Version 2.0

POLARIS

Privacy-preserving,
Instant-deployable, Industry-ready
Decentralized Application Platform

Position Paper

POLARIS Foundation | polaris@polaris.io
Copyright © 2018 POLARIS Foundation

POLARIS

시작하며 **4**

왜 POLARIS 인가요? 4

탈중앙화 플랫폼의 “Red Hat®” 5

POLARIS 생태계, "Universe” **6**

법은 “Universe" 안에 있습니다 6

블록생성자-중재자 회담 6

공개 투표 체계 7

DApp 개발 지원 8

스파클 합의 체계 **9**

전문성 증명 9

빠른 합의와 즉시 이루어지는 완결성 10

PBFT와 난수로 선택되는 검증자 10

비동기적 검증을 통한 즉각적인 완결성 11

알려진 공격에 대한 대비 11

POLARIS 멀티버스 **13**

POLARIS 탈중앙화 그리드 14

탈중앙화 그리드에서 동작하는 Blockchain-as-a-Service 14

다중체인 메인넷 14

프라임 체인 15

컴패니언 체인 15

POLARIS 협력 그리드 16

체인간 합의 17

사생활 및 데이터 보호 **18**

사생활 보호를 위한 기술들 18

코인조인 18

링 시그니쳐 19

영지식증명 19

비대칭 암호 21

트랜잭션 노출 방지 21

스마트 컨트랙트 노출 방지 22
익명 메시지 프로토콜 22
분산화된 저장 금고 23
보호된 개인 인증 24
탈중앙화 연산 26
POLARIS 연산 그리드 27
온 체인과 오프 체인 27
연산 노드 27
오프 체인 트랜잭션 생성 28
오프 체인 트랜잭션 처리 29
보상과 벌칙 31
알려진 공격에 대한 대비 32
컴포넌트로 이루어진 유연한 플랫폼 33
컴포넌트로 이루어진 코어와 플랫폼 33
다양한 산업군을 위한 프레임워크 33
스스로 개정되는 플랫폼과 거버넌스 34
거버넌스를 구축하기 위한 기술 34
스스로 이루어지는 개정 35
DApp 개발과 개발 도구 36
개발 도구, "Chain Forge” 36
즉시 이루어지는 배포 36
스마트 컨트랙트를 위한 다양한 프로그래밍 언어 지원 36
컨설팅과 기술 지원 37
연구와 기술의 발전 38
EOSIO 로 부터 38
기술을 대하는 자세 38
추가적인 개발 목표들 39
믿을 수 있는 오라클 플랫폼 39
탈중앙 저장소 41

다른 개발 목표 42

이정표 **43**

면책조항 **45**

참조 **47**

시작하며 (Introduction)

우리는 아직 탈중앙화로의 도전을 시작하는 지점에 서 있습니다. 지식과 성과를 공정하고 투명하게 나누기 위한 이 여정에 많은 프로젝트들이 참여하고 있고, 지금도 서로 협력하며 발전해나가고 있습니다. POLARIS는 선구적인 프로젝트들의 업적에 감사하며, 더 나은 탈중앙화 세상을 만들기 위한 새로운 도전을 시작하려 합니다.

북극성(polaris)은 언제나 같은 방향을 알려주는 별입니다. POLARIS 프로젝트는 긴 탈중앙화로의 여정에서 북극성과 같은 나침반이 되어 건강한 탈중앙화 생태계를 만들어 가기 위한 길잡이가 되겠습니다. 이 성명서(position paper)는 POLARIS의 완성이 아니며 이를 읽는 모든 사람과 함께 건강한 생태계를 만들어 가기 위한 바탕이자 시작점입니다.

왜 POLARIS 인가요? (Why POLARIS?)

블록체인(blockchain)[1] 또는 DAG(directed acyclic graph)[2]은 탈중앙화를 위한 도구일 뿐 탈중앙화의 주인공은 "탈중앙화 어플리케이션(Decentralized Application, 이하 DApp)"과 사용자입니다. 많은 프로젝트들이 기술의 발전 그 자체에만 집중하고 있지만 POLARIS는 앞선 기술을 담은 플랫폼과 함께 정말 좋은 DApp 생태계를 만들고자 합니다. 그 목표를 위해 많은 프로젝트들을 살펴보았고 몇 가지 꼭 해결하고 싶은 주제들을 정하였습니다.

- 좋은 정책에 대한 아이디어가 있다면 누구나 편리하게 제안할 수 있어야 하고 공정하게 논의되어 빠르고 효율적으로 결정되어야 합니다.
- 정책과 계획에 대한 합의는 투명하게 진행되고 공개되어야 하며 합의된 결과에 대해서는 네트워크의 중단 없이 최대한 반영할 수 있어야 합니다.
- 좋은 DApp에 대한 아이디어와 그 아이디어를 실현할 수 있는 좋은 구성원이 있다면, DApp을 운영할 자금이나 자원에 대한 걱정 없이 운영할 수 있어야 합니다. 또한 공익적인 목적의 DApp 역시 투명한 절차를 통한 지원을 바탕으로 운영할 수 있어야 합니다.
- 리눅스의 Red Hat®[3]처럼 탈중앙화 생태계에도 DApp 및 탈중앙화 서비스 개발에 대한 조언(consulting)을 얻고 기술 지원(technical service)을 받을 수 있는 믿을 수 있는 창구가 있어야 합니다.

---

[1] 블록체인(blockchain) : https://en.wikipedia.org/wiki/Blockchain

[2] DAG(directed acyclic graph) : https://en.wikipedia.org/wiki/Directed_acyclic_graph

[3] Red Hat® : *Red Hat* is the North Carolina based Linux distribution producer founded in 1993, which assembled the *Red Hat Linux*. (https://www.redhat.com/en)

- 하나의 플랫폼(platform) 위에서 충분한 유연함을 부여하여 하나의 DApp 만을 위한 체인, 특정 용도를 위한 체인에 대한 필요성을 최대한 줄여야 합니다.
- 큰 규모의 DApp 이나 안정적으로 운영되어야 하는 DApp을 위한 최대한 안정적인 운영 환경을 제공할 수 있어야 합니다. 또한 다른 DApp과의 상호 연동도 편리해야 합니다.
- DApp을 위한 개발도구는 편리해야 합니다. 그리고 개발이 완료된 DApp은 빠르게 배포하고 동작시킬 수 있어야 합니다. 독립된 체인의 배포와 운영 또한 블록 생성 및 블록 생성자에 대한 고민 없이 바로 운영할 수 있어야 합니다.
- 사생활 및 민감한 데이터는 완벽하게 보호할 수 있어야 합니다. 또한 블록에 기록되지 않기를 원하는 정보도 안전하게 전달할 수 있어야 합니다.
- 무거운 연산이 필요한 DApp도 완벽하게 구동할 수 있는 환경이 필요합니다. 이러한 환경을 통해 더욱 다양한 목적을 가진 DApp을 지원할 수 있어야 합니다.

POLARIS는 이 주제들을 잘 담을 수 있는 플랫폼이 되기 위해 오랜 시간 연구하며 고민하였습니다. 이제 그 고민의 결과를 함께 나눠보고자 합니다.

탈중앙화 플랫폼의 “Red Hat®” (“Red Hat®” of Decentralization Application Platform)

Red Hat®은 글로벌 오픈소스 솔루션 기업입니다. Red Hat®은 오픈소스 프로젝트의 핵심 개발에 참여하여 오픈소스 및 리눅스(Linux)[4] 생태계에 큰 기여를 하고 있으며 오픈소스 커뮤니티에도 지속적으로 투자하고 있습니다. 특히, 오픈소스 운영체제인 리눅스의 기업용 솔루션을 공급하고 오픈소스를 사용하는 기업들을 위한 개발 컨설팅 및 기술 지원 서비스를 제공하며 공동체와 함께 성장하고 있고 지금도 여전히 생태계의 중심에서 중요한 역할을 수행하고 있습니다.

POLARIS는 탈중앙화 플랫폼의 Red Hat®이 되고자 합니다. POLARIS는 DApp 및 DApp 개발자를 위한 다양한 도움을 제공하고, 여러 기술에 대해 선도적으로 연구하여 전체 생태계에 기여할 수 있도록 노력하겠습니다. 또한 탈중앙화 기술에 관심을 갖고 DApp을 개발하고 운영하려는 기업이 있다면 개발을 도울 수 있는 적합한 컨설팅과 안정적인 운영을 위한 기술 지원 서비스도 준비하고 있습니다. POLARIS는 탈중앙화 생태계와 함께 올바르게 성장하는 프로젝트가 되기 위해 최선을 다하고 있습니다.

[4] 리눅스(Linux) : https://www.linux.org

POLARIS 생태계, "Universe"(POLARIS Ecosystem, The “Universe”)

*Universe*는 POLARIS 생태계에 붙여진 이름이며 다음과 같이 구성됩니다.

- 탈중앙화의 구현체인 **DApp(Decentralized Application)**과 **DApp 개발자**(Developer)
- DApp을 사용함으로써 생태계에 참여하는 **DApp 사용자**
- *Universe*의 발전을 위해 일하는 공정한 중재자인 **POLARIS 재단**
- 기술적 이해도와 전문성을 바탕으로 Universe에 기여하는 **블록생성자**(Block Generator)
- *Universe*의 지지자인 **토큰 보유자**(Token Holder)

탈중앙화를 위한 블록체인 또는 그와 동일한 역할을 하는 기술은 그 자체만으로는 의미가 없습니다. 아무리 훌륭한 기술을 가지고 있더라도 실제 적용되지 못하는, 단지 기술을 위한 기술이라면 그 프로젝트는 결코 성공하지 못할 것입니다. 반대로 기술적으로는 아직 부족한 면이 있더라도 의사결정 과정이 투명하고 뚜렷한 목표를 향해 나아가는 프로젝트는 건강한 생태계를 구성할 수 있고 그 안에서 계속 기술이 발전하는 선순환이 이루어질 수 있습니다.

법은 “Universe" 안에 있습니다 (The Law is in “Universe”)

The Code is Law, The “Intent of Code” is Law, Stakeholders Govern the Protocol, …

탈중앙화 세상에서 분쟁을 해결하고 빠르고 올바른 합의를 이끌어 내고자 하는 많은 접근법과 그에 대한 다양한 표현이 존재합니다.

그러나 코드 자체만으로는 법이 완성될 수 없으며, 법은 *Universe*가 정의하고 지켜갈 수 있어야 합니다. 이것이 POLARIS의 거버넌스(governance)를 통해 이루고자 하는 목표입니다. POLARIS에서는 이것을 The Law is in “Universe” 라고 얘기하려 합니다.

탈중앙화 세상은 비단 앞선 기술 만으로는 도달할 수 없습니다. 공정한 정책과 이러한 정책이 흔들리지 않고 시행될 수 있도록 방향을 잡아주는 제도가 반드시 필요합니다. POLARIS는 좋은 정책과 제도에 대해 오랜 시간 고민했습니다. 제도는 공정해야 하고 더 좋은 새로운 대안이 제시되었을 때 자리를 내어 줄 수 있을 만큼 충분히 유연해야 합니다. POLARIS는 그 첫 걸음이 될 만한 거버넌스를 제안합니다.

블록생성자-중재자 회담 (Generator-Arbiter Summit)

우리는 비슷한 크기의 목소리를 가진 다양한 의견들은 합의에 이르기 굉장히 어렵다는 것을 경험을 통해 알고 있습니다. 또한 현재의 기술로는 그 각각의 의견을 빠르게 구분하고 올바르게 표현할

수도 없습니다. POLARIS는 이러한 기술적 한계를 해결하고, 체인 위의 참여자들이 납득가능한 사회적 합의를 도출할 수 있도록 블록생성자-중재자 회담을 구성합니다. 회담의 구성원들은 생태계(*Universe*)의 발전과 이익을 위한 안건을 도출하고 합의하는 역할을 맡게 됩니다.

- **전문가의 대표자 - 블록생성자 후보들의 대표**
  블록생성자 후보는 전문적 기술력을 가진 조직으로 항상 POLARIS기술과 정책의 방향에 대해 연구하고 기여하는 집단입니다. 이들은 블록생성자 후보를 대표하는 "전문가의 대표자"로서 회담에 참여합니다.

- **공동체의 대표자 - 토큰 보유자들의 대표**
  토큰 보유자들은 공동체를 이루는 가장 큰 구성원입니다. 이들은 토큰 보유자를 대표하여 그들의 다양한 입장을 듣고 대변하는 역할을 수행하며, "공동체의 대표자"로서 회담에 참여합니다.

- **공정한 중재자 - POLARIS 재단**
  중재자는 안건을 제안하고, 빠르고 편리하게 의견을 교류할 수 있도록 자리를 마련합니다. 또한 공정하고 올바른 합의를 효율적으로 이끌어내는 역할을 수행합니다. 중재자는 POLARIS 재단 또는 재단이 위임한 단체가 그 역할을 수행하며, 재단이 중재자의 역할을 위임하고자 하는 경우에는 회담을 통한 합의를 거치게 됩니다.

회담에서 어떠한 안건을 상정하였으며, 현재 어떻게 논의되고 있는지 그리고 투표의 진행 상황과 결과는 어떠한지 모두 투명하게 공개되어야 합니다. 또한 블록생성자-중재자 회담의 모든 절차는 공정해야 하며 POLARIS는 이를 뒷받침하기 위한 기능을 플랫폼에 적용하겠습니다. 회담의 구성원과 그 비율은 거버넌스에 의해 변경될 수 있으며 플랫폼이 모든 기능을 갖추기 전까지는 재단에 의해 회담이 구성되고 운영될 수 있습니다.

공개 투표 체계 (Public Voting System)

POLARIS의 모든 참여자는 중요한 의사 결정 사항에 대해서 본인의 의사를 직접 반영할 수 있어야 합니다. 또한 *회담(summit)*의 합의 과정과 무관하게 모든 참여자의 의견이 중요하다고 생각되는 안건의 경우에는 반드시 모두의 의사를 들어 보아야 합니다. 이를 위해 POLARIS는 *공개 투표 체계(public voting system)*를 운영합니다. 또*회담*에 의해 모든 운영 방향이 결정되는 것을 막기 위해 특정 중요 안건의 경우 반드시 공개 투표를 거치도록 제도화 할 것이며 *중재자*는 *회담*의 합의 결과가 심각하게 왜곡되었다고 판단된다면 그 안건에 대해 공개 투표를 진행될 수 있습니다.

*공개 투표 체계*는 모든 토큰 보유자가 투표를 통해서 본인의 의견을 표현할 수 있게 해주는 도구가 될 것입니다.

DApp 개발 지원 (DApp Development Acceleration)

POLARIS는 이더리움(Ethereum)[5]과 달리 DApp의 최종 사용자가 수수료를 내지 않는다는 장점이 있지만 DApp을 개발하기 위해서는 개발자가 일정량의 토큰을 소유하고 있거나 토큰의 소유자로부터 처리 용량을 제공받아야 합니다. 그러므로 좋은 아이디어를 가지고 있어도 경제적인 상황이 뒷받침되지 못하는 개인이나 소규모 개발팀의 경우는 DApp 개발 및 운영이 쉽지 않을 수 있습니다.

재단은 좋은 아이디어를 가지고 있으며 발전 가능성이 높은 DApp을 지원하기 위한 목적으로 일정량의 토큰을 보유하고 있습니다. 또한 지원을 받을 DApp을 공정하게 선발하기 위한 여러가지 제도를 고려하고 있습니다.

