eth2 pools

Annotated Spec

By Blox

V0.3
Updated: 8.10.20

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

The backbone of decentralized staking pools is in distributing the control of the keys that control a validator. 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.

Design Goals

- End user can stake any amount
- End user doesn't need to run any infra
- Decentralized and trustless
- CDT2.0 as an incentive token

Overview

The network has 2 actors: block producers (BP) and stakers (end user).

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 operated by pool vaults, a multi-signature construct with bonded BPs which execute on the pool's eth2 duties, and tasks assigned to them by the pools blockchain.

Pools

Pool Creation

Stakers gather 32 ETH and initiate a create pool request which is broadcasted on the ethereum mainnet.
A BP (who is randomly selected to be the next block proposer on the pools chain), looking at the ethereum mainnet, sees the deposits and includes a create pool request inside a block.

A group of VAULT_SIZE BPs are randomly selected to construct the new pool's vault, via Distributed-key-Generation(DKG).
The set from which the vault group is selected from is a subset of the whole BP set for which it's members have at least 2 ETH of "free" collateral to bond to their vault participation (see collateral section for more details).

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

Every staker in the pool will receive a reward bearing ERC20 token with which he could withdraw his stake + rewards (see bETH).

Withdrawal

A pool is perpetual by default (never liquidated).
If a threshold amount of bETH requests liquidation (by sending it to a contract and asking for liquidation) the pools blockchain will randomly choose a pool to liquidate.

Although withdrawals are not yet specified, current discussions suggest a path to specify an eth1 address to withdrawal the stake to. This is built on the eth1<>eth merger.

The way a potential flow could look like is by letting a validator set an eth1 address as the target for his withdrawal (via the withdrawal credentials).
When doing so, eth2 will be sent to that address for distribution.
See active discord discussion

PoolChain

The PoolChain has the responsibility of managing all the different vaults (and pools) in the network, creating or liquidating pools, rewarding and penalizing BPs and more.

The chain is similarly constructed to the eth2 beacon-chain as it's closely tied to its operation, as with the beacon chain, the PoolsChain has epochs of SLOTS_IN_EPOCH slots and committees in every slot responsible for attesting to the created blocks.

Epoch

An epoch is a time duration which includes SLOTS_IN_EPOCH. In an epoch, for all pools must be compiled an execution summary for the last eth2 finalized epoch.

Slot

A slot is a time duration of SLOT_DURATION in which a randomly selected BP will propose a new block and all randomly selected committees for the slot number will compile and sign an aggregated attestation.

Block

```
message BlockBody {
   uint64 Proposer = 1;
   uint64 Epoch = 2;
   bytes ParentBlockRoot = 3;
   bytes Randao = 4;
   repeated CreateNewPoolRequest NewPoolReq = 8;
   repeated StakeDeposit StakeDeposits = 9;
   repeated CDTWithdrawalRequest CDTWithdrawReq = 10;
}
```

Attestation

All BPs are divided into attestation committees of min size MIN_ATTESTATION_COMMITTEEE_SIZE, every slot can have >0 committees depending on the overall size of the BP set.
1 of the attestation committee is chosen to prepare the execution summaries for that specific committee, other committee members sign it alongside casting ffg and LMD Ghost votes (similar to eth2 beacon-chain).

```
message AttestationData {
```

```
    # Slot of the attestation attesting for.
    uint64 slot = 1;
    # The committee index that submitted this attestation.
    uint32 committee_index = 2;
    # 32 byte root of the LMD GHOST block vote.
    bytes beacon_block_root = 3;
    # The most recent justified checkpoint in the beacon state
    Checkpoint source = 4;
    # The checkpoint attempting to be justified for the current epoch and
its epoch boundary block
    Checkpoint target = 5;
    # The committees execution tasks.
    repeated ExecutionSummary ExecutionSummaries = 6;
}
```

```
message Checkpoint {
    # A checkpoint is every epoch's first slot. The goal of Casper FFG
    # is to link the check points together for justification and
finalization.
    # Epoch the checkpoint references.
    uint64 epoch = 1;
    # Block root of the checkpoint references.
    bytes root = 2;
}
```

