 이드 (YEED)

우리가 사는 현실 세상에서 화폐가 필요한 이유는 무엇일까? 우리는 화폐의 본질적인 목적이 거래의 수단 이기도 하지만 사회를 유지하기 위한 큰 힘, 즉 하나의 도구라고 생각한다. 이그드라시의 화폐인 이드(YEED)는 우리 네트워크를 유지하기 위해 사용되는 하나의 도구이며, 거래의 수단이기도 하지만 이그드라시 네트워크에 연결된 수많은 블록체인 네트워크를 연결·유지하는 것에 가장 큰 목적을 두고 있다.

일반적으로 새로운 블록체인이 생성되면 이그드라시의 줄기체인에 등록되지 않는다. 자신의 블록체인을 이그드라시 네트워크에 연결하기 위해 이드를 사용하게 되며, 시간이 지남에 따라 지불된 이드는 점차 소멸될 것이다.

신규 참여한 가지 체인은 이그드라시 네트워크에 참여하면서 그동안 어렵고 힘들게 구축하였던 다양한 블록체인 자원과 서비스 파트너십을 보다 손쉽게 누릴 수 있다. 또한, 자신이 구축한 블록체인 서비스가 훌륭하다면 자연스럽게 더 많은 파트너와 사용자를 끌어올 수 있다.

2) 신뢰도 평가 체인 : 생명수 (Sacred Water)

암호화폐에서 사용자들은 왜 네트워크 수수료를 지불해야 할까? 대부분의 암호화폐에서 네트워크 수수료를 받는 이유는 다음과 같다.

1. 채굴자에게 블록 마이닝에 대한 보상을 주기 위해서이다. 또한, 블록 사이즈는 한정적인 자원으로 채굴자는 높은 수수료를 지불하는 거래를 블록에 담으려고 노력한다.

2. 악의적인 사용자를 막기 위해서이다. 만약 네트워크 수수료를 지불하지 않을 경우, 악의적인 사용자는 무한히 많은 트랜잭션을 발생시켜 해당 네트워크를 마비시키거나, 의미 없는 정보가 블록체인에 등록되게 만들 것이다.

그러면 이러한 문제를 어떻게 해결해야 할까? 페이스북 사용자가 페이스북에 글을 쓰는 것과 블록체인에 거래 내용, 혹은 데이터를 올리는 것은 거의 같은 행위이다.

이그드라시는 누구에게나 공평한 시간이라는 자원을 기반으로 신뢰도를 측정하며 이로운 사용자에게는 혜택을 악의적인 사용자에게는 제한을 주고자 한다. 이그드라시 네트워크에서 많은 시간과 이로운 행동을 할수록 신뢰 점수는 높아지고 다양한 혜택을 받을 수 있다. 그중 하나가 수수료이다.
신뢰도 점수가 높은 사용자는 우리의 네트워크를 사용하면서 어떠한 수수료도 지불할 필요가 없다. 은행에서 높은 신용도를 가지고 있는 고객이 은행의 인프라를 사용하면서 수수료를 지불하지 않는 것과 같은 맥락이다.
물론 신뢰도가 높은 사용자에게 제공될 수 있는 것은 수수료 이외에도 많이 있다.
예를 들면 신뢰도가 최상위인 참여자는 신규 이드(YEED) 발행 시, 일정 비율의 통화를 받게 되며 결과적으로 네트워크에 기여한 공로를 보상받게 되는 정책도 시행할 수 있다.

우리가 사는 현실 세계에서도 신뢰는 거래 가능한 자원인가? 우리가 신뢰한 사람이 자신의 신뢰를 어떤 누구에게도 동일하게 부여하는 것은 불가능하다.
일정 신뢰도를 달성한 사람에게는 자신의 신뢰도를 일정 부분 소모하여, 다른 사람에게 일정 비율로 부여할 수 있는 정책도 있을 수 있다. 신뢰의 전이는 부분적으로만 가능하며 이것은 커뮤니티 합의에 따라 더욱 발전· 개선 할 것이다.

이그드라시의 신뢰도를 쌓기 위해서는 이그드라시 네트워크에 기여하면서 많은 시간을 투자해야 한다.
만약 네트워크에 악영향을 끼칠 목적으로 신뢰를 쌓은 사용자는 감시시스템 또는 네트워크 참여자에 의해 발견되어 신뢰도가 차감된다.
또한, 신뢰도 정책에 의해 수수료 무료 등의 혜택이 사라지거나, 이그드라시 자원을 활용하지 못하거나, 신뢰를 쌓을 수 없도록 만들 수 있다.

이그드라시에서 가장 중요한 자산은 이드가 아니다. 많은 사람에게 혜택을 줄 수 있는 신뢰도가 최고의 자산이다. 이그드라시는 건강한 생태계를 만들고자 하는 많은 참여자에게 더 많은 혜택과 권한을 분산할 것이며, 함께 성장할 수 있는 블록체인 생태계를 만들 것이다.

3) 신뢰 점수 생성 체인 : 생명수의 샘(Sacred Water Fountain)

네트워크 참여자들의 신뢰 점수 생성은 신뢰 점수 생성 체인에서 이루어지며, 이그드라시 네트워크에 이로운 행위를 할수록 신뢰 점수가 증가하는 알고리즘으로 설계되었다. 해당 시각에 노드를 운영하지 않았을 시, 신뢰 점수는 획득할 수 없다. 또한, 악의적인 것으로 신뢰 점수를 획득하려는 사용자를 감시 및 처벌할 수 있는 시스템도 함께 운영할 것이다.

