Open SSV Network

Flexible, decentralized, and robust Ethereum staking infrastructure protocol

Draft v0.2

Abstract

SSV.network is a decentralized ETH staking network enabling the distributed operation of an Ethereum validator. The network allows both users and operators to diversify staking risks, optimize performance, and promote decentralization across the Ethereum consensus layer. Ethereum's new and highly anticipated consensus layer (Ethereum 2.0) transforms the network from traditional Proof of Work mining to Proof of Stake and validators, enabling a wider audience of contributors to help secure the network. While the barriers to securing Ethereum have been lowered, it is still technically challenging to run a validator while ensuring liveness and safety. In addition, strict protocol rules have limited validator configuration options, leading to the centralization of components and driving network-wide disruptions. SSV.network aims to solve these limitations by splitting and operating an Ethereum validator key amongst non-trusting operators. SSV uses a secure MPC threshold scheme with a consensus layer that governs the network. Operators work together to recreate a validator key for signing; each operator has one portion of the validator key (KeyShare), a predefined threshold of KeyShares is required to create a beacon chain signature, and no single operator can perform validator duties on their own. Additionally, the original validator key can be stored securely offline - a game changer for ETH staking private key security. SSV users will pay a fee to join the network, split between the operators and the network DAO. Operators will set their own service costs and stakers will benefit from lowered fees due to open market competition between service providers.

SSV.network presents a win-win-win for stakers, operators, and the overall health of Ethereum for both the security and robustness delivered across the entire network.

Summary

Ethereum staking is a paramount advancement in the Ethereum ecosystem, part of Ethereum's move to an upgraded Proof of Stake (PoS) consensus mechanism and sharding, known as Eth2. Staking on Ethereum is different from other staking blockchains as every network operator, known as a validator (32 ETH BLS key) is required to be online 24/7 to perform network duties and unique network penalties (slashing) exist to deter malicious behaviors.

The technical requirements of an Ethereum validator resulted in adopted infrastructure similar in design between all stakers, from the smallest at-home validator to the biggest centralized exchange. At its core, a validator client (which can hold several different validator keys) is connected to one or more beacon chain nodes. The emphasis is on having a single instance of a validator key running on a single validator client otherwise, the operator can cause self-slashing by mistake (see staked.us post mortem).

Running a single validator instance is a major limiting factor in creating a robust, secure, and performant staking infrastructure. A potential single point of failure that can lead to disastrous consequences for individual stakers and the network's health as a whole.

We propose a network of Secret-Shared-Validator (SSV) operators, a unique technology that enables the distributed control and operation of an Ethereum validator. SSV uses a secure multi-party computation (MPC) threshold scheme with a consensus layer on top, that governs the network. Its core strength is in its robustness and fault tolerance which leads the way for an open network of staking operators to run validators in a decentralized and trustless way.

Vision

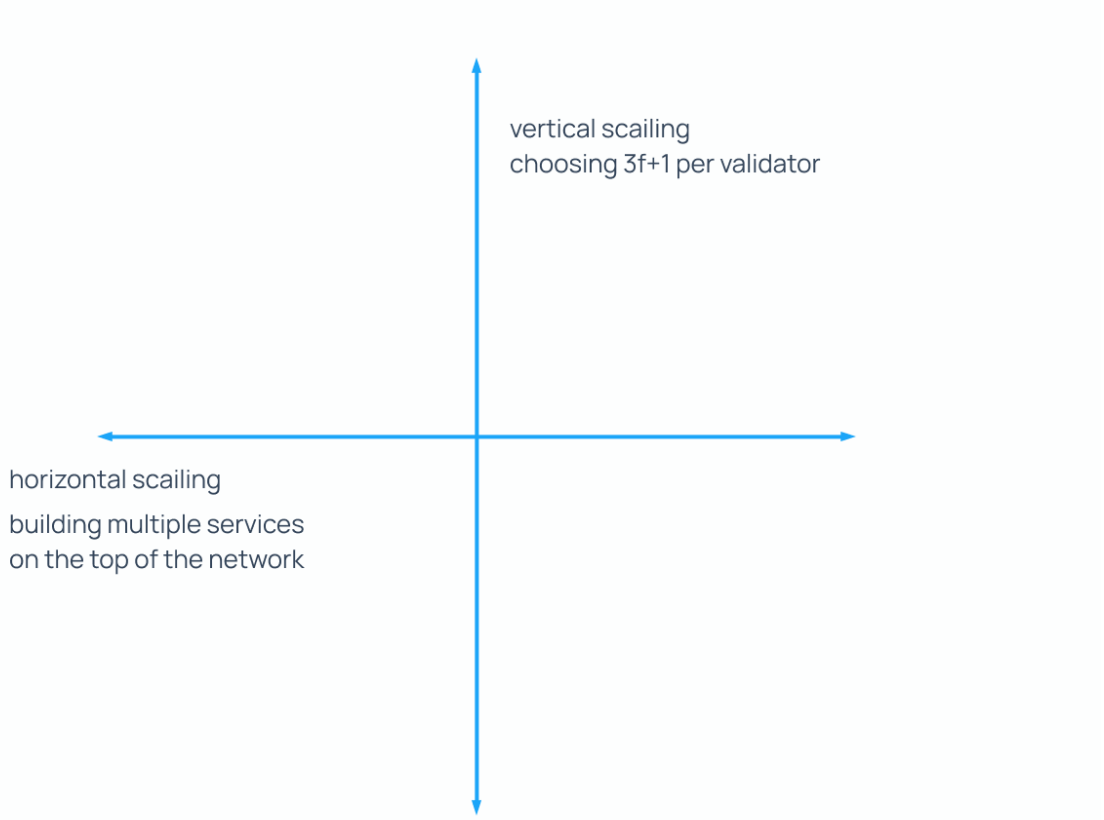
The ultimate expression of an open SSV network will offer the power and flexibility of a common cloud provider (like AWS/Azure) combined with the decentralization and robustness of a decentralized consensus protocol.