Execution Summary

The pools vault members get penalized or rewarded based on the pools performance, which only include duties finalized on the eth2 beacon chain.
An attestation committee is assigned to every pool, compiling execution summaries on that pool.

```
message ExecutionSummary {
    uint64 PoolId = 1;
    uint64 Epoch = 2;
    repeated BeaconDuty Duties = 3;
}
```

```
message BeaconDuty {
    int32 Type = 1; # 0 - attestation, 1 - proposal, 2 - aggregation
    uint64 Committee = 2;
    uint64 Slot = 3;
```

```
    bool Finalized = 4;
    bytes Participation = 5; # 24 bit of the executors (by order) which executed this duty
}
```

The number of BPs in the network is linear to the number of pools:
#_of_pools * EFFECTIVE_POOL_STAKE * TARGET_COLLATERAL_RATIO / EFFECTIVE_BP_STAKE
Example: 1000 * 32 * 1.5 / 10 = 4,800 BPs

Taking the example above, the 4,800 BPs will be divided into 37 attestation committees, each compiling 27 execution summaries.

Stake at work

The ETH that BPs are staking will also be staked on the eth2 network and managed by the protocol. Their stake will not be collateralized and could be liquidated in case of penalties.

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.
TBD - categories

Block producer

Forced exit - Inactivity

A BP can be slashed for not being active. Inactivity will cause him to leak CDT due to penalties. If the debt of CDT incurred is >= bp_max_cdt_debt the BP will be forced exited.

Slashing - Collateral liquidation

TBD - How mass slashing affects other vault composition, if 20-30% of BPs are slashed together should we check the effect on other pools? Can it bring other pools below the signing threshold?

Unauthorized asset withdraw

A pool is collateralized by it's vault members (BPs). In case a pool is liquidated without a counterpart liquidation request (assets were stolen), its vault members will be penalized and slashed.
A block proposer will include in the next block a liquidation fraud proof which includes the aggregation bits of the BPs responsible for signing the withdrawal transaction on eth2.

```
message LiquidationFraudProof {
 bytes ETH2TxId = 1; // the withdrawal transaction on ETH2
 bytes SigningBits = 2; // who, from the vault, signed ETH2TxId
}
```

BPs which signed the transaction will have their whole stake slashed (not just the stake for that vault) and exited. BPs which did not sign will get only that particular vault stake slashed but not exit the protocol.

Signing bits are calculated by iterating all different permutations over the vault set, considering at least ⅔ must sign a transaction.
TBD - calculate how many iterations that requires.
TBD - explain security in case where an attacker has ⅓ of the BPs but also < ⅓ are offline.

Stalled liquidation request

Another case in which vault members can get liquidated is when their pool has a liquidation request pending but vault members fail to execute it after max_liquidation_execution_duration. In such cases their respective collateral will be liquidated, members are not slashed.

The bETH (Bond ETH)

When a user deposits ETH to create a pool, in return it receives bETH (1-to-1 peg) to his original deposit.

As times go on and the pools network generates rewards from the deposited pools, each bETH holder will see his balance grow respectively.
The rewards index is what determines the balance growth for each bETH holder.

Rewards index

The rewards index is an ever growing value that represents the total rewards gained by the network, it's initial value is 1.
The mechanism is inspired by Compound's borrowIndex.

Every block signed in the pools network marks a new reward index value which is equal to:

`reward_index += sum_current_block_execution_summaries`
(check go-spec for details).

Say current reward_index = 100, the next pools block a total of 3 eth were rewarded for all the pools combined. The reward index will now be 103.

