Ethereum 2.0 and Beacon Chain Validator
以太坊 2.0 信標鏈驗證者

2019 June 29th (1 day before spec freeze!)

Ethereum Research

Hsiao-Wei Wang 王筱維

hwwhww

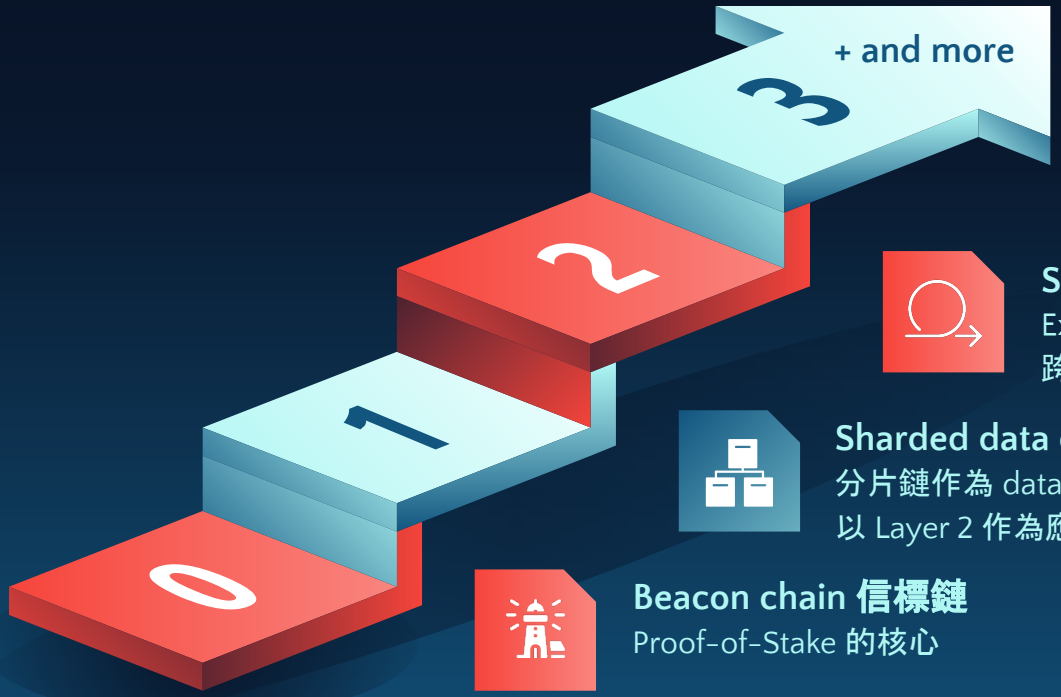
icebearhww

What you want to know...

- 以太坊 2.0？
- 信號鏈 (Beacon Chain) 是什麼？
- 我要如何成為 staking，成為一名 validator？
- 獎勵金是多少？
- 會不會很容易被罰錢(slashing)？
- 後續計畫？

為什麼以太坊 2.0 需要信標鏈 (Beacon chain)？

Roadmap



More iterations
More enhancements,
Casper CBC, STARKs,.. etc.

Shard state execution
Execution environments,
跨分片交易

Sharded data chain 分片資料鏈
分片鏈作為 data consensus
以 Layer 2 作為應用的 state execution protocol

Beacon chain 信標鏈
Proof-of-Stake 的核心

Serenity (Ethereum 2.0) Design

PoW/Eth1 Chain

Providing staking

Beacon Chain

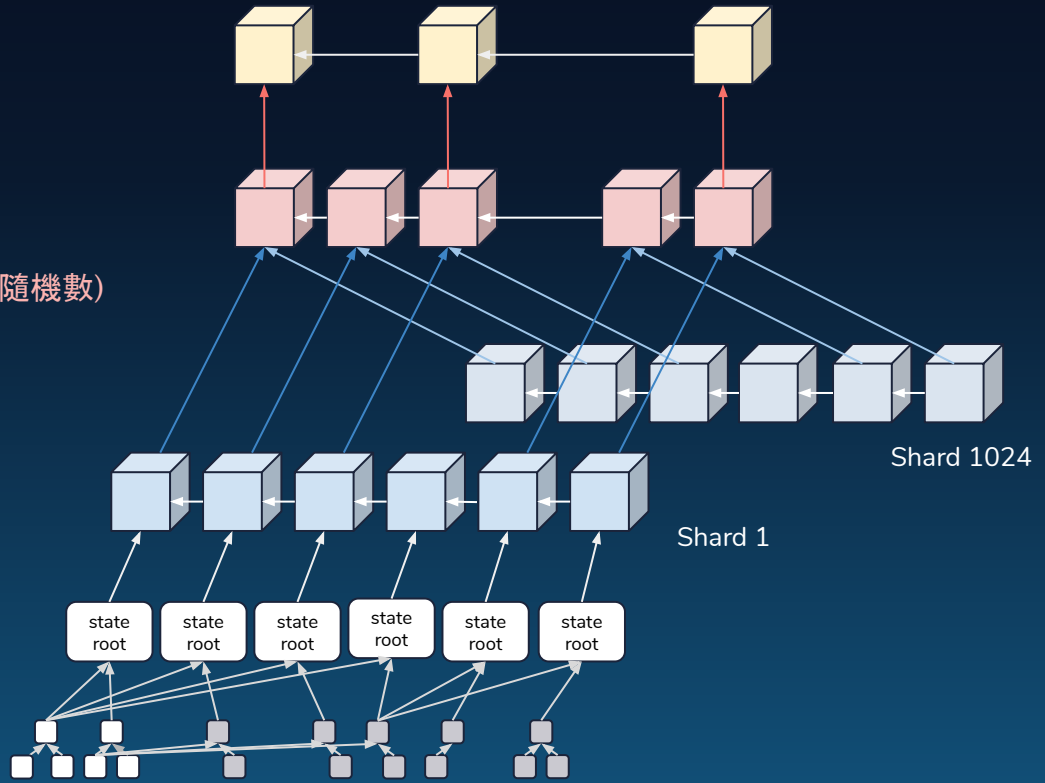
PoS core (Proof-of-Stake 的核心)
and random number generation (產生隨機數)
Shard chains coordinator