- **공개 DApp 오디션 (Public DApp Audition)**
  훌륭한 기획과 독창적인 아이디어를 담은 DApp, 좋은 의도를 가진 DApp과 개발 단체는 DApp audition에 참가할 수 있습니다. 참가한 DApp에 대한 정보는 자세하게 공개되며 커뮤니티(community)의 투표를 통해 순위가 결정됩니다. 상위 순위의 DApp들은 즉시 지원을 받을 수 있게 되고 하위 순위의 DApp들도 순위를 높이기 위해 계속 노력하고 도전할 수 있습니다.

- **회담에서 공정하게 선택되는 DApp (Objectively Chosen DApps by Generator-Arbiter Summit)**
  POLARIS 생태계에는 공익적인 목적 또는 특수 목적의 DApp도 필요합니다. 이런 목적의 DApp 들은 독창적인 아이디어가 필요하지 않을 수도 있고 홍보가 부족해 커뮤니티의 득표를 받기 어려울 수도 있습니다. 생태계에 꼭 필요한 DApp이 public audition을 통과하지 못해 운영되지 못하는 상황을 방지하기 위해 블록생성자-중재자 회담에서는 지원할 DApp에 대해 논의하고 지원 대상으로 선정할 수 있습니다.

선발된 DApp 또는 단체는 정해진 기간 동안 재단이 지원하는 처리 용량과 자원을 사용하여 재정적 부담을 줄이고 탈중앙화로의 도전을 이어나갈 수 있습니다.

이처럼 POLARIS는 좋은 DApp들을 지원하기 위한 제도에 대해 꾸준히 연구하고 있으며 DApp을 위한 최고의 환경을 제공하기 위해 노력하겠습니다.

[5] 이더리움(Ethereum) : https://www.ethereum.org

스파클 합의 체계 (Sparkle Consensus System)

*스파클 합의 체계(Sparkle Consensus System)*는 POLARIS 플랫폼이 사용하는 합의 체계(consensus system)입니다. 더 많은 단체가 자유롭게 합의에 참여할 수 있어 지나치게 집중화 되는 것을 방지하고 적당한 수의 검증자에 의한 합의를 통해 합의 속도와 탈중앙화 네트워크의 처리 성능을 높이는 것을 목표로 개발되었습니다. 또한 기존의 합의 체계가 가진 문제점을 분석하여 여러 부분을 개선하였습니다.

전문성 증명 (Proof of Profession)

POLARIS는 전문성 증명(*Proof of Profession)*이라는 자격증명을 사용합니다.
프로페션(profession)은 블록생성자 후보의 전문성을 나타내는 지표로 다음의 요소를 포함하고 있으며 *프로페션 점수(PROFESSION score)*로 표현됩니다.

- 토큰 홀더로부터의 지지 (득표)
- 노드를 구동하는 시스템의 사양
- 불안정한 시스템 운영 또는 처벌로 인한 점수의 차감
    - 블록생성자로 선정되었으나 응답이 없는 경우
    - 검증자(verifier)로 선정되었으나 응답이 없는 경우
    - 잘못된 블록을 생성하였을 경우
    - 잘못된 검증을 하였을 경우
    - 시스템 사양을 속인 것이 발각되는 경우
    - 기타 네트워크에 대한 공격
- 거버넌스(governance)에 의해 추가되는 요소
- POLARIS 플랫폼의 기능 확장을 위해 추가되는 요소

블록생성자 후보를 위한 보상은 기본적으로 블록을 생성하고 얻는 블록 생성 보상만이 존재합니다. 보상체계를 단순화 함으로써 복잡한 보상체계로 인해 발생할 수 있는 여러 위험요소를 제거할 수 있습니다. 또한 블록생성 후보자만 존재하므로 블록생성 대기후보자가 네트워크를 유지하기 위한 시스템을 제대로 운영하지도 않으면서 득표에 의한 추가 보상만을 부당하게 가져가는 등의 문제가 발생하지 않습니다.

블록생성자는 블록생성자 후보 중 난수에 의해 임의로 선정되며, 각 후보자가 블록생성자로 선정될 확률은 *프로페션 점수*에 따라 자연로그와 같은 형태로 증가합니다. 자연로그와 같은 형태의 확률을 적용함으로써 상위 블록생성자 후보의 이탈 또는 장애로 인해 발생할 수 있는 네트워크 불안정성에 대한 위험과, 검증되지 않은 신규 블록생성자 후보가 블록을 많이 생성함으로써 발생할 수 있는 위험을 최소화 할 수 있습니다. *프로페션 점수*는 시스템의 사양에 대한 점수를 포함하며 이는 블록생성자 후보들이 더 높은 사양의 시스템을 노드로 사용할 동기를 제공합니다. 이로 인해 얻어진 연산능력(computing power)은 *연산 그리드(Computation Grid)*를 원활하게 유지하기 위한 자원으로 사용됩니다.

처벌은 미래의 기대 보상을 줄이는 방법으로 이루어지며 *프로페션 점수*를 차감함으로써 블록생성자로 선정될 확률을 떨어뜨리거나 0으로 만듭니다. 또한 특정 블록생성 후보자가 악의적인 행동을 반복하거나 이상 행동을 반복하는 경우 거버넌스에 의해 블록생성 후보에서 영구적으로 배제할 수도 있습니다.

빠른 합의와 즉시 이루어지는 완결성 (Fast Consensus and Near Instant Finality)

PBFT와 난수로 선택되는 검증자 (PBFT and Randomly Selected Verifiers)

*스파클 합의 체계*는 기본적으로 PBFT(Practical Byzantine Fault Tolerance)[6]를 기본으로 이를 개선한 합의 알고리즘(consensus algorithm)을 사용합니다. PBFT 또는 PBFT 변형 합의 알고리즘에서는 네트워크와 프로토콜의 한계로 인해 검증자가 많아 질수록 합의 속도가 느려지게 됩니다. *스파클 합의 체계*는 블록생성 후보자가 매우 많더라도 정해진 수의 검증자만으로 검증을 진행하여 합의 속도를 보다 빠르게 유지할 수 있습니다. 검증자는 블록생성 후보자와 재단이 운영할 수 있는 검증 전용 노드들 중에 선발됩니다.

- 블록생성자와 검증자는 완전히 별개로 선정됩니다.
- 네트워크상의 위치를 확보한 소수의 검증자를 이용해 빠르게 합의 함으로써 가용성을 높입니다.
- 실제 동작하고 있음이 최근에 확인된 노드들 중에 선발해 응답이 오지 않을 가능성을 줄입니다. 응답하지 않을 경우 *프로페션 점수*가 낮아집니다.
- 예측할 수 없는 난수에 의해 선정되어 충분한 신뢰성을 확보할 수 있습니다.

[6] PBFT(Practical Byzantine Fault Tolerance) : Castro, M.; Liskov, B. (2002). "Practical Byzantine Fault Tolerance and Proactive Recovery". *ACM Transactions on Computer Systems*. Association for Computing Machinery. **20** (4): 398–461. CiteSeerX 10.1.1.127.6130. doi:10.1145/571637.571640.

*스파클 합의 체계*는 조절 가능한 검증 수준(verification level)을 제공합니다. 이에 따라 검증에 참여하는 검증자의 수는 각 체인의 목적에 따라 조절할 수 있습니다. 필요에 따라 보다 적은 검증자를 사용하여 네트워크의 처리 성능을 더 확보할 수 있고 반대로 더 많은 검증자를 사용하여 신뢰도를 올릴 수 있습니다.

또한 합의에 걸리는 시간을 더욱 줄이고 합의 과정을 단순화 하기 위해 Threshold cryptosystem[7] 등의 기술과 Raft[8] 등의 합의 알고리즘에 대해 검증하며 연구하고 있습니다.

비동기적 검증을 통한 즉각적인 완결성 (Near Instant Finality by Asynchronous Verification)

생성된 블록에 대한 검증(verification)은 블록의 생성과 관계없이 비동기적으로 검증됩니다. 또한 블록의 검증 결과를 다음 블록의 검증자들에게 우선적으로 전달함으로써 연쇄적인 빠른 검증과 거의 즉각적인 완결성을 제공합니다.

또한 CPU 최적화 방법으로 익히 알려진 투기적 실행(speculative execution)[9]과 같은 사전 검증 방법에 대해서도 연구하고 있습니다. 이를 통해 최대한 먼저 수행할 수 있는 부분을 확보하고 미리 검증을 진행할 수 있습니다.

네트워크를 통한 블록의 빠른 전파를 위해서 알려진 프로토콜에 대해서 다양하게 살펴보고 있으며 새로운 알고리즘에 대한 독자적인 연구 및 개발도 진행하여 더 즉각적인 검증 및 완결을 제공할 예정입니다.

알려진 공격에 대한 대비 (Known Attacks and Protection)

Discouragement Attack[10]

*스파클 합의 체계*는 미래의 기대 보상을 줄이는 방법으로 처벌합니다. 예치금이 존재하지 않고 예치금을 압수하는 등 현재 자산에 직접적인 해를 끼치는 방식으로 처벌하지 않으므로 discouragement attack에 대한 가능성이 없습니다.

Stake Grinding Attack[11]

---

[7] Threshold cryptosystem : https://en.wikipedia.org/wiki/Threshold_cryptosystem
[8] Raft : https://raft.github.io/
[9] Speculative execution : https://en.wikipedia.org/wiki/Speculative_execution
[10] Discouragement attack : https://vitalik.ca/files/casper_note.html
[11] Stake grinding attack : https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQs#how-does-validator-selection-work-and-what-is-stake-grinding

충분히 검증된 난수 생성 알고리즘을 사용하고 충분한 수의 매개변수(parameter)를 씨드(seed) 값으로 사용해 stake grinding attack을 방지합니다.

DDoS(Distributed Denial-of-Service) Attack[12]

블록을 생성할 블록생성자 및 검증자들은 직전에 결정됩니다. 미리 결정되지 않으므로 POLARIS 네트워크 외부로부터의 DDoS 공격이 매우 어렵습니다.

Dishonesty / Sybil Attack[13]

매우 작은 확률이라도 100% 공격 성공을 확신할 수 있는 경우가 발생할 수 있다면 정직하게 블록을 생성하며 공격할 기회를 기다리는 공격자가 존재할 수 있습니다.

*스파클 합의 체계*는 블록을 생성하는 시점에는 어느 검증자들이 검증을 할지 알지 못합니다. 따라서 블록생성자가 상당수의 정직하지 못한 검증자들을 확보하였다고 하더라도 공격이 100% 성공할지 확신할 수 있는 경우는 없습니다.

또한 POLARIS 재단은 네트워크가 안정 되기 전까지는 충분한 수의 검증 전용 노드를 운영하여 네트워크의 안정성을 확보합니다.

Nothing at Stake[14]

*스파클 합의 체계*는 블록의 생성자가 명확하게 선정되는 PBFT 변형 합의 알고리즘을 사용합니다. 따라서 체인의 분기(fork)가 생기지 않으므로 nothing at stake 문제가 발생하지 않습니다.

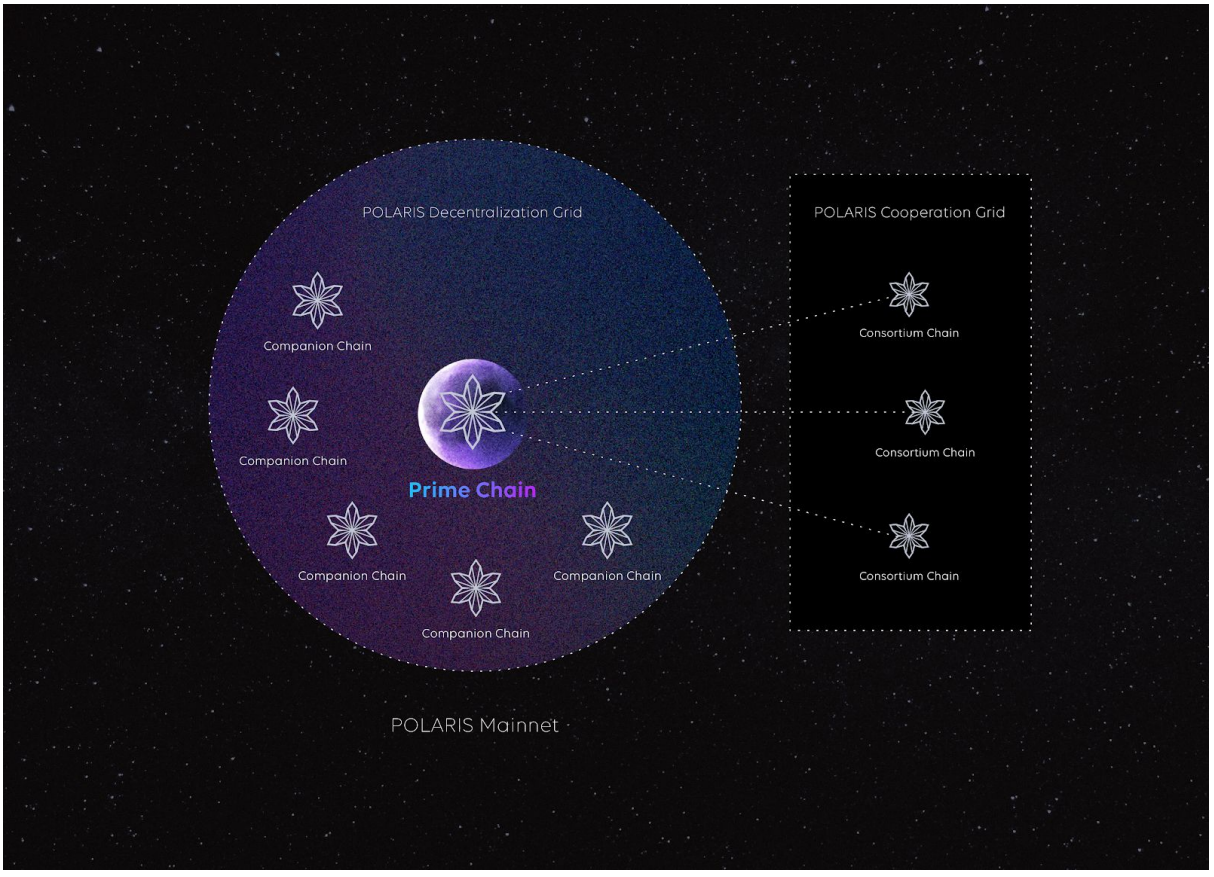
[12] DDoS(Distributed Denial-of-Service) attack : https://en.wikipedia.org/wiki/Denial-of-service_attack
[13] Sybil attack : https://en.wikipedia.org/wiki/Sybil_attack
[14] Nothing at stake : https://github.com/ethereum/wiki/wiki/Problems#8-proof-of-stake

POLARIS 멀티버스 (POLARIS Multiverse)

ORBS[15] 프로젝트는 “모든 블록체인을 아우를 수 있는 하나의 블록체인은 없을 것이라고 믿는다. (We believe that there will be no blockchain to rule all blockchains.)[16]” 라고 말합니다. 실제로 하나의 블록체인 플랫폼을 현실의 모든 산업군과 서비스가 요구하는 각각의 용도와 목적에 모두 부합하도록 만들기는 매우 어렵습니다.

이 때문에 많은 프로젝트는 특수한 목적 또는 단일 DApp에 특화된 체인을 만들고 운영하고 있습니다. 그러나 이러한 접근은 서로 다른 많은 프로토콜을 만들게 되어 체인간의 교류와 통신을 점점 더 어렵게 하고 체인의 유지와 운영을 위한 중복된 노력이 필요하게 됩니다.

POLARIS는 여러개의 독립된 체인으로 구성된 *Multichain mainnet*과 consortium network를 위한 독립된 side chain으로 이루어진 *POLARIS Multiverse*를 통해 하나의 플랫폼 위에서 충분히 유연한 생태계를 구성 할 수 있는 최적의 환경을 지원합니다.