2.2 이그드라시 특장점

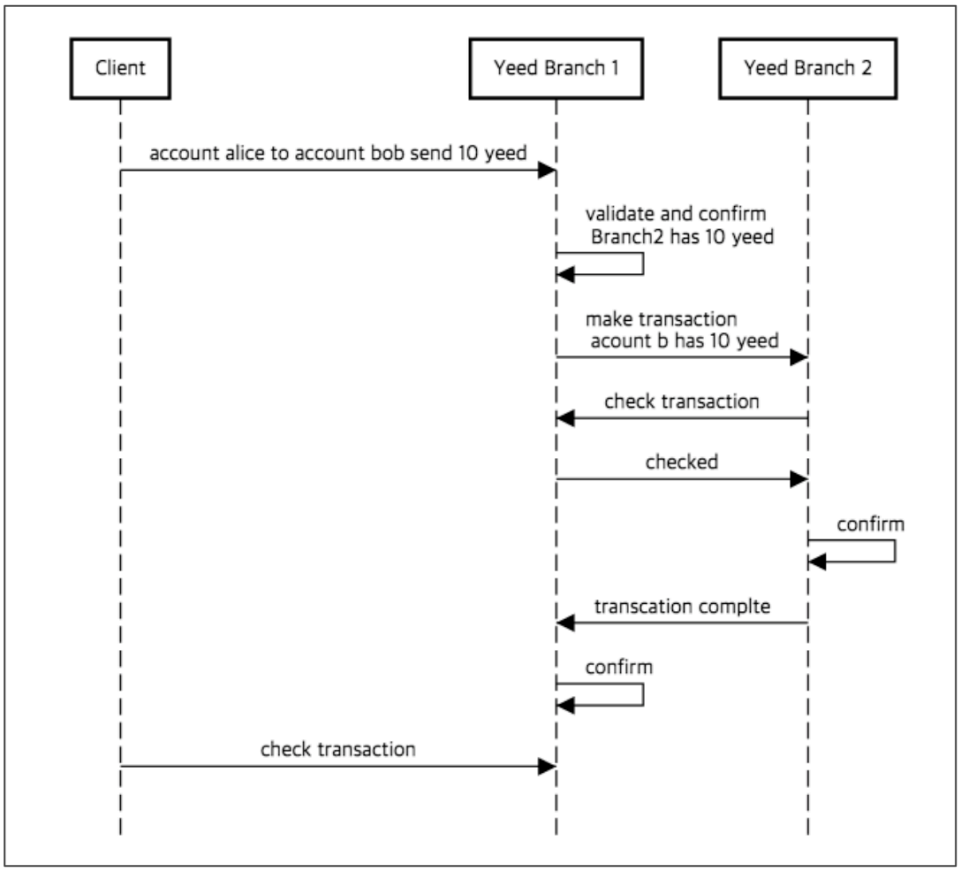
2.2.1 스마트컨트랙트 데이터 용량 문제 해결

블록체인의 분권화에 대한 가치에 더 큰 가치를 더한 것은 이더리움의 스마트컨트랙트 일 것이다. 스마트컨트랙트는 현실 사회에서 실현하지 못했던 수많은 거래를 자동화된 거래규약에 맞춰 투명하고 효율적인 세상을 만들어 갈 수 있게 해주었다. 하지만 수많은 스마트컨트랙트를 블록체인에 탑재함으로써 용량의 한계가 부닥치게 되었다.

실제 스마트컨트랙트로 이루어진 어플리케이션을 개발하면서 데이터 용량의 숙제를 풀지 못한다면 우리는 결국 원하는 비즈니스를 현실화 시킬수 없을 것이다. 그렇다면 이 난제를 어떻게 풀 수 있을까? 정답은 바로, 블록체인에 스마트컨트랙트의 무결성 정보만을 올리고 바이너리 파일은 다른 경로를 통해 받는다면 스마트컨트랙트의 용량 제한이 해소될 것이다. 또한, 스마트컨트랙트를 사용하는 언어에 제약을 받을 필요도 없고, 스마트컨트랙트 개발의 허들은 현저히 낮아질 것이다.

2.2.2 블록체인 네트워크 샤딩(Sharding)을 통한 처리 성능 향상

이그드라시는 다차원 블록체인 특징을 이용하여 네트워크 샤딩을 구현할 수 있다.



먼저 샤딩을 하고자 하는 브랜치 체인은 모두 같은 거버넌스를 가지고 있고 각각의 브랜치 체인들은 샤딩에 관련된 다른 브랜치 체인의 정보를 가지고 있어야 한다.

해당 예시는 2개의 브랜치를 가지고 샤딩을 하는 예시이며, 샤딩을 처리하는 기준은 각 브랜치 체인의 어카운트 번호를 기준으로 (예_홀수, 짝수) 가정하였다.

위와 같이 2개의 브랜치 체인으로 샤딩할 경우, Yeed Branch 1에서 Yeed Branch 1로 이동한다면 일반적일 때와 같이 1개의 거래만 발생하나 Yeed Branch 1 에서 다른 브랜치로의 이동이라면 Yeed Branch 1이 에셋을 에스크로 한 상태에서 Yeed Branch 2가 가져가는 2개의 confirm이 생기게 된다.

이를 표현하면 아래와 같다.

sharding effect = same branch 50% + other branch (3) 50% = branch sharding count / 2

해당 예제에서 2개의 브랜치 체인으로 샤딩을 한 경우이며, 해당 예제처럼 샤딩을 할 경우 샤딩의 쓰기성능(트렌잭션 처리 성능)은 1개의 브랜치 체인으로 하는 것과 동일한 성능을 올리나, 3개의 브랜치 이상으로 샤딩을 구성할 경우 점진적으로 성능이 향상된다.

이그드라시의 단일 가지 체인의 성능은 약 1,000TPS에서 10,000TPS사이로 예상하며, 블록체인 네트워크 샤딩을 통해 처리 성능을 향상시킬 수 있을 것이다.
해당 기술로 인하여 마이크로 페이먼트 같은 많은 트랜잭션 처리가 필요한 서비스도 이그드라시에서는 구현이 가능하다.

2.2.3 아카식 시스템 - BRA(Block Reassembling Algorithm)를 적용한 노드 싱크 속도 향상

현재 메인넷을 구성한 대부분의 블록체인은 스마트컨트랙트 등 자신의 블록체인에서 구현한 다양한 기능을 활용할 수 있는 풀노드(지갑)을 제공하고 있다. 하지만 대부분의 암호화폐 사용자들은 암호화폐 거래소나 라이트클라언트 노드(지갑) 서비스를 이용해 암호화폐를 거래하고 스마트컨트랙트 사용하고 있다. 왜나하면 풀노드를 구성하기가 까다롭기 때문이다. 그중 가장 큰 제약사항은 바로 모든 블록을 다운로드· 동기화 해야 하는 시간적· 경제적 이슈 때문이다.