Each pool participant that deposits ETH (and get's bETH in return) will be assigned, for that deposit, an initial rewardIndex value.
Every time the rewardsIndex gets updated in the bETH contract, a new balance for that user will be calculated as:

```
# rETH (user base balance) = 1
# initial_reward_index_value = 100
# reward_index = 103
# total_pools_value = 1000
current_balance += rETH*
                (reward_index - initial_reward_index_value)
                /total_pools_value

# equals
current_balance += 1 * (103-100)/1000 = 0.003 # 0.03% rewards
```

State Commitment to eth1

A series of contracts on eth1 (later will be emerged to eth2) manages CDT2.0 and bETH tokens. Specifically the pools state root for a finalized epoch will be committed by a special committee to eth1.
Once the state root is committed and was accepted (went without a dispute longer than STATE_COMMIT_DISPUTE_DURATION) the BP balances (CDT2.0) and reward index based on that state are considered finalized as well.

```
message StateCommitment {
   bytes StateRoot = 1; # pools chain state root as of the last block at
said epoch
   bytes Epoch = 2;
   repeated bytes Committee = 3; # compact committees (eth2 spec)
   bytes AuxCommitteesRoot = 4;
   repeated bytes NextCommittee = 5;
}
```

Commitment committees

Every COMMITTMENT_COMMITTEE_PERSISTENCE a new committee is randomly selected to commit to eth1. All other BPs are divided into auxiliary committees which have the power to dispute any commitment made by the commitment committee.

All other BPs are sub-divided into auxiliary committees which can dispute and vote on disputed state root commits. Aux committees are randomly selected every COMMITTMENT_COMMITTEE_PERSISTENCE.

Dispute

If the commitment committee signed an invalid , one of the auxiliary committees can dispute. By doing so it freezes state commitment for STATE_COMMIT_DISPUTE_DURATION in which other auxiliary committee members can vote as well.
A dispute concludes once ⅔ of the voting on the dispute has voted to one direction (TBD - should it have a forced end?).
If all aux committees voted, the majority wins.

The aux committees can be checked against the AuxCommitteeRoot from the last finalized state root commitment.

TBD - finalization length?

CDT2.0

Why use a token?

This is an important question which should be answered. To answer it we need to first ask what financial incentives do in the pools network?
BPs are the key to the network in terms of its capacity to create new pools and secure itself. A BP could be characterized as an actor with some technical knowledge, ETH and deep understanding of the eth2 staking market.
Each BP has 3 alternatives:

- Run a regular eth2 validator
- Join a pool as a staker
- Become a BP

Option 1+2 are pretty similar, option 3 requires more work and a dedicated decision of action. What could make him want to prefer option 3 over option 1/2?
If he is technical enough to run the necessary infrastructure then the answer is potential gains.

In a network setup where BPs are rewarded only from the network's own eth rewards then the added rewards over options 1/2 will come from the pools themselves.
Considering yearly eth2 rewards stabilize around 3-7% and BP number is linear to the pools ETH at stake, it seems there are just not enough rewards to make a potential BP become one.
Example:

- Total pools: 10 (320 ETH)
- BP minimal staking balance 2 ETH
- Collateral ratio: 150%
- Total BPs: 240 (320 * 1.5/ 2)
- Yearly pools reward (under 6%): 19.2 ETH (0.08ETH/ BP)

