Polkadot Summary

폴카닷이란?

> 이더리움 창시자인 개빈우드가 시작한 인터체인 프로젝트입니다. Layer 0 체인임.

0. Substrate

> 기질이란 뜻인데 반도체에서는 “기판”이라는 뜻을 가집니다. 단어를 통해 대충 유추할 수 있으시겠지만 **블록체인 개발 프레임워크** 중 하나입니다.

▼ 그래서 substrate로 어떤 블록체인 프로젝트를 빌드할 수 있느냐?

멀티 체인/인터 체인 프로젝트 빌드에 적합함

(1) 체인/디앱간의 상호운용성 (2) 확장성을 중점으로 하고

(3) Light-client-first Design (4) fork없이 업데이트 가능한 장점들도 있음

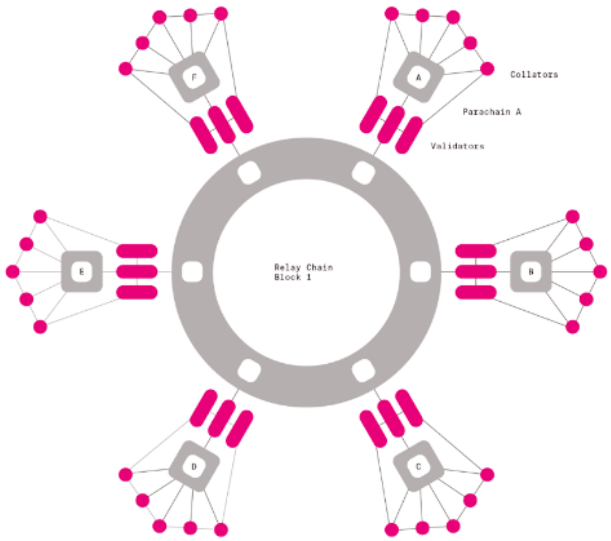
상호 운용성은 비트코인이나 이더리움같은 체인을 서로 연결할 수 있는 걸 의미한다고 생각하시면 됩니다. 폴카닷도 이걸로 만들었음. 그러니 당연히 폴카닷과도 seamless compatible

1. Architecture

> 폴카닷은 크게 **(1) relay chain**과 **(2) parachain** + **(3) bridge**로 구성되어있습니다. 아래 그림과 같이 중심에 원형모양의 릴레이 체인에 파라체인과 브릿지가 연결되어있는 구조

Relaychain
Shared security
Inter Chain Message Passing

Parachain
Blockchain that has own logic



▼ Relay chain

relay(중계하다)라는 뜻에서 알 수 있듯이 주위의 파라체인의 상태 변화를 수집/확인하며 각각의 체인을 보호하는 역할을 합니다.

파라체인을 포함한 시스템 전체를 조정하고 그 외의 작업은 파라체인에게 맡깁니다.

대충 이런 일들을 합니다.

1. 거버넌스 메커니즘
2. 파라체인 경매
3. NPoS(합의 알고리즘) 참여

참고로 스마트 컨트랙트는 지원 안함(파라체인에서 함)

▼ Parachain

대충 여러분들이 알고계시는 이더리움과 같은 Layer 1 블록체인이라고 생각하시면 됩니다. 다만 특정 목적에 따라 다양하게 설계 될 수 있습니다. ex) 스마트 컨트랙트 전용 체인, 신원 인증 전용 체인

우리 팀은 스마트 컨트랙트를 배포해야하니 파라체인에 배포하면 될 겁니다. 그 중에서도 **Astar!!!**

▼ Bridge

특수한 목적의 일종의 파라체인이라고 보시면 되는데요.

비트코인, 이더리움 같은 다른 네트워크에서 폴카닷내로 데이터를 전송하는 “다리”의 역할을 하여 다른 파라체인과 상호작용할 수 있는 로직을 가진 체인이라고 보시면 됩니다.