Shard Chains

Data chain for scaling

State Execution Engine

State execution result



Incentives for Honest Validator

Incentives – rewards

Incentives – rewards 獎勵金

Block proposer reward

① 納入越多其他驗證者的投票 (*attestations 證明*) 與交易

attestations

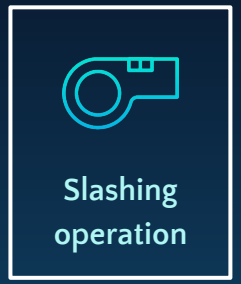
Incentives – rewards 獎勵金

Block proposer reward

① 納入越多其他驗證者的投票 (*attestations 證明*) 與交易

② 作為 Whistleblower 舉報者: 納入越多的 Slashing Operation

舉報者



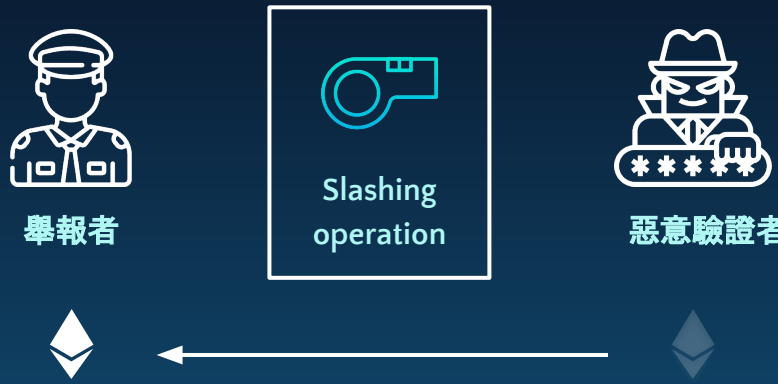
惡意驗證者

Incentives – rewards 獎勵金

Block proposer reward

① 納入越多其他驗證者的投票 (*attestations 證明*) 與交易

② 作為 Whistleblower 舉報者: 納入越多的 Slashing Operation



Incentives – rewards 獎勵金

Block proposer reward

① 納入越多其他驗證者的投票 (*attestations 證明*) 與交易

② 作為 Whistleblower 舉報者: 納入越多的 Slashing Operation

Casper FFG reward

投給正確的信標鏈

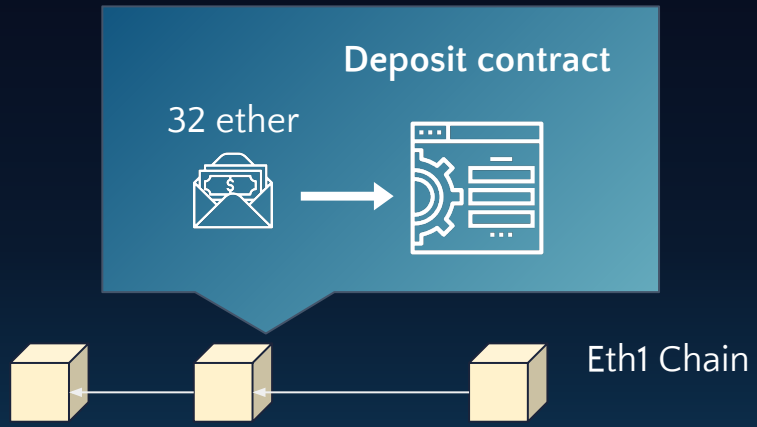
Crosslink reward

投給正確的分片鏈

如何成為信標鏈驗證者？
How to become a validator?

