In the last few months, we have seen interest and participation in ETH staking grow significantly among different segments of users. [ETH staking ratio: 22.89%]

Everyone from home and retail stakers to large investors seem to be following the positive narrative surrounding the possible formation of Ethereum ETFs and the coming EIPs, like 4844, that will help scale the network to make transactions faster and cheaper than ever before.

However, the fact hasn't changed that running an Ethereum validator requires a 32 ETH deposit, and with the price of 1 ETH hovering around $1,600, doing so remains elusive for many average users and retail stakers.

Additionally, running a solo staking node isn't necessarily an easy task for those not technically inclined, and many that have 32 ETH simply aren't comfortable taking on the risks associated with running a node at home.

We believe it is this perfect storm of staking challenges that has pushed many users toward more centralized staking services and Liquid Staking (LSD) protocols, and tilted the balance of Ethereum from more decentralized to more centralized.

Liquid Staking protocols offer an easy way for users with varying budgets, even very small ones, to participate in staking by running 'pooled' validators, where the funding is crowdsourced. Additionally, very little technical ability is required, opening the door to ETH staking up to just about everyone.

Enter the issue of centralization

and the risks it poses to Ethereum.

When it comes to liquid staking providers, Lido is currently the biggest, dominating the space by a significant margin and controlling almost 33% of the total ETH staked. This staked ETH powers large pooled validators that run on a rather limited set of operator nodes that are curated and vetted by the Lido DAO.

Now, you may be asking, "Why is this a problem?"

It's important not to forget the reason why staked ETH exists. It is the heart of Ethereum's Proof of Stake consensus mechanism and is responsible for securing the Ethereum blockchain. It does this via validators that each require a separate deposit of 32 ETH. These validators come to consensus every 6 minutes or so, agreeing on the blockchain's last state and verifying the transactions included in the last block.

The theory securing Ethereum is that 32 ETH is enough collateral "at stake" for validators to act honestly and in the best interests of the blockchain instead of maliciously or in a way that could harm the network.

To enforce this, the blockchain rewards validators that perform their duties honestly and on time, and penalizes validators that don't.

If a validator is offline when a request comes to perform a duty (a relatively minor infraction), the Beacon Chain reacts by deducting a small amount of ETH from its balance. However, if a validator behaves dishonestly or maliciously, in an attempt to steal funds or rewrite the blockchain's history, it will be "slashed" and could lose its entire ETH balance.

Centralized staking providers that control a significant portion of the total staked ETH pose a significant risk, as they could prevent the blockchain from finalizing. This may not be an intentional act on their part, and instead be the result of an attacker compromising the centralized staking provider's network.

However, it is important to note that regardless of the reason, if the blockchain cannot be finalized, the potential for negative consequences are high. Taking this one step further, a majority could potentially rewrite the history of the blockchain, in a coordinated 51% attack, with the intent of stealing funds and taking control of the network.

Additionally, censorship risks tend to surface when the blockchain is more centralized, while a wide, decentralized validator base helps keep block censorship to a minimum.

Turning risk into opportunity

For forward-thinkers like the SafeStake team, these challenges are opening up a world of possibilities that have the potential to improve not only ETH staking, but the Ethereum ecosystem as whole.

SafeStake operates as a highly decentralized DVT infra and protocol on a permissionless network of decentralized nodes, offering many benefits. Stakers can utilize SafeStake to maximize their validator rewards and minimize their risks, while the Ethereum blockchain enjoys a major upgrade to its defenses against the risks that centralization poses.

An added layer of decentralization for blockchain health

As Ethereum centralization concerns continue to mount, SafeStake's DVT solution and permissionless network of node operators offers a layer of decentralization that can protect the blockchain and its users, while still allowing large staking

services to control large amounts of staked ETH and validators.

With SafeStake, validators that currently run on a single node controlled by a single operator can be securely distributed to run on multiple nodes, each of which is controlled by an independent operator. Four operators make up a “committee” that manages the validator by consensus. The network is “permissionless” because operators are free to join and leave the SafeStake network without permission.

It is SafeStake’s permissionless network of independent, decentralized operators, with varied hardware configurations and geographic locations, that would make a coordinated attack on the Ethereum blockchain next to impossible. For large staking providers, SafeStake can function as a harm reduction measure, and it would no longer matter how much of the share of staked ETH a staking provider controlled. If they implement SafeStake for decentralization, their potential harm is greatly reduced.

How SafeStake works

SafeStake distributes the operations of an Ethereum validator by splitting the validator private key into multiple ‘key shares.’ These shares are then distributed to the operators in the committee that will manage the validator on behalf of the staker. For stakers, this offers a turnkey solution, enhanced private key security, and fault tolerance that keeps the validator online, maximizing staking rewards.

The SafeStake protocol runs on a set of smart contracts, written in Solidity, that handle validator and operator registration and cancellation, key share restoration, and fee management.

The SafeStake design leverages BLS threshold signatures via a non-interactive threshold signature scheme, Distributed Key Generation (DKG), and runs on the Lighthouse consensus client.

Instead of iBFT (Istanbul Byzantine Fault Tolerance) or its cousin qBFT, SafeStake utilizes Hotstuff (a high-performance BFT consensus library) to manage the signature operations of the operator committee to maintain and operate an Ethereum validator by consensus. HotStuff provides high levels of security, performance, and reliability, and significantly reduces slashing risks for validators running on SafeStake.

