Blox

eth2 pools mini paper

Updated: 16.9.20

Pools is a protocol for distributed staking infrastructure for eth2 staking. By distribuite infrastructure we mean the separation between the financing and running an eth2 validator.

The backbone of decentralized staking pools is in distribuiting the control of the keys that control the validator and its withdrawal key. You can think of it as a giant multisig setup with some M-of-N threshold for signing attestations, block proposals and withdrawal transactions.
A good starting point could be this presentation.

Draft go-spec

Overview

The network has 2 actors: block producers (BP) and staker.

A BP is a bonded actor (staked) which has the responsibility of executing eth2 validator assignments and pool network assignments (producing a block and signing it).

A pool is a collection of ETH deposited by a staker.

Pools are controlled by the network via a pool committee (or committee in short), a collection of BPs, randomly chosen, to be assigned to a pool. Their responsibility is to execute the eth2 duties for that pool. For their work they will earn rewards depending on their performance.

Pools

Pool Creation

Stakers gather 32 ETH and initiate a create pool request which is broadcasted on the ethereum mainnet.
A BP, looking at the ethereum mainnet, sees the deposits and includes a create pool request inside the block.

The next epoch BP is nominated as the Distributed-key-Generation(DKG) leader, responsible for listening for communications that result in a successful/ non-successful DKG.
128 randomly chosen BPs will be deterministically selected to execute the DKG which produces a withdrawal and validation pub keys.
The nominated DKG leader will publish (when broadcasting his block) the result of the DKG.

Successful DKG: leader and participants are rewarded.
Un-successful: participants are penalized.

In order to create new pools the network as a whole needs to be collateralized at 150%, under which new pools will be created.

A pool has a liquidation time.

A pool can be a single staker with an existing validator which distributes shares to the validators via Verifiable-Secret-Sharing(VSS).

Every staker in the pool will receive a tokenized ERC20 share of that pool with which he could withdraw his stake + rewards when the pool is terminated.
Token fungibility - TBD

Pool liquidation

When the termination time is up, the committee will initiate a withdrawal to a designated smart contract for distribution.
This could be on eth1 (as described here) or in eth2 (if ready)

Pool Operation

Every beacon-chain epoch each pool has 128 BPs (committee) which are responsible for executing the pool's duties. They are rewarded for that.

When a BP produces a block it gathers a pool execution summaries object for each pool which includes the duties the pool had in that epoch, if that duty was finalized and who from the 128 BPs participated in executing the duty.
Only finalized duties will be included in the summary so to not revert back rewards if the beacon-chain reorganizes and forks.

A BP will be included in the summary if he acted upon the duty within the time limits correctly.

Block production

Becoming a BP

A BP is represented by a public address for which a fixed amount of stake was put as collateral (A user wishing to stake more can simply run more BPs).
Once a BP is activated (approved by the network) he will then be assigned duties to perform, deterministically, for which he will gain rewards or suffer penalties.

Block voting

Every epoch, a block voting committee is randomly chosen to vote on that block.
It's threshold is ⅔ of the committee.

Block production rewards

A BP that proposed a block has a special reward

Block voting committee BPs will be rewarded in CDT per the proposed block for their committee work.

The pools ethereum contract has a minting admin key which is distributed across X active BPs. To withdraw the rewarded CDT from the pool chain to ethereum mainnet a BP would need to post a withdrawal request on the pool chain. A specialized, randomly selected, committee will need to sign that request and will post it's signature.
The requester will post the signature on ethereum mainnet which will be verified on chain (2 BLS pairings where th pk is known from the minting admin key).

Random Deterministic Committees

Pools uses VRF as means to deterministically calculate committees that play different roles in the protocol.
Given a random seed, which each node can calculate deterministically by traversing all transaction and block data, we calculate the different committees via Swap-or-Not algorithm used in eth2.
The seed is concatenated with categories and then hashd so to produce different committees for different purposes.

- Pool committee - seed + []byte("pool <id> committee")
- Block voting committee - seed + []byte("block voting committee")

- Block proposer - seed + []byte(“block proposer”)
    - select at position 0

The concatenated byte slice is hashed with sha256

Collateral

Collateralization ratio and block rewards

The ration is: (BP collateral in ETH)/(sum of pool balances).
A 1:1 ratio is when the network is fully collateralized with the assets it manages.
A 1:10 ratio is when the network is 10% collateralized.

New pools are created with 150% collateralization. A pool’s committee has a ⅔ threshold for signing, that ⅔ need zero incentives for malicious behaviour.
If each committee BP puts 150% collateral (over his relative committee signing power) that any ⅔ that will be malicious and try to steal the pool’s stake will be stealing exactly their stake. A zero sum game.