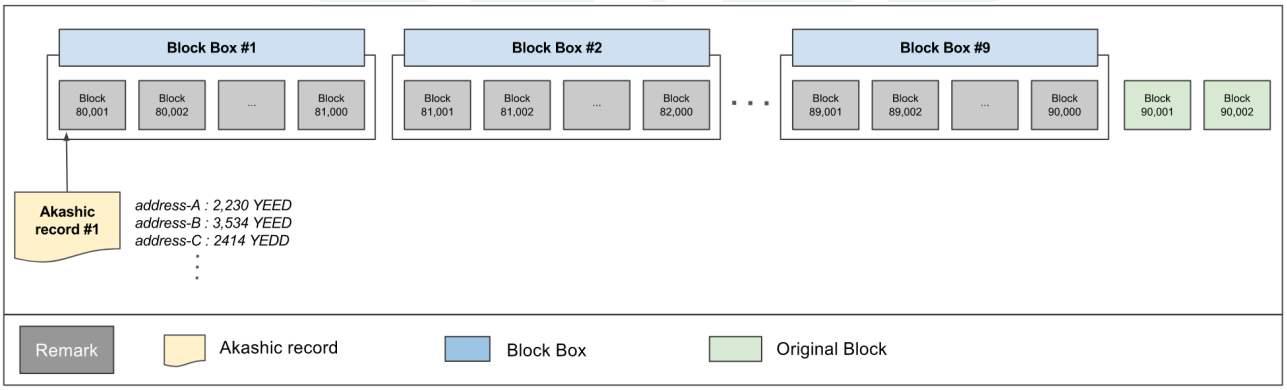
예를 들어 비트코인의 경우, 블록 동기화 시간이 약 14일, 이더리움의 경우에도 약 8일간의 시간이 필요하다(480만 블록 / 2018년 1월 기준)

다른 블록체인 플랫폼의 풀노드를 구성하고자 하는 사람들은 해당 문제 때문에 제네시스 블록부터 동기화를 하는 게 아니라 인터넷에서 공유되는 어느 정도 블록이 동기화되어있는 지갑을 P2P네트워크에서 받음으로써 동기화 시간을 절감한다. 하지만 P2P네트워크의 특성상(토렌토 등) 신뢰성이 보장되지 않은 지갑을 받음으로써 바이러스 등의 위험에 노출되는 위험을 감수해야만 한다.

이그드라시는 효율적이고 안정적인 블록 동기화를 위해 블록 재조합 알고리즘(BRA : Block Reassembling Algorithm)을 통하여 구현하고자 한다.

블록 재조합 알고리즘은 아래와 같이 3가지 구성 요소로 이루어져 있다.

- 아카식 레코드 (AR : Akashic Record) : N개의 블록 이전의, 모든 거래의 결과값의 집합
- 블록 박스 (BB : Block Box) : N개의 블록을 하나의 박스에 담은 블록들의 집합
- 블록 (OR : Original Block) : 일반적인 블록체인의 블록



아카식 레코드는 제네시스 블록부터 특정 시점의 블록까지의 모든 거래의 결과(모든 계정의 트랜잭션 결과값)를 저장한 집합이며(data checkout), 블록 박스는 여러 개의 블록을 하나의 박스에 담은 블록들의 집합이다.

BRA을 구현하기 위해서는 AR과 BB를 정해진 정책에 따라 결과값을 해싱하여 블록에 저장하고, 실제 AR과 BB의 바이너리 데이터는 이그드라시 파일 공유 네트워크에 등록된다. 실제 BRA을 이용해 노드를 싱크를 할 경우, 이그드라시 파일 공유 네트워크에서 해당 블록 데이터를 병렬로 다운로드 받은 후, 이글드라시 블록에 저당된 BRA의 해쉬값과 대조하여 파일의 무결성과 보안성을 담보 받을 수 있다.

이그드라시는 블록체인의 장점을 훼손하지 않으면서 모든 네트워크 참여자들이 더 쉽게 블록체인 네트워크에 참여할 수 있는 방법을 제시하는 것이다.
또한 BRA는 신규 노드들이 선택에 따라 풀블록을 동기화 할 것인지, 옵셔널하게 사용할 수 있다.

다음은 BRA을 이용해 실제 블록 싱크 속도를 얼마나 높일 수 있는지 예시를 만들어 보았다.

- 시나리오
  -현재 블록의 높이가 4,890,002 인 상황에서 신규로 참가하는 노드가 있다고 가정하자.

- BRA 운영 정책
  - AR (Akashic Record) : 100,000 번째 블록마다 아카식 레코드의 결과값을 저장
  - BB (Block Box) : 10,000 개의 블록마다 블록 박스를 생성

- BRA 적용 결과

◦ 이그드라시 블록 싱크 속도
1 AKASHIC RECORD + 9 BLOCK BOX + 2 REGIONAL BLOCK SYNC TIME = 약 30분

◦ 타 블록체인 블록 싱크 속도
4,890,002 BLOCK * BLOCK SYNC TIME = 약 8일

위 적용 결과와 같이 BRA는 블록 사이즈가 커지면 커질수록 블록 싱크 속도와 노드의 리소스를 최소화 시킬 수 있는 기술이다. 궁극적으로 현재 블록체인이 고심하고 있는 블록사이즈의 이슈도 함께 해결할 수 있으며, 나아가 미래의 IoT 디바이스에도 적용하여 블록체인의 실제 적용 범위를 넓혀나갈 것이다.

2.2.4 파일 공유 네트워크 (File sharing on P2P Network)를 통한 저장 용량 문제 해결

이그드라시의 파일 공유 네트워크는 스마트컨트랙트, 아카식레코드, 블록박스, 체인 리소스 등이 등록된다.
어플리케이션은 코드로만 존재하는 것이 아니라 어플리케이션을 서비스하기 위한 다양한 형태의 리소스와 함께 구동된다.

이그드라시는 파일 공유 네트워크를 통해 블록체인상의 데이터 제한에 자유를 제공할 것이며, 이를 통해 더욱 다양하고 다채로운 블록체인 서비스를 제공할 수 있을 것이다.

2.2.5 다차원 블록체인을 통한 상호운용성 보장

이그드라시를 다차원 블록체인이라고 칭하는 이유는 블록 생성 타임이 서로 다른 블록체인을 연결할 수 있기 때문이다. 서로 다른 블록체인을 연결하기 위해서는 먼저 블록체인의 시간 개념을 이해해야 한다.
비트코인은 10분당 1개의 블록이 생기며, 이것은 비트코인의 시간이다. 하지만 이더리움의 블록생성 시간은 15초이고 이는 비트코인과 같지 않다.

그렇다면 두 체인 간 어떻게 연결할 수 있을까? 이그드라시는 아카식 슬라이스(Akashic Slice)라는 체인 연결 프로토콜을 적용하여 이 과제를 해결하였다. 서로 다른 블록체인의 데이터를 교환하는 그 시점에 노드의 블록 결과를 사진을 찍듯이 저장하는 것이다. 쉽게 예를 들어, 한 사람이 창문을 통하여 밖을 바라보고 있고, 그 창문 밖으로 자동차가 지나가고 있다고 가정하자. 그 사람은 자동차의 사진을 찍음으로써 그 자동차가 창문을 지나갔다는 증거를 남길 수 있다.