SSV.network will afford any staker and staking service provider with fast and secure distribution of a validator key between various Ethereum clients, cloud providers, and geolocations. The network introduces a radical change to existing staking practices, removing the requirement of keeping validator private keys online 24/7. With an SSV implementation, validator keys are securely stored offline while only the 'KeyShares' are distributed between operators and kept online. Cold storage offers superior security to end user's validator keys.

Professional SSV operators will be assessed and judged by a community of stakeholders, resulting in a decentralized and transparent network scoring of their quality, experience, and service. An SSV operator could offer a variety of nodes across different geolocations, infrastructure setups (including cloud options), and software versions (beacon node implementations for example) to maximize decentralization and reduce any single points of failure.

Using the network will be open and simple for anyone who wants to run an Ethereum validator; from DIY users all the way to staking pools and big institutional staking services.

Different services can be built by anyone on top of the SSV network by using it as staking infrastructure. This type of horizontal scaling is complemented by vertical scaling, individual stakers choosing multiple operators to run validators.

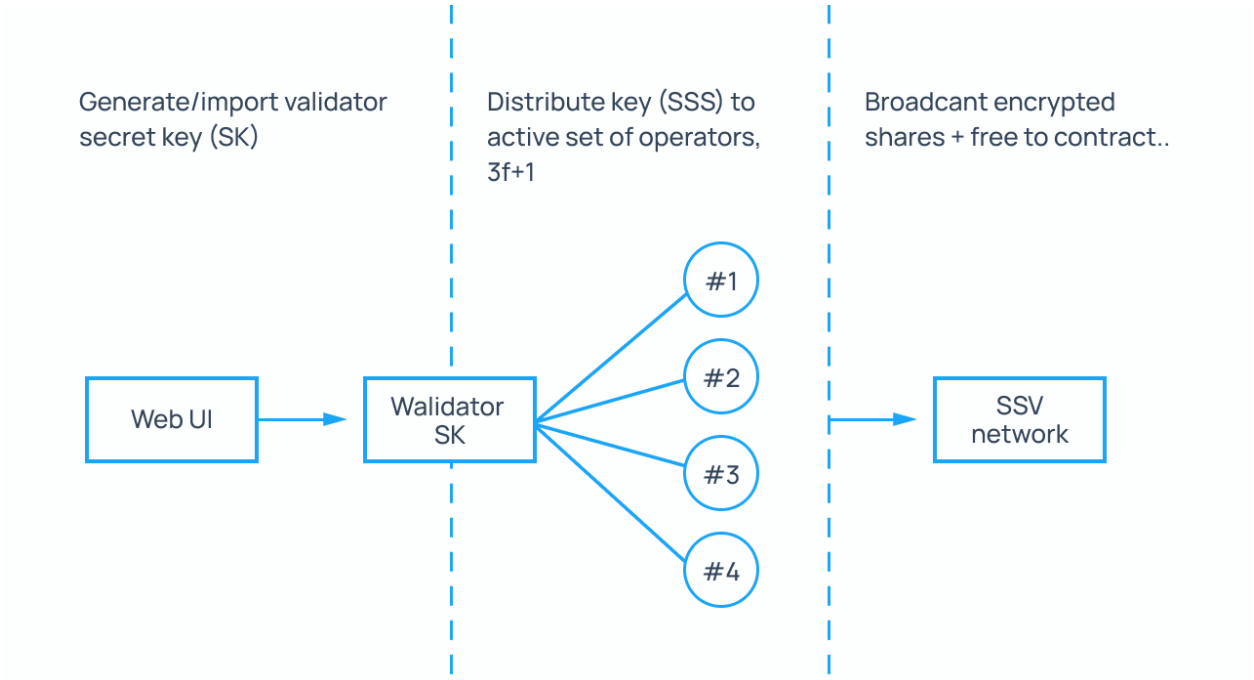


The above is necessary to prevent centralization of power in the hands of few big staking providers as occurred with mining pools in Ethereum's legacy Proof of Work (PoW) chain.

