2020年11月版
Ethereum 2.0 概要

Daniel Tehrani - Blockchain engineer@ICOVO

流れ

- 自己紹介
- Ehtereumとは？
- Ethereum2.0とは？
- Ethereum2.0、変更点・導入される技術
  - Proof of stake
  - Sharding
- Beacon Chain
- Phases
- Ethereum2.0 tech deep dive
- 株式会社ICOVOによるEthereum2.0の取り組み

自己紹介

Daniel Tehrani（ダニエル・テヘラニ ）

元舞鶴高専生。高専を1年半で中退し、株式会社Gene.A.Idolsでチーフ・エンジニア。スマート・コントラクト（ERC721）の開発等。2020年7月にフリーランスに。ICOVOメンバー（Ethereum2.0ノード関連のリサーチ など）。日本育ち。

What is Ethereum?

- パブリックブロックチェーン
- 分散型アプリケーション (DApps) やスマート・コントラクトを構築するためのプラットフォーム

What is Ethereum2.0?

- Ethereumの大型アップグレード
- Ethereumが抱えている問題（スケーラビリティ、環境負荷、etc）を解決するために新しい技術を導入

Why?

以下の問題を解決するため・耐性を強化するため

- スケーラビリティ
- セキュリティ
- サステナビリティ

Ethereum2.0、変更点・導入される技術

- Proof of work(マイニング) → Proof of stake
- Sharding

Proof of stake

Proof of work から Proof of stake へ

Proof of work

- マイニングの能力を基にコンセンサスを得る
- 悪意のある行動をしたら消費した電力が無駄に → 正しい行動をするインセンティブ

Proof of stake

- コインの保有量を基にコンセンサスを得る
- 悪意のある行動をしたらコインを失う → 正しい行動をするインセンティブ

Proof of stake：Stakingとは？

- 最小32ETHを預ける
- チェーンのバリデートをし、報酬を得る（約1%〜25%）
- プロトコル通りの行動をしなければ、ステークを没収される

Staking エコノミクス

- ステークされているETHが少なければ少ないほど、バリデータあたりのリターンは大きくなる
- ステークされているETHが多ければ多いほど全体の発行量は増え、バリデータあたりのリターンは少なくなる

Total Network Stake	Validator Interest	Network Issuance
1,000,000	8.02%	0.08%
2,000,000	5.67%	0.11%
3,000,000	4.63%	0.13%
5,000,000	3.59%	0.17%
10,000,000	2.54%	0.24%