[15] ORBS : https://orbs.com/
[16] ORBS Position Paper : https://orbs.com/orbs-position-paper/

POLARIS 탈중앙화 그리드 (POLARIS Decentralization Grid)

*스파클 합의 체계*의 블록생성자 후보들은 POLARIS 네트워크의 블록 생성 및 검증을 위해 자발적으로 참여하여 POLARIS를 위한 공용 탈중앙화 네트워크(public decentralized network)인 *POLARIS 탈중앙화 그리드(POLARIS Decentralization Grid*를 구성합니다. *탈중앙화 그리드*의 참여자는 추후 구성될 *POLARIS 연산 그리드(POLARIS Computation Grid)*에도 의무적으로 참여하여 고성능 연산을 위해서도 사용됩니다.

또한, 이렇게 만들어진 탈중앙화 네트워크는 블록생성과 검증, 스마트 컨트랙트(smart contract), 연산의 수행 외에 다른 용도로 매우 유용하게 활용될 수 있습니다. POLARIS는 잘 구성된 *탈중앙화 그리드*를 활용하여 다양한 기능을 수행할 수 있는 2nd layer platform을 제공할 예정입니다.

탈중앙화 그리드에서 동작하는 Blockchain-as-a-Service

(Blockchain-as-a-Service on Decentralization Grid)

Blockchain-as-a-Service (이하 BaaS)는 운영을 위한 인프라(infrastructure)에 대한 고민 없이 독립적인 체인을 운영하고 DApp을 더 손쉽게 구현할 수 있는 방법을 제공합니다. 그러나 실제 독립적인 체인 위에서 DApp을 운영하는데 있어 가장 어려운 점 중의 하나는 블록을 생성할 생성자를 모집하고 결정하는 것입니다. 아무리 편리하게 모든 환경을 구성할 수 있다고 해도 블록생성자 또는 채굴자(miner)를 구성하는 것에 많은 노력을 들여야 한다면 아무런 의미가 없습니다. 따라서 이에 대한 해결책을 제시하지 못한다면 진정한 BaaS라고 얘기하기 어렵습니다.

POLARIS는 *탈중앙화 그리드*를 공유하는 *스파클 합의 체계*를 이용하여 블록생성자 구성에 대해 전혀 고민할 필요 없이, DApp과 체인의 기능에만 집중할 수 있는 BaaS 환경을 제공합니다. 또한 운영을 위한 편리한 제어 환경도 준비하고 있습니다.

다중체인 메인넷 (Multichain Mainnet)

POLARIS 메인넷(mainnet)은 *탈중앙화 그리드*에 의해 블록이 생성되고 유지되는 독립된 여러개의 체인(chain)으로 이루어져 있습니다. 목적에 따라 체인을 분리하여 운영할 수 있어 다른 체인의 운영상황에 따른 장애나 DApp에 의한 상호 간섭을 최대한 피하여 네트워크의 안정적인 유지가 가능합니다. 또한 각각의 체인들은 독립적으로 블록을 생성하며, 병렬로 동작하기 때문에 체인이 늘어남에 따라 노드를 추가하거나 노드의 시스템적인 변경 없이도 네트워크를 확장(scaling)할 수 있습니다.

프라임 체인 (Prime Chain)

*프라임 체인(Prime chain)*은 POLARIS 멀티버스를 운영하기 위한 체인으로 단 하나만 존재하며 운영에 필요한 여러가지 정보를 담고 있습니다.

- POLA 지갑(wallet) 및 예치(staking) 정보
- *컴패니언 체인*과 메인넷의 제어 및 유지를 위한 정보
- Self-amendment 를 위한 정보
- 계정(account)을 위한 정보
- 블록생성자 후보군을 유지하기 위한 정보
- 기타 *POLARIS Universe* 를 위한 정보

*프라임 체인*은 우선순위가 가장 높은 체인으로 *프라임 체인*에서는 DApp이 구동되지 않아 DApp의 트랜잭션으로 인한 영향으로 부터 자유로우며 독립적으로 운영되어 안정성을 유지합니다.

컴패니언 체인 (Companion Chain)

하나의 체인위에서 운영되는 다수의 DApp들은 서로의 상황에 따라 영향을 받게 될 가능성이 있습니다. 또한 여러개의 DApp 들에 의해 많은 트랜잭션이 발생할 경우 트랜잭션이 지연되어 중요한 처리가 늦어질 수 있습니다. POLARIS는 트랜잭션이 많은 DApp이나 네트워크의 안정성이 중요한 DApp, 같은 기업 또는 단체 운영하는 DApp들을 위해 별도의 체인을 운영할 수 있습니다. 별도의 *컴패니언 체인*을 운영하기 위해서는 정해진 양 이상의 POLA를 예치(staking)하거나 예외적인 필요성이 인정되는 경우 거버넌스(governance)에 의한 결정이 필요합니다.

*컴패니언 체인*은 하나 이상이 동시에 존재하며 *프라임 체인*뿐만 아니라 다른 *컴패니언 체인*과도 완전히 독립적으로 동작합니다. 다른 체인의 영향을 받지 않고 병렬로 블록이 생성되어 유지되기 때문에 전체 네트워크의 처리 용량(throughput)은 *컴패니언 체인*의 개수와 비례하여 빠르게 늘어나게 됩니다.

*컴패니언 체인*은 privacy preserving 기능을 독립적으로 적용할 수 있고 검증자 수의 조절을 통한 검증 수준(verification level)의 변경도 가능합니다. 이러한 유연한 설정을 통해 특정 DApp 또는 기업, 산업을 위한 가장 효율적인 체인을 구성할 수 있습니다. 추후 POLARIS 플랫폼의 발전에 따라 독립적으로 변경하고 설정할 수 있는 기능이 계속 추가될 예정입니다.

POLARIS 메인넷에는 일반적인 DApp들을 위한 *범용 컴패니언 체인(general companion chain)*이 기본적으로 한 개 존재합니다. *범용 컴패니언 체인*은 트랜잭션이 빠르게 증가하여 트랜잭션의 지연이 지속적으로 발생하는 경우 추가로 생성되어 트랜잭션을 분산하게 됩니다.

POLARIS 협력 그리드 (POLARIS Cooperation Grid)

Side chain은 각 산업군이나 다양한 목적의 서비스가 가지고 있는 특징을 살리면서 유연하고 자유롭게 최적화를 할 수 있는 훌륭한 방법입니다. 또한 확장성(scalability) 문제를 해결할 수 있는 좋은 접근법이기도 합니다. 그러나 side chain은 체인을 운영하기 위한 별도의 거버넌스를 마련하고 블록생성을 위한 독자적인 생태계를 구성해야 합니다. 또한 기존 플랫폼의 수정을 위한 전문적인 인력이 필요하거나 별도의 side chain 특화 프로젝트에 의존해야 하는 어려움이 있습니다.

*POLARIS 협력 그리드*는 POLARIS 플랫폼을 사용하고 *POLARIS 탈중앙화 그리드*와 서로 교류하며 동작하는 여러개의 다양한 side chain(child chain)들이 구성하는 네트워크입니다. 특수한 목적을 가진 별도의 네트워크를 구성해야 하는 기관 또는 단체는 POLARIS 플랫폼을 사용하여 *POLARIS 협력 그리드*에 참여함으로써 side chain 구성을 위한 별도의 플랫폼에 의존하지 않고도 목적에 맞는 네트워크를 자유롭고 편리하게 구성할 수 있습니다.

- **허가형 / 컨소시엄 네트워크 (Permissioned / Consortium Network)**
  특정한 목적을 위해서는 모두에게 공개되지 않고 권한이 있는 개인 또는 단체에게만 접근이 허용되는 허가형 네트워크(permissioned network)를 구성해야 할 필요가 있습니다. POLARIS는 “허가형 네트워크를 위한 side chain(permissioned side chain)”을 쉽게 구성할 수 있을 뿐만 아니라 메인넷의 체인과의 쉬운 연동을 위한 API를 지원하여 제한된 네트워크의 장점과 공개된 네트워크(public network)의 장점을 모두 살릴 수 있습니다.

- **교체가능한 다양한 컴포넌트 (Pluggable Diverse Component)**
  *POLARIS 연합*에 속한 체인은 다중체인 메인넷의 바깥에서 동작하기 때문에 더 많은 자유도가 주어집니다. 이에 따라 POLARIS 플랫폼이 메인넷을 위해 기본적으로 제공하는 여러가지 설정과 변경 가능한 컴포넌트 외에도 더 많은 부분의 변경이 가능합니다.

  별도의 합의 알고리즘을 선택할 수 있고 자유로운 노드의 구성이 가능하며 특수한 암호화 알고리즘의 적용도 가능합니다. POLARIS는 *스파클 합의 체계*와 DPoS-BFT 외에도 PBFT, Raft, PoW 등의 합의 알고리즘 컴포넌트(component)를 추가로 개발하여 지원할 예정입니다. 또 더 많은 부분에 대한 손쉬운 변경이 가능하도록 계속 확장할 계획입니다.

체인간 합의 (Cross Chain Consensus)

*POLARIS 멀티버스*는 여러 체인으로 이루어져 있기 때문에 체인과 체인 사이의 의사소통이 원활하게 이뤄져야 합니다. POLARIS의 *다중체인 메인넷*에서는 서로간의 통신을 위해 동일한 프로토콜을 사용하고 편리하게 이용가능한 API와 명령(Command)도 제공합니다. 이를 이용해 메인넷의 *프라임 체인*과 *컴패니언 체인*들 사이에서는 쉽게 정보를 교류할 수 있습니다.

하지만 *POLARIS 협력 그리드*에 속한 side chain은*스파클 합의 체계*가 아닌 다른 합의 알고리즘을 선택할 수 있고 특별한 필요성으로 인해 메인넷이 사용하는 프로토콜과 다른 프로토콜을 사용해야 할 수 있습니다. 이러한 경우 체인 간 어떻게 의사소통을 해야하며 어떤 솔루션을 사용해야 하는지 등의 합의에 관련 한 문제가 발생할 수 밖에 없습니다. 특정한 체인 내에서 검증 된 내용이더라도 다른 체인의 입장에서는 쉽게 신뢰할 수 없는 외부의 데이터이기 때문입니다.

POLARIS는 스마트 컨트랙트를 통한 체인간 합의를 위한 편리한 인터페이스(interface)를 기본적으로 제공합니다. 이를 이용하여 POLARIS 메인넷의 내용을 side chain에 기록 할 수도 있고 반대로 side chain의 내용을 메인넷으로 가져와 기록 할 수도 있습니다. 또 이를 확장하여 스마트 컨트랙트를 지원하는 다른 탈중앙화 플랫폼과의 정보 교환도 지원할 수 있습니다. POLARIS는 체인간 합의를 더 효율적으로 수행하기 위해 스마트 컨트랙트를 이용하지 않는 다양한 방법에 대해서도 연구 중입니다.

사생활 및 데이터 보호 (Privacy Preserving and Data Protection)

블록체인의 거래 기록은 상태를 시간 순서대로 기록하고 변경하는 것을 의미합니다. 누적된 기록은 모두에게 투명하게 공개되므로 시간이 지남에 따라 사용자의 이용 패턴이 드러나고 이를 통한 사용자의 추적 가능성도 있습니다. 하지만 우리는 거래 또는 거래 과정 중에서 모두에게 드러나서는 안되는 민감한 사항이 존재한다는 것을 알고 있습니다. 개인 정보나 기업의 기밀문서 혹은 외부에 유출되지 말아야 하는 거래 정보 등 많은 정보들은 외부의 열람으로부터 보호되어야 합니다.

POLARIS는 보호가 필요한 정보에 대한 안전장치를 제공하기 위해 영지식증명(Zero-knowledge proof)[17]과 비대칭 암호(Asymmetric cryptography)[18]를 사용하여 익명성을 확보하고 단말간 통신 데이터를 암호화 할 수 있는 기술을 지원합니다.

사생활 보호를 위한 기술들 (Privacy Preserving Technologies)

현재의 탈중앙화 생태계에는 익명성을 보장하기 위한 다양한 기술들이 소개되어 있고 이 기술들을 이용한 많은 프로젝트들이 있습니다. POLARIS는 사생활과 데이터를 더 안전하고 효율적으로 보호하기 위해 다양한 기술들에 대해 연구하고 있습니다.

코인조인 (CoinJoin)

Dash[19]에서 사용하는 이 방식은 기본적으로 여러 트랜잭션을 한 곳에 모았다가 다시 목적지로 보내는 방식입니다. 이렇게 중간자를 이용해 전송하는 방법을 사용하면 트랜잭션들의 출발지가 중간자에 의해 모두 섞이기 때문에 정확한 출처를 파악하기 어려워집니다. 이렇게 트랜잭션을 섞는 중간자의 역할을 믹서(Mixer)라고 합니다. 이 방식은 특정 컨센서스를 필요로 하지 않아 비교적 구현하기 쉽고 증명(proof)이 가볍다는 장점이 있습니다.

하지만 정상적인 동작을 위해서는 신뢰할 수 있는 믹서를 선택해야 하고 믹서가 온라인 상태여야하며 출처를 혼란시키기에 충분한 단위의 트랜잭션들이 모일 때 까지 전송이 지연 될 가능성이 있는 등의 단점도 가지고 있습니다. 그리고 이 방식만으로는 완전하게 트랜잭션을 감출

[17] 영지식증명(Zero-knowledge proof) : https://en.wikipedia.org/wiki/Zero-knowledge_proof
[18] 비대칭 암호(Asymmetric cryptography) : https://cryptography.io/en/latest/hazmat/primitives/asymmetric
[19] Dash : https://www.dash.org

수 없으며 브라우저의 비밀모드나 네트워크를 우회하는 등의 예방조치를 함께 사용하여야만 기본적인 수준의 익명성을 가질 수 있습니다.

링 시그니쳐 (Ring Signature)

Monero[20]의 링 시그니처는 해당 트랜잭션에 서명하는 사람이 누구인지를 직접 밝히지 않고 사용자 그룹으로 서명하여 트랜잭션을 발생시켜 실제 사용자가 누구인지를 감추고 거래를 입증하는 방식입니다. 링 시그니처는 사용자가 트랜잭션을 작성할 때 근처의 비슷한 다른 트랜잭션을 자동으로 인풋으로 넣어 서명하기 때문에 믹서가 필요하지 않습니다. 또한 이 과정을 여러번 수행할 수록 서명에 포함되는 인풋 트랜잭션이 많아져 원래 사용자를 찾을 확률이 낮아지고 익명성이 강화됩니다. 더불어 트랜잭션에 포함 된 금액도 감출 수 있기 때문에 CoinJoin방식에 비해서 더 향상 된 익명성을 가집니다.

그러나 여러 트랜잭션의 내용이 모여 하나의 또 다른 트랜잭션을 만들기 때문에 트랜잭션이 매우 커지게 되고 그 만큼 많은 저장공간이 필요해 확장성이 떨어진다는 단점을 가지고 있습니다. 또 트랜잭션을 분석하면 실제 사용자에 대한 확률적인 유추가 가능한 경우도 있습니다.

영지식증명 (Zero-knowledge proof)

영지식증명은 증명자가 알고있는 어떠한 비밀에 대해 그 비밀을 직접 밝히지 않고도 “알고 있다는 사실이 참”이라는 것을 검증자에게 증명하는 방식입니다. 증명자는 사실을 증명하기 위해 검증자의 검증에 대한 답변을 제외하고는 어떤 것도 노출하지 않습니다. 지금까지 블록체인에 적용된 영지식증명 구현으로는 zcoin[21]과 pivx[22]의 zerocoin 방식과 zcash[23]의 zk-SNARKs 방식이 있습니다.