만약 다른 블록체인 플랫폼이 우리가 제시하는 체인 연결 프로토콜과 프로토콜을 통해 줄기 체인에 연결할 수 있다면 우리의 네트워크 리소스(이드, 신뢰도, 다른 DApp)를 사용할 수 있을 것이고, 이는 거버넌스의 문제만 해결된다면 이미 나와 있는 블록체인 플랫폼도 이그드라시에 연결되어 하나의 가지 체인 처럼 동작할 수 있다.

2.2.6 블록체인 스타터 & 스마트 키트 (Blockchain Starter & Smart Kit)

이그드라시는 독립적인 블록체인 개발사를 위해 블록체인 개발 모듈을 제공한다. 각 모듈은 자신의 비즈니스 니즈와 경영 전략에 맞게 신속성· 유연성· 편리성을 충족시킬 수 있는 맞춤형 블록체인 개발 키트이다.

이그드라시는 블록체인 기술 발전에 기여하기 위해 블록체인 개발 키트를 위한 별도의 예산을 편성하고, 오픈 소스 환경을 구현하고자 한다. 이것은 이그드라시가 계획하고 있는 인큐베이팅 사업 중에 하나로 각 참여자의 기여도에 따라 인센티브를 지불할 것이다.
블록체인 기술에 관심이 있거나 공헌하고 싶은 사람은 누구나 참여할 수 있고, 이 기술은 누구나 자유롭게 사용할 수 있다.

블록체인 개발 키트를 2가지 형태로 구성하였다.

블록체인 인프라 개발 키트는 블록체인의 기본이 되는 요소들을 모듈화하여 블록체인 비기너들이 자신들의 비즈니스를 블록체인상에 빠르고, 신속하게 적용할 수 있도록 도와준다.

1. **블록체인 인프라 개발 키트 (Blockchain Starter Kit)**
   - 합의 알고리즘 (PoW, PoS, PoI 등)
   - 암호화 알고리즘 (ECDSA, Hash 등)
   - 자료 구조 (Merkle tree, Patricia tree 등)
   - 노드/지갑 구성 (Full node, Light node, Web node 등)
   - 특화 기능 (Smart Contract, Zero-Knowledge Proof 등)

블록체인 스마트 키트는 샤딩, 라이트닝 네트워크 등 블록체인의 한계점을 극복하기 위한 신기술 개발과 인공지능, 사물인터넷, 유전학 등의 4차 산업에 블록체인이 적용될 수 있도록 기여할 것이다. 이그드라시는 이러한 환경을 만드는 작은 동기를 부여할 뿐이고, 블록체인에 대한 열정과 역량을 겸비한 참여자들이 이를 통해 인류에 기여할 수 있는 선구자가 되기를 기대한다.

2. **블록체인 스마트 키트 (Blockchain Smart Kit)**
   - 확장성 기술 (Sidechain, Sharding, Lightning Network 등)
   - 상호운용성 기술 (Multidimensional Blockchain, Atomic swap 등)
   - 데이터 용량 절감 기술 (Akashic Record, Block Box, File sharing on P2P Network 등)
   - 4차 산업혁명 기술 (Big Data, IoT, AI, RT 등)

2.3 이그드라시 거버넌스

2.3.1 합의 알고리즘

블록체인은 불특정 다수의 P2P 네트워크 환경에서 구동되기 때문에 "정보 도달의 시차, 시스템의 오동작과 장애 그리고 데이터의 위변조"의 과제를 해결해야 한다.
합의 알고리즘은 이와 같은 환경에서 네트워크 참가자가 단일 결과에 도달할 수 있도록 각 노드에서 만든 블록의 정당성을 검증하고, 이를 전체 네트워크에 공유하기 위해 고안된 것이다.

비트코인은 PoW(Proof of Work)란 계산량에 근거한 합의 알고리즘으로 최초로 P2P 네트워크상에서 누구나 참가 가능한 전자화폐시스템을 실현했다. 그러나 블록체인이 분기되는 구조를 가짐으로써 짧은 체인을 사용하고 있던 노드가 긴 체인으로 전환되면 계좌 잔액이 변경되거나 거래 자체가 없었던 일이 되는 경우가 종종 있다. 비트코인은 이런 현상을 방지하기 위해 거래가 확정되더라도 6블록 가량 기다리지 않으면 다음 거래를 할 수 없는 등 제한을 설정하고 있는 지갑도 존재한다. 이는 파이널리티(데이터의 완결성)가 불확실한 것으로 금융 기관에서 비트코인을 도입하기 힘든 이유 중 하나이다. 또한, 분산화된 데이터의 신뢰성을 검증하기 위해 복잡한 연산이나 다수의 노드 합의 시간도 타 합의 알고리즘보다 길어진다. 이로써 처리 성능(응답 시간과 처리량)을 올리는 것이 어려우며 무엇보다 실시간으로 처리해야 하는 업무는 기본적으로 적합하지 않은 구조를 가진다.

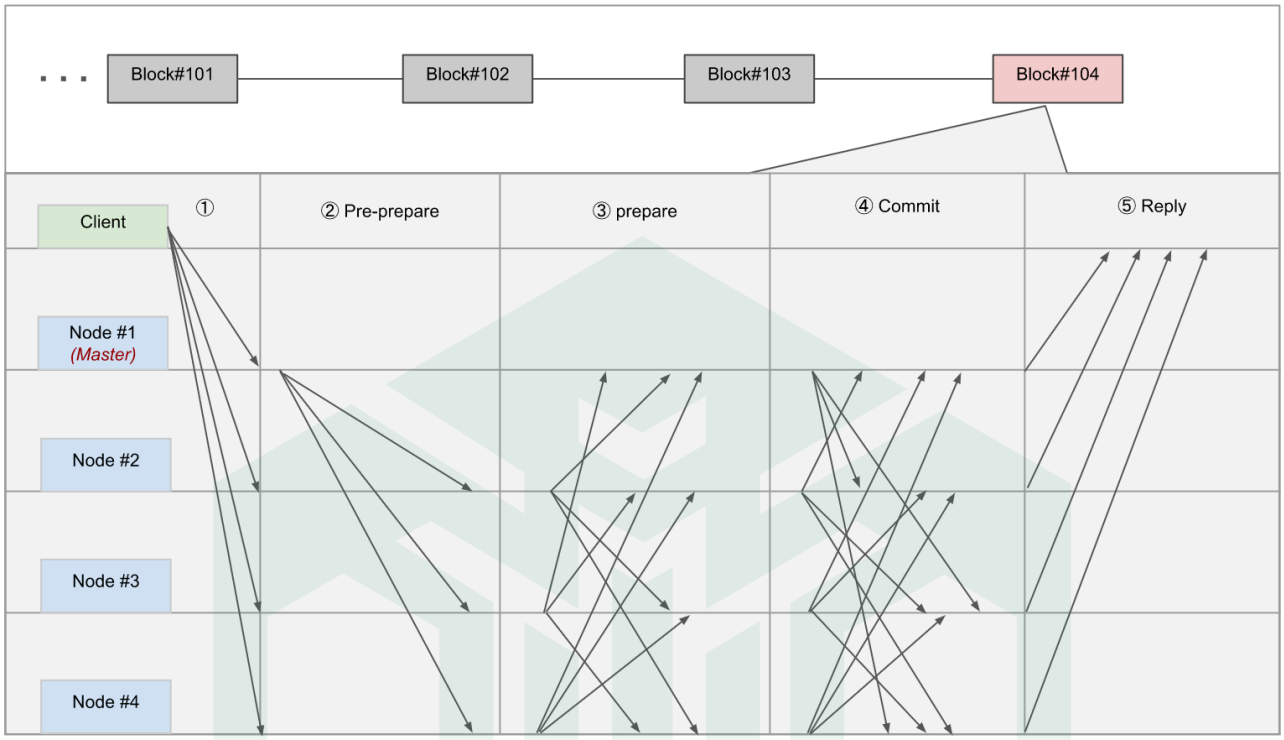
이더리움의 경우 PoS(Proof of Stake)를 적용 중에 있으며, 이 알고리즘은 화폐를 더 많이 보유한 노드가 우선하여 블록을 생성하는 것이 특징이다. 이것은 "대량의 통화를 소유하고 있는 노드는 그 통화 가치를 지키기 위해 시스템의 신뢰성을 손실하지 않을 것이다."라는 전제를 바탕으로 하고 있다. 기본적인 구조는 PoW와 다르지 않으며 화폐의 양에 따라 해시 계산의 난이도가 낮아지기 때문에 PoW보다 노드의 자원소비나 처리 속도면에서 개선된 모델이라고 할 수 있다. 하지만 PoW와 PoS 모두 파이널리티의 불확실성과 성능 문제는 여전히 해결해야 할 과제로 남게 된다.