Eth2 Launch Pad

https://launchpad.ethereum.org/

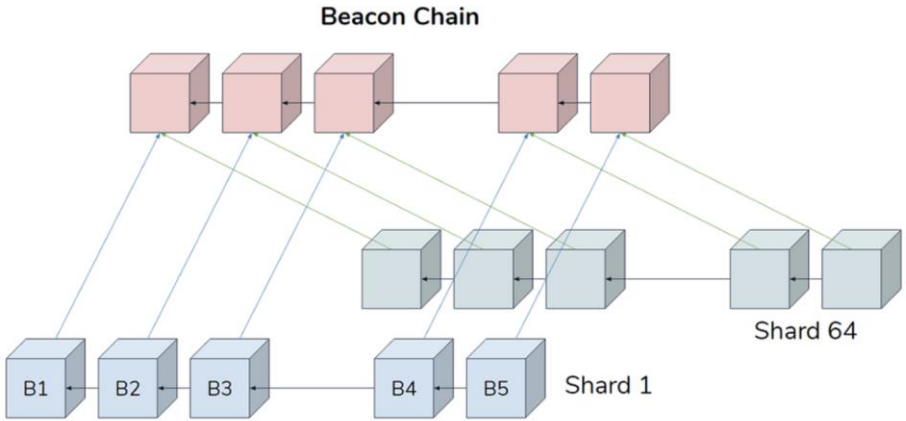
Staking pool

- 技術面を抽象化
- 32ETH以下からステークできる
- 参入コストが低い

Sharding

Sharding

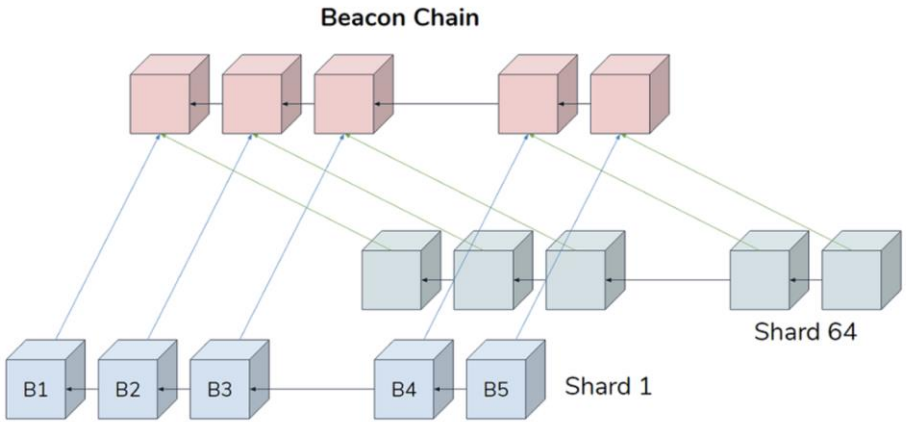
- Shardingとは？ → チェーンを分割すること
- 処理能力向上



The Beacon Chain Ethereum 2.0 explainer you need to read first より

Beacon Chain

- Proof of stakeシステムとShardingの統制



The Beacon Chain Ethereum 2.0 explainer you need to read first より

Beacon Chain Explorer

https://beaconscan.com/

Phases

Phase 0 ：Beacon Chainがスタート（2020年12月1日の予定）

Phase 1 : Shardingの実装（2021年中の予定）

Phase 1.5 : EthereumとEthereum2.0のドッキング（〜21/22年）

Phase 2 : 未定（Shardingをさらにパワーアップ？）

ETH2 technical deep dive

Sharding

Ethereumの課題

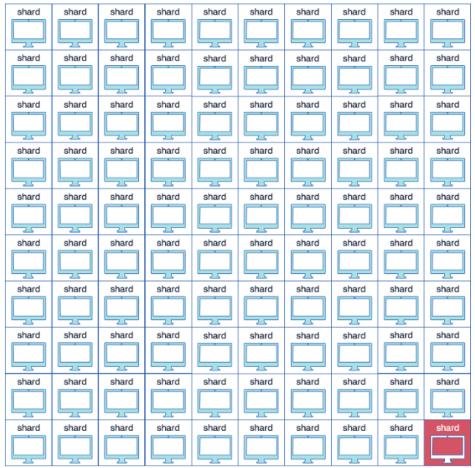
- 全てのノードが全てのトランザクションを実行しなければならない

スケールさせるには

1. ノードの処理能力を上げるなど、垂直なスケーリング
2. 並行処理など、水平なスケーリング ← 中央集権化しない

Sharding

- Beacon chainにて、バリデータが64のサブセットに分けられ、各shardに割り当てられる　→ セキュリティも分散してしまうのでは？



1% Attack

“In 100 shards system, it takes only 1% of network hash rate to dominate the shard.”

Credits Hsiao-Wei Wang

Sharding : RANDAO

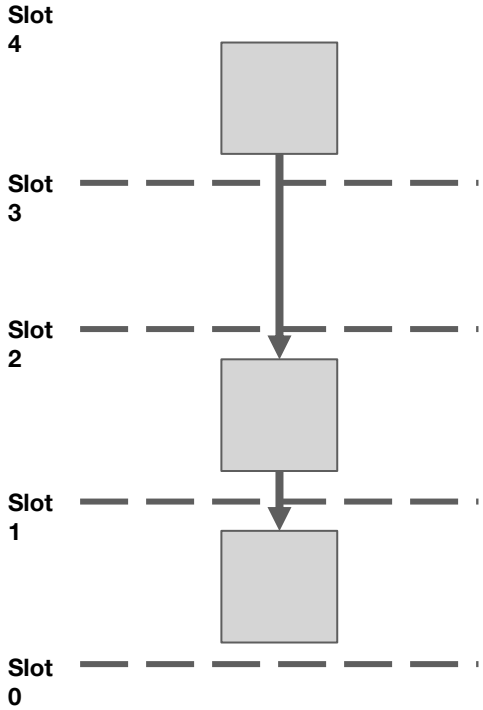
- 擬似乱数を生成する
- 定期的にバリデータセットをシャッフルし、shardへの再割り当てを行う