- **제로코인 (Zerocoin)**
  제로코인은 확률적으로 출처를 찾기 어렵게 하는 방식과는 달리 영지식증명을 통해 트랜잭션의 생성자와 수신자의 연결고리를 완전하게 끊을 수 있습니다. 제로코인은 필요한 만큼의 코인을 기존 주소에서 소각하고 새로 발행하여 사용하는 방식으로 소스와 타겟의 연결고리를 제거하며, 소각하는 코인의 정보를 공개하지 않고 실제로 소각을 했다는 것을 증명 하는데에 영지식증명을 사용합니다. 제로코인은 앞서 설명한 방식들에 비해서 한 번에 더 많은 수의 익명 트랜잭션을 확보할 수 있고 더욱 강화된 익명성을 보장 받는다는 장점을 가지고 있습니다.

[20] Monero : https://getmonero.org
[21] Zcoin : https://zcoin.io
[22] PIVX : https://pivx.org
[23] Zcash : https://z.cash

하지만 이와 같은 강력한 익명성을 확보하기 위해 처음 한 번 신뢰 설정(trusted setup)을 해야 한다는 불편함이 있고 증명의 크기도 20k 정도로 큰 편입니다. 또한 고정된 단위의 금액만 사용할 수 있다는 제약이 있습니다. 제로코인은 기존 코인을 소각하고 새로 발행할 때 우리가 흔히 사용하는 현금처럼 1코인 5코인 10코인 50코인 100코인 1000코인 등의 미리 정해진 단위로만 발행할 수 있으며 사용할 때에도 현금을 사용하듯 4코인을 소비하기 위해서는 5코인을 내고 1코인을 거슬러 받아야 합니다. 이렇게 정해진 단위로 코인을 사용해야 하기 때문에 비슷한 지출을 정기적으로 하는 등의 특정 패턴이 드러날 수 있고 이를 통해 실제 사용자에 대한 추적이 가능할 수 있습니다.

- **간결한 비상호작용 영지식증명 (zk-SNARKs)**
  Zerocoin을 발전시킨 Zcash는 zk-SNARKs를 사용하여 증명의 사이즈가 1k 정도밖에 안되고 검증도 더 빠릅니다. 그리고 모든 트랜잭션의 연결이 기본적으로 끊어져 있기 때문에 익명성을 얻기위해 코인을 소각했다 발행하는 번거로움도 없고 미리 정해놓은 화폐 단위로 사용 할 필요도 없어 훨씬 편리합니다.

  하지만 신뢰 설정을 하는 과정이 복잡하고 여러가지 제약사항도 있습니다. 만약 이 설정이 잘못되면 위조코인이 생성될 수 있는데 이 경우 강력한 익명성으로 인해 정확한 발행량 추적을 할 수 없어 매우 주의해야 합니다. 그리고 증명을 위해 복잡한 수학연산이 필요하기 때문에 트랜잭션 생성에 많은 시간이 소요된다는 단점도 있습니다.

- **연구중인 영지식 기술 (Beyond zk-SNARKs)**
  zk-SNARKs는 지금까지의 구현 중 가장 뛰어나지만 명확한 단점을 가지고 있습니다. 이러한 문제점을 보완하기 위해서 많은 연구자들이 zk-STARK[24]와 bulletproof[25]등의 기술을 연구하고 있습니다.

  Starkware의 zk-STARK는 zk-SNARKs의 핵심 연구원들이 모여 진행하는 프로젝트입니다. zk-STARK는 zk-SNARKs의 문제점 중 하나인 신뢰 설정을 하지 않고도 익명성을 확보할 수 있도록 개선했습니다. 그리고 계산 과정을 간결하게 하여 증명 생성 시간과 검증 시간이 더 빠릅니다. 하지만 생성되는 증명의 크기가 너무 커서(약 1MiB) 실제 시스템에 적용하기는 어려워 연구진들은 이 크기를 줄이는데 힘쓰고 있습니다.

  bulletproof는 stanford 대학교의 연구원들이 진행하는 프로젝트입니다. zk-STARK와 마찬가지로 신뢰 설정을 하지 않고도 익명성을 확보 했으며 증명을 작게 만들 수 있도록

[24] zk-STARK : https://www.starkware.co/
[25] bulletproof : https://crypto.stanford.edu/bulletproofs/

하는 기술입니다. 증명의 크기가 작고 증명을 생성하는데 컴퓨터의 연산능력도 적게 사용하도록 합니다. 대신 다른 프로젝트들에 비해 검증을 하는데 시간이 더 오래 걸립니다.

두 프로젝트 모두 기존의 문제점을 해결하고 있지만 실제로 사용하기 위해서는 아직 보완해야 할 점이 많고 또 충분한 검증이 이루어지지 않았기 때문에 더 많은 연구가 필요합니다.

이 외에도 많은 기술들이 알려져 있고 현재도 활발히 연구되고 있지만 현재까지의 사생활 보호기술들은 서로 뚜렷한 장단점을 가지고 있어 우열을 가리는 것은 쉽지 않습니다. POLARIS는 확장성이 높고 강한 익명성을 보장할 수 있는 영지식증명을 바탕으로 꾸준한 연구와 개발을 통해 POLARIS 플랫폼에 가장 적합한 방식을 적용해 사용자의 정보를 보호 할 계획입니다.

비대칭 암호 (Asymmetric Cryptography, Public-key Cryptography)

*탈중앙화 그리드*는 서로 연결 된 독자적인 네트워크를 구성하고 있으며 이 네트워크는 정보와 데이터의 전송을 위해 활용 할 수 있습니다. 이렇게 전송되는 정보들은 블록에 기록되지 않으며 이렇게 전송되는 정보를 보호하기 위해서는 블록 외의 데이터들을 암호화할 수 있어야 합니다.

비대칭 암호(asymmetric cryptography)는 데이터를 암호화하고 복호화하는데 서로 다른 두 개의 키를 사용하는 방식을 말하며 일반적으로 공개키와 개인키를 사용합니다. 송신자가 수신자의 키를 이용해 메시지를 암호화 하고 전체 노드로 전파하면 메시지를 전파받은 대상 중 적합한 키를 가진 실제 수신자만이 해당 메시지를 복호화하여 확인할 수 있습니다.

POLARIS는 일대일(peer-to-peer) 통신에 비대칭키를 이용해 정보를 암호화 하는 프로토콜을 기본적으로 제공하여 정보 보호를 위한 추가 구현이 필요하지 않습니다.

트랜잭션 노출 방지 (Transaction Privacy Preserving)

거래의 기록에는 여러 내용이 포함될 수 있지만 핵심적인 내용은 '누가, 누구에게, 무엇을 전송했는가' 입니다. 그러므로 트랜잭션을 익명화 하기 위해서는 해당 트랜잭션의 송신자(sender), 수신자(receiver), 수량(amount)을 감춰야 하며 이를 통해서 사용자의 자산을 안전하게 보호할 수 있습니다. POLARIS에서는 *POLARIS 멀티버스*와 사생활 보호기능을 함께 사용하여 이를 쉽게 적용할 수 있습니다. 사생활 보호기능이 포함된 별도의 체인이 필요할 경우 체인을 운영하고자 하는 주체는 *멀티버스*를 통해 사생활 보호기능이 적용된 체인을 생성하고 그 체인을 사용함으로써 송신자와 수신자를 감추며 거래에 대해 증명할 수 있습니다.

DApp은 이러한 사생활 보호기능이 적용된 *컴패니언 체인*위에서 동작 할 수 있으며 필요한 경우 트랜잭션에 대한 상세 내용을 공개하지 않고도 결과와 증명을 *프라임 체인*에 기록하여 신뢰를 유지할 수 있습니다.

스마트 컨트랙트 노출 방지 (Smart Contract Privacy Preserving)

스마트 컨트랙트는 크게 트랜잭션 또는 트랜잭션들의 묶음으로 볼 수 있습니다. 하지만 스마트 컨트랙트가 일반적인 트랜잭션과 구분되는 점은 입력과 결과가 있다는 것 입니다. 이 때문에 사용자의 정보를 제대로 보호하기 위해서는 이 입력과 결과도 알 수 없도록 보호해야 합니다.

POLARIS는 트랜잭션의 송신자, 수신자, 수량 정보 외에 스마트 컨트랙트의 입력과 결과도 감출 수 있습니다. 이 정보를 공개적인 접근으로부터 보호함으로써 사용자들은 *탈중앙화 그리드*에서 보안이 중요한 거래와 정보 자체의 가치가 높은 거래도 진행할 수 있고 보험이력이나 질병의 치료기록 등 개인의 민감한 정보에 대한 처리도 안전하게 진행할 수 있습니다.

익명 메시지 프로토콜 (Incognito Messaging Protocol)

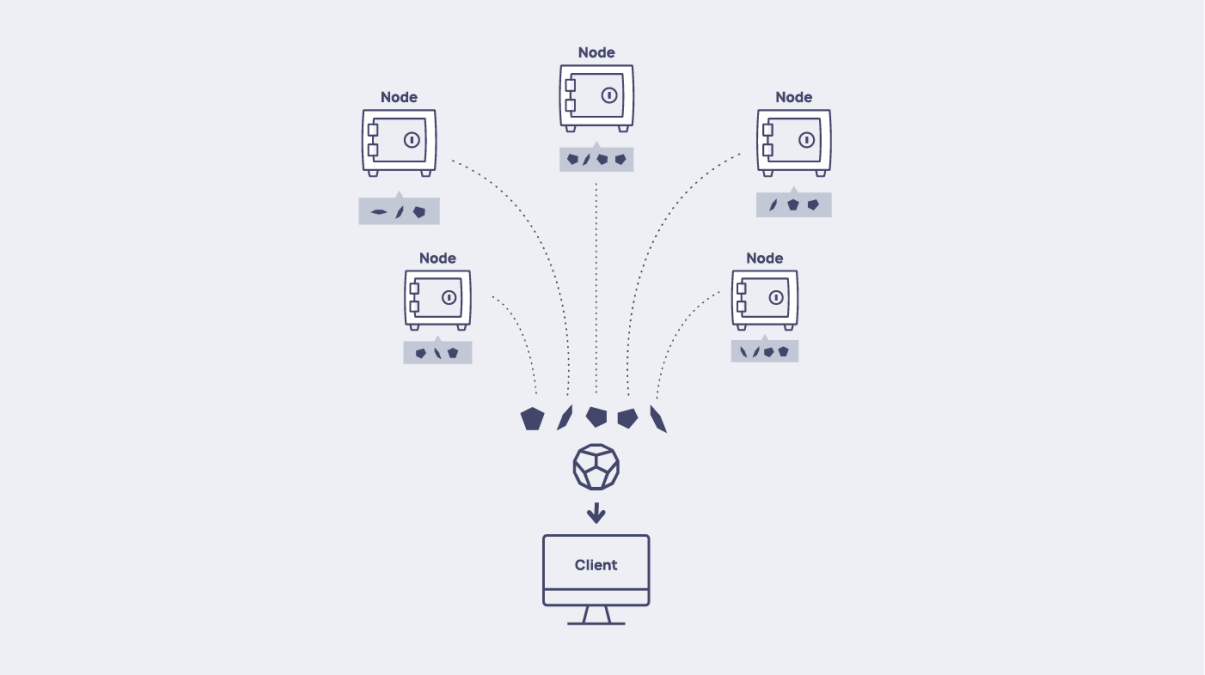
개인의 프라이버시(privacy)는 보장되어야 합니다. 설령 국가의 기관이나 특정 단체가 개인의 대화 내용을 알려고 하더라도 대화 당사자의 허락이 없이는 대화 내용이 공개되어서는 안됩니다. 비단 개인간의 사적인 대화 뿐만 아니라 공적인 대화에도 보안이 필요합니다. 직장에서 나누는 대화는 그 하나하나가 기업 기밀이 될 수 있기 때문에 보안이 철저히 보장되는 메시지 전달 도구의 사용이 요구됩니다.

프라이버시가 보장되는 메시지 전달도구(메신저, messenger)의 수요는 날이 갈수록 늘어나고 있지만 중앙화된 주체가 존재할 경우 메신저의 주체가 되는 기업이나 담당자에 의해서, 또는 사설 탐정과 해커에 의해서, 공권력에 의해서 대화 내용의 유출이 언제든지 가능합니다. 유출된 비밀로 인해 기업은 막대한 손실이 발생할 수 있고 개인은 큰 상처를 입을 수 있습니다.

POLARIS는 프라이버시가 완벽히 보장되고 추적이 매우 어려운 분산된 보안 메시지 전달 플랫폼을 제공할 예정입니다. 이를 위해 여러 기술들을 연구하며 적용하고 있습니다.

- Kademlia P2P network
- Shared key exchange
- Secure packet routing
- P2P packet storage

분산화된 저장 금고 (Distributed Vault for Digital Secret Including Private Key)



개인 키는 현대 사회를 살아가는 사람들에게 있어 가장 중요한 디지털 비밀 정보(digital secret)입니다. 개인 키는 암호화뿐만 아니라 서명 및 인증을 위해서도 사용되며 특히 암호화폐 계정에 접근할 수 있는 아주 중요한 열쇠입니다. 따라서 개인 키를 안전하게 보관하는 것은 매우 중요한 일입니다. 하지만 암호화폐가 활성화되면서 암호화폐 거래소를 포함하여 개인 키를 탈취하려는 시도가 날이 갈수록 많아지고 있습니다. 탈취되지 않더라도 개인 키를 잃어버리거나 개인 키를 보관한 하드웨어의 고장으로 인해 자신의 디지털 자산에 영원히 접근하지 못하는 사례가 종종 발생하고 있습니다.

이러한 문제는 비단 개인 키에만 해당되는 문제는 아닙니다. 현대 사회에서는 디지털로 보관할 수 있는 그리고 디지털로 보관해야만 하는 비밀 정보가 늘어나고 있습니다. 온라인 계정의 비밀번호나 금융 거래를 위한 비밀번호 뿐만 아니라 물리적인 잠금장치를 해제하기 위한 비밀번호와 개인 정보가 담긴 문서 및 사진 등 비밀 정보의 양은 계속 늘어나고 있습니다.

이러한 디지털 비밀 정보를 보관하는 방법은 여러가지가 있습니다. 하드웨어 혹은 소프트웨어 지갑에 보관하거나 믿을 수 있다고 판단되는 중앙화된 온라인 저장소에 보관할 수 있습니다. 하지만 지갑에 접근하기 위한 키를 잃어버리거나 하드웨어 지갑이 고장이 나면 영원히 자신의 디지털 비밀 정보에 접근하지 못하게 되기도 하고, 하드웨어 지갑의 경우 지갑을 복구하기 위해

12개 이상의 나열된 단어를 이용하는 등 또 다른 디지털 비밀 정보를 제공하기도 합니다. 중앙화된 온라인 저장소의 경우 보안 결함 또는 정직하지 않은 내부자에 의한 위험을 감수해야만 합니다.

POLARIS에서는 비밀 공유(secret sharing) 기술을 이용하여 디지털 비밀 정보를 잘게 쪼개고 여러 노드가 나누어 보관하는 분산화된 저장소를 제공할 예정입니다. 어느 노드도 정보에 대한 전체 조각을 가지고 있지 않아 특정한 노드의 정보가 보안 결함에 의해 공개되더라도 전체 정보가 유출되지 않습니다. 또한 (t,n)-threshold scheme 을 사용하여 나누어 가진 전체 조각(n개)중 임의의 개수(t개) 이상을 모으면 복구가 가능하기 때문에 지정된 개수 이상의 노드만 정상 동작한다면 언제든지 디지털 비밀 정보를 쉽게 복원 할 수 있습니다.

보호된 개인 인증 (Personal Authentication with Privacy Protection)

우리는 온라인으로 제공되는 다양한 서비스를 사용하고 있습니다. 정부나 공공기관의 민원 서비스, 금융 서비스, 게임 개발사에서 제공하는 게임 서비스 등 많은 서비스에 하루에도 여러번 접근하고 있습니다. 그러나 현실의 '나'와 온라인 상의 '나'를 연결하는 것은 매우 복잡하고 번거로운 일입니다. 모든 사이트마다 "나"에 대해 등록해야 하고 일정 주기마다 갱신해야 하는 경우도 있습니다.