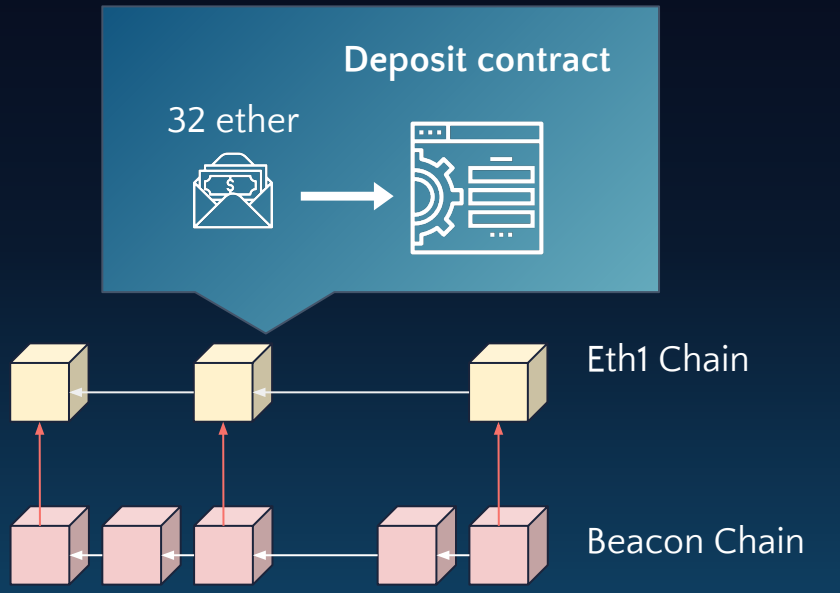
Join the Staking

1. Deposit `MAX_DEPOSIT_AMOUNT` (32 ether) to a special **deposit contract 抵押合約**



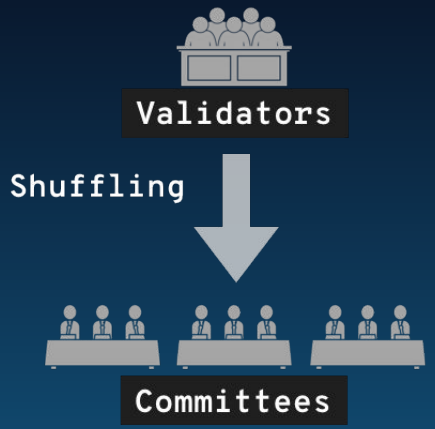
Join the Staking

1. Deposit `MAX_DEPOSIT_AMOUNT` (32 ether) to a special **deposit contract 抵押合約**
2. Watch the deposit contract status (event log)



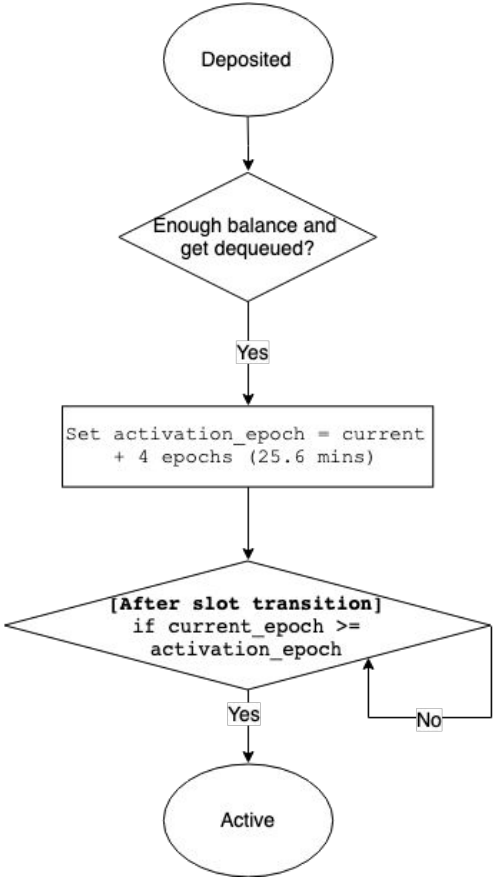
Join the Staking

1. Deposit `MAX_DEPOSIT_AMOUNT` (32 ether) to a special deposit contract 抵押合約
2. Watch the deposit contract status
3. Wait to get pseudo-randomly sampled by shuffling function



Activation 激活

1. 確認餘額是否足夠 (>= 32 ether)
2. Waiting queue
3. 設定 activation epoch number
4. 時間到則成為 **active** validator



驗證者的職責（Phase 0）

1. Proposing the valid ***beacon block***
2. Creating ***attestations 證明***

驗證者的職責（Phase 0）

1. Proposing the valid ***beacon block***
   a. **RANDAO** reveal for random number generation
   b. Choose the best vote of Eth1 chain references (Eth1Data)
   c. Include beacon operations
2. Creating ***attestations 證明***

```
class BeaconBlock(Container):
    slot: Slot
    parent_root: Hash
    state_root: Hash
    body: BeaconBlockBody
    signature: BLSSignature

class BeaconBlockBody(Container):
    randao_reveal: BLSSignature
    eth1_data: Eth1Data  # Eth1 data vote
    graffiti: Bytes32  # Arbitrary data
    # Operations
    proposer_slashings: List[ProposerSlashing,
MAX_PROPOSER_SLASHINGS]
    attester_slashings: List[AttesterSlashing,
MAX_ATTESTER_SLASHINGS]
    attestations: List[Attestation, MAX_ATTESTATIONS]
    deposits: List[Deposit, MAX_DEPOSITS]
    voluntary_exits: List[VoluntaryExit,
MAX_VOLUNTARY_EXITS]
    transfers: List[Transfer, MAX_TRANSFERS]
```

