Implementing Ethereum Serenity with Proof of Stake + Sharding
What is Ethereum?
Ethereum - A Decentralized World Computer

- Open source blockchain
- Decentralized global virtual machine
- Consisting of tens of thousands of nodes
- Unlimited possibility of use cases
  - DAOs
  - ERC Tokens
  - DApps
What Does It Mean To Scale Ethereum?
Today’s Transaction Maximum Throughput

- **Bitcoin**: 7 tx/s
  - Average: 3 tx/s

- **Ethereum**: 27 tx/s
  - Average: 12 tx/s

- **Visa**: 24,000+ tx/s
  - Average: 1,667 tx/s
Today’s Blocktimes

10 minutes  14 seconds  ?
How Transactions Fit Into Blocks

- Blocks typically consist of the highest paying transactions that fit within a block gas limit
- Miners mine transactions and collect gas fees
- Miners vote on the gas limit
- Current default algorithm for gas limit calculation is at least 4.7M but targeting 150% of recent 1024 block exponential moving average. Changes are limited by a factor of 1/1024 in either direction.

<table>
<thead>
<tr>
<th>Block 5912518</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - Transaction w/ 21000 gas</td>
</tr>
<tr>
<td>2 - Transaction w/ 21000 gas</td>
</tr>
<tr>
<td>3 - Transaction w/ 153251 gas</td>
</tr>
<tr>
<td>74 - Transaction w/ 46548 gas</td>
</tr>
</tbody>
</table>

Gas Used 7,987,062  
Gas Limit 8,000,029
Ethereum Average GasLimit Chart

Source: Etherscan.io

Click and drag in the plot area to zoom in
How Can We Scale?
Blockchain Trilemma

Scalability

Decentralization

Security
Idea: Increase the Block Gas Limit!

Issues to consider

- Bigger blocks means each block requires more computational power
- Full nodes require more resources to verify blocks
- Less decentralized
Idea: Reduce the Time Between Blocks!

Issues to consider

- Fast blocks means higher probability of forks
- More forks makes blockchains vulnerable to attacks
- Less secure
Blockchain Trilemma

Scalability

Decentralization

Security
Two Types of Scaling Solutions

Layer 1 - On chain

- Higher throughput on the protocol layer
- More difficult to implement
- Satisfies the trilemma
- Benefits layer 2

Layer 2 - Off chain

- Higher throughput enabled by less on-chain operations
- Easier to implement
- More flexible and customizable
- May not be as secure or decentralized as layer 1
Ethereum 2.0
What is Ethereum 2.0?

“A big, multi-year long, upgrade to massively increase the blockchain’s scalability with **sharding**, increase security with **proof of stake**, and improve its **programmability** by changing a bunch of technical things we got wrong the first time.”

– Vitalik Buterin, Creator of Ethereum
Phase 0
Beacon Chain
Beacon Chain

**Validator Registry**
- 1 way deposit via deposit contract
- 32 ETH minimum to join
- 18 ETH ejection balance
- Exits / Withdraws

**Reward / Penalties**
- Calculated every epoch
- Validator slashing
- Liveness penalty
- Participation reward

**Shuffling / Randomness**
- Calculated during epoch transition
- RANDAO model
- Randomly distributed validator pool
- Verifiable delay function (soon™)

**Proof of Stake Finalization**
- Block justification via Casper FFG
- Allows finalization of ETH 1.x
Casper - Friendly Finality Gadget

- Validators have ETH at stake
- Energy efficient consensus mechanism
- Finalized checkpoints
- Lower barrier to entry
Becoming a Validator

1. Sends 32eth to deposit contract
2. Node processes deposit log
3. Wait for a new ETH1 voting period
4. Wait for a new finalized epoch
5. Get put into an activation queue
6. Wait to get rotated out of the queue
7. Active!

Minimum activation time ~2.134 hours
Validator Responsibilities

**Proposer** - A validator selected to create a beacon chain block

**Attester** - A validator that is part of the committee that creates attestation and creates crosslink to a recent shard block on a shard chain

**Committee** - A randomly sampled subset of validators
Proposing a Beacon Block

1. Assemble the block body
2. Execute the state transition
3. Sign the block
4. Broadcast to network
Beacon Block Processing

Beacon block

Verify slot → Verify parent root → Verify BLS sig → Verify randao → Mix randao

Count ETH1 data votes → Update latest eth1 data

Process block header

Process randao

Process eth1 chain data


Process beacon chain transaction objects
Attesting

1. Determine Casper FFG, Crosslink, and LMD Ghost votes
2. Aggregate similar attestations
3. Sign the attestation
4. Broadcast to network
Validator Rewards and Penalties