이그드라시는 PBFT(Practical Byzantine Fault Tolerance)기반의 DPOA(Delegated Proof Of Authority)로 설계하여, PoW와 PoS가 가진 파이널리티와 성능 문제를 개선할 수 있다.

먼저 PBFT(Practical Byzantine Fault Tolerance)에 대해서 알아보도록 하자.

PBFT는 노드의 참가자 중 1명이 마스터 노드(Master Node)가 되고 자신을 포함한 모든 노드에 블록 처리 요청을 보내며, 그 요청에 대한 결과를 집계한 뒤 다수의 값을 사용해 블록을 확정한다.
만약 부정한 노드 수를 N개라고 하면 노드 수는 3N+1개여야 하며, 확정에는 N+1개 이상의 노드가 필요하다.

다음은 PBFT의 블록 처리 과정을 도식화 하였다.



PBFT 처리 절차

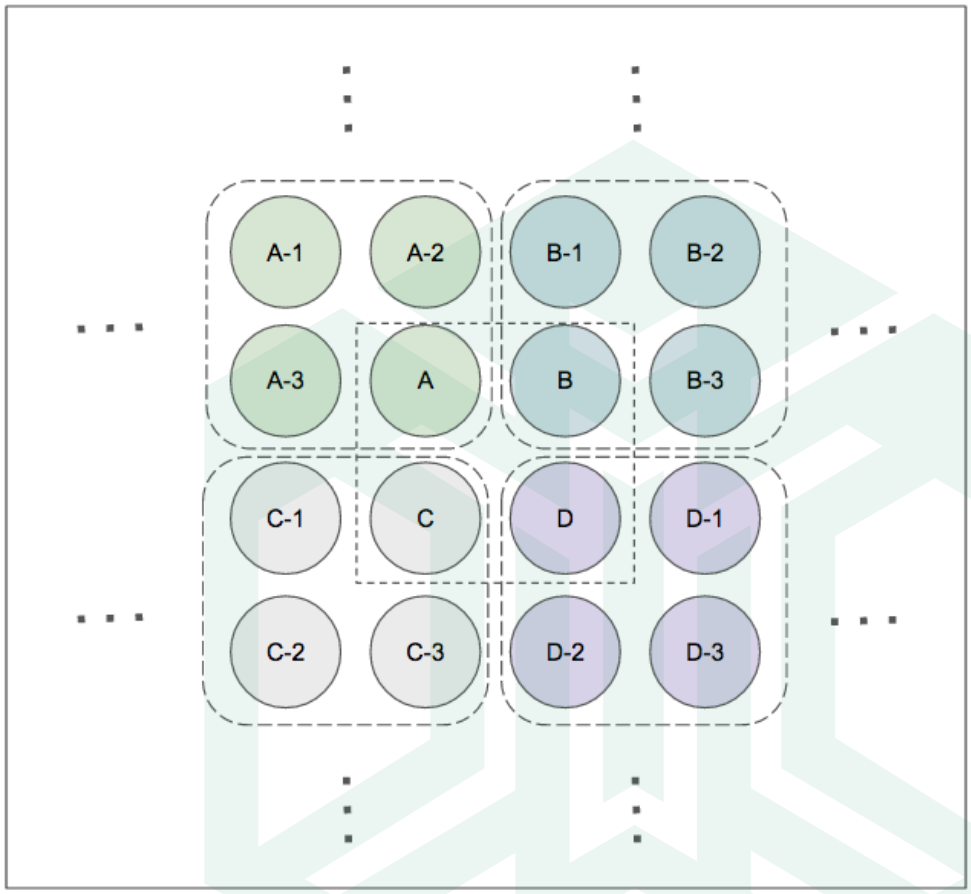
① 클라이언트가 모든 노드에 요청을 브로드캐스트
② Node#1(Master)가 되고 순차적으로 명령을 다른 노드에 전달
③ 각 노드는 ②의 명령을 받으면 Node#1(Master)를 포함한 모든 노드에 회신
④ 각 노드는 ③에서 전달된 명령을 일정 수 이상(2N) 수신하면 Node#1(Master)를 포함한 모든 노드에 수신한 신호를 전송
⑤ 각 노드는 ④에서 보낸 명령을 일정 수 이상(2N) 수신하면 명령을 실행하고 블록을 등록해 Client에 Reply를 반환

PBFT는 PoW나 PoS와 달리 다수결로 의사결정을 한 뒤 블록을 만들기 때문에 블록체인의 분기가 발생되지 않는다. 다시 말해서, 한 번 확정된 블록은 변경되지 않기 때문에 파이널리티를 보장받을 수 있게 되는 것이다.(블록체인의 분기가 발생할 수 없는 구조임)
또한 PoW나 PoS와 같이 특정 조건을 만족시킬 때까지 연산을 반복하지 않기 때문에 성능적으로도 매우 우수한 알고리즘이다.