驗證者的職責（Phase 0）

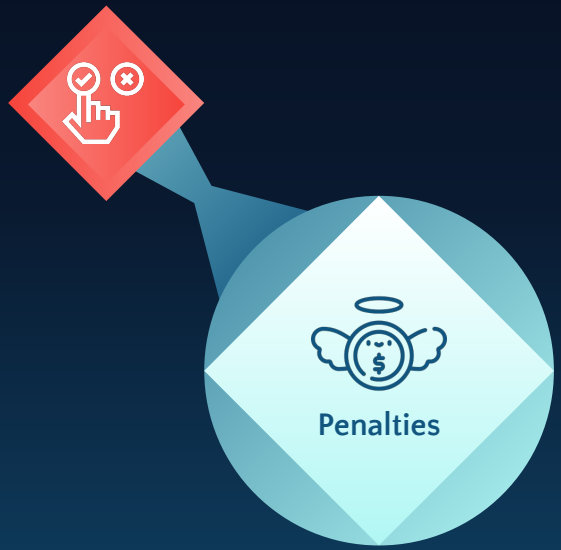
1. Proposing the valid ***beacon block***
2. Creating ***attestations 證明***
    a. Vote for canonical beacon chain block
    b. Vote for Casper FFG source and target
    c. Vote for canonical shard chain block (crosslink)

```
AttestationData

{
    # LMD GHOST vote
    beacon_block_root: Hash

    # FFG vote
    source: Checkpoint
    target: Checkpoint

    # Crosslink vote
    crosslink: Crosslink
```

