한 번에 끝내는
블록체인 개발 A to Z

Chapter 2

Blockchain 2.0 - Ethereum

Chapter 2

Blockchain 2.0 - Ethereum

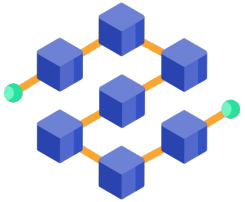
Ethereum 2.0

Ethereum 2.0

기존 Ethereum 네트워크의 비싼 수수료와 낮은 확장성 문제를 해결하기 위해 새로운 기술을 적용한 Ethereum 네트워크를 출시하고 기존 네트워크와 병합하여 과거의 기록을 그대로 유지하는 것이다.

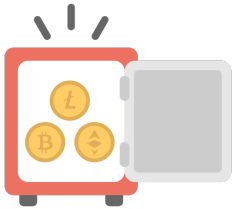
Ethereum 1.0

PoW

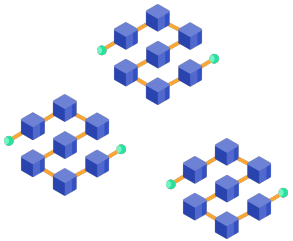


Single Blockchain

Ethereum 2.0



PoS



Multi Layer Blockchain

Ethereum 2.0 RoadMap

❶ Phase 0

PoS로의 합의알고리즘 전환이 이루어지게 된다. 합의 알고리즘이 이루어지는 Beacon Chain이 운영된다.

❷ Phase 1

Multi Layer Blockchain을 위해 Sharding과 Roll-Up기술이 적용된다. Phase 1에서는 64개의 Shard Chain이 운영될 예정이다.

❸ Phase 2

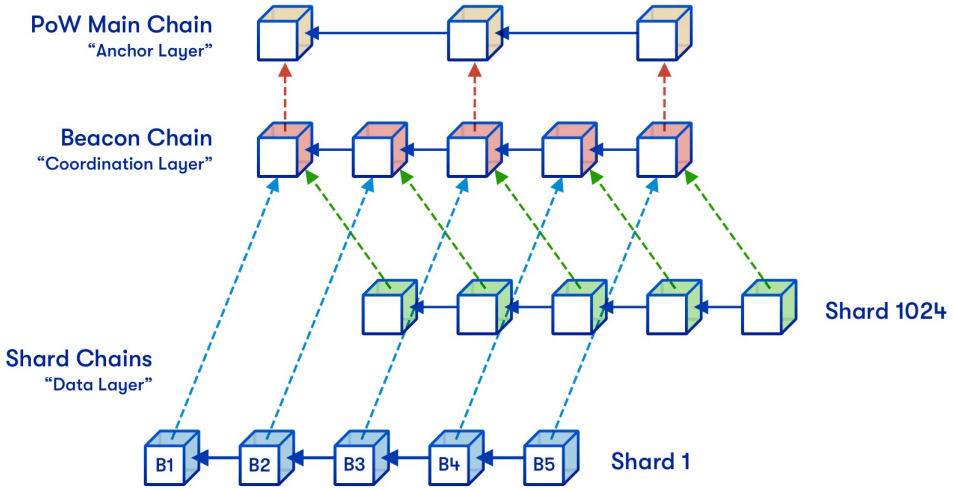
Ethereum 1.0 네트워크가 Shard Chain 중 하나로 변환된다.

❹ Phase 3

EWASM이 지원되고 Shard Chain에서도 Contract와 Transfer가 실행이 됩니다.