Use Cases

Solo Stakers

A solo staker is a DIY user depositing one or more Ethereum validators (32 ETH). As of now, a DIY user runs their own validator client alongside a beacon and Eth1 node which can be run by a 3rd party.



Instead of running a single validator instance susceptible to technical issues, hacking, and high maintenance costs, with SSV a DIY staker can run their validator in a decentralized manner while still having full control over their validator keys.

A validator key is split into secure KeyShares (via a web app), each KeyShare is encrypted for the specific operator selected and is broadcasted to the Ethereum network. Operators can decrypt and validate the KeyShares to start operating the validator. No single operator ever knows the original private validator key!

From a solo staker's perspective, SSV offers DIY level security with the added benefit of relying on 3rd party operators for optimizing validator performance. An ETH staker's validator key can be stored offline as opposed to existing staking solutions where validator keys must be kept online at all times.

Recommended operator number per validator: 4 or 7

Staking Pool

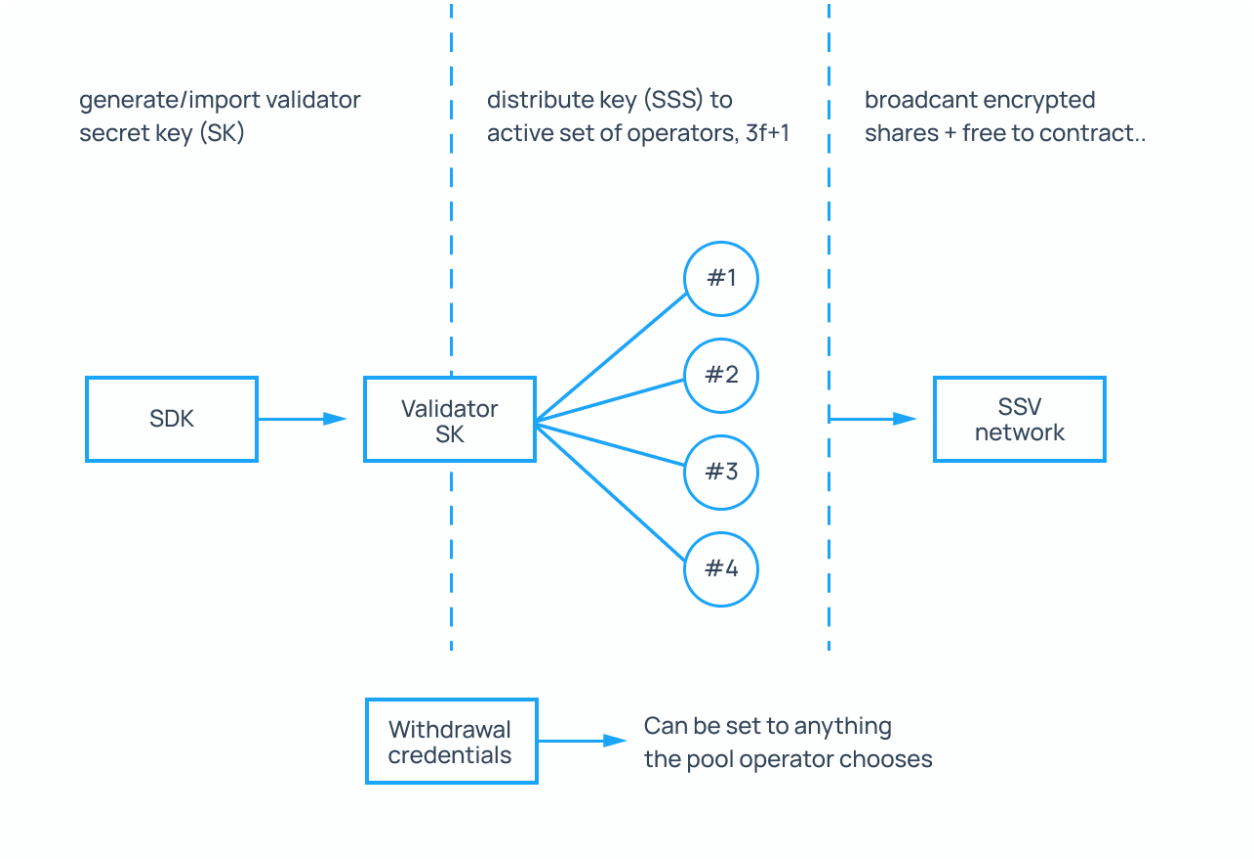
A staking pool is a service that offers the ability to stake a flexible amount of ETH (not in 32 ETH multiples) alongside tokenizing the staked ETH for improved liquidity. Staking pools usually have their withdrawal credentials point to a smart contract while their validator key is run by one or more centralized entities.