Penalties and Slashings

Penalties and Slashings

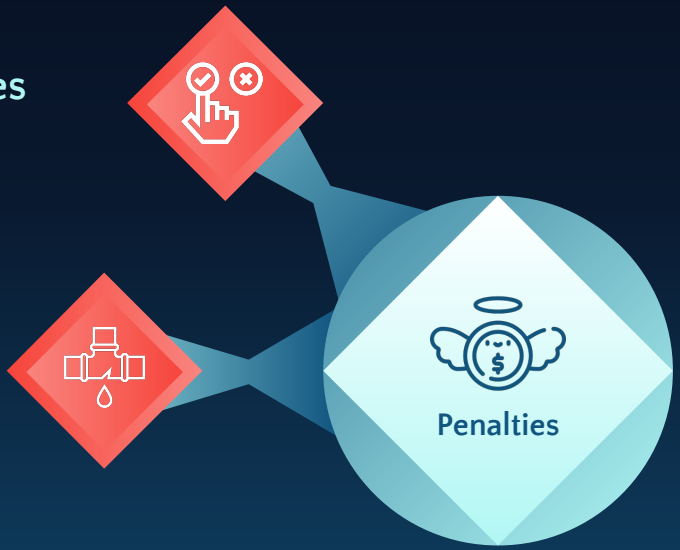
Casper FFG penalties



Penalties and Slashings

Casper FFG penalties

Inactivity leak penalties

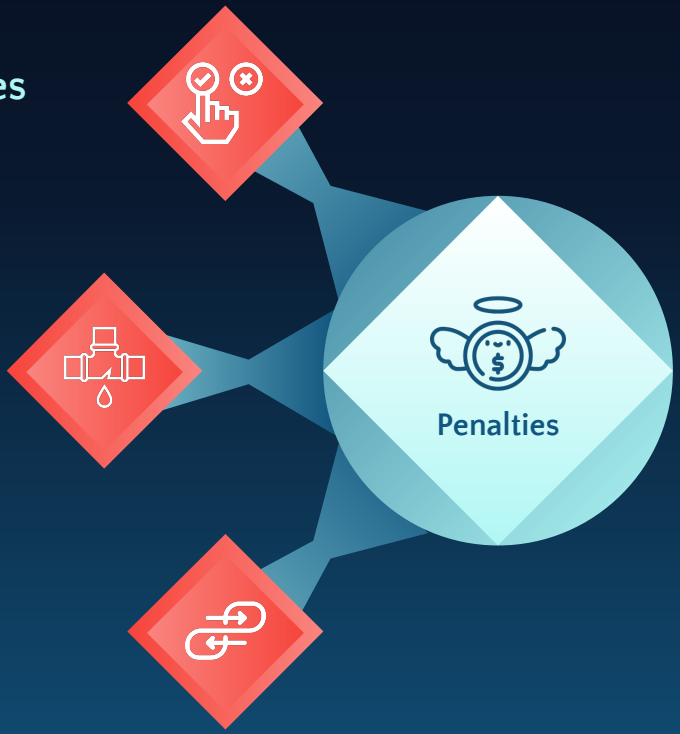


Penalties and Slashings

Casper FFG penalties

Inactivity leak penalties

Crosslink penalites

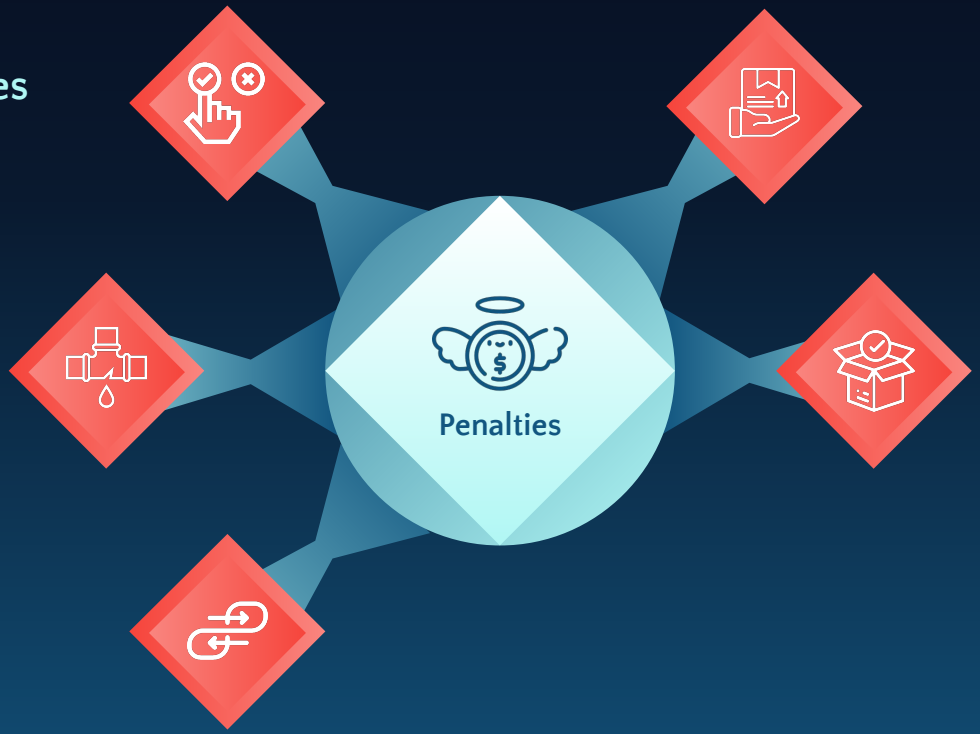


Penalties and Slashings

Casper FFG penalties

Inactivity leak penalties

Crosslink penalites



Proposer slashing

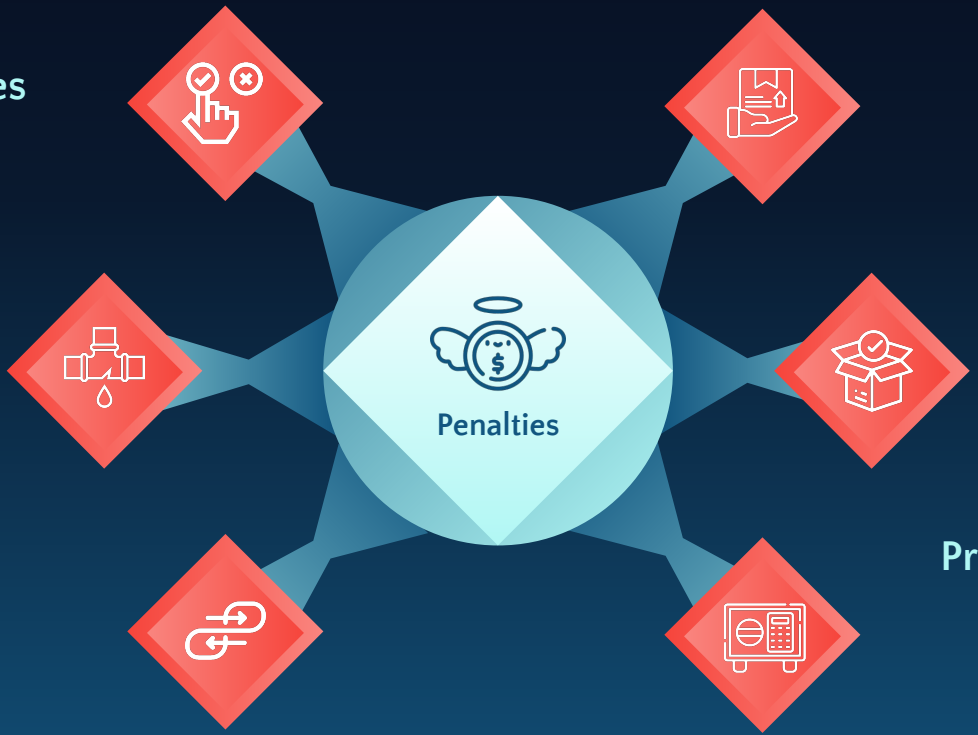
Attester slashing

Penalties and Slashings

Casper FFG penalties

Inactivity leak penalties

Crosslink penalites



Proposer slashing

Attester slashing

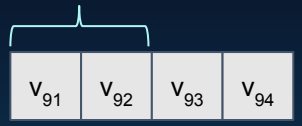
Proof of custody game penalites (Phase 1)