또한 개인의 신뢰도를 측정하고 제공할 수 있는 확실한 방법이 없기 때문에 온라인으로 거래를 하거나 서비스를 주고 받기 위해서는 어느 정도의 위험을 감수해야만 합니다. 개인간의 중고 거래 사기, 악의적인 사용자에 의한 게임 내 경제 시스템의 붕괴 등은 주변에서 어렵지 않게 접할 수 있습니다. 이러한 불편함을 개선하고 개인에 대한 신뢰성을 제공하기 위해 POLARIS는 탈중앙화 환경의 개인 인증 서비스를 제공하려고 합니다.

탈중앙화 네트워크를 이용하면 필요한 정보를 개인이 소유한 디바이스(device)나 중앙화 서버가 아닌 탈중앙화 환경의 노드에 분산하여 보관하기 때문에 분실이나 보안 위협으로 부터 비교적 안전합니다. 또한 블록체인의 불변성과 신뢰성을 이용하여 조작될 수 없는 개인의 신상 정보와 그에 대한 신뢰성을 제공하는 것 또한 가능합니다. 그 예로 개인의 학력 정보나 경력 정보에 대한 신뢰성 확보를 위해 학교에서 학력 증명을 제공하고 기업이 경력 증명을 제공하는 등의 방법을 사용할 수 있습니다.

개인 인증 서비스를 제공하기 위해서 반드시 고려해야 할 점은 개인 정보의 보호입니다. 다른 사람의 개인 정보에 쉽게 접근할 수 있게 된다면 프라이버시 침해가 발생할 가능성이 높아지고 범죄에 노출될 수도 있습니다. 이런 문제를 방지하기 위해 개인 정보는 암호화하여 안전하게 보관해야 하고 본인 스스로가 자신의 개인 정보에 대한 권한을 가지고 통제할 수 있는 방법도 제공합니다. 사용자는 자신의 정보를 열람할 수 있는 대상과 공개 정도를 지정할 수 있습니다.

POLARIS 플랫폼은 네트워크의 ‘나’와 실제의 ‘나’를 연결하기 위해 전통적인 패스워드 기반의 인증 서비스 외에 생체 인식 정보를 사용할 예정입니다. 생체 인식 정보는 쉽게 디지털화가 가능하며 분실이나 위조의 가능성이 적기 때문에 신뢰도가 높으며 이미 검증된 생체 인식 장치들이 널리 쓰이고 있어 접근이 어렵지 않습니다.

개인 인증 서비스는 POLARIS의 다양한 기능들과 자연스럽게 연동 됩니다. POLARIS 플랫폼을 사용하는 DApp은 개인 인증서비스를 이용하여 신뢰할 수 있는 개인간의 계약 서비스를 제공할 수 있습니다. 또한 분산화된 저장 금고를 이용하기 위한 인증을 위해서도 사용됩니다.

탈중앙화 연산 (Decentralized Computation)

상태에 대한 트랜잭션(transaction) 데이터 처리와 달리, encoding / decoding 과 같은 복잡한 연산 또는 대용량 데이터 처리는 일반적인 트랜잭션으로 처리하기에 적합하지 않습니다. 대용량 트랜잭션을 검증하기 위해서는 동일한 양만큼의 컴퓨팅 연산이 필요하므로, 블록 생성자들이 검증 과정을 건너뛰고자 하는 유인(Verifier's Dilemma[26])이 존재하기 때문입니다. 이는 네트워크의 신뢰성에 심각한 취약점이 될 수 있습니다.

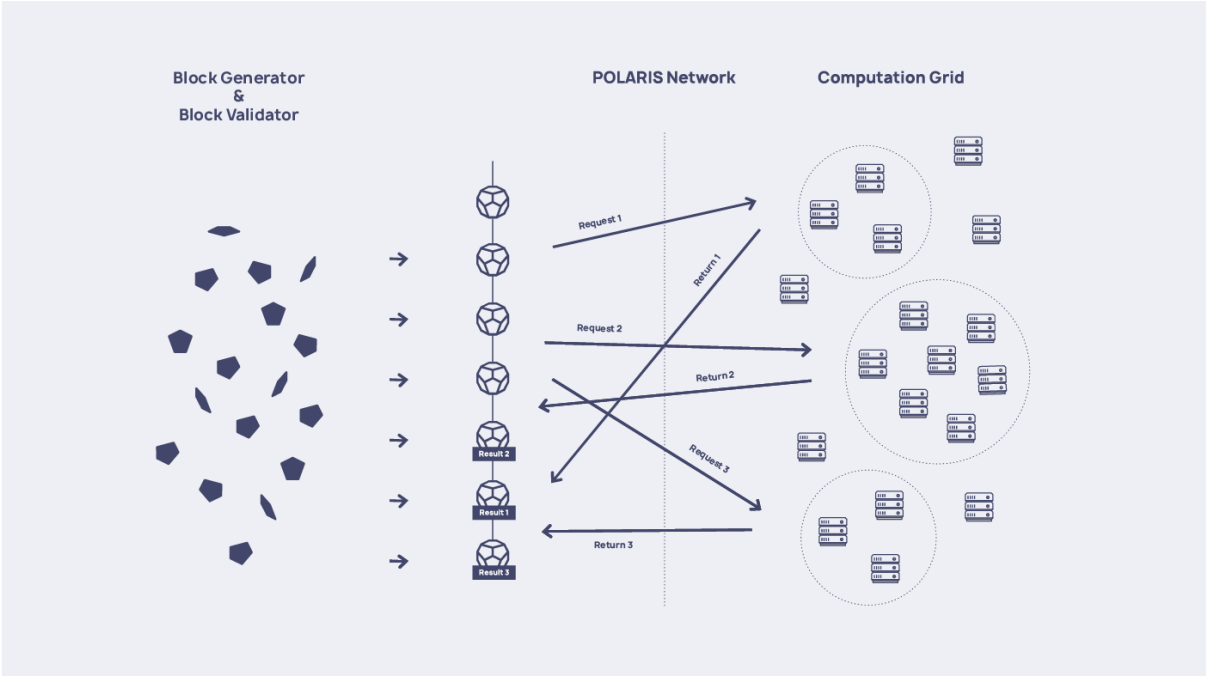
이더리움을 비롯한 많은 블록체인 프로젝트들은 스마트 컨트랙트를 지원하고 있지만 실질적으로 스마트 컨트랙트를 이용하여 DApp을 구현하는 데 있어서는 많은 제약 사항이 존재합니다. 이더리움의 경우 블록당 Gas(수수료) 총량 제한이 있어 Gas를 아무리 많이 제시한다고 해도 복잡한 계산을 수행하기에는 한계가 있습니다. EOS의 경우도 마찬가지입니다. 이더리움과 달리 EOS 토큰 보유 지분에 비례하여 네트워크 자원을 사용할 수 있지만 트랜잭션의 최대 크기를 제한한다거나 노드에 의해 복잡한 계산은 거부될 수 있다는 점에서는 DApp 개발의 한계점으로 지적됩니다.

POLARIS는 기존 플랫폼의 이러한 한계점을 극복하고 진정한 탈중앙화 생태계를 구축하기 위해 복잡한 연산을 전담하여 처리할 수 있는 *POLARIS 연산 그리드(POLARIS Computation Grid)*를 구축할 계획입니다.

*연산 그리드*는 컨트랙트 트랜잭션으로 인한 간섭을 최소화하여 트랜잭션 처리 용량(throughput)을 높이며, 하나의 트랜잭션으로 많은 양의 계산을 수행해야 할 경우에도 전체 네트워크에 영향을 주지 않고 처리할 수 있습니다.

[26] Verifier's Dilemma : Loi Luu, Jason Teutsch, Raghav Kulkarni, and Prateek Saxena. *Demystifying incentives in the consensus computer*, pages 706–719, New York, NY, USA, 2015. ACM. (https://dl.acm.org/citation.cfm?id=2813659)

POLARIS 연산 그리드 (POLARIS Computation Grid)



온 체인과 오프 체인 (On-chain and Off-chain)

만약 무거운 계산을 온 체인(on-chain)방식으로 수행하면 온 체인을 유지하는 모든 노드들이 무거운 계산을 동일하게 수행해야 합니다. 이에 따라 많은 중복 계산이 발생하여 리소스 낭비가 발생하고 다른 트랜잭션들이 바로 처리되지 못하고 무거운 계산을 수행하는 시간만큼 지연됩니다.

이를 피하기 위해 *연산 그리드*는 온 체인에서 계산을 수행하지 않고 오프 체인으로 계산을 수행합니다. 무거운 연산을 담을 트랜잭션을 온 체인 네트워크인 *탈중앙화 그리드*에서 오프 체인 네트워크인 *연산 그리드*로 이동시켜 일정 수준의 신뢰성을 확보할 수 있는 최소한의 노드들만 연산을 처리하고 그 결과만을 온 체인에 반영하여 트랜잭션 부하를 최소화합니다. POLARIS의 온 체인 네트워크인 *탈중앙화 그리드*는 계산된 결과가 담긴 트랜잭션을 이용하여 자신의 스마트 컨트랙트 상태를 업데이트합니다.

연산 노드 (Computation Node)

*연산 그리드*의 적정 노드 수를 예측하기는 쉽지 않습니다. 또한 네트워크 초기에는 대용량 연산이 많이 발생하지 않을 것이기 때문에 *연산 그리드*에 참여한 노드들이 아무 보상도 받지 못한 채 유휴상태로 대기하고 있을 가능성이 큽니다. 그러면 *연산 그리드*에서 이탈하는 노드가 많아지고 결국 신뢰성을 확보할 수 있는 적정 수준의 노드 수를 유지하지 못하게 될 수도 있습니다. 반대로

대용량 연산이 몰릴 경우 *연산 그리드*에 참여하는 노드의 수가 급격히 늘어나기 힘들기 때문에 유연한 대처가 불가능합니다. 충분히 준비된 연산 능력과 신뢰성을 확보하기 위해서는 자유 시장 논리에 의해 *연산 그리드*를 유지하기 보다는 정책적으로 접근할 필요가 있습니다. POLARIS는 블록생성자 후보가 *연산 그리드*에서 임의로 이탈할 경우 벌칙을 부여하여 *탈중앙화 그리드*의 모든 노드들은 모두 *연산 그리드*에 참여하도록 강제화 합니다.

온 체인 네트워크(*탈중앙화 그리드)*와 오프 체인 네트워크(*연산 그리드*)를 구성하는 노드는 모두 동일하지만 네트워크는 완전히 분리되어 작동합니다. 즉, 오프 체인 연산의 중간 과정이 온 체인에 영향을 미치지 않고 오직 결과만 온 체인에 반영됩니다. 하지만 동일한 노드가 온 체인 연산과 오프 체인 연산을 동시에 수행한다면 온 체인과 오프 체인을 분리한 의미가 줄어들 수 있습니다. 따라서 두 연산을 동시에 수행하지 않고 주기적으로 역할 분담을 하여 수행해야 합니다. POLARIS에서는 *탈중앙화 그리드*와 *연산 그리드*를 구성하는 노드를 일정 주기(1 epoch)마다 무작위로 새로 선정합니다. 각 네트워크를 구성하는 노드의 숫자는 대용량 연산을 위한 트랜잭션의 발생 빈도에 따라 유연하게 조정됩니다. *연산 그리드*에 선정된 노드들은 해당 주기 동안 블록 생산과 블록의 검증작업에는 참여하지 않고 오직 대용량 트랜잭션 처리에만 집중합니다.

*연산 그리드*에 참여하여 수행한 대용량 연산에 대한 신뢰도를 정량화하기 위해 각 노드는 별도의 “트러스트 점수(TRUST score)“를 가집니다. 이 점수는 *스파클 합의 체계*의 *프로페션 점수*를 구성하는 요소 중 하나로 *연산 그리드*의 대용량 연산 작업에 대해 소홀하지 못하도록 방지합니다. 지속적으로 정확한 연산 결과를 제출하면 *트러스트 점수*가 증가하고 잘못된 연산 결과를 제출하면 *트러스트 점수*가 대폭 감소합니다. *트러스트 점수*가 높을수록 연산에 대한 보상을 더 많이 받을 수 있기 때문에 노드들이 정확한 연산을 하도록 유도할 수 있습니다. *트러스트 점수*는 오프 체인 트랜잭션이 발생했을 때 계산에 참여할 노드들을 선정하는 기준이 되며, 높은 *트러스트 점수*를 가진 노드들은 적은 수의 노드만으로도 계산 및 합의를 할 수 있습니다.

오프 체인 트랜잭션 생성 (Off-chain Transaction Generation)

스마트 컨트랙트의 모든 연산을 오프 체인으로 처리하는 것은 오히려 성능을 떨어뜨릴 수 있습니다. 연산이 간단한 경우 오프 체인에서의 연산 결과를 온 체인으로 옮기는 과정이 더 많은 자원을 사용 할 수도 있기 때문입니다. 따라서 연산의 크기에 따라 온 체인에서 처리할 것인지 오프 체인에서 처리할 것인지를 결정하는 것이 중요합니다. POLARIS에서는 이를 자동으로 처리할 계획입니다. DApp 개발자는 컨트랙트의 연산에 대해 온 체인에서 처리할지 오프 체인에서 처리할지 고민하고 결정할 필요없이 동일한 방식으로 트랜잭션을 만들 수 있습니다. 트랜잭션을 전달받은 노드가 자체적인 메커니즘에 의해 트랜잭션의 연산량을 예측하고 그에 따라 일정 수준 이상의 대용량 트랜잭션을 자동으로 오프 체인 트랜잭션으로 변환하여 *연산 그리드*로 넘길

것입니다. 트랜잭션의 연산량을 예측하는 메커니즘은 완벽하지 않을 수 있지만 최적의 부하 분산(load balancing)을 위해 지속적으로 살펴보고 개선해 나갈 예정입니다.

트랜잭션이 정상적으로 완료되려면 실제 연산량에 비례하는 충분한 양의 자원이 확보되어야 합니다. 따라서 개발자는 트랜잭션을 발생시키기 전에 예상되는 연산량을 감당할 수 있는 충분한 양의 토큰을 예치해야 합니다.

일반적으로 오프 체인에서 트랜잭션을 처리하기 위해서는 다음과 같은 정보가 필요합니다.

- **상태 트리**
  컨트랙트의 연산을 수행하기 위해서는 컨트랙트의 이전 상태를 알아야 하므로 컨트랙트의 상태 트리를 오프 체인에 넘겨주어야 합니다. 노드들은 계산을 수행한 뒤 결과에 따라 이 상태 트리를 업데이트합니다.

- **코드**
  오프 체인에서 수행할 스마트 컨트랙트의 코드를 넘겨주어야 합니다.

- **계좌 정보**
  오프 체인에서 수행할 스마트 컨트랙트의 계좌와 그와 관련된 모든 계좌의 정보를 넘겨주어야 합니다.

- **연산 한도**
  오프 체인에서 수행할 스마트 컨트랙트 연산에 대한 계산의 한도입니다. 계산에 참여한 노드들은 연산을 수행하다가 인스트럭션 개수가 해당 한도를 초과하면 연산을 그만두고 "실패(fail)"를 반환합니다. 연산 한도는 트랜잭션을 발생시킨 사용자의 토큰 예치량에 의해 결정됩니다.