---

2. Interoperability(상호 운용성)

> 폴카닷에서 가장 핵심이 되는 feature인 걸로 보이네요. 상호 운용성은 **멀티 체인 운용 가능 및 다른 체인의 Dapp도 같이 운용 가능한** 것으로 생각해주시면 될 것 같습니다.

▼ XCM/XCMP

XCM (cross consensus message), XCMP (cross consensus message protocol)

둘 다 파라체인간 통신 방법에 대한 것을 다루며

XCM은 형식이고 XCMP는 전달 메커니즘입니다.

▼ Bridge

앞서 설명했지만 비트, 이더, 제트 캐시같은 다른 체인으로부터 완결성을 판단하여 데이터를 폴카닷내로 가져오는 다리 역할을 합니다. 파라체인과 마찬가지로 릴레이 체인에 연결되고 폴카닷 합의 메커니즘을 통해 보호됩니다.

---

3. Consensus

> **NPoS (Nominated Proof of Stake)**을 합의 알고리듬으로 채택하고 있음

PoS에 딱봐도 뭔가 지명해서 대표자 몇 명 뽑아서 검증할 것 같은 냄새가 나는데 그거 맞습니다. 정치 조금 아시면 **공천 및 선출 시스템 with 네이티브 토큰**으로 이해하시면 됩니다.

지명자는 토큰 얼마 걸어놓고 검증자 후보 공천하고 그 후보들 중에 선출되면 선출된 검증자와 해당 지명자가 보상을 나눠갖는 구조, 단 검증자가 cheating을 한다면 걸어놓은 토큰(DOT)을 잃게 됨 ㅠㅠ

▼ PoS

지분 증명은 지분(스테이킹한 토큰)이 많을수록 블록에 많이 기록할 수 있는 권한이 주어짐

▼ NPoS

✅ 아래 Main Actors에서 **validator와 nominator**를 읽고 오면 더 이해하기 쉽습니다.

✅NPoS는 네이티브 토큰을 staking하고 perfomance에 따라 보상을 받는 컨셉은 동일하지만 권한에 있어서 약간 차이가 있음

기본 컨셉은 다음과 같음

1. **DOT 홀더**는 폴카닷의 네이티브 토큰인 **DOT을 스테이킹**하여 **Nominator**가 될 수 있음.
2. Nominator는 **자신이 신뢰하는 validator 후보 목록을 자신의 DOT과 함께 제출** 할 수 있는데
3. Validator 후보 중 **일부가 선출**되면 **보상을 선출된 validator와 공유**할 수 있음
4. “믿을 수 있는 후보들”을 지속적으로 제출한다면 **낮은 risk로 지속적인 수익**을 얻을 수 있으므로 **cheating할 확률이 줄어듬** + **홀더들의 nominator 참여 유도 가능**
5. 선출 과정에서 지분이 낮은 후보는 제거되고 **지분이 높은 validator를 선출**할 수 있음
6. 선출된 Validator는 **릴레이 체인/파라체인에 새로운 블록을 추가**하는데 중요한 역할을 수행

그 외에도 완결성과 관련된 GRANPA, 블록 생성 엔진인 BABE에 대해 더 알아보려면

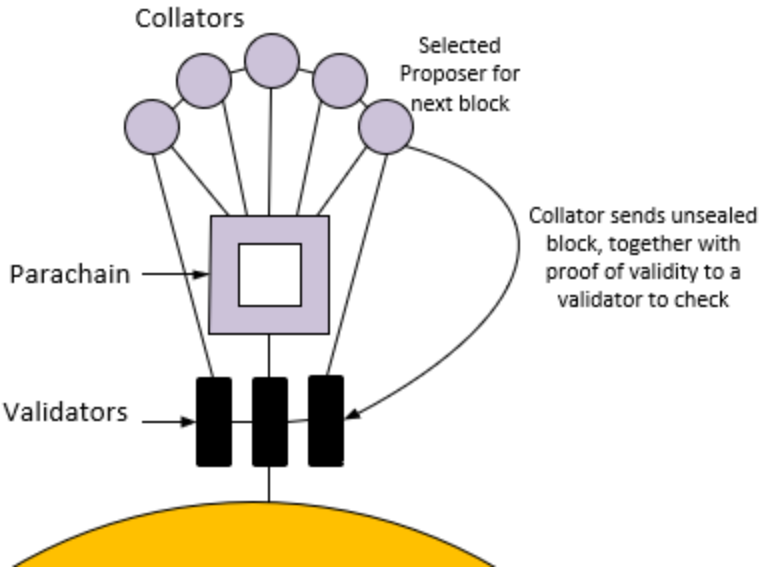
🖊GRANPA : https://medium.com/decipher-media/polkadot-합의-파트-2-grandpa-bbd0300b091d