Validator Churn: 盡可能減少對於穩定性的影響

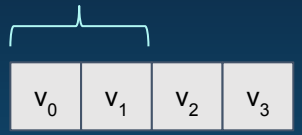
- Waiting queues
  - Activation
  - Exit
- **Churn limit of the given state,**

  based on the active validator count.

churn_limit=2



v.exit_epoch <= current_epoch

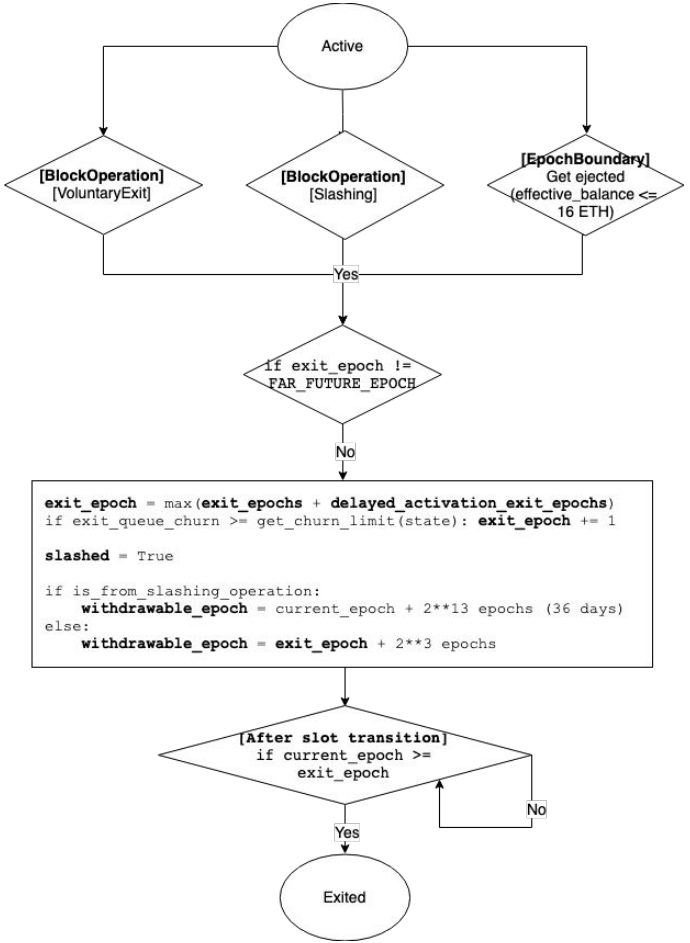


Voluntary Exit 自願退出

1. Send a **`VoluntaryExit`** operation
2. Withdraw
    a. [Phase 0] *Withdrawable*
    b. [Phase 2] Can be *Withdrawn*

Exit: 三種情況

1. 主動離開
2. 被檢舉 (Slashing Operation)
3. 餘額不足



Phase 0 Spec Freeze!

- 預計 6 月 30 日 spec code freeze
- 凍結後短期內不會有重大規格修改
- 作為各客戶端今年的測試鏈目標

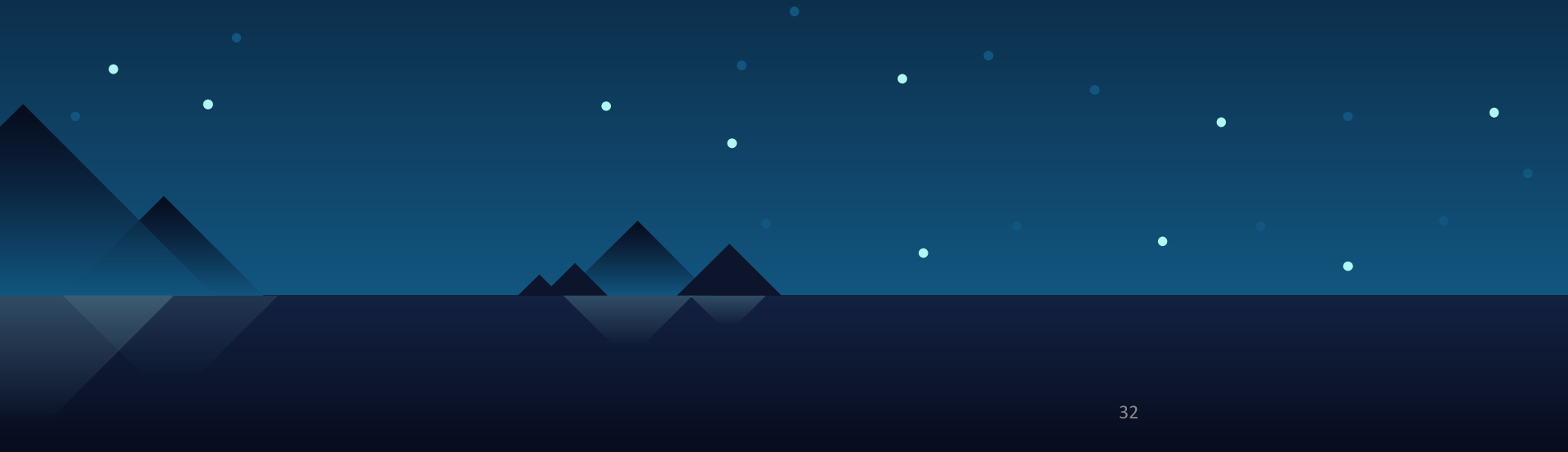
What's next

- Stable testnet 穩定的測試鏈
- Interop testnet (Cross-client) 跨客戶端的測試鏈
- Audit: BLS signature, deposit contract, spec
- 部署抵押合約，開放 staking
- 達最低驗證者數 (65,536) -> genesis

