

Polkadot: 분권화된 웹3.0의 블록체인 간 상호운용을 위한 플랫폼

강형석

Overview

폴카닷이란?

The Polkadot logo, featuring the word "Polkadot." in a light gray, stylized script font.

폴카닷은 블록체인들이 연결하고
지키는 네트워크!

폴카닷은 공유되는 보안 아래 블록체인 프로젝트끼리 협력을 할 수 있게 해줍니다.

폴카닷은 새로운 블록체인들이 뭉하던 다른 블록체인들과 통신할 수 있게 해주며 보안을 보장해줍니다.



모두의, 모두를 위한, 모두에 의해
만들어진 오픈소스 프로토콜

Polkadot.

폴카닷은 웹3재단이 만든 오픈소스 프로젝트입니다.

웹3재단은 폴카닷을 만들기 위해 100명이 넘는 개발자들을 포함한 5개이상의 팀을 선정했습니다.

- Parity Technologies
- ChainSafe
- Polkascan
- SpeckleOS
- Polkadot js

폴카닷에서의 블록체인:

Polkadot.



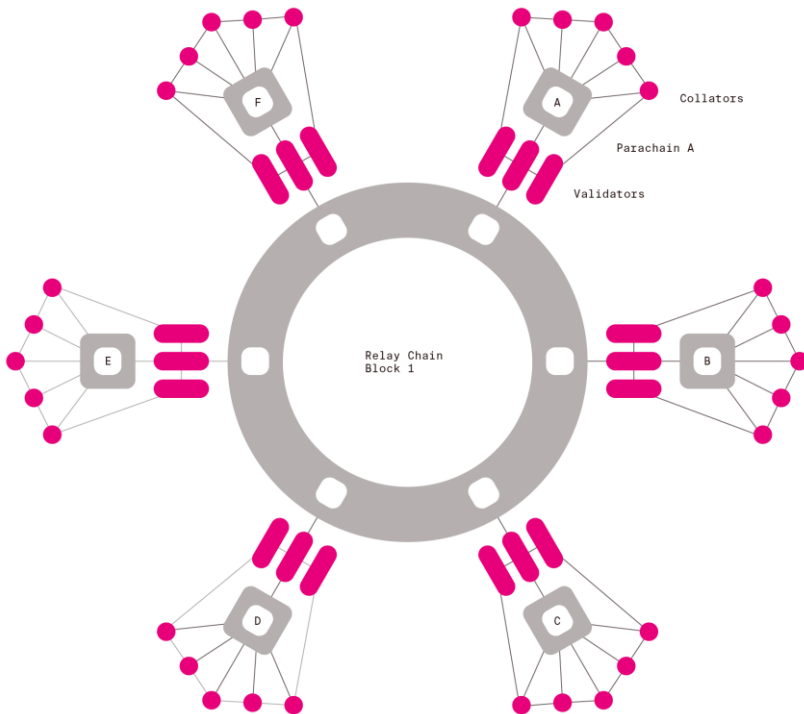
릴레이체인

체인 간 보안을 담당하고 블록체인 간 데이터 전달



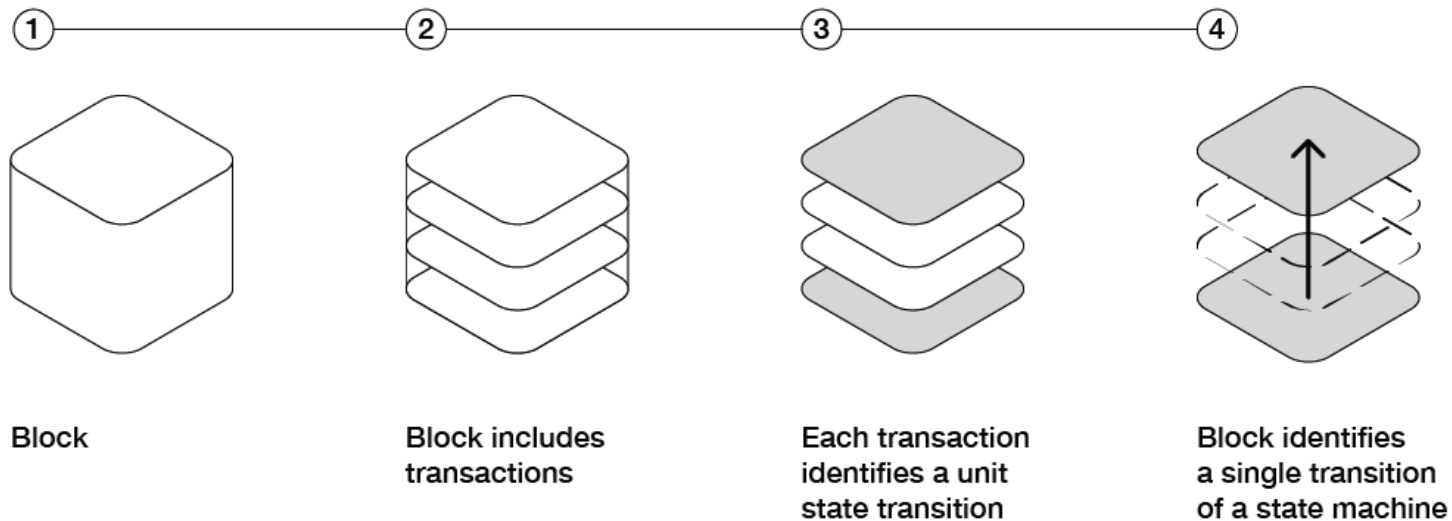
패러체인들

각각의 로직을 가지고 있고 트랜잭션들을 처리
블록체인



폴카닷에서의 블록체인:

Polkadot.



Graphic: Blockchain as a state transition machine

폴카닷에서의 블록체인:

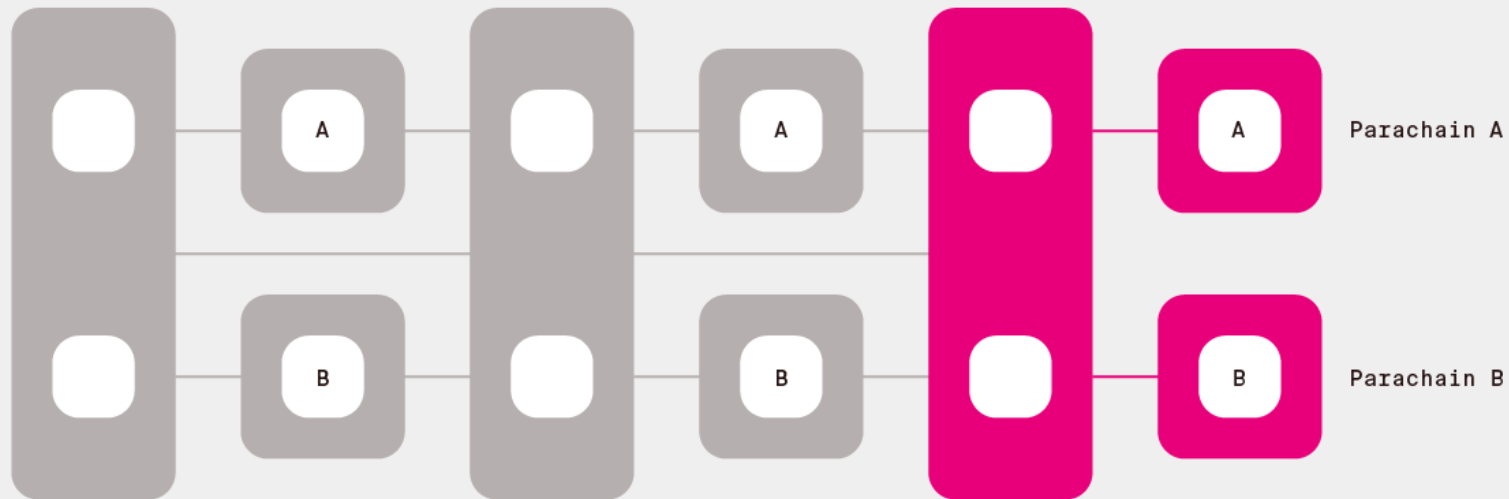
Polkadot.

Data structure
connected by hashes

Relay Chain
Block 1

Relay Chain
Block 2

Relay Chain
Block 3



핵심 분석

구성 요소: 기술

Polkadot.