Beacon Chain

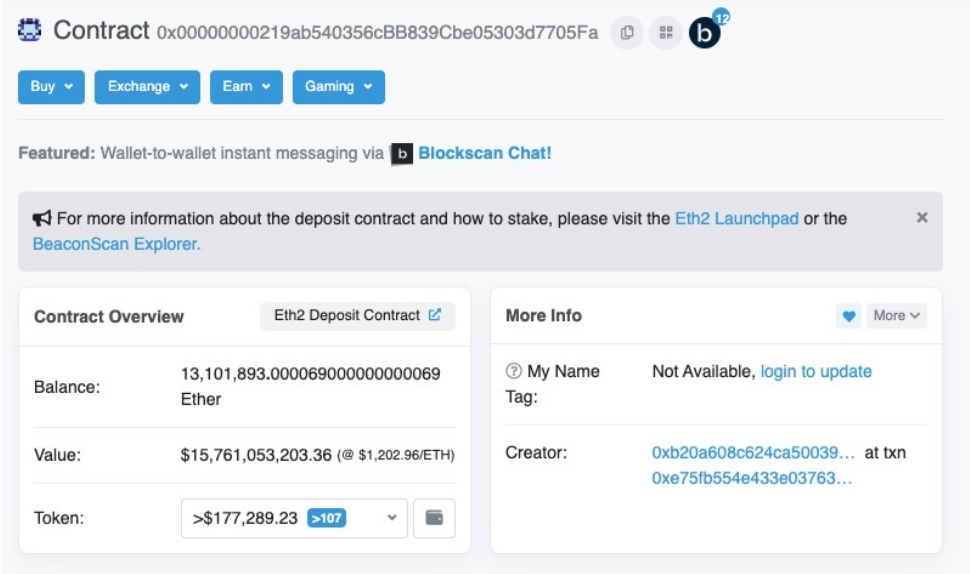
- Beacon Chain이란 PoS 합의 알고리즘으로 블록체인 전체의 합의 알고리즘을 이행하는 메인 체인을 뜻한다.
- Crosslink로 Shard Chain들의 상태 정보가 주기적으로 Beacon Chain상에 저장된다.
- 32ETH를 예치하여 Validator가 되면, 합의 알고리즘에 참여할 수 있으며 이를 통해 일정한 보상을 받을 수 있다.
- PoS 알고리즘으로 Gasper(LMD Ghost + Casper FFG)을 사용하고 있다.



(출처 : quantstamp.com)

Validator

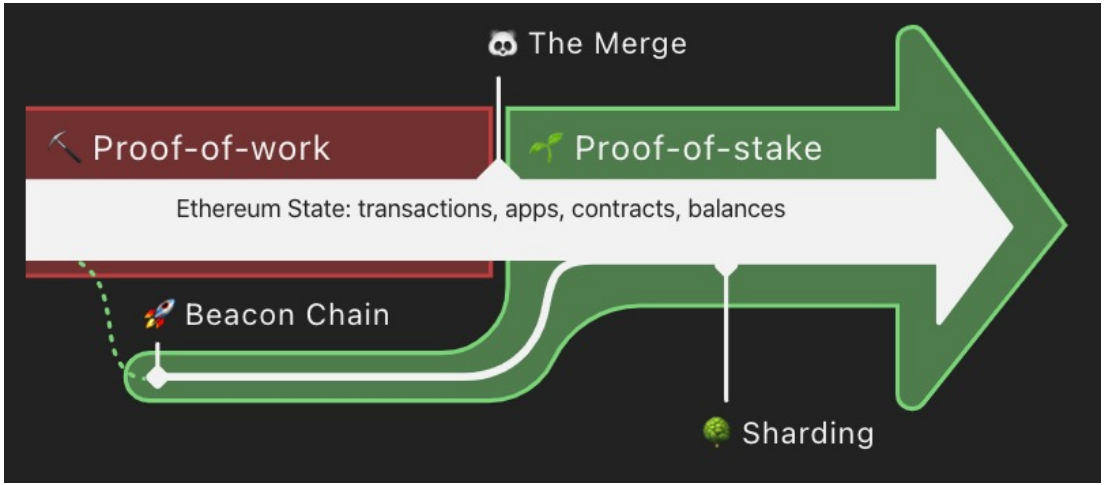
- Beacon Chain에 참여하기 위해서는 Beacon Chain 노드 운영과 32ETH를 1.0의 deposit Contract에 등록하여야 한다.
- 검증인들 중 랜덤으로 선정하여 블록 제안(Proposal)을 slot마다 진행합니다.
- 위원회는 epoch(64slot)마다 선정되어 Beacon Chain과 Shard Chain의 블록 유효성 검증을 진행합니다.
- 검증인들은 유효성에 대해 투표를 통해 블록 완결성(Finalized)를 보장합니다.
- 잘못된 투표를 하는 경우 예치한 ETH에서 삭감되게 됩니다.