- Phase 1&2 prototyping 第一和第二階段原型實作與測試

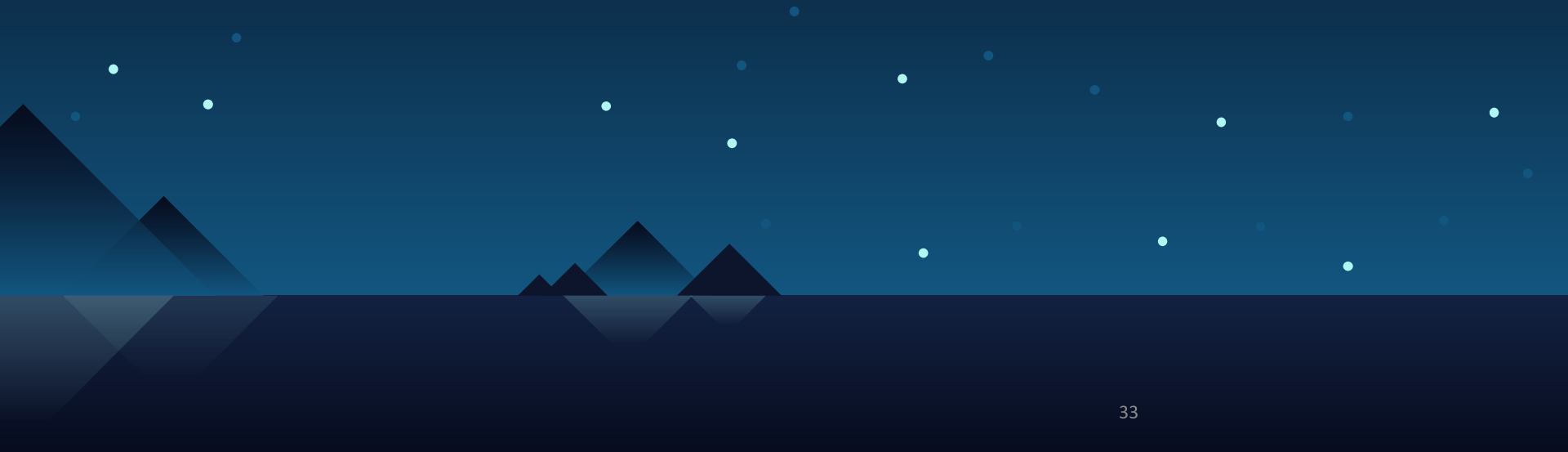
- gitter: @hwwhww
- Spec: github.com/ethereum/eth2.0-specs
- Python client: trinity.ethereum.org

Thank you!

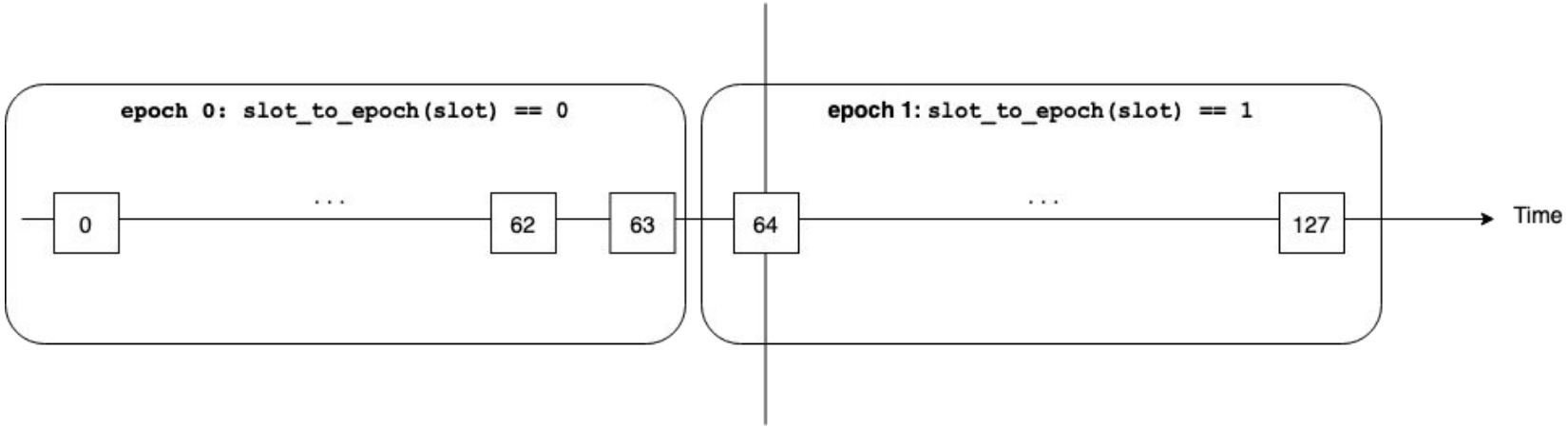


Resource credit

- Slide template: 24Slides.com
- Icons: designed by Freepik from www.flaticon.com



