Eth2 Implementers’ Call #26 - 2019-10-24

[Quick contemporaneous notes by Ben Edgington]

Agenda: https://github.com/ethereum/eth2.0-pm/issues/89
Livestream: https://www.youtube.com/watch?v=DXGeC7cg71Y

Testing and Release updates

Phase 0 0.8.4 released today. Mainly testing updates, and networking updates - both driven by findings at interop. No state-transition changes.

Semi-major release planned soon:
- To address output of audits, eg. attacks on fork choice
- Removal of crosslink scaffolding while Ph1 is settled

Testing [Proto]
Muskoka infrastructure for testing and performance testing of the clients. Proto will reach out to each client team in the next week.

Fuzzing [Mehdi]
Sigma Prime picked up the fuzzing work. Differential fuzzer working for main block processing aspects of the spec, 0.8.3 (same as 0.8.4).
Beacon state can be loaded from a file and passed to all fuzz targets.
zrnt, pyspec and Lighthouse currently supported.
Making consistency improvements.
Adding epoch transitions.
Coverage improvements with mutators.
Libprotobuf mutator.
Planning to work with teams to onboard Nim, Go, Java, Javascript over the next weeks.

Client updates

Lighthouse:
Working on discv5 standardisation. Talking to Prysm about testing. Working on implementing topics.
Eth1 integration in progress.
Slashing protection in progress. [Can share the docs for this.]
Optimisations to Rust BLS; looking at Herumi library for BLS.
Combine Beacon node and Validators into one binary.

Artemis:
BLS new hash to curve implementation.
Noise JVM implementation complete.

Handel integration.
Code cleanup and handover to prod dev.
Harmony team merge.

Harmony:
Working through Artemis merger.
Fork choice tests. Can share test vectors when done.
Finishing discv5 implementation. Just working on testing at the moment. Goal to interop with Geth implementation.

Prysm:
Debugging testnet.
PR to removing crosslinks.
Implementing naive aggregation strategy.
Herumi BLS is faster than previous lib, and passing tests.
SSZ caching library.
End-to-end testing, and fuzz testing strategies.

Lodestar:
New team member.
Optimisations: state transition; generalised caching mechanism.
Finishing discv5.
Updating networking spec.

Nimbus:
GitHub Ethereum2 clients repo created to store scripts for running multi-client testnets. All teams have been invited to join as admins.
Eth1 integration almost done.
Looking forward to participating in joint testnet linked to Goerli.
Implementing native libp2p - users can choose between daemon and native.
Fuzzing framework developed. Focusing on low-level first: SSZ, crypto, etc. Will integrate with Sigma Prime fuzzer soon.
Had to update Nim version 1.2.

Trinity:
Making pylibp2p more complete.
Fixed beacon chain sync.
Eth1 chain integration.

Shasper:
Working to join other client testnets and fix issues that arise.
Fixing issues with Casper engine.

Research Updates

Phase 1 changes proposed by Vitalik. Fewer shards, but crosslinking every slot.

In response, remove cross-links altogether from Phase 0 until Ph1 is settled. PR is currently up for review.

Vitalik
Working on several Ph1 optimisations and simplifications. Looking for feedback and opinions.

Justin
BLS standardisation: we are in a good place. The spec has not changed for a few months, except for a minor security change. Riad Wahby is addressing standardisation, and any possible patent infringements. There is a meeting of interested parties November 16th-22nd and expect freeze then.

Herumi library for BLS. This seems to be significantly faster than others, like Milagro. Lighthouse testing suggests 2.4x as fast (relies on x86 assembly for the highest performance. Arm is supported, but ~30% slower per pairing). Language integration has not been so easy, so considering a grant to improve this. It may be possible to make the mcl pairing library even faster, and do formal verification. Guido is working on fuzzing Herumi.

Mary Maller has described a way of aggregating signatures that is cheaper. May not be relevant at Layer 1.

Deposit contract formal verification to be completed in a couple of weeks. Discussing deposit creation website. Lots of testing, UI, etc. before deployment.

Protolambda
SSZ specs being put into a new repo. Improved specification with change control.

Cayman [Chainsafe]
Establishing a monthly light client call aimed at getting light client technology into production (for both Eth1 and Eth2). Announcement coming in the next few days. First call in 2-3 weeks.

Networking

PR for the naive attestation aggregation is in place.

Felix [EF]
Discv5. Big improvements to spec: topics documented. Go and Rust implementations interoperable for basic DHT - Felix believes both are 100% spec compliant.
Two open problems:
(1) Topic radius estimation is not well defined. Current code is “horrible”.
(2) Audit is in progress (Least Authority): recommend a proof-of-work system for node identities. Felix unsure on the merits of this - would welcome feedback on this issue.

Trenton [Whiteblock]
Have released a repo of testing methodologies for libp2p. Seeking feedback.

Testnet Discussion

The pending v0.9 of Ph0, including udpates to remove crosslinks etc., is a prerequisite in the view of most teams. Should not be too hard to implement - mostly removing stuff.

Meanwhile, more single client testnets probably the next step (public; semi-public), with a dash of multi-client testing.

Whiteblock offers to help spin up testnets.

Chainsafe has “millions” of Goerli Eth and is happy to fully fund testnets :-)

Note: PoA testnets may be more suitable for when we do incentivised networks.

[Discussion about experiences of running testnets, tooling, block explorers, etc.]

Danny to write proposals for shared testnets before the next call. Resume conversation in two weeks. Discuss monitoring and visualisation etc. in the Eth2/pm repo, along with any other testnet issues.

Terence: what aggregation strategy to use for joint testnets?
Danny: We will need at least the “naive strategy” before too long. Move towards favouring Mainnet over Interop configurations in testnets now.

Chat highlights

From danny to Everyone: 03:04 PM
https://github.com/ethereum/eth2.0-pm/issues/89
release: https://github.com/ethereum/eth2.0-specs/releases/tag/v0.8.4

From danny to Everyone: 03:27 PM
phase 0 simplification PR: https://github.com/ethereum/eth2.0-specs/pull/1428

From Mikhail Kalinin to Everyone: 03:36 PM
https://github.com/herumi/bls

From Hsiao-Wei Wang to Everyone: 03:36 PM
mcl: https://github.com/herumi/mcl

From danny to Everyone: 03:36 PM
https://github.com/herumi/mcl

From Leo BSC to Everyone: 03:39 PM

https://eprint.iacr.org/2019/1177

From Trenton Van Epps to Everyone: 03:39 PM
Libp2p bechmarking discussion:
https://community.whiteblock.io/t/gossipsub-tests/17

From Leo BSC to Everyone: 03:39 PM
Is this the recent paper on BLS aggregation?

From danny to Everyone: 03:42 PM
naive aggregation pr: https://github.com/ethereum/eth2.0-specs/pull/1440
expanding of topic descriptions in discv5: https://github.com/ethereum/devp2p/pull/120
pow on node identities: https://github.com/ethereum/devp2p/issues/122

From Trenton Van Epps to Everyone: 03:49 PM
Whiteblock benchmarking Libp2p discussion:
https://community.whiteblock.io/t/gossipsub-tests/17

Repo with methodology: https://github.com/whiteblock/gossipsub-testing