Existing staking pools (Rocketpool, Lido, Stakewise) generally aggregate users' ETH into batches of 32 ETH and assign it to external network operators. Operators in turn activate and manage the 32 ETH pool validator key on behalf of the stakers.

With an SSV implementation, staking pool providers will be able to split validator keys between their network operators seamlessly. Instead of one operator for each 32 ETH pool, SSV allows many operators for each pool. SSV based pool staking allows for:

- Fault tolerance and decentralization - groups of operators per pool instead of single operator design.
- Superior security practices - validator keys are kept offline, no operator has access to validator keys.
- Customizability - a pool service can pick and choose between operators and optimize for cost and security on behalf of its stakers. Operators can be added and removed with ease.

A staking pool can add the SSV network as an additional infra provider or easily set it as its main provider by programmatically connecting to the network via its smart contracts. No different than how most pools work and operate today.



Recommended operator number per validator: 7 or 10

Staking Providers

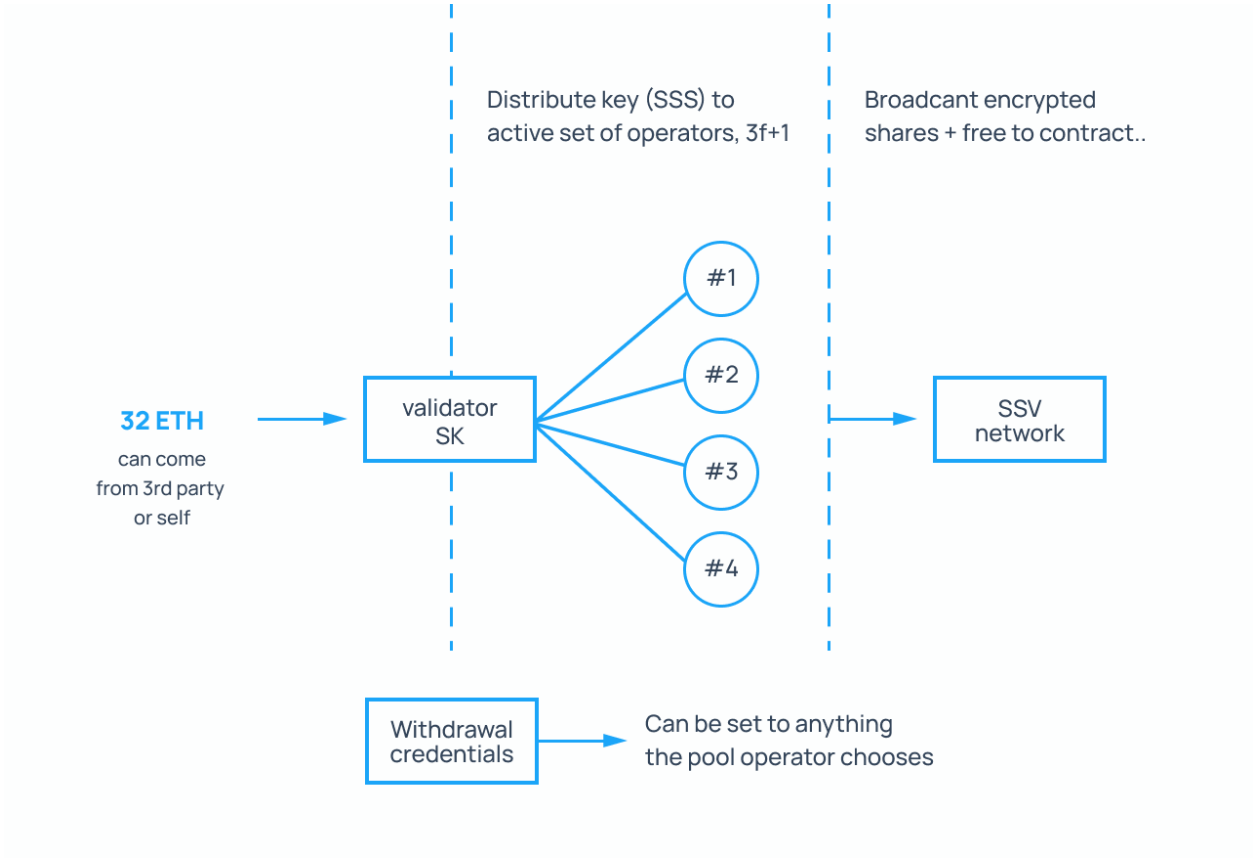
Staking providers are specialized companies that offer end-to-end solutions for staking; some for retail users, some for other staking services, and some for both. Examples range from Stakefish to Coinbase and Kraken.