다른 탈중앙화 대용량 연산을 위한 프로젝트와는 달리 POLARIS에서는 온 체인 네트워크과 오프 체인 네트워크를 구성하는 노드들이 동일합니다. 이러한 효율적인 네트워크 구성으로 인해 연산에 필요한 정보들을 스마트 컨트랙트의 생성자 또는 수행자가 따로 전달할 필요가 없어 대용량 연산을 수행하는 DApp의 작성이 더욱 쉬워집니다.

오프 체인 트랜잭션 처리 (Off-chain Transaction Processing)

오프 체인 트랜잭션이 발생하면 *연산 그리드*의 노드들은 모두 그 트랜잭션을 수신하며, 별도의 분산 랜덤 알고리즘에 의해 계산을 수행할 노드가 결정됩니다. 선정된 노드들은 트랜잭션의 연산을 수행하여 그 결과에 서명하고 제출(전파)합니다. 계산에 참여한 노드 중 2/3 이상이 동의한 결과를

정답으로 간주하며 만약 2/3 이상이 동의한 결과가 없을 경우, 더 많은 노드를 재선정하여 다시 연산에 참여시킵니다.

정답이 정해지면 *탈중앙화 그리드*로 결과를 반환하며, 각 노드는 제출한 결과의 정답 유무에 따라 *트러스트 점수*가 상승 또는 하락합니다. 정답을 제출하면 점수가 증가하며, 오답을 제출하면 점수가 50%이상 대폭 감소합니다. 높은 점수는 곧 꾸준히 정답을 제출했다는 뜻이므로 점수가 높은 노드들은 적은 수의 노드들만 모여서 연산을 수행해도 그 결과값에 대해 일정 수준 이상의 신뢰성을 보장할 수 있습니다.

이러한 원리를 이용하여 연산에 참여하는 노드의 숫자를 결정합니다. 일정 수준의 신뢰성을 보장하기 위한 *트러스트 점수*의 임계치를 정해 놓고, 노드들의 점수 합이 그 총량을 넘도록 노드들을 선정합니다. 노드들은 난수에 의해 순서가 정해지고 앞에서부터 차례로 선정이 되다가 각 노드들의 *트러스트 점수*의 합이 정해진 임계치를 넘어서는 순간 노드 선정이 마감됩니다. 모든 노드들이 다른 노드들의 *트러스트 점수*와 선정 순서를 알고 있으므로 노드 선정에 합의할 수 있습니다.

연산 결과 합의에 필요한 최소 노드수는 3개이며 1개 또는 2개 노드의 *트러스트 점수*의 합이 임계치를 넘더라도 3개의 노드가 선정됩니다.

플랫폼과 각 노드는 몇 가지 순서와 규칙에 의해 연산을 수행합니다.

- 오프 체인 트랜잭션이 발생하면 사용자의 토큰 예치량에 따라 설정된 연산 한도에 비례하여 **최대 수행시간 타이머(maximum execution time timer)**가 시작됩니다
- 연산 결과가 하나 둘씩 모여 ⅔ 이상이 동일한 결과를 제출하게 되면 그 순간 또 다른 타이머(timer)인 **완결 타이머(finalization timer)**가 시작됩니다. 그렇지 않으면 **완결 타이머**는 시작되지 않습니다
- 두 타이머중 어느 하나라도 만료가 되면 더 이상 연산 결과를 제출할 수 없습니다. 그 때까지 제출된 결과 중에 선정된 노드의 ⅔ 이상이 동의한 결과가 없으면 연산 노드를 더 많이 재선정하여 다시 연산을 수행합니다. 이 때 **최대 수행 타이머**도 다시 시작됩니다.
- 만약 두 타이머가 만료되기 전에 연산 결과를 제출하면 이미 결과 합의에 이르렀다고 하더라도 정해진 보상을 받을 수 있습니다.

보상과 벌칙 (Incentive and Penalty)

*연산 그리드*에 참여한 노드들에 대해 보상은 *트러스트 점수*와 *프로페션 점수*를 높여주는 것 이외에 블록 생성 보상과 마찬가지로 토큰 인플레이션에서 일정 비율을 보상으로 지급할 수 있습니다. 추가 보상이 필요하다고 판단되는 경우 그 보상 비율은 거버넌스에 의해 결정됩니다.

*다만, 연산 그리드*에 대한 별도의 보상이 주어질 경우 몇 가지 사항을 고려해야 합니다.

- 연산을 많이 수행한 노드가 더 많은 보상을 가져야 합니다.
- *트러스트 점수*가 높은 노드가 더 많은 보상을 가져야 합니다.
- 연산을 더 빠르게 수행한 노드가 조금 더 많은 보상을 가져야 합니다.

이러한 원칙에 따라 *연산 그리드*에 참여한 각 노드는 해당 기간(epoch) 동안 자신이 수행한 연산 결과와 수행 시간, *트러스트 점수*에 따라 차등적으로 보상을 부여받게 됩니다. 따라서 각 노드들은 자신의 보상을 높이기 위해 시스템의 사양과 *트러스트 점수*를 꾸준히 높여나갈 것입니다.

잘못된 결과를 제출하거나 잘못된 행동을 하는 노드들에게는 벌칙을 부여하고 일정 기간동안 보상 기회를 박탈함으로써 처벌할 수 있습니다. 또한 잘못된 행동의 종류와 벌칙의 강도는 거버넌스에 의해 언제든 바뀔 수 있습니다.

- **연산 결과를 늦게 제출하거나 제출하지 않은 경우**
  타이머가 만료될 때까지 연산 결과를 제출하지 못했다는 것은 노드의 시스템 사양이 너무 낮거나 네트워크나 시스템에 관련된 장애가 발생했거나 일부러 제출하지 않았을 경우 등 입니다. 위의 경우 모두 노드에게 책임이 있으므로 *트러스트 점수*가 소폭(5 ~ 10%) 감소합니다

- **잘못된 연산 결과를 제출한 경우**
  잘못된 연산 결과를 제출하는 경우는 POLARIS 시스템 버그이거나 악의적으로 잘못된 연산 결과를 제출하는 경우 뿐입니다. 시스템 버그일 경우 다른 노드들도 마찬가지로 잘못된 연산 결과를 제출할 것이므로 결국 악의적인 경우가 아니면 합의되지 못하는 결과를 제출할 확률이 거의 없습니다. 따라서 오답을 제출했을 경우에는 악의적인 행동을 했다고 간주하여 *트러스트 점수*를 대폭(50%) 감소시킵니다. 억울한 경우가 있을 때에는 증거 자료를 제출하면 거버넌스에 의해 점수가 복구될 수도 있습니다.

- **의도적으로 *연산 그리드*로 부터 이탈하는 경우**
  블록생성자 후보 노드는 물리적인 시스템 자원을 상대적으로 많이 사용하는 대용량 연산을 피하기 위해 *연산 그리드*로 선정된 후 네트워크로부터 이탈하려고 할 수 있습니다. 이런

상황을 막기 위해 *연산 그리드*로 선정된 시간의 20%이상 동작할 수 없는 상태인 노드는 다시 *연산 그리드*로 선정되어 자신의 역할을 마무리 할 때까지 블록생성자로 선정될 확률이 0이 됩니다.

알려진 공격에 대한 대비 (Known Attacks and Protection)

Sybil Attack

새로운 노드를 많이 만들어서 *연산 그리드*에 참여하여 연산 결과의 조작을 시도할 수 있습니다. 하지만 각 참여 노드는 최소한의 신분을 밝혀야 하고 실제 연산에 참여하는 노드는 난수에 의해 임의로 선정되기 때문에 공격의 성공률은 매우 낮습니다.

또한 *연산 그리드*에 처음 참가하는 노드들은 기본적으로 낮은 *트러스트 점수*를 가지고 있어 합의를 위해 더 많은 노드들이 필요하여 악의적인 노드들이 ⅓ 이상이 선정될 확률은 매우 낮습니다. 만약 ⅓ 이상이 악의적인 신규 노드들로 선정되어 연산 결과 합의에 실패했다고 하더라도 ⅔ 이상을 점유하지 못했다면 더 많은 노드들이 다시 선택되어 연산을 다시 수행하기 때문에 공격의 성공 가능성은 더 낮아집니다.

DoS(Denial-of-Service) Attack

무한 루프(infinite loop)에 빠지는 연산을 이용해 *연산 그리드*를 공격할 수 있습니다. 하지만 노드들은 사용자의 토큰 예치량에 기반한 한도만큼의 연산을 모두 수행하면 즉시 "실패"를 반환하므로 무한 루프에 빠지지 않습니다.

따라서 트랜잭션을 발생시키는 개발자는 자신의 코드가 완료되기 위해 반드시 적절한 양의 토큰을 예치해야 합니다. 계산에 참여한 노드들에 의해 연산 결과가 “실패"로 합의하게 되면 연산 보상은 절반만 주어집니다. 이를 통해 연산에 참여한 노드들의 묵시적인 담합을 방지할 수 있습니다.

Free-Riding

계산에 참여한 이기적인 노드가 실제 연산은 수행하지 않았으면서 다른 노드로부터 전파받은 정답을 자신이 계산한 정답인 것처럼 제출할 수 있습니다. 이 것을 방지하기 위해 연산을 완료한 노드는 정답을 먼저 전파하지 않고 정답의 해시(hash)값과 임의로 선정된 난수의 해시값, 또 그 둘을 조합한 값의 해시값을 먼저 전파합니다. ⅔이상의 노드가 제출한 후에 실제 정답과 각 노드가 사용한 난수를 전파하는 방식으로 정답의 사전 공개를 피하면서 합의를 할 수 있습니다.

컴포넌트로 이루어진 유연한 플랫폼 (Componential and Flexible Platform)

탈중앙화 플랫폼과 관련 기술은 매우 빠른 속도로 발전하고 있습니다. 또한 전체 생태계를 운영하기 위한 정책 또한 빠르게 변화하고 있습니다. 새로운 기술과 정책을 적용하기 위해서는 어쩔 수 없이 코드 수정이 일어나야 하고 때로는 일정 시간동안 네트워크를 중단해야 할 수도 있습니다. POLARIS는 필요에 따라 편리하고 안전하게 코드를 수정할 수 있는 구조를 만들고 정책 변경으로 인한 네트워크의 중단을 최대한 피할 수 있는 방법을 고민하였습니다.

컴포넌트로 이루어진 코어와 플랫폼 (Componential Core and Platform)

가장 적합한 side chain을 구성하여 *POLARIS 협력 그리드*에 참여하기 위해서는 플랫폼의 여러 부분과 정책에 대한 수정이 필요할 수 있습니다. POLARIS는 코어(core)와 플랫폼을 component로 구성할 계획입니다. 또한 합의 알고리즘을 선택하여 구동할 수 있도록 component로 제공합니다. component로 제공되는 기능들은 POLARIS 개발팀 그리고 오픈 소스 공헌자(contributor)들에 의해 계속 늘어날 예정입니다.

또한 현재의 탈중앙화 플랫폼들은 OS(Operating System)의 커널(kernel)에 가깝습니다. 핵심 동작 로직만 가지고 있을 뿐 코어(core)를 확장하고 DApp을 연결하는 실제 “플랫폼”이라 할 수 있는 환경은 아직 많이 부족합니다. POLARIS는 충분히 유연한 플랫폼과 더 잘 정의된 플랫폼 API[27]를 제공하고자 합니다. 개발자는 이를 이용해 간단한 DApp을 작성하는데 사용할 수 있을 뿐만 아니라 마켓플레이스와 같은 복잡한 서비스를 쉽게 구성할 수 있고 규모가 큰 2nd layer platform도 편리하게 작성할 수 있습니다.

다양한 산업군을 위한 프레임워크 (Framework for Various Industrial Domain)

기존 산업에서 탈중앙화를 적용하는 것이 어려운 이유 중 하나는 산업별로 특화된 프레임워크(framework)가 부족하다는 것입니다. POLARIS는 금융, 물류, 회계 등 다양한 산업군을 위한 프레임워크를 추가로 제공합니다. 제공되는 프레임워크는 산업군에 따라 가장 적합한 합의 알고리즘의 적용이 가능하며 편리한 개발을 위한 전용 API가 추가될 예정입니다.

[27] API : https://en.wikipedia.org/wiki/Application_programming_interface

스스로 개정되는 플랫폼과 거버넌스 (Governance on Self-amended Platform)

현재 운영중인 탈중앙화 네트워크 또한 더 나은 방향으로 발전하기 위해 좋은 정책과 새로운 기술들을 적용해야 하고 그러기 위해서는 코드의 수정을 피할 수 없습니다. 그렇지만 정책이나 기술을 변경하기 위해서 네트워크를 중단하는 일은 많은 손실과 혼선을 유발할 가능성이 있습니다. 그러므로 변화하고 발전하는 POLARIS 생태계(*POLARIS Universe*)를 효율적으로 지원하기 위해서 플랫폼 스스로 새로운 정책과 기술을 적용하고 그 변화를 동작 중인 네트워크에 자연스럽게 녹여낼 수 있는 기능이 필요합니다.

POLARIS는 불필요한 분쟁을 피하고 올바른 정책을 공정하고 편리하게 결정할 수 있도록 온 체인 거버넌스(on-chain governance)를 이루는데 필요한 기술과, 거버넌스를 통해 결정 된 정책을 쉽게 전체에 전파하고 또 적용할 수 있는 self-amendment 기술을 제공합니다. CARDANO[28] 프로젝트가 추구하는 "네트워크를 파괴하지 않으면서, 이미 배포된 시스템을 업그레이드할 수 있는 능력 구축 (Building in the ability to upgrade post-deployed systems without destroying the network)", 그리고 Tezos[29] 프로젝트가 구현하고 있는 self-amendment 기술은 이러한 기능을 구현하고자 하는 훌륭한 노력입니다. POLARIS는 다른 프로젝트의 앞서가는 기술을 연구하는 동시에 독자적인 개발을 통해 더 나은 self-amendment 기술을 구현할 계획입니다.

거버넌스를 구축하기 위한 기술 (Technology for POLARIS Governance)

POLARIS는 공정하고 손쉬운 합의를 위해 회담과 공개 투표 기능을 지원합니다. 그리고 회담을 통해 합의된 의견이나 투표 결과를 투명하고 빠르게 적용하기 위해서는 다양한 조절인자(parameter)들을 체인 위에서 즉시 적용할 수 있어야 합니다. 이를 위해 POLARIS는 역할별로 필요한 기능들을 구현하고 API와 명령(Command)으로 제공합니다. 이 기능들을 통해 인플레이션(inflation) 비율이나 인플레이션에 의해 생성된 토큰의 배분 비율 등을 조절할 수 있고 이런 조절인자에 의해 구성되는 POLARIS 네트워크는 더 효율적으로 운영될 수 있을 것입니다. 그 밖에 POLARIS는 더 많은 조절인자를 즉시 네트워크에 적용할 수 있도록 필요한 기능을 꾸준히 추가할 예정입니다. 예를 들어, DFINITY[30]의 Algorithmic Governance[31]는 세세한 합의를 줄이면서도 더 많은 조절인자를 적절하게 유지할 수 있는 좋은 대안 중 하나입니다. POLARIS는 그들의 발전과 연구 결과를 꾸준히 살펴보며 배우고 있습니다.

[28] CARDANO : https://www.cardano.org/
[29] Tezos : https://tezos.com/
[30] DFINITY : https://dfinity.org/
[31] DFINITY's Algorithmic Governance: https://dfinity.org/tech

스스로 이루어지는 개정 (Self-amendment)

온 체인 거버넌스를 통해 POLARIS는 체인의 발전을 특정 집단이 모여서 논의하거나 투표로 결정하지 않고 실제 체인 위의 프로토콜을 통해 결정할 수 있습니다. 그런데 결정 된 정책이나 수정사항을 정상적으로 체인에서 사용하기 위해서는 모든 노드에 수정사항이 전파되고 반영되어야 합니다. 만약 어떤 노드는 수정 사항을 반영하고 어떤 노드는 반영하지 않은 상태에서 트렌젝션을 주고받게 된다면 체인이 정상적으로 동작할 수 없고 체인이 분리되거나 네트워크가 멈추는 현상까지 발생할 수 있습니다.