- Proposing a block yields higher reward than attestations
- Rewards and penalties are calculated every epoch
- Penalties increase exponentially when finality has not occurred for more than four epochs

<table>
<thead>
<tr>
<th>Total ETH validating</th>
<th>Max annual issuance</th>
<th>Max annual network issuance</th>
<th>Max annual return rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1MM</td>
<td>181,019</td>
<td>0.17%</td>
<td>18.10%</td>
</tr>
<tr>
<td>3MM</td>
<td>313,534</td>
<td>0.30%</td>
<td>10.45%</td>
</tr>
<tr>
<td>10MM</td>
<td>572,433</td>
<td>0.54%</td>
<td>5.72%</td>
</tr>
<tr>
<td>30MM</td>
<td>991,483</td>
<td>0.94%</td>
<td>3.30%</td>
</tr>
<tr>
<td>100MM</td>
<td>1,810,193</td>
<td>1.71%</td>
<td>1.81%</td>
</tr>
</tbody>
</table>

2,097,152 ETH required to start ETH 2.0
Phase 1
Shard Chains
Shard Chains

- Introduces the parallel shard chains
- 64 shards, data only
- Shard chains are linked to the beacon chain by crosslinks once per epoch
- Expected to come to consensus on 10Mb/s of data
Use Cases

- ZK Rollup
- ZK Rollup Rollup
- Decentralized twitter
- GPG key server
- Website hosting
- Data layer for private/enterprise blockchains
- Generalized small / medium amounts of storage
Phase 1.5
Merging eth1 & eth2
Phase 1.5

- Until phase 1.5, the Ethereum we use today on mainnet will continue as a proof-of-work blockchain and transactions will continue to be processed by miners.
- Starting in phase 1.5, eth1 will officially become a shard and transition to proof-of-stake.
- For end users and dapps, this change should be *seamless*. 
Phase 2
State Execution
State Execution

- Replace EVM with eWASM
- Asynchronous cross shard transactions
- Contract yanking (migrating shards)
- Ethereum 2.0 becomes useful to average contract developer / users
- In research and design phase, development likely to start early 2020
- Development can start in parallel to phase 0 and phase 1
Building Ethereum 2.0
From Research to Implementation

- Explore new ideas
- Collaborate on ethrear.ch, in person, online channels
- Propose changes to the Ethereum 2.0 specification

- The spec changes are reviewed by other researchers and implementation teams
- Spec release targets are tagged

- Implementation teams design new features
- Features are proposed in github and reviewed within the team
Prysm Feature Lifecycle

- Design document
- Tracking issues
- Implementation
- Pull request review
- Canary analysis / testing
- Release
Running Validators

This is NOT investment advice!
Prysm Client Design

Diagram:
- Prysm Validator
- Prysm Beacon Node
- Network
ETH 2.0 Issuance and Rewards

Source: https://docs.ethhub.io/

- **Max annual issuance**
- **Max annual return rate**

<table>
<thead>
<tr>
<th>Amount of ETH staked</th>
<th>ETH2 maximum annual issuance</th>
<th>Maximum annual return for validators</th>
</tr>
</thead>
<tbody>
<tr>
<td>1,000,000</td>
<td>181,019</td>
<td>1.81%</td>
</tr>
<tr>
<td>3,000,000</td>
<td>313,534</td>
<td>5.72%</td>
</tr>
<tr>
<td>10,000,000</td>
<td>572,433</td>
<td>10.45%</td>
</tr>
<tr>
<td>30,000,000</td>
<td>991,483</td>
<td>18.10%</td>
</tr>
<tr>
<td>100,000,000</td>
<td>1,810,193</td>
<td>20.00%</td>
</tr>
</tbody>
</table>
Validator profits/yield

- Costs are low and do not scale linearly with the number of validators in operator
- Long term commitment: cannot unlock funds until phase 2
- Liveness penalties can cost up to half of validator balance (16 ETH)
- Rewards are higher for early adopters
- Staking is not without risk!

Based on 10MM at stake and ETH price at $405
Become a validator and help secure eth2.

Earn continuous rewards for providing a public good to the community.

GET STARTED

- https://medalla.launchpad.ethereum.org/
- https://prylabs.net
Recap

- Ethereum 2.0 introduces proof of stake and blockchain sharding
- Ethereum 2.0 is a new blockchain; not a hard fork
- Ethereum 2.0 is a phased rollout, expected to complete in 2021
- Ethereum 2.0 phase 0 is available to test today, launching this Q4 2020
Prysmatic Labs
@prylabs