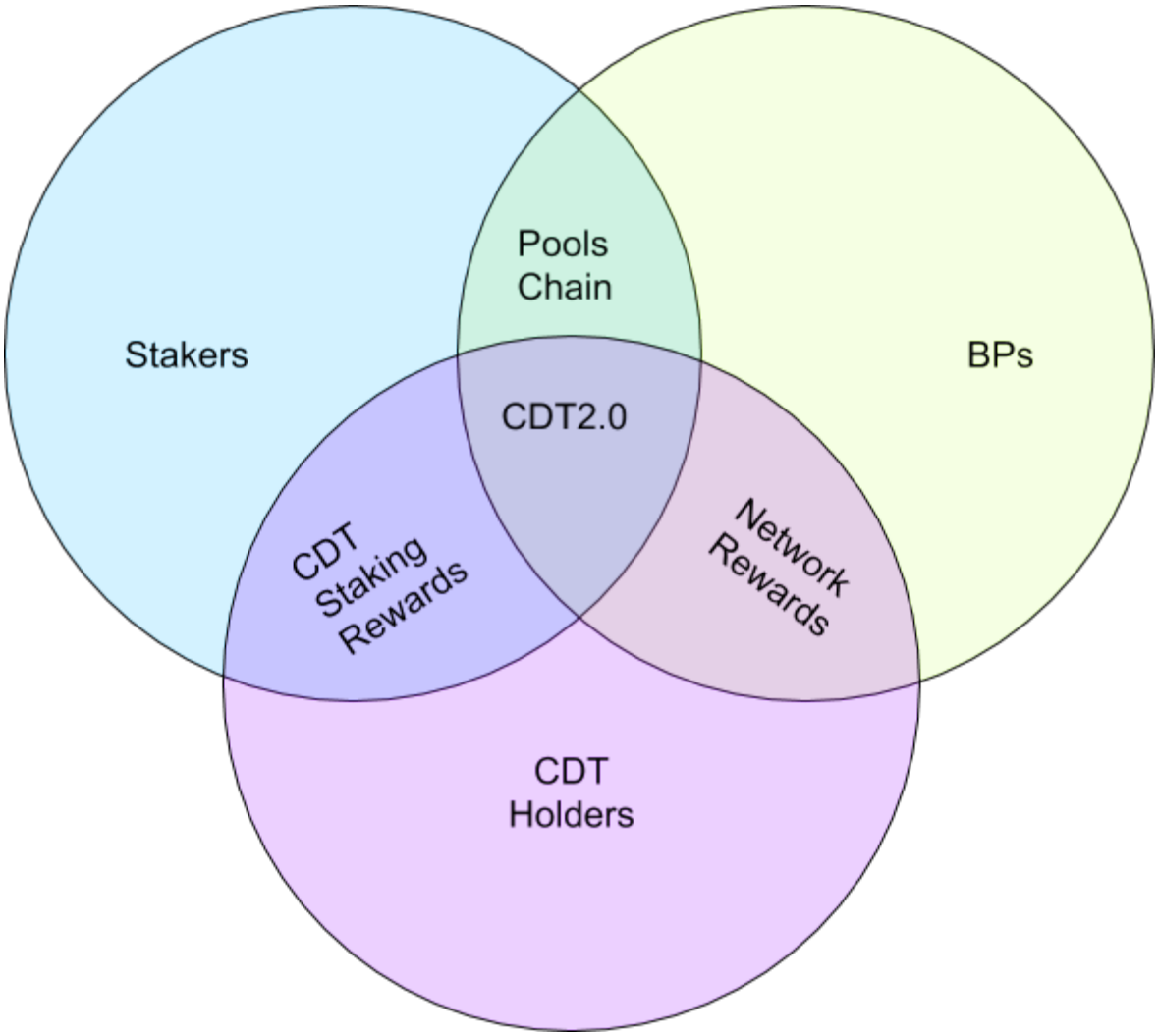
To create a sufficient incentive to become a BP and maintain the network, another source of rewards needs to be found.

CDT 2.0 Tokonomics

Most blockchains have some inflation policy which is the result of minting tokens as rewards to their block producers (miners, stakers, etc.).
As CDT is an already existing token, such an inflation will act as a fee imposed on all CDT holders.
The tokonomics of CDT2.0 should take into consideration the following challenges:

- Inflation rate
- Counteract the inflation “fee” imposed on CDT holders
- Pools users should pay a fee for the service they receive
- Sustainable model which scales.