POLARIS에서는 이러한 상황을 방지하기 위해 결정 된 정책과 필요한 수정사항을 체인을 통해 전파하려 합니다. 그러면 POLARIS의 각 노드들이 수정사항을 전달받아 자동으로 정해진 시점에 프로그램을 업데이트 할 수 있습니다. 체인을 통해 수정사항을 전파하는 방법은 여러가지가 있을 수 있는데 그 중 수정사항을 블록에 담아 체인을 통해 전달하고 노드에 반영하는 예시는 아래와 같습니다.

1. 노드는 블록을 전달 받을 때 마다 블록을 검증하고 저장하는 과정에서 해당 블록에 반영해야 할 수정사항이 포함되어 있는지 확인합니다.
2. 수정사항이 포함되어 있는 경우 블록에는 수정사항에 관한 추가 정보가 포함되어 있으며 노드는 특히 아래의 정보를 확인합니다.
    - 수정사항의 종류
    - 수정사항의 내용
    - 수정사항이 반영되어야 할 블록넘버
3. 노드는 확인 한 수정사항이 인플레이션 비율이나 인플레이션에 의해 생성 된 토큰을 분배하는 비율등을 변경하는 간단한 설정이나 조절인자(parameter)의 수정일 경우 변경되어야 할 내용을 언제나 적용할 수 있도록 미리 준비합니다.
4. 확인 한 수정사항이 노드 프로그램 코드의 수정이나 새로운 프로토콜의 반영 등 노드 프로그램이 수정되어야 할 경우 필요한 코드를 자체적으로 컴파일 하거나 네트워크에서 다운로드 받아 적용 할 바이너리를 준비합니다.
5. 노드는 약속된 블록넘버가 되면 수정사항을 반영하여 새로운 정책으로 동작합니다.

POLARIS 플랫폼은 위와 같은 기술을 구현함으로써 새로운 정책을 적용하기 위해 네트워크를 멈추는 상황을 최소로 줄일 수 있습니다.

DApp 개발과 개발 도구 (DApp Development and Development Tools)

개인 또는 기업이 기존의 서비스에 탈중앙화를 적용하려면 상당히 많은 노력이 필요합니다. 이미 오랜 시간 동안 잘 다듬어진 여러 도구와 플랫폼을 사용하여 개발하던 기존의 중앙화된 응용프로그램과는 달리 DApp 을 위한 환경은 아직 너무나 부족합니다. 이를 해결하기 위해서는 적절한 지원, 잘 갖추어진 플랫폼, 개발을 위한 잘 정리된 문서 그리고 이 모든 것을 편리하게 활용할 수 있는 개발 환경이 반드시 필요합니다.

POLARIS는 이에 대한 해결책으로 다음의 목표를 가지고 있습니다.

개발 도구, "Chain Forge” (Development Tools, “Chain Forge”)

잘 정돈된 플랫폼과 API를 제공하는 것만큼 그것들을 쉽게 사용할 수 있도록 도와주는 개발도구도 중요합니다. 많은 개발 자원에 빠른 접근이 가능해야 하고 복잡한 API도 쉽게 사용할 수 있어야 합니다. 또한 테스트(test) 및 디버깅(debugging)도 어렵지 않아야 합니다. POLARIS는 DApp 개발 및 서비스 구성을 위한 개발 도구인 *Chain Forge* 를 제공하고 꾸준히 업데이트하겠습니다.

즉시 이루어지는 배포 (Instant Deploy)

POLARIS는 DApp 을 바로 deploy 하여 운영할 수 있도록 지원합니다. 또한 독립적인 *companion chain* 의 구성이 필요한 경우에도 *POLARIS Multiverse* 환경을 이용하여 즉시 체인을 구성할 수 있는 관리 도구를 제공합니다.

스마트 컨트랙트를 위한 다양한 프로그래밍 언어 지원 (Diverse Programming Language Support for Smart Contract)

개발자에게 개발 언어(programming language)는 서예가의 붓과 같습니다. 개발자에게 익숙한 개발 언어를 사용할 수 없다는 점은 스마트 계약(smart contract)의 작성을 어렵게 하는 장애물 중 하나입니다. 용도에 따라 적절한 도구를 선택하는 것도 중요하지만 일반적인 경우에는 익숙한 도구가 가장 빠르고 편리합니다. POLARIS는 DApp 개발자의 저변 확대와 편의성 향상을 위해 스마트 계약을 위한 개발 언어를 확장해 나가겠습니다.

컨설팅과 기술 지원 (Consulting and Technical Support)

좋은 DApp 을 기획하고 설계하기 위해서는 기존의 중앙화된 응용프로그램과는 다른 많은 지식과 정보를 알아야 합니다. 또한 DApp 을 개발하는 과정에서 마주하게 되는 새로운 기술에 대한 조언, 운영 상황에서 발생하는 문제에 대한 빠른 분석 및 해결에 대한 지원 역시 꼭 필요합니다.

재단은 외부 전문 업체와의 협약을 통해 기획과 설계, 개발에 대한 전문적인 자문(consulting)과 기술 지원(technical support)을 제공할 예정입니다.

연구와 기술의 발전 (Research and Technology Improvement)

탈중앙화는 블록체인 또는 그와 동일한 역할을 할 수 있는 기술, 그리고 코드(code)로 만들어지는 기술의 구현체에 의해 이루어지고 유지됩니다. 그러므로 기술과 코드는 탈중앙화 생태계를 구성하는 매우 중요한 기본 요소입니다.

POLARIS는 경쟁에서 앞서 나갈 수 있도록 치열한 기술 연구 및 개발 계획을 가지고 있습니다.

EOSIO[32] 로 부터 (From EOSIO)

새로운 탈중앙화 플랫폼을 개발하는데 있어서 기존 프로젝트의 결과물을 이용할지, 아니면 처음부터 다시 개발할지를 결정하는 것은 어려운 일입니다. 어느 방식으로 결정하더라도 명확한 장점과 단점이 있습니다. POLARIS는 이에 대해 많이 고민하였고, 기존의 잘 만들어진 플랫폼을 활용하기로 결정 하였습니다. POLARIS 프로젝트는 기존의 프로젝트들과는 많은 부분이 다른 전혀 새로운 플랫폼이지만 기존의 검증된 플랫폼을 기반으로 필요한 부분을 하나씩 바꿔 나가는 것이 좀 더 빠른 결과를 낼 수 있을거라 기대하기 때문입니다. 충분한 시간 동안 시작의 기준으로 삼을 만한 많은 프로젝트를 검토하였고 그 결과 EOSIO 가 가장 적합하다고 판단하였습니다.

EOSIO는 앞서가는 훌륭한 프로젝트 중의 하나입니다. 많은 훌륭한 프로젝트가 있지만 EOSIO는 현재의 중앙화된 산업이 탈중앙화된 생태계에 더 쉽게 참여할 수 있는 구조를 가지고 있습니다. 더불어 EOSIO가 현재 제공하고 있는 트랜잭션(transaction) 처리 속도는 상용화 수준에 가장 가깝습니다. WebAssembly[33] 를 구동할 수 있는 잘 만들어진 WAVM[34] 이 이미 완성되었다는 것도 EOSIO 의 장점입니다.

POLARIS 는 EOSIO 를 바탕으로 EOS DApp 과의 단방향 호환성을 계속 유지하고 독자적인 기능 또한 계속 추가해 갈 것입니다. 또한 우리의 결과물 중 EOSIO 와 공유할 수 있는 부분들은 EOSIO 에 기여하고 새로운 기술 개발을 위해 협력해 나갈 것입니다.

기술을 대하는 자세 (Attitude towards Technology)

우리는 미래의 기술 발전과 연구 결과에 대해 미리 예측할 수 없다는 사실을 알고 있습니다. 또한 현재에 잘 알려진 기술이 머지않은 미래에는 새로운 기술에 자리를 내어줄 수 있다는 것 또한 잘

[32] EOSIO : https://eos.io/
[33] WebAssembly : https://en.wikipedia.org/wiki/WebAssembly
[34] WAVM : https://github.com/EOSIO/eos/tree/master/libraries/wasm-jit

알고 있습니다. 많은 프로젝트들이 이로 인해 정해진 로드맵(roadmap)을 지키지 못하거나 자주 수정하는 것은 어쩌면 당연한 결과일 수 있습니다.

POLARIS는 새로운 기술의 빠른 적용과 편리한 개발을 위해 잘 구성된 좋은 코드를 작성하고 쉽게 변경 가능한 플랫폼을 구축하여 기술 변화에 더 유연하게 대응하겠습니다. 또 합의 알고리즘 변경을 포함한 모든 정책과 기술의 발전에 대해 항상 열린 자세로 살펴볼 것입니다.

POLARIS는 관련 기술에 대해 다음과 같이 연구하고 발전시킬 예정입니다.

- 협력사와 지속적인 기술 연구 및 개발
- 산학협동 연구를 통한 선도 기술 연구 및 검증
- 다른 프로젝트와의 활발한 파트너십(partnership)
- 업계 기술 동향에 대한 끊임없는 관심과 조사

추가적인 개발 목표들 (Additional Development Items)

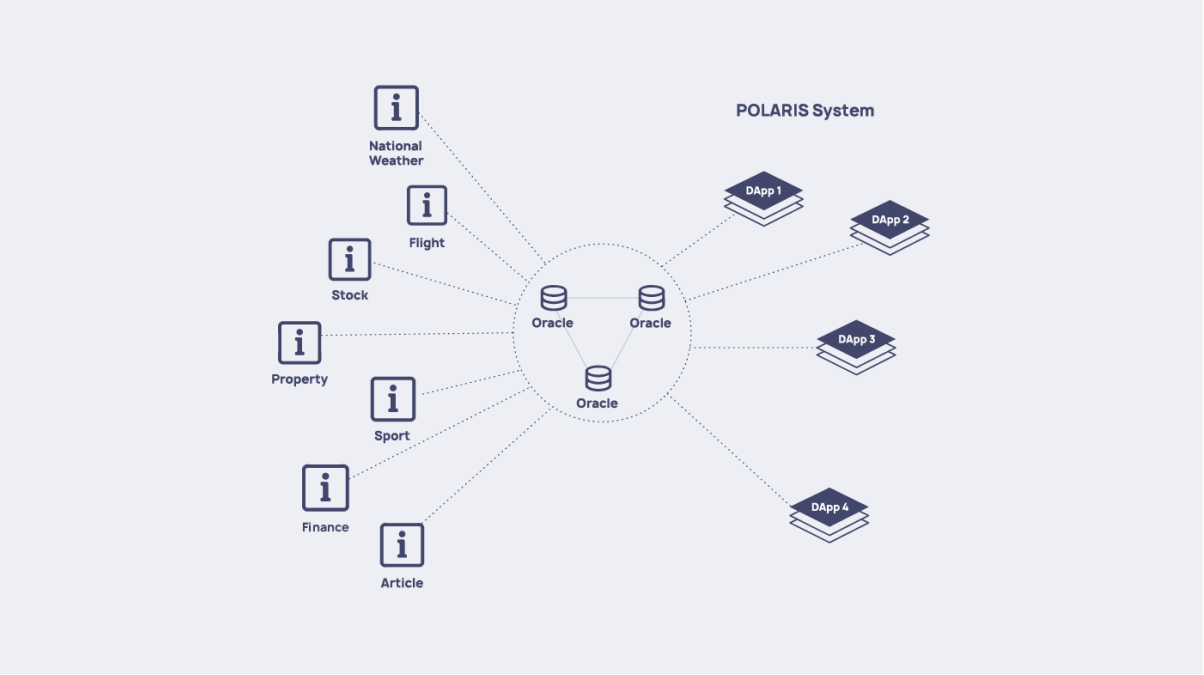
DApp이 필요로 하는 다양한 기능을 플랫폼이 제공하기 위해서는 블록체인이나 DAG과 같은 코어(core) 기술만으로는 해결하지 못하는 많은 문제들이 있습니다. 더불어 *탈중앙화 그리드*를 구성하고 있는 세계 각지의 많은 노드들을 더 잘 활용할 필요성도 있습니다.

POLARIS에서는 DApp이 편리하게 활용할 수 있는 많은 기능을 플랫폼에 담고, 생태계에 도움을 줄 수 있는 기능을 추가적으로 지원하기 위한 여러 개발 목록들을 가지고 있습니다. 앞으로도 기술의 발전과 연구 결과에 따라 꾸준하게 개발 목표를 정비하고 목록을 추가해 나갈 예정입니다.

믿을 수 있는 오라클 플랫폼 (Reliable Oracle[35] Platform)

탈중앙화 플랫폼에서 스마트 컨트랙트를 수행하기 위해서는 플랫폼 외부의 정보가 필요한 경우가 있습니다. 그러나 외부가 제공하는 정보는 플랫폼 내부에서 검증되지 않아 바로 신뢰하기 어렵습니다. 항공기 지연에 대해 보상해 주는 보험 상품을 스마트 컨트랙트로 작성하는 경우, 항공기의 지연 여부에 대한 정보를 어디서 어떻게 가져올 것인지 또 가져온 정보에 대해 충분히 믿을 수 있는지에 대한 많은 고민이 필요합니다. POLARIS는 이러한 문제를 해결하기 위해서 신뢰할 수 있는 오라클(oracle) 시스템을 구축하고 스마트 컨트랙트에서 쉽게 사용할 수 있는 잘 정의된 API를 제공할 예정입니다.

[35] Oracle : https://blockchainhub.net/blockchain-oracles/



신뢰할 수 있는 외부 정보를 제공하기 위해서는 두 가지 조건을 만족해야 합니다.

- **정보 제공자는 정보를 조작하지 않아야 합니다.**
  스포츠 경기 결과 처럼 비독점적인 정보의 경우 제공자가 정보를 조작했는지 검증하는 것은 간단합니다. 여러 곳의 출처로부터 동일한 조건의 정보를 모아 서로 비교해보면 됩니다. 악의적인 정보 제공자가 절반이 넘지 않는다면 반 이상의 제공자가 동의한 정보를 진실로 간주할 수 있습니다.

  하지만 독점적인 정보인 경우에는 정보의 진실성을 검증하는 것은 매우 어렵습니다. 이 경우에는 정보 제공자의 신뢰도에 따라 데이터의 신뢰도가 결정됩니다.

- **정보를 온 체인(on-chain)으로 가져오는 과정에서 정보가 조작되지 않아야 합니다.**
  정보 제공자가 진실된 정보를 제공한다고 해도 오라클 시스템이 온 체인으로 데이터를 옮기는 과정에서 데이터를 조작할 수 있습니다.

  POLARIS는 여러 개의 독립된 노드를 이용한 분산 오라클 시스템을 구성하여 정보의 조작이 어렵도록 합니다. 각 독립된 노드는 누구의 영향도 받지 않으며 적당한 인센티브에 의해 지속적으로 정직하게 행동하도록 유도할 수 있습니다. 또 서로가 서로를 검증하면서 악의적인 오라클 노드를 보고함으로써 별도의 보상을 받을 수도 있습니다. 각각의 노드는 더 많은 보상을 얻기 위해 더 신뢰성이 높은 데이터 제공자를 끊임없이 찾아야 하며 서로 경쟁하는 과정을 통해 더 높은 신뢰성이 확보되는 선순환을 유도합니다.

