Eth2 Implementers' call #23

Agenda: https://github.com/ethereum/eth2.0-pm/issues/68
Livestream: https://www.youtube.com/watch?v=Av74vZRXeKo

HWW: "Just realized that the first eth2 call in on August 2, 2018… so it's over 1 year!!"

Testing and Release updates

Missing BLS tests have been added plus SSZ generic tests.
0.8.3 release next Tuesday, just includes some more tests, clarifications, typo fix: no substantive changes.
This is the interop target for September.

Proto requests final input from teams on testing formats ahead of the release.

Deposit contract: RV found a Vyper compiler bug while auditing the deposit contract. Adding an SSZ root parameter to the contract.

Mid-late Sept there will be some substantive changes:
Removal of some of the light-client apparatus since it is not delivering what we require (https://github.com/ethereum/eth2.0-specs/pull/1329)
Temporary removal of transfers for improvements.
(https://github.com/ethereum/eth2.0-specs/issues/1343)

Client updates

Yeeth:
Focusing on validator client only. May use Lighthouse (?) BC node.
Danny: see Moloch proposal for generic BC client.

Harmony:
Finished Validator API implementation. Implemented RocksDB for chain storage. Eth1 integration. Finished gossipsub in JVM libp2p, testing with libdaemon. Shahan has finished Noise implementation in JVM libp2p. Phase 0 near release. Could be usable for interop. Started work on 0.8.2 - needs lots of work on testing. Working on QA. Developing a fuzzer.

Trinity:
Focusing on network spec for interop. Pylibp2p, working on Secio. Fixing some issues. Wire protocol. Discv5 - want to refactor the Eth1 version for Eth2.

Artemis:

Intro from Shahan. SSZ debugging and deserialisation implementation. State tests. Rust libp2p implementation (Mothra). Working on metrics for productisation.

Lighthouse:
Optimise DB - cold and hot implementation.
Testnet stability.
Updating networking stack, in particular syncing.
BLS standardisation.
Connection to Eth1 deposit contract.
HTTP API.

Prysm:
Update to latest networking spec, sync.
RPC queries.
New fork choice rule.
Benchmarking/optimisation. Target 1s slot time.
New BLS library improves performance: 40x speedup for aggregation

Lodestar:
Erik Tu joined team.
0.8.2 spec tests.
Breaking out subcomponents as separate modules.
Networking for interop: Discv5 half done. Libp2p in progress.

Nimbus:
Dmitry Ryajov will work on libp2p
New SSZ implemented.
Eth1 deposit contract interaction.
Bootstrap Eth2 genesis from Ganache: https://github.com/status-im/thundercloud
New network spec.
Libp2p working on Windows.

Update from Protolambda:
Working towards Interop
Make comparison table of everybody's dev status and features. This will help with integration testing and identify gaps (keystore, genesis start, logging...)
Whiteblock will circulate a survey and talk 1-1 with teams.
Raul K doing something similar for libp2p - could cooperate.

Networking

Felix Lange on discv5
https://github.com/ethereum/devp2p/blob/master/discv5/discv5.md
Started an audit of the spec draft with Least Authority last week. Another couple of weeks work needed.
Would like to do interop testing of his implementation with anyone else's.

Q about security in topic information [Mikhail]

Mike Goelzer from PL:
Bounties projects coming up at EthBerlin. https://github.com/libp2p/devgrants

Shahan:
Noise implementation in JVM libp2p. Works but incomplete. Working on making it more robust.

Whiteblock:
Webinar coming up in a couple of hours.

Harmony:
block compression ideas: https://hackmd.io/ZCOiGwjLRy6il6yuAnF05w
Allows inclusion of more attestations per block.
Other trade-offs are possible. Need benchmarking and real-world data.
See also https://github.com/ethereum/eth2.0-specs/issues/1331

Unstructured aggregation strategies study. Attestation delivery could be an issue
An issue: BFT vs scalability https://hackmd.io/iHDZAzwlRE2uwv3hsB-9Gw

See index:
https://github.com/harmony-dev/beacon-chain-java/wiki/Research-documents-(ENG)

Research

Vitalik
PR#1186 was merged (Merkle proof verification - provides a generalised index)
Unfinished PR - Beacon chain updates for Phase1
Default light client syncing algorithm better defined
=> there is enough info now to start building light clients
Need infrastructure to start testing lightclients (can't really test them properly until Ph1)
Thinking about making light clients more privacy-preserving (but adds a lot of overhead).

Justin:
Phase 0 bounties. 5Eth/1000Dai for substantive changes that are merged before Eth2 genesis. https://github.com/ethereum/eth2.0-specs/issues/1345
BLS standardisation: feature complete and no known issues (so considered frozen). New BLS spec will be merged into dev branch for now, bit not into master. Want at least some of the implementers to start playing with it. Constant-time hash function is the main work, rest is minor. The three IETF standards are not yet ratified, so there may yet be changes... but Ethereum is first to implement.
Also standardisation around key stuff: checksums, keystores, wallets. Aiming to be minimalist.