SafeStake also implements Multi-Party Computation (MPC) and BLS (signing) protocols on top of HotStuff to allow the operator committee to aggregate a signature that is equivalent to the original, for the purpose of signing data and proposing blocks on the Beacon chain. The original signature is never recreated for any purpose and the private key is no longer needed to run the validator, offering the ultimate security.

[

Banner Image _(1200 x 630 px)-2

1200×630 84.7 KB

](https://ethresear.ch/uploads/default/original/2X/a/a75871c4c63c8ec213ed6e4084162dbc95a69cb0.jpeg)

Distributed Key Generation (DKG)

Here, it is important to note that the DKG protocol only becomes necessary in SafeStake Stage 2, when ‘mini-pools’ are created for the purpose of running ‘pooled’ validators. In this scenario, multiple ETH depositors are involved, and no party should ever have custody or knowledge of the private key, whether it be a depositor or operator.

To handle this, when a mini-pool is initiated via 4 ETH deposit from the “initiator,” SafeStake’s built-in DKG protocol activates automatically, allowing the operator committee to seamlessly and securely generate the private key for the new validator. No actions are required from the operators, and no party (including SafeStake) ever has knowledge of the private key or the secret used to distribute the shares.

Furthermore, to avoid potential points of failure, SafeStake implements a network of decentralized oracles.

Architecture

SafeStake Stage 1

In Stage 1, the protocol supports importing validators created by single 32 ETH deposits. Users can import their validator quickly and easily by dragging-and-dropping the validator’s keystore file into our browser-based Dapp and choosing four operators for the committee.

The Dapp securely splits the private key on the client side and sends one share to each operator in the committee. Now, the operator committee manages the validator on behalf of the staker, signing data and proposing blocks on the Beacon Chain, while the staker pays the operators a monthly service fee in DVT tokens for their services.

SafeStake Stage 2 - Liquid Staking Pool

SafeStake's liquid staking pool is made possible by special operators, known as "initiators," who will create mini-pools by making an initial 4 ETH deposit. The remaining 28 ETH required for a new validator will be gathered from the liquid staking pool from multiple deposits each as low as 0.1 ETH.

In Stage 2, a new validator will be spun-up each time the staking pool reaches 28 ETH, and providing an "initiator'' operator has made an initial 4 ETH deposit. Everyone contributing ETH to run the pooled validator will earn staking rewards in proportion to their deposit, with a slightly larger portion going to the initiator, as they are assuming all slashing risks for the validator.

Now, let's take a deeper dive into how SafeStake Stage 2 works:

- An operator on the SafeStake network, called an "initiator," deposits 4 ETH Stakers who use SafeStake to earn staking rewards with only 4 ETH and selects three other operators to manage the validator with them as a committee. This setup is known as a 'mini-pool.'
- The protocol calls an assembly function in the contract to assemble a group of user participants in the mini-pool.
- Then, participants (operators) in the mini-pool go through a Distributed Key Generation (DKG) ceremony that generates the validator private key. The key is securely split and encrypted into four key shares, and the shares are distributed to the operators in the committee.The Validator key is never reconstructed by the participants, as tthe protocol generates the key using Multi-Party Computation (MPC), ensuring no single party can discover the shared secret and recreate the key.
- Now, the operator committee runs the Threshold Signature scheme, and the initiator completes the 4 ETH deposit via the mini-pool contract that is created.
- The mini-pool contract enters the SafeStake queue to receive the additional 28 ETH needed to create the validator.
- Once these 28 ETH are collected from the pool, the validator enters the Beacon Chain queue to become active on the network.

Once a validator is active on SafeStake, the robust architecture creates the most fault-tolerant, secure, and decentralized environment for validators, maximizing staking rewards and contributing to the overall health and decentralization of the Ethereum blockchain.

Of course, the SafeStake network and the benefits it provides rely heavily on the independent, decentralized network of operators that provide much of the necessary hardware and software that power the network. Therefore, SafeStake operators must agree to be held accountable to the following standards, or risk being forcibly removed from the network:

1. Stay online and meet minimum performance criteria to be designated either a 'Verified' or 'Unverified' operator.

A 'Verified' operator has been vetted by the SafeStake DAO, while 'Unverified' operators have not undergone vetting. Verified operators will likely be held to higher standards than Unverified operators, with more information to follow in future communications.

1. Remain current with the most recent Beacon Chain blocks and execute all tasks assigned to the committee.
2. Randomly be chosen as a coordinator to formulate tasks for the committee based on the duties of validator related to Beacon Chain responsibilities.
3. Refrain from suggesting tasks or engaging in behavior that could result in a penalty for the validator.

Conclusion

SafeStake aims to make ETH staking accessible to everyone, not only those with 32 ETH. Soon, users will be able to stake much smaller amounts of ETH via SafeStake to earn rewards for securing the blockchain.

For stakers of all sizes, SafeStake can help maximize rewards and minimize risks, while enhancing validator private key security.

For users of Ethereum and the blockchain itself, SafeStake offers protection from the risks centralization has already created, like censorship, and the potential risks that loom, like coordinated attacks, theft of funds, and putting control of the network in the hands of a few instead of many.

At SafeStake, we look forward to a bright and decentralized future for Ethereum and its users.