The main value proposition staking providers offer is an infrastructure that runs the Ethereum staking stack, from Ethereum and beacon nodes to validator clients.

The main benefits SSV can bring to a staking provider are significantly reducing operational risks and costs. As current protocol rules dictate having a single validator instance, any setup is vulnerable to such single points of failure. Staking providers invest heavily to work around that issue in development, devops, IT, and through expensive insurance policies. All

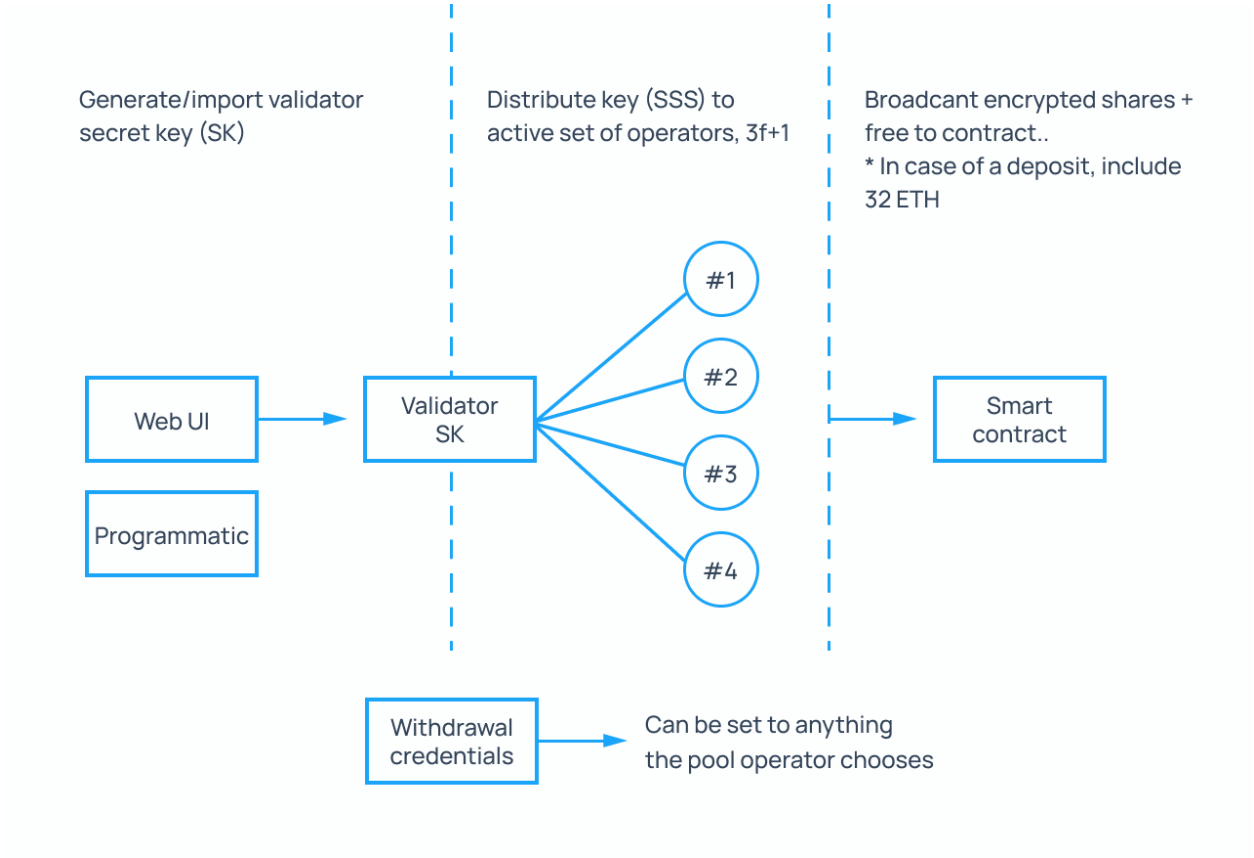
in order to minimize downtime and the risk of slashing. With SSV rather, responsibility is distributed between operators, eliminating this single point of failure and resulting in much lower operational risk and cost.

Staking services can use SSV as part of their backend staking infrastructure or may elect to become an operator in the SSV network.



Recommended operator number per validator: 7 or 10

Distributing a Validator - Technical Overview



All a user has to do is generate a valid Eth2 validator key (pk). With a pk, a user selects a set of valid SSV operators and distributes their KeyShares of the pk (Shamir-Secret-Sharing). Once all operators receive their share, the user broadcasts a tx to the contract that includes a list of operators and fees. This can be done programmatically or via a web UI.

Each operator in the Cluster will receive one KeyShare. Attestations and proposals will be handled by the user's chosen Operator Cluster.