하지만 PBFT에도 단점은 있다. PoW, PoS는 노드가 1개만 남아 있더라도 블록체인이 운영되지만 PBFT는 일정 수 이상의 노드를 충족해야지만 블록체인이 운영된다는 것이다. 즉, 마스터 노드의 단일 실패점을 해결해야 한다는 것이다.

이그드라시는 이 과제를 노드의 계층화(마스터 노드 & 하위 노드)를 통해 해결할 수 있도록 설계하였다. 기본적으로 블록 검증은 정해진 알고리즘(Round robin 방식 및 시계열 방식 등)에 따라 10초마다 블록을 생성하도록 설계하였으며 이 블록 생성 타임은 테스트 넷 과정을 통해 가장 최적의 시간으로 조정될 수 있다.

각 마스터 노드는 이그드라시 권한 위임 정책에 따라 자신의 대표 권한을 소속된 하위 노드에 위임함으로써 일정 수 이상의 노드를 유지함과 동시에 단일 실패점(single point of failure)을 개선할 수 있도록 설계하였다.



위 도식화는 이그드라시의 노드 운영 구성을 묘사한 것이다. 노드 중 A-D 알파벳으로 표현한 것은 마스터 노드이며, 알파벳-숫자로 표현된 노드는 해당 마스터 노드의 하위 노드이다. 노드의 블록 생성은 짜여진 알고리즘에 의해 랜덤하게 구동되며, 특정 노드의 장애 또는 지연 등이 발생했을 때, 권한 이양 프로세스가 구동되어 즉각적으로 구동하기 때문에 장애에 매우 강력한 내성을 가지는 구조이다.
또한, 노드의 권한으로 부정 사용을 하고자 해도 과반수 이상을 획득해야 하며, 마스터 노드가 거짓말을 한다 해도 모든 참가자가 마스터 노드의 움직임을 감시해 부정 행위라고 판단되었을 시, 다수결로 마스터 노드를 교체할 수 있다.

다음은 이그드라시의 합의 알고리즘인 위임된 권한 증명 방식(DPOA; Delegated Proof Of Authority)를 소개한다. 퍼블릭 블록체인은 기본적으로 신뢰할 수 없는 불특정 다수의 노드로부터 합의를 끌어내야 한다. 비트코인은 “작업량을 기준”으로, 이더리움은 “보증금을 담보”로 블록을 보증하도록 설계되었다.
기본적으로 블록체인은 익명성을 기반으로 한 시스템으로 해당 어카운트의 신뢰성을 측정하기 어렵다.
하지만 이그드라시의 어카운트는 현실 세계와 유사한 신뢰도를 적용받음으로써 인터넷 또는 블록체인상의 또 다른 디지털 신분을 만들어 갈 수 있다.

이그드라시는 1) 신뢰할 수 없는 블록체인 세상에서 신뢰를 쌓아갈 수 있는 블록체인 세상을 만들고자 한다. 2) 그 신뢰는 이그드라시의 가지 체인인 신뢰도 평가 체인에서 각 노드의 행위에 따라 증감 또는 차감된다. 3) 이그드라시의 마스터 노드는 오랜 기간동안 가장 많은 공헌을 한 노드, 즉 신뢰도가 가장 높은 노드로써 이그드라시 네트워크에서 그 신뢰성을 검증받은 노드가 마스터 노드 그룹의 투표로 임명될 것이다. 4) 이로써 각 마스터 노드는 이그드라시 줄기 체인의 “블록 보증”과 이그드라시 네트워크의 정책을 제안, 개정, 결정 등을 할 수 있는 가장 중요한 “권한"을 가지게 된다.

이그드라시는 신뢰할 수 없는 환경에서 신뢰할 수 있는 환경으로, 당장 이익을 쫓는 참여자에서 장기적으로 이로운 비전을 추구하는 참여자로 구성된 블록체인 생태계를 만들고자 한다.

2.3.2 마스터 노드의 거버넌스

마스터 노드는 이그드라시 자체 신뢰도 평가 체인을 통해 선출되며, 마스터 노드의 3/4이 참여하고, 과반수가 찬성하여야 최종 마스터 노드로 임명된다. 마스터 노드 그룹은 이그드라시 생태계의 운영 정책, 네트워크 참여자들의 상벌 정책, 그리고 YEED의 통화 정책 등을 투표 및 결정할 수 있다. 또한, 마스터 노드의 권한은 ‘권한 위임 모델'에 따라 마스터 노드를 위임, 이양, 퇴출 할 수 있다.
이그드라시의 마스터 노드는 안정성과 보안성을 기준으로 각 대륙별로 분산화하여 구성할 예정이며, 마스터 노드의 수는 테스트넷 과정을 통해 가장 이상적인 숫자를 산정할 것이다.

2.3.3 마스터 노드의 인센티브

이그드라시는 다차원 블록체인의 정책으로 직접 금전적 보상은 취할 수 없는 구조이다. 하지만 이그드라시의 마스터 노드로서 명예와 YEED가 소모되지 않는 불멸 체인의 제안, 수수료 무료 등의 혜택을 받을 수 있다.
이그드라시 마스터 노드는 블록 검증 미참여, 정책 미참여 등의 규칙 위반, 증거가 불분명한 악의적 행위 시 마스터 노드의 이양, 중지 등이 될 수 있으며, 악의를 품고 부정행위를 할 경우 즉시 퇴출당할 것이다. 또한, 대표자 노드의 침해 여부를 신고하고, 그 신고가 인정받았을 경우, 해당 대표자는 비활성화될 것이며, 신고인은 신고 정책에 따라 일정 비율만큼의 보상을 받을 수 있다.

2.3.4 이그드라시 화폐(이드, YEED)의 정책

이드는 이그드라시 내부에서 사용하는 화폐로써 최초 100억 개가 발행된다. 최소 1년 동안 이드의 소각만 일어나게 될 것이며, 전체 발행량은 점점 줄어들 것이다. 이그드라시는 네트워크 참여자의 신뢰도에 따라서 거래 수수료가 차별화되며, 일정수준 이상의 신뢰도를 쌓은 계정은 거래 시 수수료가 무료이다.

이드의 가장 큰 용도는 신규 가지 체인을 생성하고 유지하기 위해 사용된다. 이드의 양 만큼 가지 체인의 생명력이 부여되고, 시간이 지남에 따라 그 이드는 점점 소멸된다. 이그드라시의 생태계가 발전되고 풍성해 짐에 따라 이드의 가치와 이그드라시의 줄기 체인과 가지 체인은 함께 성장한다. 신뢰도가 낮은 계정의 수수료는 이그드라시 인큐베이팅 예산으로 사용되며, 이는 이그드라시 생태계를 더욱 성장하게 한다.