Depending on the BPs total stake, he can participate in several pools.

Example:
A pool is 32 ETH, its committee consists of 128 BPs (⅔ = 86, ⅓ = 42).
Each committee BP will put ~0.372 ETH collateral.
86 * 0.327 = 32ETH.
Total pool collateral = ~47.62ETH (~150%)

Stake at work

The ETH that BPs are staking will also be staked on the eth network and managed by the protocol. That will be their base reward.
The CDT reward from the protocol is value added.

Network Incentives

Individual BP rewards are tied to their participation in pools and the general collateralization of the network.
A BP has a base reward per pool per epoch he participates in + a variable reward which depends on the collateralization level of the entire network. The target is to have at least 150% collateralization, at which point the variable reward is the highest, to create an incentive for new BPs to join.

As with other blockchains, the $ value of the CDT reward is a central incentive for BPs.

Here is a quick summary of the different scenarios and their impact on the network

CDT reward $ value	Demand for new pools	Effect
⬆	⬆	Fast network growth as more BPs and pools demand to enter
⬆	-	Network capitalization goes much higher than 150% which lowers the variable rewards. $ rewards will go up per BP
⬇	-	Network capitalization will probably go towards 100% as incentives for becoming a BP are lower. A cycle of forced pool liquidations will occur to make capitalization ratio higher.
⬆	⬇	Network capitalization goes much faster and higher than 150% which lowers the variable rewards. $ rewards might go up per BP
-	⬆	Network capitalization reaches 150% or even lower, maximizing CDT rewards but carries more risk of forced pool liquidations if no new BPs join the network
⬇	⬆	Network capitalization will probably go towards 100% as incentives for becoming a BP are lower. A cycle of forced pool liquidations will occur to make capitalization ratio higher.
⬇	⬇	Long term network decline as

		the demand for its use is going down.
-	-	Network equilibrium point

Example 1 - Network bootstrapping at current state

Setup

- ETH2 at stake 3M
- ETH2 staking yearly reward 8.85%
- ETH price $400
- BP CDT yearly reward 15% (150M CDT)
- Network collateralization 150%
- CDT price $0.01

Suppose the pools network has 500 BPs and 333 pools (150% collateralization), total network eth2 at stake 833 pools (BPs + pools), equal to ~26.7K ETH (~$11M).
The BPs, at 100% uptime, will gain on average 300K CDT worth $3K on top of a normal 32 ETH pool which will make 2.832ETH worth $1,132.
In total a BP will earn ~$4.2K a year for his work (~34% APR).

Depending on different network settings those numbers can vary, the point of this example is to show the network status if it would have started today.

Example 2 - Network Scaling

Setup

- ETH2 at stake 10M
- ETH2 staking yearly reward 4.85%
- ETH price $3,000
- BP CDT yearly reward 15% (150M CDT)
- Network collateralization 150%
- CDT price $5

Suppose the pools network has 50K BPs and 33.3K pools (150% collateralization), total network eth2 at stake 83.3K pools (BPs + pools), equal to ~2.67M ETH (~$8B).
The BPs, at 100% uptime, will gain on average 3K CDT worth $15K on top of a normal 32 ETH pool which will make 1.552ETH worth $4,656.
In total a BP will earn ~$20K a year for his work (~21% APR).

Depending on different network settings those numbers can vary, the point of this example is to show the network status under large scale (effectively holding ~27% of the total eth2 stake).

For decentralization and security reasons, no single service (even if decentralized like Blox pools) should hold above 33% of the total eth2 at stake.

Penalizable events

Personal

A personal penalty will be applied to a specific BP or a subgroup he temporarily belongs to (pool assignment)

Committee performance < min

The protocol should guarantee a min performance (one can think of 90%) for the pools. If a committee falls under this threshold in a particular epoch it's validators should be penalized.

Pool liquidation did not execute

At epoch E a pool is marked as terminated, every committee assigned to that pool from epoch E needs to execute a pool liquidation. If failed by epoch E+T (where T being max liquidation deadline) all committees in those epochs should be penalized.

Non participation

At epoch E a block producer BP has a duty to perform but misses or miss perform it.
Examples: Beacon duty, create pool DKG, block production and so on

Global

A global penalty is a penalty afflicted over the entire BP group in extreme situations

Unauthorized withdrawal

A withdrawal that happened before the life end of a pool or to an unauthorized destination

Pool slashed

During epoch E a pool was slashed.

Research

- Secret PSS by algorand
- Churp PSS

- tBTC and keep network