The Network

Overview

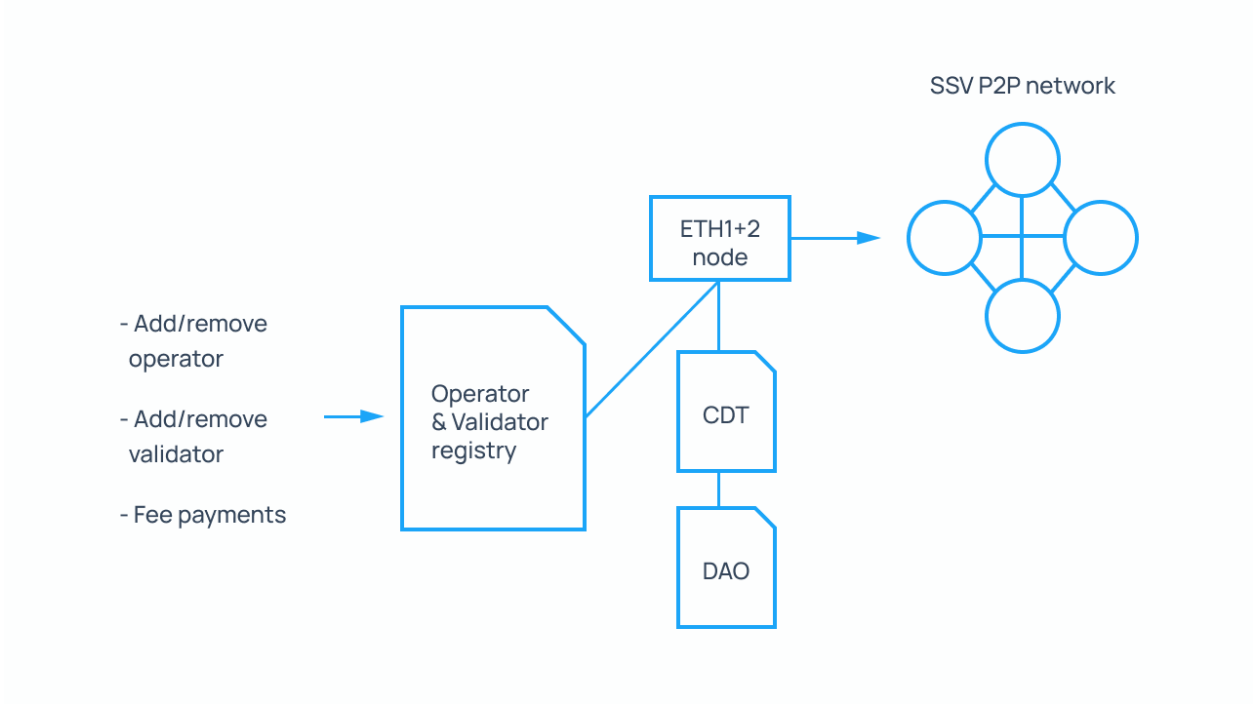
The SSV Network consists of 3 main 'pillars' - Stakers, Operators, and DAO members. Operators and stakers can take on dual roles, both staking ETH and assisting other users to manage their stake. Anyone can act as a DAO member and take a meaningful role in governing the network.

A flourishing ecosystem requires all three components to grow and prosper. Stakers rely on best-in-class operators and operators need to have strong incentives to offer their services to stakers. The protocol as a whole requires a strong DAO to ensure the network remains fully decentralized and benefits all participants equally.

The SSV.network has 2 layers:

- SSV Network
- Management / governance Ethereum contracts layer.

The SSV layer is the execution layer, it reads the current operator list and validator assignments (alongside operator shares) from the Ethereum contracts and operates the validators it's assigned to. The contract layer is the management / governance layer where actions like adding an operator, creating a validator, and paying fees occur.



The network has 3 main actors

- SSV Operators - Usually an LLC which has previous experience running blockchain infra, involved in Ethereum and Eth2 in particular. Looking to increase their offering, reduce infra costs and risks, or a combination of all three. E.g. Blox Staking, Stakefish, Staked.us, etc.
- Stakers
  Any service/user that has an inflow of ETH and makes the 32 ETH deposit. E.g. Blox Staking users, DIY validators, RPL operators, Lido, etc.
- SSV token holders
  The backbone of the network, in charge of network governance and operator ranking.

Give/get table per actor		
	Give	Get
operators	• computing resources • reputation	• revenue (SSV token) • reduced operating risk • reputation
stakers	• fee • staked ETH	• staking infra • reduced dtaking risk • decentralization • ETH rewards
SSV token holders	• community and network value	• protocol decision making • SSV token network usage

DAO & Governance

The DAO is the decision-making component of the SSV network. It gives the SSV token community the power to make crucial decisions that will guide the network. The DAO has the following responsibilities:

- Operator Scoring - SSV operators are scored via a governance decision, 0-100. The score is crucial for users to decide which operators to use; as with any service, the better the operator the more users it will have. A governance decision can also reduce scoring and even revoke an operator.