오라클 시스템을 여러 개의 노드로 분산하는 것은 신뢰성을 높일 수 있는 좋은 방법이지만 더 많은 노드의 합의가 필요해 처리 성능은 낮아질 수 있습니다. 이를 보완하기 위해 자동 수집을 사용할 수 있습니다. 자동 수집을 위한 항목은 온 체인에서 자주 사용될 것이라고 예상되는 정보들로 구성되며, 사용자의 특별한 요청이 없어도 오라클 시스템에 의해 자동적으로 수집됩니다. 자동 수집 항목은 사용자의 요청에 대한 통계에 따라 적절하게 변경되어 효율성을 유지합니다.

오라클 정보에 대한 사용자의 요청이 발생하면 정보 수집을 담당할 오라클 노드들을 선정합니다. 선정된 오라클 노드들은 수집한 정보에 대해 합의를 수행하며 합의 결과에 따라 정보를 저장하고 사용자에게 반환합니다. 데이터를 수집할 오라클 노드들을 예측할 수 없는 난수에 의해 선정하여 적은 수의 노드가 참여하더라도 정보의 조작을 어렵게 만들 수 있습니다.

외부 정보 중에는 날씨 정보와 같이 수집 기관이나 수집 시기에 따라 달라지는 정보들이 있습니다. 날씨는 시시 각각 변하고 측정 장비마다 값이 다르므로 특정 정보 하나만을 진실로 간주할 수 없습니다. 이러한 정보는 수집된 정보를 특성에 맞게 조합하여 결과에 합의하는 것이 합리적이며 합의된 결과에 얼마나 근접한지를 판단하여 보상을 지급할 수 있습니다.

탈중앙 저장소 (Decentralized Storage)

지금까지의 탈중앙화 플랫폼들은 용량이 큰 데이터의 전송에 한계를 가지고 있습니다. 블록의 크기를 키우게 되면 블록의 처리와 전송을 위한 부하가 커지게 되어 블록의 크기는 어느정도의 제한이 있으며 용량이 큰 데이터는 블록에 저장할 수 없습니다. POLARIS는 이를 극복하기 위해 데이터를 분산하여 탈중앙화 노드들에 저장하는 별도의 프로토콜을 제공할 계획입니다.

데이터를 분산하여 저장하는 방법으로는 가장 먼저 이미 널리 알려진 토렌트 프로토콜(torrent protocol)[36]을 생각해 볼 수 있습니다. 토렌트 프로토콜은 데이터를 일정한 크기로 나눠 여러 사용자들에게 분산하여 저장하고 데이터가 필요 할 때에는 서로간의 직접 연결(peer to peer)을 통해 파일을 주고 받습니다. 이를 탈중앙화 플랫폼에 적용하기 위해서는 데이터가 변조되지 않았음을 검증해야 하고 데이터를 저장한 모든 노드가 네트워크에서 사라져 더 이상 파일을 구할 수 없어지는 상황을 방지해야 합니다. POLARIS는 신뢰도를 높이고 네트워크를 더 잘 활용하기 위해 토렌트 프로토콜과 InterPlanetary File System (IPFS)[37] 및 관련 프로젝트에 대해 연구하고 있습니다. 또한 다수의 사용자의 참여를 유도하고 이탈을 방지할 수 있는 가장 적합한 보상 방법에 대해서도 검증하고 있습니다.

[36] torrent protocol : http://www.bittorrent.org/beps/bep_0003.html
[37] IPFS : https://ipfs.io/

다른 개발 목표 (Other development Items)

탈중앙화 거래소 (DEX)

POLARIS 멀티버스에 존재하는 토큰들 간의 교환을 쉽게 해 줄 수 있는 탈중앙화 거래를 위한 플랫폼을 제공하고자 합니다.

향상된 웹 어셈블리 가상머신 (Enhanced WebAssembly Virtual Machine)

가상머신이 시스템에서 사용하는 자원을 최대한 줄이고 성능을 높이는 것은 DApp의 동작 속도 및 노드의 처리용량 향상과 직접적인 관련이 있습니다. 이를 위해 현재의 가상머신을 레지스터 머신(register machine) 으로 변경하는 등의 방법을 통해 가상머신을 지속적으로 개선해 나갈 예정입니다.

체인간 교류 지원 (Interchain Support)

다른 프로토콜을 가진 탈중앙화 플랫폼 사이의 정보 교류를 위한 표준은 아직 정해지지 않았습니다. POLARIS는 필요하다면 표준을 만드는 작업에 적극적으로 참여하고 또한 표준이 정해진다면 사용이 편리한 인터페이스(interface)를 플랫폼에서 빠르게 지원하여 다른 플랫폼과의 연결에 불편함이 없도록 지원할 계획입니다.

이정표 (Milestone)

POLARIS는 다음과 같은 기술 및 정책 이정표를 가지고 있습니다. 각 이정표 기간 내에서의 세부적인 일정과 진행사항은 구체적인 내용과 함께 수시로 공개할 예정입니다.

- ***CYGNUS*** ***(the swan)*** - 2018. 4Q

  POLARIS의 테스트넷(testnet)이 동작을 시작합니다. 네트워크의 안정성을 점검하고 새로운 기능들에 대한 연구 및 개발이 진행됩니다. 이 기간 동안 테스트넷은 재단 또는 재단이 지정하는 임의의 블록 생성자에 의해 블록을 생성하고 네트워크를 유지합니다.

- ***DELPHINUS*** ***(the dolphin)*** - 2019. 2Q

  첫 번째 연구 및 개발 결과를 포함한 POLARIS의 메인넷(mainnet)이 동작을 시작합니다. 이 기간에는 네트워크의 안정성을 최대한 유지하고 DApp 참여를 장려하기 위해 POLARIS 재단과 재단에 의해 선발된 블록 생성자 후보가 탈중앙화 그리드에 참여합니다.

  또한 DApp 지원을 위해 블록 생성자-중재자 회담을 통해 DApp의 선발이 시작되고 커뮤니티(community)에 의해 DApp을 선발하기 위한 공개오디션이 준비되기 시작합니다.

- ***AQUILA*** ***(the eagle)*** - 2019. 4Q

  스파클 합의 체계(sparkle consensus system)이 구현되고 공개투표 제도(public voting system)를 위한 기본적인 기능이 완성되어 일부 블록 생성자는 모든 참여자의 투표에 의해 선발되기 시작합니다. 추후 POLARIS 재단에 의해 선발된 블록 생성자와 공개투표에 의해 선발된 블록 생성자의 비율은 블록 생성자-중재자 회담의 합의 결과에 따라 조정됩니다.

  기본적인 프라이버시 보호(privacy preserving)와 정보 보호(data protection) 기능이 플랫폼에 추가되어 동작을 시작합니다.

- ***PEGASUS*** ***(the winged horse)*** - 2020. 2Q

  대용량 데이터 처리 및 무거운 연산을 위한 *연산 그리드(Computation Grid)*가 구성되고 이를 위한 새로운 프로토콜이 적용됩니다. 이때부터는 복잡한 연산도 POLARIS 네트워크 내에서 빠르게 처리할 수 있습니다. 확장성(scalability)을 더 높이기 위한 다양한 기술들이 검증을 마치고 적용되어 더 빠른 처리 속도를 필요로 하는 곳에서도 POLARIS 네트워크를 사용할 수 있게 됩니다.

다양한 온 체인 거버넌스(on-chain governance)가 적용되고 관련된 플랫폼이 공개되어 다양한 조절 인자(metadata)를 즉시 변경할 수 있습니다. 이에 따라 인플레이션 및 토큰 분배 또한 블록 생성자-중재자 회담의 결정에 의해 즉시 변경됩니다.

- ***HERCULES*** ***(Heracles, the hero)*** - TBA
  HERCULES 기간에 적용될 내용은 기술의 발전과 정책의 변화에 따라 추후 결정되어 공개됩니다.

면책조항 (Disclaimer)

이 백서는 POLARIS 재단(POLARIS Foundation)에서 배포하는 문서로 POLARIS에 관한 정보 제공의 목적으로 작성되었습니다. POLARIS 재단은 POLARIS 프로젝트를 진행하는 사업의 주체이며 백서 초기 버전 발간 당시에는 법적인 실체가 없는 온라인 상의 프로젝트 조직입니다.

POLARIS에 대한 기관 투자자들의 투자 계약이 시작되기 전 싱가포르에 법인이 설립될 예정이며, 법인의 형태는 비영리법인, 영리법인, 재단법인 등 다양할 수 있습니다. POLARIS 재단은 가칭이며, 실제 법인 설립 후 추진 주체의 명칭은 변경될 수 있습니다. 백서 상의 POLARIS 재단은 통상 POLARIS 프로젝트 추진을 위해 설립할 법인을 지칭합니다.

이 백서에 서술된 기술적, 법적 내용은 개발 과정의 결정에 따라 언제든 변경될 수 있으며, 백서의 내용은 어디까지나 발간 당시의 계획입니다. 이 개발 계획과 일정, 내용에 대해 POLARIS 재단은 어떤 것도 보장하지 않습니다.

이 백서의 내용과 직간접적으로 관련된 기술적, 법적 및 재정적 문제에 대한 불확실성과 모호성을 명확히 하고 향후 불필요한 분쟁 등을 피하기 위하여 귀하는 이 장의 내용을 면밀히 인지하여야 합니다. 또한 귀하가 이 백서와 관련한 어떤 결정을 하고 행동을 취할 때 귀하가 조금이라도 불확실한 점이 있다면 귀하는 합당한 전문가의 조력을 받아야 합니다.

귀하가 향후 POLARIS 토큰(POLA) 관련 거래, 계약 또는 투자와 관련하여 본 백서를 법적 근거로 삼거나 법적으로 의존해서는 안 됩니다. 이 백서는 POLARIS 토큰 등의 투자, 판매 등을 권유하는 문서에 해당하지 않으며, 이를 근거로 아무도 POLARIS 토큰의 투자 등과 관련하여 어떠한 법적 계약을 할 의무가 없습니다.

POLARIS 토큰의 투자 등에 대한 귀하와 POLARIS 재단의 계약, 또는 다른 내용의 계약과 관련하여, 구체적 계약의 조건 및 내용은 해당 계약의 당사자 간 서면 합의에 의해 정의될 것이며, 이 백서가 해당 계약 내지 기타 계약의 조건 및 내용이 되는 것은 아닙니다. 특히 해당 계약 및 기타 계약과 이 백서 간에 불일치가 발생하는 경우 해당 계약의 내용이 우선합니다.

POLARIS는 프로젝트 추진을 위한 투자금을 받고 투자자에 대해 POLARIS 토큰을 제공합니다. POLARIS에서 사용하는 주 토큰의 가치는 언제든지 제로(0)가 될 수 있으며 어떠한 환금성도 보장하지 않습니다.

POLARIS 토큰은 암호화폐(cryptocurrency) 또는 디지털 자산(digital asset)에 해당할 뿐, 법정 통화, 법정 화폐, 채권, 주식 등 유가증권, 파생상품 등에 해당하지 아니하고, 이와 같이 분류하거나 해석 또는 취급해서는 안 됩니다.

POLARIS는 개발 과정 중 개발 방향과 내용이 언제든 변경될 수 있습니다. 이 사실을 고지했음에도 불구하고 투자한다는 것은 투자자가 이 사실을 충분히 이해하고 있음을 의미합니다. 투자에 대한 판단은 귀하가 전적으로 판단하고 결정해야 하는 사항입니다.

POLARIS 재단과 그 계열사, 모회사, 자회사, 관계회사 등과 각 회사의 임직원은 관련 법률, 규정 및 규칙에서 허용하는 한도 내에서, 그리고 이 백서와 관련된 모든 경우에, 귀하의 어떤 종류의 손실에도 책임을 지지 않습니다.

그 손실은 재정적 또는 비재정적 손실은 물론, 데이터의 손실 등 포괄적인 유·무형의 손실을 모두 포함하며, 이에 한하지 않습니다. 귀하가 암호화폐의 투자, 공모, 거래 등이 법적으로 금지되었거나 제한된 국가의 국적자, 시민권자이거나 기타 거주권 등을 가진 주민인 경우 POLARIS 토큰을 획득할 자격이 없습니다.

POLARIS 재단은 추후 POLARIS 개발과 운영 과정에서 필요에 따라 개발 또는 운영, 개발 및 운영 모두를 담당할 별도의 자회사를 단수 또는 복수로 설립할 가능성이 있습니다.

EOSIO는 케이만군도에 설립된 회사인 Block.one의 등록상표이며 모든 권리는 Block.one에 있습니다. POLARIS, POLARIS 재단과 그 계열사들은 Block.one과 아무런 법적 관련이 없습니다.

귀하는 이 장의 면책조항을 포함한 이 백서의 내용을 전부 인지하고, 그 진정성을 인정하며 이에 동의한다는 점을 명백히 합니다.

참조 (Reference)

1) **Blockchain** : https://en.wikipedia.org/wiki/Blockchain
2) **DAG** : https://en.wikipedia.org/wiki/Directed_acyclic_graph
3) **Red Hat®** : Red Hat is the North Carolina based Linux distribution producer founded in 1993, which assembled the Red Hat Linux. https://www.redhat.com/en
4) **Linux** : https://www.linux.org
5) **Ethereum** : https://www.ethereum.org
6) **PBFT** : Castro, M.; Liskov, B. (2002). "Practical Byzantine Fault Tolerance and Proactive Recovery". ACM Transactions on Computer Systems. Association for Computing Machinery. 20 (4): 398-461. C iteSeerX 10.1.1.127.6130. doi:10.1145/571637.571640 https://dl.acm.org/citation.cfm?doid=571637.571640
7) **Threshold cryptosystem** : https://en.wikipedia.org/wiki/Threshold_cryptosystem
8) **Raft** : https://raft.github.io/
9) **Speculative execution** : https://en.wikipedia.org/wiki/Speculative_execution
10) **Discouragement attack** : https://vitalik.ca/files/casper_note.html
11) **Stake grinding attack** : https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQs
12) **DDoS attack** : https://en.wikipedia.org/wiki/Denial-of-service_attack
13) **Sybil attack** : https://en.wikipedia.org/wiki/Sybil_attack
14) **Nothing at stake** : https://github.com/ethereum/wiki/wiki/Problems
15) **ORBS** : https://orbs.com/
16) **ORBS Position Paper** : https://orbs.com/orbs-position-paper/
17) **영지식증명** : https://en.wikipedia.org/wiki/Zero-knowledge_proof
18) **비대칭 암호** : https://cryptography.io/en/latest/hazmat/primitives/asymmetric
19) **Dash** : https://www.dash.org
20) **Monero** : https://getmonero.org
21) **Zcoin** : https://zcoin.io
22) **PIVX** : https://pivx.org
23) **Zcash** : https://z.cash
24) **zk-STARK** : https://www.starkware.co/
25) **bulletproof** : https://crypto.stanford.edu/bulletproofs/
26) **Verifier's Dilemma** : Loi Luu, Jason Teutsch, Raghav Kulkarni, and Prateek Saxena. Demystifying incentives in the consensus computer, pages 706-719, New York, NY, USA, 2015. ACM. https://dl.acm.org/citation.cfm?id=2813659
27) **API** : https://en.wikipedia.org/wiki/Application_programming_interface
28) **CARDANO** : https://www.cardano.org/
29) **Tezos** : https://tezos.com/
30) **DFINITY** : https://dfinity.org/
31) **DFINITY's Algorithmic Governance** : https://dfinity.org/tech
32) **EOSIO** : https://eos.io/
33) **WebAssembly** : https://en.wikipedia.org/wiki/WebAssembly
34) **WAVM** : https://github.com/EOSIO/eos/tree/master/libraries/wasm-jit
35) **Oracle** : https://blockchainhub.net/blockchain-oracles/
36) **torrent protocol** : http://www.bittorrent.org/beps/bep_0003.html
37) **IPFS** : https://ipfs.io/

POLARIS

Copyright © 2018 POLARIS Foundation