New light client design is “awesome” - minimal spec is extremely simple, low overhead, lower bandwidth than Bitcoin SPV. Looking into a further possible 10x bandwidth optimisation. Opens door to bridges with other blockchains.
“Quantum apocalypse insurance” - validators can commit to a secret with a quantum secure sig (e.g. Lamport). If quantum computers break BLS, there is then a path to transition to a different secure platform. (Optional feature.) Adds a field to the transfer mechanism.

Will Villanueva (Quilt):
Benchmarking multi-merkle proofs in sparse merkle trees.
eWASM team doin patricia merkle tree with RLP.
Continuing to build out Ph1 as a platform to support Scout.
New repo that wraps Scout: abstracts away some complexity

Runtime Verification:
Progressing K implementation of the spec. Will then create testing framework and run tests.
Deposit contract verification nearly complete.

Interop

Vans being booked to transport people in waves to the site.
Will be fully catered.
Quilt team has some space in their cabin.

Other news

Protolambda:
Gamifying testnet participation and attack.
NFT Collectible for participating in the Eth2 launch under discussion.
^^^ call for ideas on both of the above.

Lighthouse:
Has been working on fuzzing. Found an SSZ bug.
Differential fuzzing has gone quiet.

Chat (the highlights!)

From danny to Everyone: 03:04 PM
https://github.com/ethereum/eth2.0-pm/issues/68

From Mamy to Everyone: 03:09 PM
light clients: https://github.com/ethereum/eth2.0-specs/pull/1329

From Justin Drake to Everyone: 03:09 PM
https://github.com/ethereum/eth2.0-specs/issues/1343
^^ Tracker for issues around transfers

From danny to Everyone: 03:21 PM
here is the PR for removal of light client infra from phase 0

From Mamy to Everyone: 03:23 PM
https://github.com/status-im/thundercloud

From danny to Everyone: 03:23 PM
https://github.com/ethereum/eth2.0-specs/pull/1329

From Hsiao-Wei Wang to Everyone: 03:24 PM
Just realized that the first eth2 call in on August 2, 2018… so it's over 1 year!!

From danny to Everyone: 03:24 PM
woww

From danny to Everyone: 03:33 PM
https://github.com/ethereum/devp2p/wiki/Discovery-Overview

From Jannik Luhn to Everyone: 03:34 PM
https://github.com/ethereum/devp2p/blob/master/discv5/discv5.md

From danny to Everyone: 03:35 PM
https://github.com/libp2p/devgrants

From Trenton Van Epps to Everyone: 03:38 PM
Webinar signup: https://zoom.us/webinar/register/WN_GjWAB_7qQUyN67gIQ43YDg

From danny to Everyone: 03:45 PM
https://hackmd.io/ZCOiGwjLRy6il6yuAnF05w
related eth2.0specs issue — https://github.com/ethereum/eth2.0-specs/issues/1331

From matt garnett to Everyone: 03:51 PM
Sorry what was the PR that changed the merkle proof verification format?
thanks!

From Hsiao-Wei Wang to Everyone: 03:51 PM
https://github.com/ethereum/eth2.0-specs/pull/1186

From Mikhail Kalinin to Everyone: 03:52 PM
A list of documents related to attestation dissemination and aggregation can be found here
https://github.com/harmony-dev/beacon-chain-java/wiki/Research-documents-(ENG)

From danny to Everyone: 03:52 PM
https://github.com/ethereum/eth2.0-specs/pull/1316

From matt garnett to Everyone: 03:54 PM
where is the best place to understand the current light client design / thoughts?
Is it https://github.com/ethereum/eth2.0-specs/blob/dev/specs/light_client/sync_protocol.md
?

From Hsiao-Wei Wang to Everyone: 03:56 PM
@matt some ideas in design rationale doc:
https://notes.ethereum.org/s/rkhCgQteN#Persistent-committees

From Justin Drake to Everyone: 03:57 PM
What is the context for PIR?

From danny to Everyone: 03:57 PM
light clients

From Justin Drake to Everyone: 03:57 PM
Oh I see

From danny to Everyone: 03:58 PM
asking for ansewers to arbitrary functions
probably not the sync alg

From matt garnett to Everyone: 03:58 PM
thanks @hww

From Hsiao-Wei Wang to Everyone: 03:59 PM
https://github.com/ethereum/eth2.0-specs/issues/1345
^^^^ 5 ETH phase 0 bounties

From matt garnett to Everyone: 04:02 PM
Q I had on determining the “full state” of an EE: if all a wasm binary defines is a function that takes a pre-state + input and returns a post state how can light client servers save the full state? Any thoughts on this at all or is it left as an exercise the reader (implementer)