- Fee - Users choosing operators will need to pay a fee that is split between the staking providers and network DAO. For example, 80% of the fee goes to operators, 20% to the DAO. Each operator can set his own fee, denominated in SSV tokens, such that a user selecting X amount of operators will pay the sum of set fees (example: A user selecting operators O1, O2, O3, O4 with the respective monthly fees 10, 12, 20, 5 will pay 47 SSV tokens per month). (fee market research appendix) This dynamic fee setting approach will make the market adjust and regulate the fee

for running an SSV validator, depending on the number of operators selected. More operators make the validator more distributed at a higher price point. A user could choose to diversify the type of operators to normalize risk/cost ratio, choosing a mix of some first-tier operators (at higher cost) and cheaper operators.

- DAO fees - Fees collected by the DAO will be managed by the DAO, various approaches can be taken. From circulating the collected SSV token to grants all the way to burning.
- Grants - The DAO will decide on grant distribution to different initiatives for and by the community.
- Other decisions - Key decisions requiring a community decision will be passed by the DAO.

The SSV token

The SSV token is a new ERC20 (+ERC223) token created specifically for the open SSV network. All DAO decisions (fee payments, etc.) will be carried out with the token.

The amount of SSV token paid depends on 3 main parameters: # of validators, ETH APR, and ETH price. The higher those 3 parameters, the higher the amount of SSV tokens circulating in the network for fee payment.

Example:

- Total ETH at stake, 10M(post merge)
- SSV network manages 10% of all validators (1M ETH = 31,250 validators)
- SSV network fee is 2% of earned rewards by the validators (most staking services take around 10% currently which leaves an 8% profit gap).
- ETH APR (post merge) is estimated at 25%
- ETH price $4,000

- Total yearly rewards generated: 1M * 25% = 250K ETH ~= $1B
- SSV fees ~= $1B * 2% = $20M

Vote - Replacing CDT with SSV token

SSV token will first be launched as a candidate to replace CDT with a DAO decision. As this transition is significant, it has been designed as a gradual process.

- At SSV token genesis a new token contract will be created with significant technical advancements (full ERC20 + 223 compatibility, lower decimal precision, minting function controlled by the DAO).
- A bridge contract will be created in which CDT holders can deposit CDT and receive the SSV token with a fixed (pre-determined) ratio. The bridge is bi-directional.
- Votes in the DAO are SSV token controlled.
- Various incentivization programs will be created to boost SSV technology adoption (incentivized testnet for example) that enables the earning of SSV tokens.

SSV Network - Application Extensions

The bare bones SSV feature set can be extended using the iBFT consensus layer to include crucial “Applications” that can enhance the network in meaningful ways. Though the list of such applications is endless, we can identify 2 applications of great importance:

- Decentralized validator oracle - information regarding validators is not yet available to the ethereum EVM, this could change in the future though estimates place such op-codes support in the 1-2 years range.
  iBFT can solve this limitation in a secure way by periodically coming to consensus between a committee of operators on various validator parameters (balance, exited, slashed, etc), then broadcasting the result to a dedicated smart contract.

- MEV (or VEV) layer - As Validator Extracted Value (VEV) becomes more prominent (after the merge), SSV can leverage it in an optimized and decentralized way as a network. This will outperform any single operator implementing VEV alone.

Application extensions are an example of ways to extend the SSV network further, any plans for such extensions will be proposed and agreed upon by the SSV token holders.

Network Operators

The SSV.network operators are highly specialized entities that run SSV software. The software contains the SSV protocol implementation and integration to the Ethereum contracts that manage the network.

Responsibilities

An operator has the following responsibilities:

- Promote and strive for an open, transparent, and decentralized Ethereum staking industry.
- Run the latest community version of SSV.
- Communicate authentic uptime and support service level agreement (SLA) to existing and potential users.
    - Target up time is 99% and support SLA is 24H
    - This includes any change in service that can affect network DAO scoring
- Keep secret the validator KeyShares received from users and delete them once service is complete.
- Be transparent with every relevant network decision made.

Economics

Since Beacon Chain genesis a semi-standard cost basis emerged from the various staking services, ranging from 0.1-0.3 ETH/year ($160-$480 at current prices).

- BloxStaking - $180/year (0.061 ETH at time of writing)
- Staked.us - 0.3 ETH
- Stakefish - 0.1 ETH
- Lido 10% of profits (at current 7.5% yearly rewards) - 0.24 ETH

As mentioned above, current staking infrastructure dictates a single operator running a single validator instance. SSV changes this along with the way fees are distributed between operators. An operator running X validators earns P for each validator. X also represents their market share for a particular segment; all other things constant, it also represents the probability of a new staker choosing the service versus another.