(출처 : etherscan.io)

The Merge

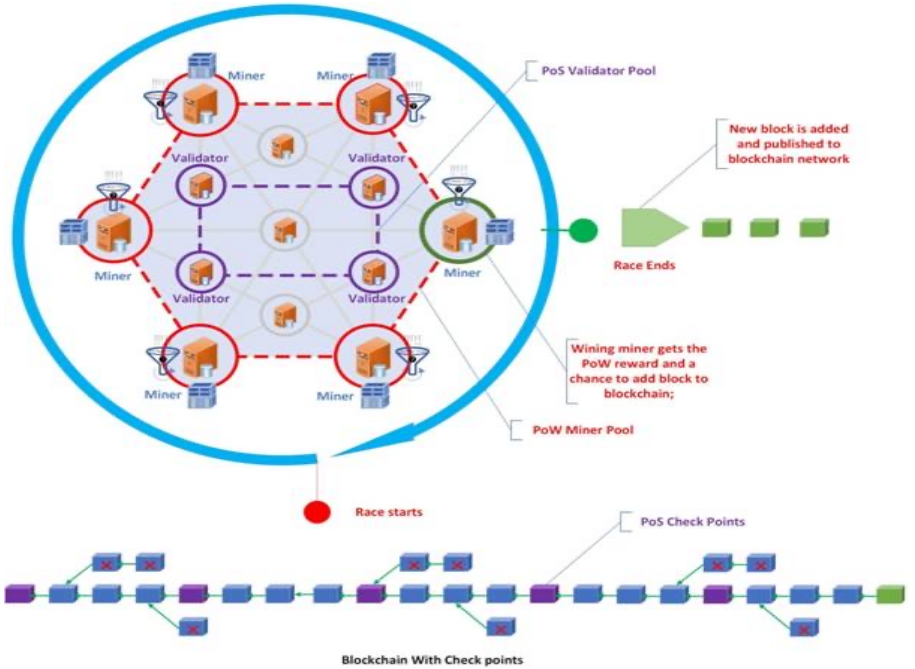
- The Merge는 PoW 알고리즘이 종료되고, PoS로 완전한 전환 시점을 뜻합니다.
- PoW의 종료를 위해서 채굴 빙하기를 도입하여, Difficulty를 매우 높은 수준으로 올려 채굴자체가 불가능한 상태로 만들게 됩니다.
- 현재 9월 19일에 Merge가 이루어질 것으로 예측되게 됩니다.
- The Merge 이후 Ethereum 1.0은 Execution Layer로 계속 동작하고 블록 생성 및 전파는 Beacon Chain으로 이루어지게 됩니다.



(출처 : Ethereum.org)

Gasper

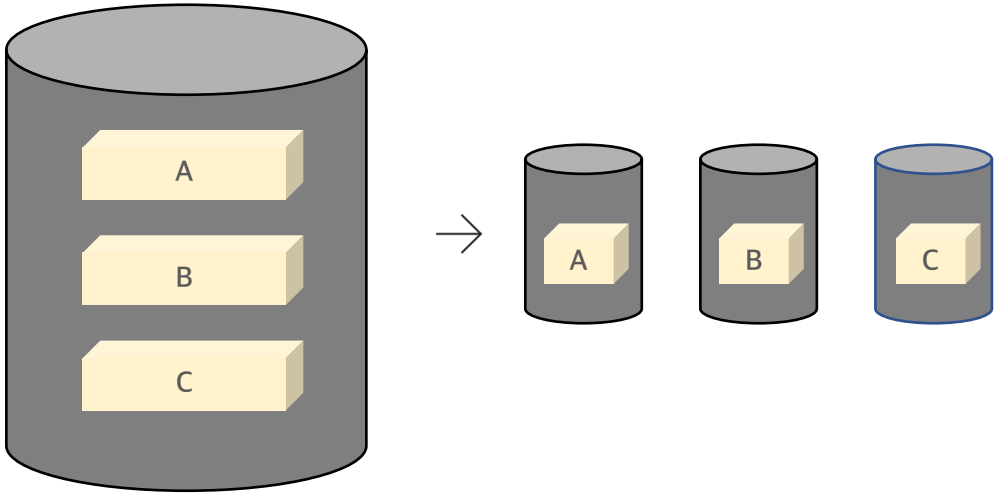
- Gasper는 Casper FFG 알고리즘과 LMD Ghost Fork Rule이 결합된 PoS 합의 알고리즘이다.
- PoS의 기본적인 알고리즘과 동일하게 전체 지분 중 2/3 이상의 투표를 얻어야 승인이 되며, 이를 Finalized라고 부릅니다.
- 하지만 매 블록마다 투표를 하는 것이 아닌 Epoch의 가장 마지막 블록에 대해서만 투표를 하고 이를 Checkpoint라고 부릅니다.
- LMD Ghost은 기존 Ethereum 1.0의 GHOST 알고리즘의 수정버전으로, 가장 많은 메시지를 받은 블록체인을 선택하는 것입니다.