2.4 USE CASE

2.4.1 분산형 거래소 (DEX : Decentralized Exchange)

말 그대로 “분산화된 거래소" 이다. DEX에서는 코인의 모든 입출금은 블록체인에서만 이뤄진다. 거래소가 제공하는 토큰화된 내부 지갑이 아닌 블록체인 상에서 직접 접속하는 이그드라시의 개인 지갑에서 바로 거래할 수 있다. 분산화된 거래소는 입출금을 임의로 막는 등의 임의 조작 및 해로운 행위가 불가능하며 기존의 중앙화된 거래소의 코인 해킹 문제 및 개인정보 유출 등에 자유롭다.
이그드라시 DEX 거래소는 기존 중앙 집중식 거래소가 가진 접속 지연, 해킹 위험, 신뢰성 이슈를 개선한 안전한 탈중앙 거래소의 게임체인저가 될 것이다.

2.4.2 댑 스토어 (DSB : DApp Store Of Blockchain)

이그드라시의 가지 체인은 하나의 블록체인인 동시에 DApp 이다. 기존의 이더리움의 경우, A라는 DApp을 실행하기 위해서 전혀 상관없는 B, C, D를 모두 다운로드 해야 되는 Data 저장의 비효율성이 이슈가 된다.
하지만 이그드라시는 각 DApp이 하나의 블록체인이자 독립된 서비스이기 때문에 특정 DApp에 관련된 가지 체인만 다운로드를 하면 된다. 이것은 토렌트에서 스타워즈 영화를 다운받기 위해 토렌트 전체 영화를 다운받지 않아도 되는 것과 같은 맥락이다. 더불어 이그드라시는 다차원 블록체인으로 이그드라시 네트워크에 연결된 모든 DApp을 사용자들이 쉽고 편리하게 이용할 수 있게 Apple의 App Store와 같은 환경을 제공하게 된다. 여러분은 어떤 모습이 상상되는가? 여러분들이 상상한 바로 그 모습이 이그드라시의 DApp Store가 될 것이다.

2.4.3 가까운 미래의 일상

다음은 우리가 생각하는 가까운 미래에 한 상황이다.

피터가 비즈니스 미팅이 생겨 스마트폰의 스케줄에 미팅 장소와 시간을 기록했다. 미팅 장소에 가기 위해 건물을 나오면 건물 앞에 자율주행차가 대기하고 있다. 차에 올라타면 자율주행차는 최적의 경로로 미팅 장소를 향해 주행한다. 주행 완료 후에는 자율주행차를 내려 미팅 장소로 향한다.

이그드라시가 위 상황에서 어떻게 동작할까? 미팅일정을 기록하는 순간 스마트폰에 탑재된 이그드라시는 가장 근처에 있는 자율주행차를 호출한다. 가장 가깝고 평판이 좋은 자율주행차가 할당되면 자율주행차는 즉시 목표지점으로 도착하여 피터를 기다린다. 피터가 탑승한 순간 비용이 기록되며 도착지에 도착하는 즉시 비용이 결제된다. 결제가 이뤄지는 순간 자율주행차에 관한 평판이 상승하며 자율주행차 가지 체인의 토큰을 가진 비율만큼 해당 계정에 수익은 자동으로 배분이 된다. 즉 자율주행차에 투자하고 싶은 사람은 특정 자율주행차 가지 체인의 토큰을 사들여 투자할 수 있다.

만약에 피터가 나타나지 않는다면 피터에 대한 평판점수는 깎이게 되며 자율주행차를 호출하는 데에 비용이나 대기시간이 증가하는 불이익이 발생하게 된다.

3. 이그드라시 핵심 및 결론

3.1 What kind of, Discriminate, Blockchain? (어떤, 차별점이 있는, 블록체인?)

이그드라시의 핵심 메커니즘은 1) 분산화로 인해 태생적으로 느린 처리 속도(중앙화 시스템보다 상대적으로 느릴 수밖에 없는)와 2) 불특정 다수의 검증 노드에 의지하여 블록체인 네트워크를 유지할 수밖에 없는 경제적 인센티브의 이슈 3) 지속적으로 증가하는 블록체인 용량과 블록 싱크 속도를 인정하고, 이를 극복하기 위해 가장 현실적이고 실현 가능한 방법을 제시하고자 한다.

3.1.1 각 블록체인의 독립성과 처리 성능 보장

1) 메인 체인 처리 성능 최적화

이그드라시의 줄기 체인은 모든 가지 체인의 연결하는 통로로서 역할을 하며 다음과 같이 처리 성능/용량에 최적화를 구현하였다.

- **블록 데이터 크기 경량화**
  줄기 체인이 보유하는 데이터는 각 가지 체인의 주소 정보 등 최소한의 정보만을 저장하여 데이터 크기 자체를 최소화 하였으며, 시간이 지남에 선형적으로 증가되는 데이터 크기 이슈를 경감시켰다.

- **블록 생성의 합의 절차 및 방법 최적화**
  우리는 DPOA(Delegated Proof Of Authority) 합의 알고리즘을 적용하였다. 본 합의 알고리즘은 안정성· 신뢰성을 기반으로 설계되었으며 합의 절차/연산/시간의 간소화 및 합의 참여자 수를 최적화하여 처리 속도를 향상했다.

2) 각 블록체인(DApp)은 자신만의 독립적인 네트워크, 거버넌스 보장

각각의 모든 블록체인은 어떤 상위 체인에 종속되지 않고, 자신만의 독립적인 블록체인 네트워크, 거버넌스, 데이터, 코인, 서비스 등을 가져야 한다. 자신에게 필요하지 않은 다른 블록체인(DApp)의 데이터를 보유하고, 그 데이터를 유지하는데 리소스를 사용하지 말아야 한다. 또한, 다른 체인의 거래 지연 등으로 인해 자신의 서비스 및 네트워크에 영향을 미쳐서는 안 된다.

우리는 줄기 체인과 가지 체인이라는 개념을 도입하여 이 문제를 해결하였다. 요약하자면 각 블록체인 서비스의 특성과 목적에 따라 별도의 블록체인으로 구성하여 일반 사용자들이 블록체인 상의 DApp을 이용할 때 지연 없는 서비스를 받을 수 있다. 이를 통해 진정한 의미의 DApp이 구동되는 환경과 서비스되는 생태계가 만들어질 것이다.