In an SSV network the probability of being selected as an operator is Q fold if Q represents the average number of SSV operators per validator, but the rewards are P/Q as well (considering the cost of running a validator on an SSV network is the same).

X*Q*P/Q = X*P - yielding the same economic result for an operator as compared to current staking infrastructure.

Though revenue potential is identical, the operational risk and costs are significantly lower in SSV as slashing and downtime are much less likely to occur when working as a group. Overall, profit for an operator should shoot up significantly. As an example:

In a regular staking network with 1000 validators and 10 operators:

- Operator #1 has 100 validators, representing a 10% market share (which also represents a 1/10 probability of being selected as an operator for a new validator).
- Operator #1 earns $10/year per validator.

An equivalent SSV.network with 1000 validators and 10 operators exists. All validators on the SSV network are operated by 4 operators.

- Since 4 operators are required per validator, the probability of being selected as an operator for a new validator is 1/10*4
- The revenue per operator is 10/4 = $2.5 (considering same costs)
- The revenue probability for an SSV operator is 1000*1/10*4*10/4 = $1,000
- The above is exactly the same revenue the operator would have achieved working alone

Network Stakers

Stakers leverage the SSV.network and its operators to stake their ETH. Stakers can be divided into 2 main groups:

Solo stakers - usually a private person or a group with 32 ETH or more which stake directly on the SSV network. Solo stakers will have the added benefit of cost optimization and complete control over the node setup process.

Staking services - any staking service that integrates SSV as part of its core infrastructure has the choice between being both a staker and an operator, or solely using SSV as a staking infrastructure. A staking service with an SSV offering will usually create and hold validator private keys on behalf of their users. Validator KeyShares will be diverted to the selected Operators in SSV.network. From the perspective of a staking service, there is clear added value in reducing infrastructure overhead. In addition, a 'free market' of staking operators will require expertise for optimal selection (much like running complex cloud operations).

Economics

Stakers are the main revenue source for operators and the DAO itself. Using the network will require payment in the network native token, SSV. As mentioned above, a portion of the fee will be diverted to the DAO treasury and the lion share will be earned by network operators.

The more operators chosen by a stakers, the higher the cost will be. The added value in fault tolerance and decentralization will require the staker to pay more operators accordingly.

For example, operator fee is 10 native tokens/month, the minimal setup of 4 operators will cost 40 tokens/month. 12 operators will require 120 tokens/month.

Appendix - Ethereum Staking Market

The Ethereum staking market is in its infancy, but, considering it is only 6 months old (Dec 2020), it has made great strides.

As of April 2021 there is ~4M ETH at stake (3.4% of circulating supply) across various setups (See preliminary list in the appendix below).

Staking providers can be grouped into:

- Non-Custodial: Staker controls both keys (validator + withdrawal)
- Semi-Custodial: Staker controls the withdrawal key, a service controls the validator key
- Centralized: Staker controls no key, staking service controls both keys.
- Tokenized (Pools): Semi or non-custodial. The stake is tokenized for liquidity.

	non-custodial	semi-custodial	custodial/ centralized	tokenized (pools)
pros	• decentralized • secure	• very easy to setup and run • not technical	• very simple and non-technical • sometimes tokenized	• Defi competible
cons	• more technical • more maintenance • not liquid while stakedd	• less decentralized and secure	• fully centralized	• less decentralized and secure

Comparison between staking providers

Two big events will determine the future of Ethereum staking:

1) The merge: A development milestone in which the Eth1 and Eth2 chains will be merged, terminating PoW and fully securing ethereum with PoS.The merge is set to increase ETH staking rewards as stakers will earn transaction fees as well, how much exactly is still unknown.

2) Enabling withdrawals: From Eth2 genesis until withdrawals are enabled, stakers can't liquidate their staking positions natively. Enabling withdrawals will create a much needed liquidity option for Ethereum staking; as a result, the amount of ETH at stake will increase significantly as price risk (having ETH is locked for staking) will be eliminated.

Appendix - Staking Services List

1. Blox Staking
2. Allnodes
3. Blocfi
4. Celsius
5. Binance
6. Staked
7. Kraken
8. Bitcoin Suisse AG
9. Chorus One
10. Stake.fish
11. BisonTrails
12. Coinbase
13. Cake Defi
14. Blockdaemon
15. Lido
16. MyContainer
17. Stkr
18. C.R.E.A.M
19. Stakingtogether.com
20. Rocket pool
21. StakeWise
22. Staking Facilities
23. Attestant
24. AllYouCanStake
25. Dragon Stake
26. StakedTech
27. P2P.org
28. MIDL.dev
29. Stereum
30. Guara Wallet
31. Condefi
32. Stafi
33. CYBavo
34. Bitfrost
35. MyContainer
36. SharedStake

37. Figment
38. Codefi