Goal of the post

: to gather feedback from the community on our Ethereum delegated staking protocol and associated risks.

Protocol Summary:

a non-custodial, delegated staking protocol where the stakers generate the validator keys and retain them. The validator keys are shared with the node operators after encryption with their public keys. Upon the creation of a validator node, the staker receives both a T-NFT and a B-NFT representing the stake; (liquid) staking derivatives. The T-NFT is transferable for liquidity. The B-NFT is non-transferable and soul-bound to the staker. The B-NFT represents the ownership of the validator keys and inherits the responsibility to exit the node when necessary. In exchange, the B-NFT holder earns higher yield than the T-NFT holder.

[

스크린샷 2023-02-17 11.58.13

870×736 86.4 KB

](https://ethresear.ch/uploads/default/original/2X/3/35fa341d08b4724b2a39bf9bb81b672209394b30.png)

The protocol aims to be a non-custodial and permission-less staking delegated protocol where the solo stakers generate and retain their validator keys. Anyone can join as node operators and stakers.

Delegated Staking via Auction Mechanism

The protocol uses an auction mechanism to select node operators who will run the validator nodes:

- Step (1):

The node operator places a Bid

in ETH (e.g., 0.01 ETH) and uploads their public key for the opportunity to run the validator node. This auction revenue is shared between protocol participants.

- Step (2):

The staker stakes their 32 ETH by submitting their validator key encrypted by the public key of the winning node operator with the highest bid.

- Step (3):

The node operator receives the encrypted validator key, decrypts it with their private key, then runs the validator node.

A few points:

- Either the staker or the node operator can exit the validator node using the validator key. Yes, both can sign the slashable messages.
- We provide a desktop app for key generation and encryption/decryption with ECIES. For forward secrecy, the node operator generates many keys and uses a different key for encryption with each individual validator. In the future, we plan to leverage EIP-5630 and / or sharded keys with Distributed Validator Technology (DVT).
- For cost efficiency, we use off-chain IPFS storage for key exchange. Node operators store their public keys on IPFS. Stakers store their encrypted validator keys on IPFS and upload this location hash on-chain for the node operator to locate, obtain, and decrypt the keys.

NFTs for Ownership/Responsibility Representation

When the deposit to the beacon chain is made:

- a new withdrawal safe contract is created and used for the withdrawal credential. The partially or fully withdrawn funds will be directed to the contract.
- the staker receives a transferable T-NFT and non-transferable B-NFT that represent claims of 30 ETH and 2 ETH, respectively, from the 32 staked ETH.
- The T-NFT can be traded for liquidity. That is, the staker can liquify 93.75% (= 30/32) of their staking position.
- The B-NFT cannot be traded; it represents ownership of the validator keys. This NFT acts as both insurance against slashing and a commitment to exit the validator node when either the T-NFT holder requests or the node malfunctions.

In exchange for the additional responsibility, the B-NFT holder earns higher yield than the T-NFT and eETH holders.

Mechanism to exit the validator node

In our protocol, only the B-NFT holder or the node operator can exit the validator node using the validator key. In the case of a slashing event, the B-NFT's 2 ETH serves as a deductible for slashing insurance.

The T-NFT holder can send an exit request to the corresponding B-NFT holder. Upon the request, it records the timestamp and begins a timer emitting an event to which the corresponding B-NFT holder must listen. If the timer expires and the validator has not been exited, then the B-NFT holder's claim is reduced progressively from 2 ETH down to 1 ETH. The node operator receives a reward upon exit of the expired validator in order to incentivize them to exit the validator in case the B-NFT holder is unwilling or unable to do so. In order to prevent the case where none of the node operator and the B-NFT holder exits the node, the staking rewards to them decrease after the timer expires.

In the case of a slashing event, we arrange an insurance to cover the loss of the T-NFT holder. The B-NFT's 0.5 ETH is used to pay the deductible for the insurance which covers the loss of the T-NFT holder up to 6 ETH. The payout to the B-NFT holder decreases up to 1 ETH.

Once the node exits, the payouts for the principal to the T-NFT and B-NFT holders are:

- Payout to the B-NFT holder = 2 - (Expense for Deductible) - (Progressive Slashing up to 0.5)
- Payout to the T-NFT holder = (32 - Slashing Penalties) + (Insurance Payout) - (Payout to the B-NFT holder)

Slashing Penalties

Expense for the Deductible

Insurance Payout

Payout to the B-NFT holder

Payout to the T-NFT holder

0

0

0

2

30

0.5

0

0

1.5

30

0.5

0.5

0

1.5

30

1

0.5

0.5

1.5

30

…

…

…

1.5

30

6

…

5.5

<1.5

30

6.5

…

5.5

1.0

30

7

…

5.5

1.0

29.5

…

…

5.5

1.0

…

16

0.5

5.5

1.0

20.5

Permission-less withdrawals

The protocol provides permission-less withdrawals. Each validator node is associated with an individual withdrawal safe contract to which the partially or fully withdrawn funds are directed. For partial withdrawals, any individual can trigger the distribution of the skimmed rewards as long as the contract's balance is below 8 ETH. If the balance is above 8 ETH, the B-NFT holder must exit the node and fully withdraw the funds. For full withdrawals, the protocol relies on Oracle data or the explicit agreement between the interested parties on their payouts.

Fractional Staking and Liquid Staking Derivative (eETH)

The protocol supports fractional staking with its Liquid Staking Derivative, eETH, which allows users with less than 32 ETH to participate in staking by depositing their ETH and minting eETH. Anyone with 2 ETH can participate in the auction as a staker with an additional 30 ETH from the liquidity pool. The minted B-NFT goes to the person who brought 2 ETH and generated the validator keys, while the minted T-NFT goes to the protocol contract. These B-NFT accumulators enjoy the higher yields while performing their duties.

Thanks for reading through it. Any questions/feedbacks on our protocol and associated risks are appreciated!