안전하고 보안이 검증되며 효율적인 프로그래밍 언어: Rust



웹어셈블리: (패러체인을 위한) 호환성있고, 빠르며, 지지를 받고 있는 컴파일 언어



Libp2p: Protocol Labs에서 만든 크로스-플랫폼 p2p 프로토콜



이종적인: 다양하고 상호 보완되는 기능들로 이루어진 생태계를 지향



규모 가변적: 매우 효율적인 중심 레이어를 통해 온체인에서나 오프체인에서도 규모가 작게 또는 크게 변화는 상황에서도 대비가 가능함



안전한: 경제학적인 게임들로 보호되는 견고하고 형식을 갖춘 시스템을 갖춰야 함



릴레이 체인



검증자



패러체인



조합기



블록

릴레이 체인

Polkadot.



릴레이 체인은 패러체인들에게 보안을 제공하고 서로 통신을 주고 받게끔 합니다.

검증자들

Polkadot.



검증자는 스테이킹된 풀 노드로서 블록이 검증을 받고 릴레이체인에 블록을 더하는 책임을 가짐.

fishermen(릴레이체인이나 블록체인을 감사하여 잘못된 점을 잡는 자)가 될 수 있음.

패러체인들

Polkadot.

Parachains are parallelizable blockchains ("para-chains") that comprise the Polkadot network.

각각의 패러체인은 고유한 아키텍처를 가질 수 있음(e.g. UTXO, account-model, zk-snark)



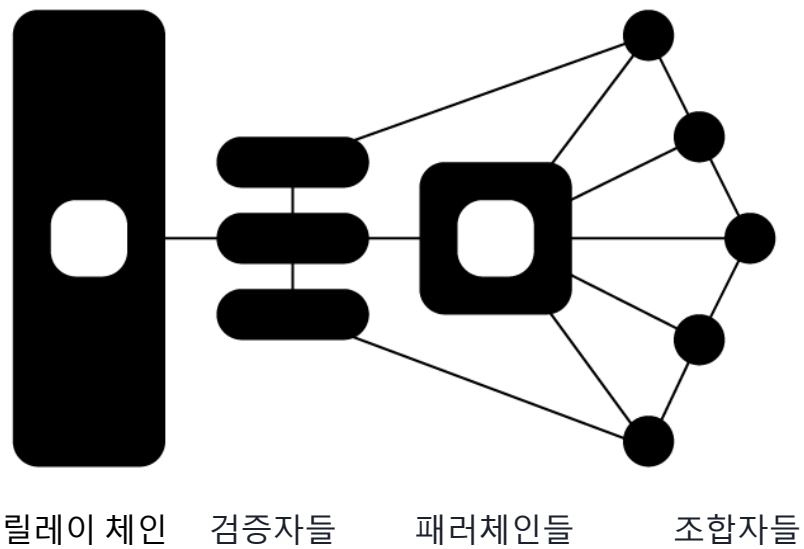
조합자들은 패러체인이나 외부 체인에서 보이는 블록들의 트랜잭션들을 모아봤다가 블록을 만든 다음, 블록에 대한 증명값을 릴레이체인의 검증자들에게 보냄.



fishermen이 될 수 있음.

One Parachain

Polkadot.