🖊 BABE : https://medium.com/decipher-media/polkadot-합의-파트-3-babe-d2057f53fb4

4. Main Actors

> 폴카닷에 참여하는 참가자들은 크게 다음과 같이 나눌 수 있습니다.
> **(1) Validator(검증자) (2) Collator(대조자) (3) Nominator(지명자)**
> **기본적으로 세 가지 Role 전부 DOT(Token)을 Staking해야 참여가능합니다.**

▼ Collator (대조자)



1. Collator는 **특정 파라체인의 full node**이자 릴레이 체인을 위한 full node를 유지하는 역할
    - full node는 블록체인의 모든 정보를 담은 노드를 의미함

2. **파라체인의 트랜잭션을 수집**하고 릴레이 체인의 검증자를 위해 **state transition proof를 생성**하여 검증자에게 **unsealed block과 함께 넘겨줌**.
    - state transition proof : 상태 전이 증명
    - unsealed block : 대략적으로 확정되지 않은 블록이라고 생각하시면 됩니다.
3. **XCMP**를 사용하여 **다른 파라체인과 메시지를 주고 받을 수 있음**
    - XCMP는 cross consensus message protocol로 파라체인간 통신 프로토콜이라고 생각하시면 됩니다.
4. Validator와 달리 **네트워크를 보호하지 않음**
5. **파라체인 블록이 유효하지 않을 경우** Validator가 이를 거부함
6. Collator는 **트랜잭션 검열**을 통해 시스템을 악용할 수 있지만 이론적으로 honest한 collator 한명만 있으면 검열을 막을 수 있음

▼ Validator (검증자)

기본적으로 **(1) Collator로부터 온 proofs를 검증**하고 **(2) 다른 검증자와 합의**를 통해 **릴레이 체인을 보호**합니다.

1. **릴레이 체인에 새로운 블록을 추가**하고 + 모든 **파라체인에 새로운 블록을 추가**하는데 중요한 역할을 함
2. **파라체인 검증자**는 off-chain 합의에 참여하고 블록 생산자가 on-chain을 포함하도록 후보 영수증을 트랜잭션 풀에 제출함
3. **릴레이 체인 검증자**는 각 파라체인이 규칙을 준수하고 trustless한 환경에서 shard간의 메시지를 전달할 수 있음을 보장해준다.

❗❗❗ 만약 합의 알고리듬을 준수하지 않을 경우 검증자가 staking한 **DOT의 일부 또는 전부를 제거해버리는 페널티**를 부여함

▼ Nominator(지명자)

기본적으로 **신뢰할 수 있는 검증자들을 선택**하고 **DOT을 스테이킹하여 릴레이 체인을 보호**하는 역할을 함.

1. DOT 홀더라면 **검증자 후보를 지명**하여 **DOT을 추가로 얻을 수 있음**

2. 후보자 지명과 함께 DOT을 스테이킹하기 때문에 선출된 검증자가 **네트워크 규칙을 따르지 않으면 페널티를 받아** 스테이킹해둔 DOT을 잃을 수도 있음
3. 제출한 검증자 후보 중 **선출된 검증자가 있고** 해당 검증자가 네트워크 규칙을 지킨다면 잠재적으로 받을 수 있는 **Staking reward를 검증자와 공유**할 수 있음.