3) 이그드라시 네트워크 참여자들을 위한 다양한 블록체인 기술 · 서비스 도구 제공

이그드라시는 각 가지 체인의 처리 성능 및 블록체인 비즈니스 플레이어들에게 다양한 기술 서비스를 제공한다.

- 블록체인 네트워크 샤딩(Sharding)을 통한 처리 성능 향상

- BRA(Block Reassembling Algorithm)를 적용한 노드 싱크 속도 향상
- 파일 공유 네트워크(File sharing on P2P Network)를 통한 데이터 저장성 향상
- 스마트 컨트랙트 데이터 저장성 향상
- 블록체인 스타터 & 스마트 키트 (Blockchain Starter & Smart Kit)를 통한 블록체인 서비스 적용 편의성· 효율성 향상

3.1.2 이기적인 채굴 경쟁 해결 및 신뢰 기반의 경제적 인센티브 보장

1) 이기적인 채굴 경쟁 체제 해결

퍼블릭 블록체인 상에 블록 합의를 담당하는 노드(=채굴자)는 블록체인을 유지하기 위한 가장 중요한 요소이다. 하지만 처리해야 할 트랜잭션이 많아짐에 따라 거래 수수료가 가장 높은 트랜잭션을 담기 위한 노드(=채굴자)의 이기적인 경쟁이 발생하고 있다.

이그드라시는 DPOA를 적용하여, 이기적인 채굴 경쟁 문제를 해결할 수 있다. 이그드라시 블록체인 검증자는 PoW, PoS처럼 암호화폐로 인센티브를 받는 것이 아니라, 우리 이그드라시 네트워크의 정책을 결정할 수 있는 권한을 가지게 된다. 그러기 때문에 이그드라시의 블록 검증자는 경제적 인센티브로 인한 이기적인 채굴을 하지 않으며, 우리 네트워크를 더 건강하고 풍성하게 만드는 일에 기여할 것이다.

2) 신뢰 기반의 경제적 인센티브 보장

이그드라시에는 각 가지 체인과 사용자들의 신뢰도를 평가하는 별도의 가지 체인(신뢰도 가지 체인)이 존재한다. 이 체인은 누구에게나 공평한 “시간”이라는 자원을 기반으로 신뢰도를 측정하고, 악의적인 사용자는 징벌을, 선의적인 사용자에게는 수수료 면제 등의 경제적 인센티브를 보장하도록 설계하였다.

3.1.3 블록체인 간 상호연동· 확장성 보장

이그드라시는 각 블록체인의 비즈니스 요구에 따라 다른 블록체인을 연결할 수 있는 블록체인 플랫폼이며 줄기 체인과 가지 체인이 그 역할을 담당한다. 줄기 체인은 우리가 구글을 검색할 때, 도메인 서비스를 사용하는 것과 같이 우리 이그드라시 네트워크에 연결된 모든 가지 체인의 정보를 가지고 있다. 가지 체인은 줄기 체인이 보유한 각각의 가지 체인의 정보 중에 자신들의 비즈니스에 필요한 서비스를 선택하여 본인의 비즈니스와 연결할 수 있다.

위에서 설명한 각 블록체인의 독립성, 경제적 인센티브의 보장, 그리고 다른 블록체인 비즈니스가 연결 가능할 때, 비로소 진정한 의미의 자유 경쟁 시장이 시작될 것이다.

초기에는 각 블록체인이 자신만의 블록체인과 서비스를 만드는데, 시간을 집중해야 할 것이다. 이후 각 블록체인은 우리 이그드라시에 있는 다른 훌륭한 블록체인 서비스를 발견하게 될 것이고, 서로 간의 연결을 통해 또 다른 형태의 비즈니스 모델을 만들 수 있다는 것을 경험하게 될 것이다. 이러한 융복합 서비스가 늘어날수록 우리 네트워크는 더욱 풍성해질 것이고, 이를 사용하는 이용자들은 우리의 블록체인 생태계에 매료될 것이다.

3.2 What kind of, Incentive, TO ME? (나에게, 어떤, 인센티브를?)

이그드라시는 모든 블록체인 생태계 참여자가 경제적 인센티브를 받을 수 있도록 설계하였다. 부와 권력을 가진 누군가가 독점하는 것이 아닌, 모든 네트워크 참여자가 투명하고, 공정하고, 합리적인 블록체인 생태계를 만들어 가는 것을 목표로 한다.

3.2.1 암호화폐 개발자

타 블록체인의 트랜잭션 지연 등을 고려하지 않고, 자신의 비즈니스 일정에 따라 서비스를 개발 및 제공할 수 있다. 자신의 비즈니스 전략에 따라 각 가지 체인을 연결할 수 있으며, 아토믹 스왑 등과 같은 별도의 체인 연결 등에 드는 개발 리소스를 없앨 수 있으며 이그드라시에서 제공되는 다양한 블록체인 기술들을 활용할 수 있다.

3.2.2 암호화폐 채굴자

가지 체인 채굴자: 이그드라시에서 제공하는 체인 신뢰도 정보를 기반으로 신뢰성 있는 체인을 선별할 수 있으며 이에 따라 채굴자는 안정적인 채굴 수입을 보장받을 수 있다.
이그드라시 전체: 많은 채굴자의 유입으로 가지 체인을 포함한 이그드라시 체인 전체의 안정적인 네트워크 생태계를 만들 수 있다.

3.2.3 암호화폐 사용자 (투자자 or 서비스 사용자)

이그드라시에서 제공하는 신뢰도 체인 정보를 기반으로 신뢰성 있는 블록체인 서비스를 선별할 수 있으며, 투자자에게는 안정된 투자율을, 서비스 이용자에게는 안정적인 서비스를 받을 수 있는 환경을 제공한다. 또한, 신뢰도가 높은 이용자는 수수료 면제 등의 부가적인 혜택을 받을 수 있다.

3.2.4 암호화폐 서비스 제공자

이그드라시에서 제공되는 블록체인 스타터 & 스마트 키트 (Blockchain Starter & Smart Kit)를 이용하여 자신만의 서비스를 보다 신속하고 효율적으로 구현할 수 있으며, 이그드라시에 연결된 풍부한 블록체인 서비스를 연결하여 지속적이고 확장 가능한 다양한 융복합 서비스를 만들 수 있다.

3.2.5 암호화폐 거래소

이그드라시 신뢰 평가 정보를 이용하여 특정 체인(코인)의 문제로 인한 거래소· 거래소 사용자의 피해를 사전에 인지하고 예방할 수 있다. 또한, 규격화된 지갑 모듈을 받아 코인 상장 등에 드는 개발 리소스를 최소화하고, 거래소 자체의 코인 상장/운영 등의 비즈니스 전략을 맞게 거래소 이익을 극대화할 수 있다.