(출처 : https://www.coding-bootcamps.com/blog/how-proof-of-stack-consensus-works-in-ethereum.html)

Sharding

- Sharding이란 하나의 서버에 모여있던 데이터들을 분산관리 하는 것이다.
- 데이터베이스 서비스에서 성능 향상을 위해서 많이 사용되고 있는 기술이다.
- Ethereum 에서는 1.0에서 하나의 체인에 있던 Dapp들을 여러 Chain상에 분할하여 네트워크 처리속도를 높이고자 도입하였다.
- 이를 통해 현재 30tps 수준의 처리성능을 100,000 tps 성능까지 높일 수 있다.

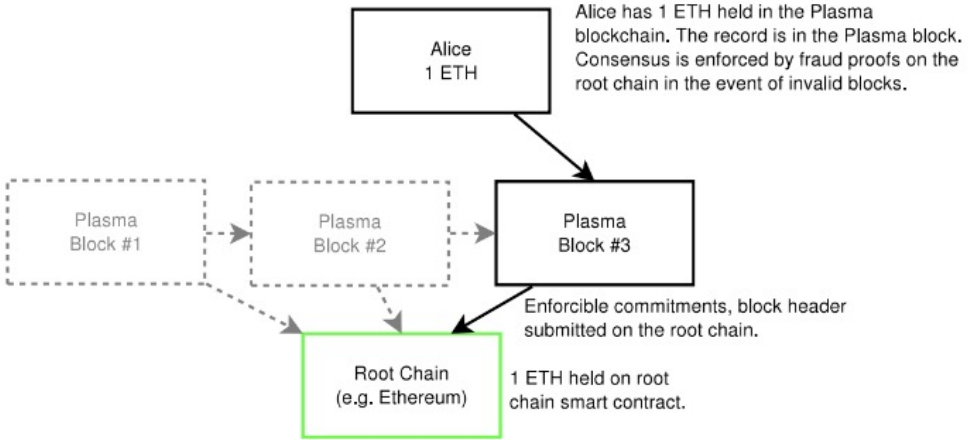


Ethereum 1.0

Ethereum 2.0

Plasma

- Plasma는 Joseph Pool이 제안한 블록체인의 확장성을 해결하는 방안으로 제시하였다.
- Merkle Tree는 모든 정보가 결국 Root Node에 저장되는 것을 착안하여 메인 체인 아래에 Child Tree를 만드는 방식이다.
- Child Tree의 정보는 Plasma상에 저장되고 이의 Root Node 값을 Ethereum상에 저장하여 데이터 위변조를 방지한다.
- Plasma 네트워크상에서 문제가 발생 시 이전 Block을 통하여 네트워크 탈출이 가능하다.



(출처 : plasma whitepaper)

Rollup

Rollup이란 Off-Chain에서 실행한 트랜잭션을 실행하고 Main Chain으로 결과 데이터를 올려 Main Chain의 보안성을 그대로 활용하는 기술을 뜻한다.

Optimistic Rollups

- Optimistic Rollup이란 실행된 트랜잭션이 모두 정상이라고 가정하고 의심되는 거래 발생 시 검증하는 방식
- Fraud Proof은 의심 거래가 발생하였을 때, 모든 거래를 재실행하여 모든 값을 대조한다.
- 사기를 밝혀낸 검증자에게 보상이 주어지고, 사기를 승인했던 검증자에게는 패널티가 발생하게 됩니다.
- EVM 대신 OVM을 통해 Rollup을 지원하는 Contract 배포가 가능합니다.

Zero-knowledge Rollups

- Off-Chain 거래를 On-Chain상으로 업로드할때 거래데이터 뿐 아니라 zk-Snark 증명이 함께 올라가게 됩니다.
- 거래 데이터 업로드 시 모든 주소를 Merkle Tree Index로 변환하여 전송 데이터를 대폭 줄일 수 있습니다.
- Transactor, Relayer로 구분된 역할을 지니며, Transactor는 거래를 생성하고 Relayer는 거래를 모아 zk-Snark증명 생성 후 Layer 1에 전달합니다.
- Zk Rollup은 거래 검증에 대한 증명이 함께 올라가기 때문에, 검증기간이 없어서 실행속도가 빠릅니다.