릴레이
체인

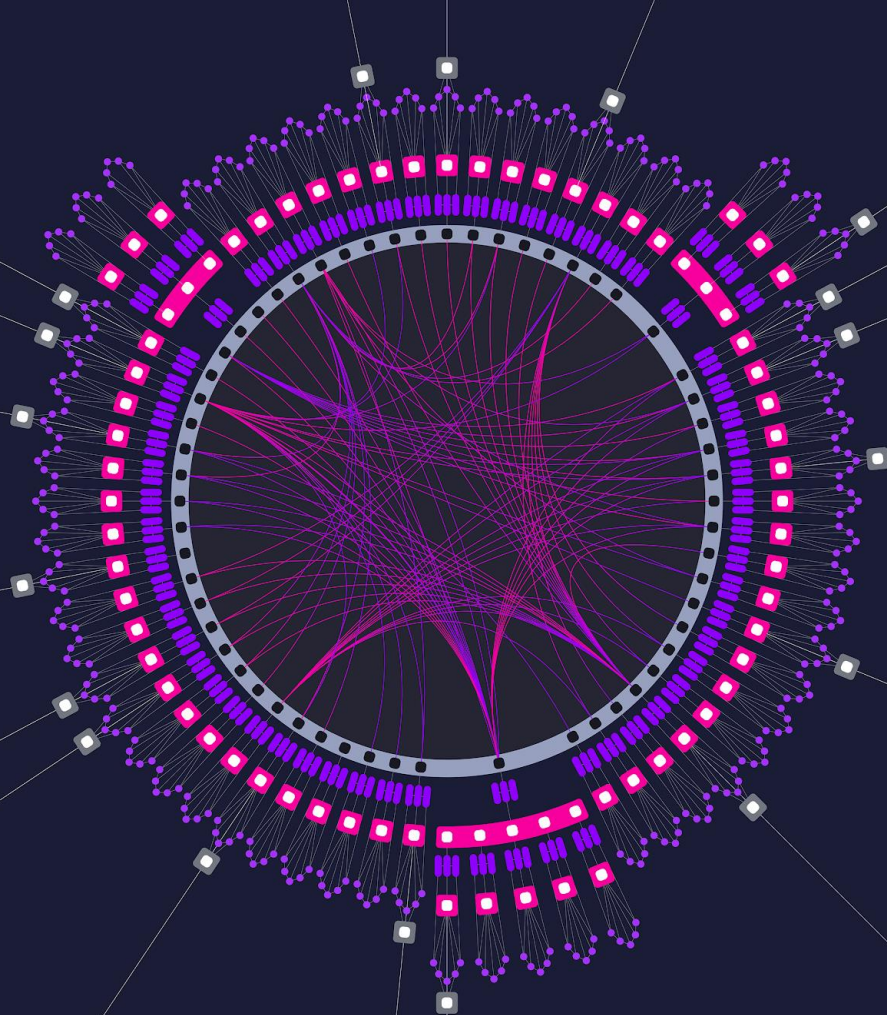
검증자들

패러체인(
들)

조합자들

외부
블록체인

A world running on Polkadot



컨센서스

CONSENSUS:

Polkadot.

Goals



낮은 진입장벽: 검증자가 되는데 드는 비용이 낮음



블록 결정과정에서 독립된 블록생성

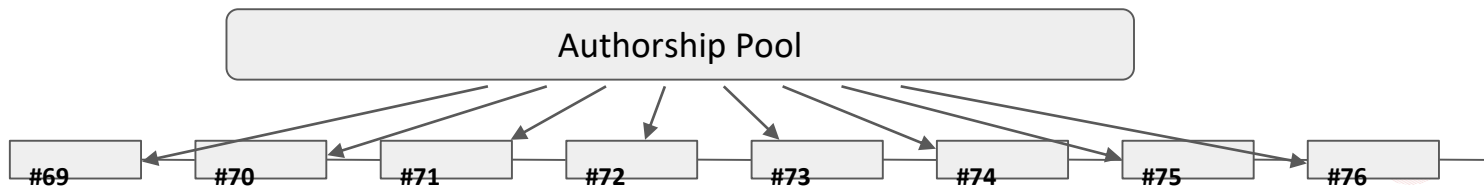


블록체인에 기반한 컨센서스

CONSENSUS:

Polkadot.

Block Production



라운드 기반의 확률적으로 안전한 시스템



무작위로 선택되는 수많은 검증자 풀



블록을 더할 순서가 오기 전에 미리 알려주는 시스템

CONSENSUS:

Polkadot.

Finality Gadget



전 세대(검증자들)에서부터 투표를 받음



작고, 집중되어 있고, 스테이킹이 많이 된 풀



잘못 처리할 경우 $\frac{1}{3}$ 의 스테이킹된 자산이 사라짐

CONSENSUS:

Polkadot.



PARALLEL VALIDATION GROUPS
Validators partitioned to allow scaling



RELAY-CHAIN PROOF-OF-STAKE
Guarantees shared canonicity of parachains



ECONOMIC FINALITY
Ensures that transactions can not be reverted

The DOT

The DOT Token:

Polkadot.



폴카닷 네트워크를 움직이는 The DOT token

DOT token은 4개의 독립된 목적들을 위해
존재하는데: 네트워크에 대한 거버넌스, 플랫폼
운용, 패러체인 간 연결, 패러체인 간 상호운용을
위해 존재합니다.

네트워크에 대한 거버넌스

Polkadot 투자자들은 프로토콜에 대한 주권을 가집니다. 검증자가 있는 데 외 다른 플랫폼들에서는 릴레이 체인 운용자(DOT 소지자)들이 특권을 지닙니다. 이에는 프로토콜을 고치거나 업그레이드하는 것을 포함합니다.



새 패러체인은 릴레이체인에 연결되는데 DOT토큰을 묶어두는 것을 필요로 합니다. 만
료기간이 끝나지 않는 이상 패러체인은 폴카닷 릴레이체인에서 분리될 수 없습니다.