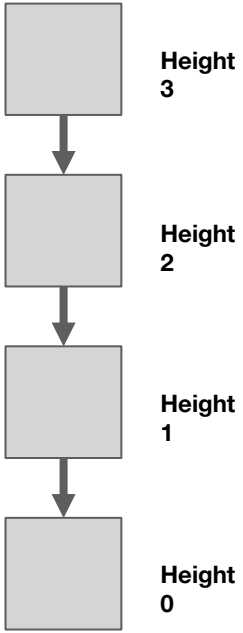
Slots and Epochs

Slots

- 12秒毎にSlotにブロックが追加される
- Beacon chainとShard chains、両方に適用される概念

SlotとBlock高の違い





Epochs

- 32slotsで1epoch
- 1slot = 12秒
- 1epoch = 6.4分

The Ethereum 2.0 Beacon Chain Explained より

Validators

バリデータ

- バリデータは、ProposerかAttesterとして仕事をする

Proposer

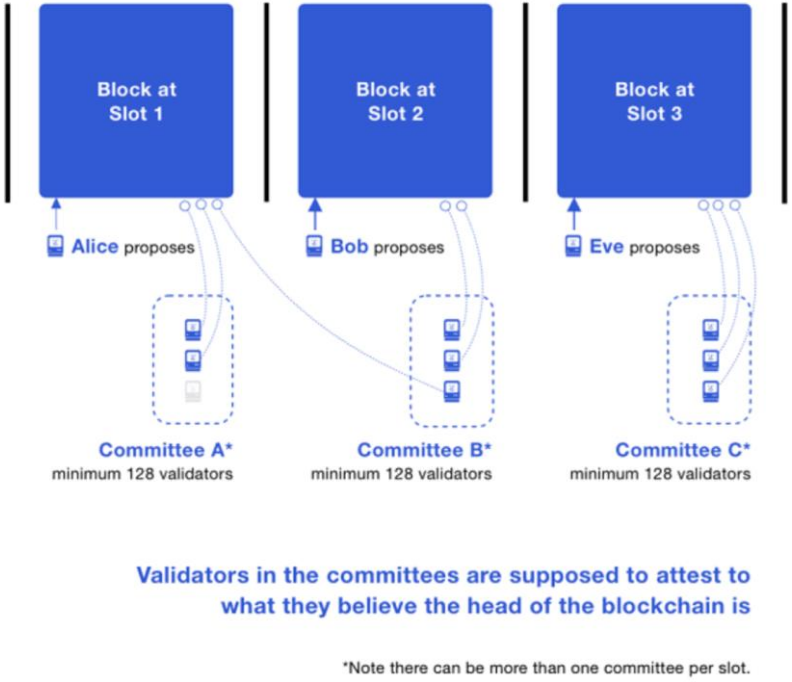
- ブロック生成
- ランダム（擬似的）に選ばれる

Attester

- Proposerが生成したブロックに投票をする
- ランダム（擬似的）に選ばれる

Committees

- バリデータの集合
- 最小128のバリデータで1つのcommitteeが作られる
- epochの初めにslot毎にcommitteeが割り当てられる
- バリデータは、1epoch内で1つのcommitteeにしか属せない
- committee内のバリデータは、チェーンの先端であると"信じる" ブロックに投票する



The Ethereum 2.0 Beacon Chain Explained より

4096のバリデータがいる場合

- 各epochの初めに、4096のバリデータが32のスロットに分けられる。スロットに割り当てられたバリデータで128バリデータのcommitteeが作れられる。

12288のバリデータがいる場合

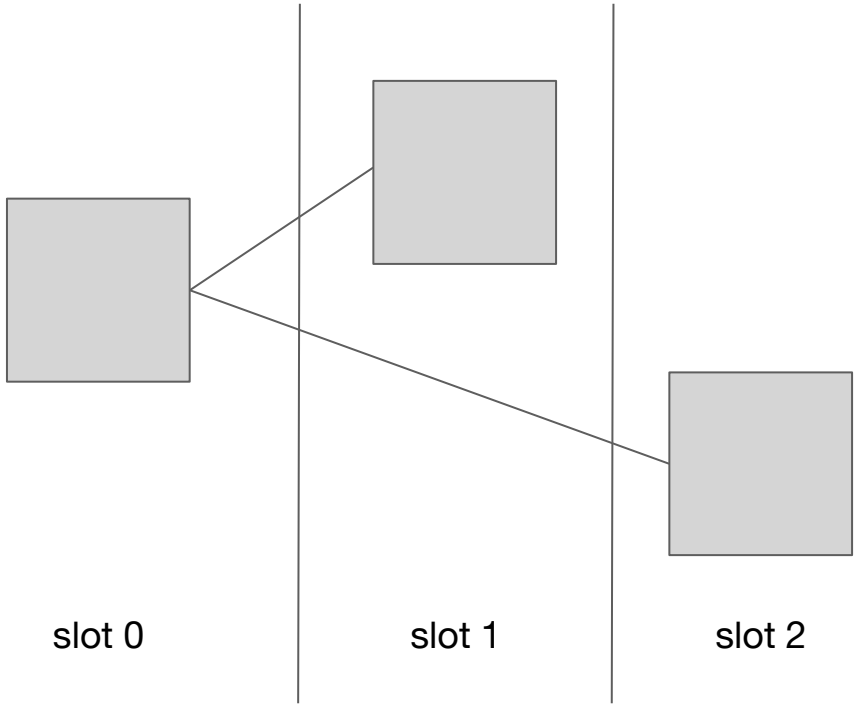
- 各epochの初めに、12288のバリデータが32のスロットに分けられる。各スロット、128バリデータのcommitteeが3つ作れられる。
- slot3のcommittee Bはshard30を担当する、slot 12のcommittee Aはshard 5を担当する。

投票（LMD GHOST）

- Attesterは、先端であるブロックに投票する

- slot2担当のAttesterはslot1のブロックを無効にしたい/ブロックの存在を知らない
  → 「slot 0が先端 」という票を入れる

- このチェーン先端の決め方をLMD GHOSTという



株式会社ICOVOによるEthereum2.0への取り組み

Ethereum2.0で安全に・簡単にStakingができる環境の提供

ONGOING

ETH2.0 PoS Project

Token ETH2.0 node pre-installed

Staking Server