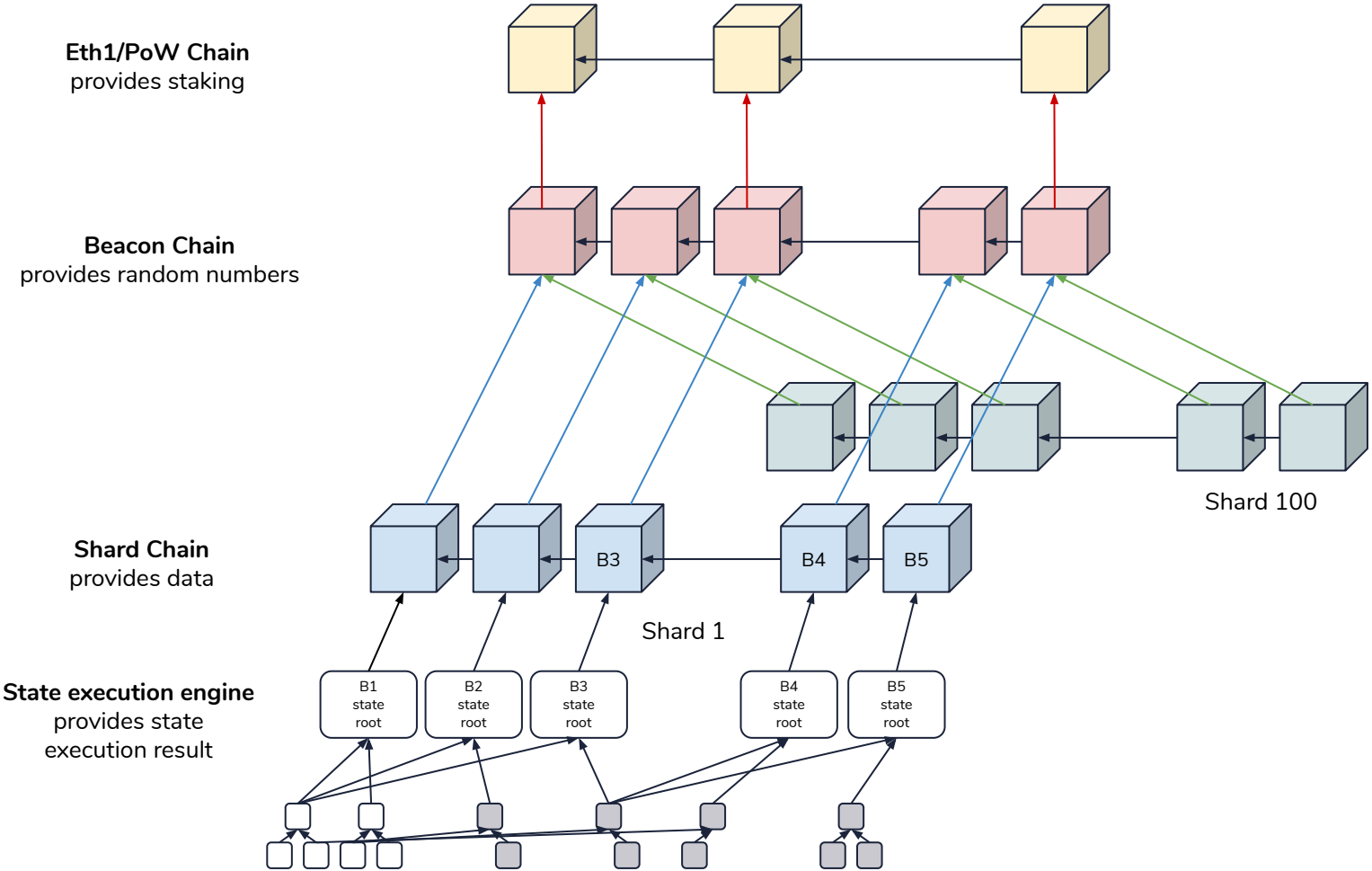
Epoch boundary: process epoch on the first slot of the next epoch



① Cache state root
② Process slot
③ If (state.slot +1) %SLOTS_PER_EPOCH==0: process epoch
④ state.slot += Slot(1)

Computation and Network Requirements

1. Worst case: 4M validators in BeaconState
2. Network propogation
3. BLS signature aggregation


Eth1/PoW Chain
provides staking
Beacon Chain
provides random numbers
Shard Chain
provides data
State execution engine
provides state
execution result
B3
B4
B5
Shard 1
Shard 100
B1
state
root
B2
state
root
B3
state
root
B4
state
root
B5
state
root