Below is a description of the tokenmoics of CDT2.0 which is the relationship between block producers, stakers and CDT holders.



Block producers

Block producers are the actors in the network that secure it, collateralize, perform pool duties and more. They are the most involved type of actor with the highest risk (and highest reward). CDT2.0 will have a built rewards minting specification for the BPs different duties. Each duty will award (or penalize) the relevant BP.

The minted CDT will be distributed among the active BPs based on those duties. If say, 150M CDT were to be minted yearly, all of them in that year will be distributed as rewards.
From the above it becomes obvious that the more BPs are active the lower the CDT (amount) each of them will receive as rewards but the more potential pools can be created which increases network value.
This is designed for the network to self-regulate and find its equilibrium in terms of the number of BPs vs the reward they get.

Stakers

A staker is not required to put any work in his staking other than ETH, while gaining access to instant liquidity. No IT or infrastructure cost.
For this service, he will pay a fee out of his rewards. Technically some of the earned bETH will be taken as the fee to the network.

CDT holders

Miniting CDT as rewards to the BPs is a form of fee on all CDT holders. Inflation is measured by 2 factors:

- New CDT created
- CDT token velocity.

If many new CDTs were created but their velocity was 0 (meaning none were transferred) then the impact of minting them is close to 0.

To accommodate inflation, the fee collected from stakers will be distributed to anyone who staked his CDT for a certain period of time (gave up liquidity for the reward).
Here at play are:

- Number of CDT at stake
- Total bETH fees
- bETH/ CDT price

The more pools there are the more rewards the network generates, the more bETH will be distributed to CDT stakers.

Network Incentives

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.

Network Correctness

- Safety (nothing bad ever happens)

- Liveness (something good eventually happens)
- Availability (new txs will be processed)
- Consistency (unreliable)

Research

- Crypto building blocks
    - Secret PSS by algorand
    - Churp PSS
- Consensus
    - tBTC and keep network
    -
- CAP
    - Seth Gilbert CAP overview
- Tokenized stake
    - Stakewise(2 token system)
    - Dharma (non-fungible)
    - RocketPool (3 token system)
- eth1<>teh2 merger
    - Phase 1.5 summary
    - Optimistic rollups
        - Security analysis
        - overview

Protocol specification

Node

Name	value	Description
SLOTS_IN_EPOCH	32	
SLOT_DURATION	12 seconds	
MIN_ATTESTATION_COMMITTEEE_SIZE	2^7 = 128	The min size of the attestation committee
MAX_ATTESTATION_COMMITTEEE_SIZE	2048	
MAX_SUMMARIES_PER_COMMITTEE	30	
EFFECTIVE_BP_STAKE	10	The max effective amount of ETH a bonded BP needs to have.
BP_VAULT_BOND_ALLOCATION	2	The amount of bond (stake) every vault BP needs to allocate, in ETH.
EFFECTIVE_POOL_STAKE	32	Per eth2 spec

Vault

Name	value	Description
TARGET_COLLATERAL_RATIO	1.5	In percentage, 150% collateral.
VAULT_SIZE	24	Number of BPs in a vault committee

Rewards & Penalties

Name	value	Description
BP_MAX_CDT_DEBT	31110 epochs = ~ 2 weeks	A BP will usually earn CDT for his work, in case he is inactive he will start leaking CDT due to penalties. This is the max debt a BP can incur before being forced exited.
max_liquidation_execution_duration	221 epochs = ~ 1 day	A liquidation request will include an epoch by which the liquidation needs to

		happen. The max amount of peoch is defined by this param.

ETH1

Name	value	Description
STATE_COMMIT_DISPUTE_DURATION	~ 48H	The max time that a committed pools state root can be disputed on, after this period it’s considered finalized
COMMITTMENT_COMMITTEE_PERSISTENCE	24H	The amount of time the commitment committee will be eligible to commit the pools chain state root.