The DOT Token:

Polkadot.



운용

게임 이론을 이용하여 DOT 토큰을 가진 사람이 블록체인 생태계 내에서 정직한 행동을 할 시 인센티브를 제공합니다. 불순한 의도를 가진 사람들이 묶여 검증자를 만들고 스테이킹을 한 경우 토큰이 소각됩니다. 이는 네트워크를 안전하게 유지시켜줍니다.

패러체인 간 상호운용

블록체인 간에 정보를 서로 주고받아야 하는 경우가 있는 경우 DOT토큰을 수수료로 지불해야 할 수도 있습니다. 그러나 이를 항상 요구하는 것만은 아닙니다.(e.g. 상호운용만을 위한 패러체인이 있는 경우).

핵심

참된 상호운용성:

Polkadot.



폴카닷은 토큰 외에도 블록체인 간 데이터, 자산 전송을 가능하게 해줍니다. 폴카닷에 연결되는 것은 폴카닷 네트워크 안에 있는 다른 다양한 블록체인들과 상호운용이 되는 기회를 줍니다.

경제학으로나 트랜잭션으로나

Polkadot.

두마리 모두를 잡은 스케일



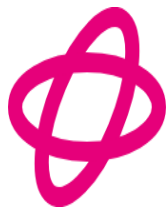
폴카닷은 네트워크 안에 있는 블록체인들을 유지하기 위해 공통된 검증자들을 선정함으로써 전례없는 scalability를 제공합니다. 폴카닷은 복수 병렬의 블록체인 사이에 트랜잭션을 수행하게 해줌으로서 트랜잭션 상의 scalability도 제공합니다.



서브스트레이트를 이용해서 수분 안에 블록체인 하나를 만들어보세요. 폴카닷에 연결한 다음 런칭 첫 날부터 상호운용과 무결성을 확보해보시기 바랍니다. 이렇게 단순한 개발과정으로서 폴카닷 네트워크가 자랍니다.

실행 중 코드 수정 기능으로 포킹 없는 업그레이드

Polkadot.



폴카닷은 도중에 멈춤이 없는 네트워크입니다. 포킹없이 외부 상호작용에 적응하고 업그레이드가 가능하기 때문이죠. 이는 폴카닷이 외부 변화에 적응하고 더 좋은 기술이 나타났을 시 업그레이드가 가능하게 해줍니다.



폴카닷은 폴카닷의 검증자들에 의해 복수의 블록체인들의 무결성이 인정되는 “풀에 의해 유지되는 보안”이라는 개념을 고안합니다. 블록체인들은 폴카닷에 연결되면 첫 날부터 무결성을 보장받을 수 있으며, 이는 폴카닷 네트워크에 연결되는데 강력한 인센티브로 작용합니다.

유저의, 유저에 의한, 유저를 위한 네트워크 거버넌스:

Polkadot.



폴카닷은 오픈소스 거버넌스 시스템이 내장되어 있습니다. 온체인 거버넌스로 업그레이드가 진행되어 폴카닷의 개발과정이 커뮤니티의 가치를 대변합니다.

폴카닷이 기존 블록체인에게 주는
것들?

Polkadot.



(체인 간)상호작용



실험



이주

로드맵

WHERE ARE WE NOW?

Polkadot.



PoC-1: Governance, staking, basic UI, and forkless upgrades



PoC-2: "co-finalization" of non-communicating parachains and basic light client



PoC-3: Implementation of hybrid consensus described in these slides.



PoC-4: Full staking; Nominated Proof of Stake scheme

WHAT'S NEXT?



PoC-5: Interchain message passing, Cumulus (Substrate chains can become parachains)



PoC-6-8: Implementation of Validity/Availability game



In parallel: developer tools for parachains



Some teams building on Polkadot:

-Melonport

-Edgware

-AdEx

-Agoric

-Aragon

-Chainlink

-iExec

-Ocean

-Clovyr

CALL FOR CONTRIBUTORS

Polkadot.



Researchers



Parachain Implementers



Educators



Community Leaders

FIND OUT MORE

Polkadot.



polkadot.network

wiki.polkadot.network



web3.foundation

Grants: grants.web3.foundation



[@polkadotnetwork](https://twitter.com/polkadotnetwork)



[#polkadot-watercooler:matrix.org](https://matrix.org/#polkadot-watercooler)