DVT solution for ETHx

by Stader

Litepaper

Table of Contents

1. Executive summary
2. Introduction
3. The current state of ETH staking ecosystem
4. Solution: Stader’s ETHx
5. DVT explained
    - 5A. How DVT works
    - 5B. Benefits of DVT
    - 5C. Challenges with DVT
6. Stader’s proposed DVT solution
    - 6A. Added safety for staked funds
    - 6B. Reduced security collateral
    - 6C. Better returns for node operators
    - 6D. Current state of implementation
7. Stader’s DVT pilot
8. DVT pilot insights
9. Appendix
10. Conclusion

| 1

Executive Summary

Staking on Ethereum is critical to the integrity of the consensus mechanism and credible neutrality of the network.

The Ethereum network has $40bn worth of staked ETH which is ~20% of the overall market cap of ~$200bn. While the absolute Ethereum securing the network is high, there are several challenges associated with staking on Ethereum:

- High concentration of stake among a few entities with ~50% stake with 4 entities
- High capital requirements for spinning up permissionless validators - currently the lowest at 4 ETH with Stader's ETHx
- Potentially high network costs for achieving very good performance levels

One way to solve the problem of high concentration with fewer entities is to bring in more and more permissionless NOs into the Ethereum staking ecosystem. With Stader's ETHx, the entry for permissionless NOs becomes easier as the bond amount is reduced to 4 ETH per validator.

We believe Distributed Validator Technology could prove to be a beneficial solution for solving these challenges further. Its built-in fault tolerance allows the validators to operate even if some nodes are down, making it a more secure setup to run a validator. This would mean that higher performance levels could be achieved by NOs. And since the risks of slashing & penalties are lower, the bonds could be further reduced by ~50% vis-a-vis 4 ETH for permissionless NOs. As participation becomes easier for permissionless NOs and more beneficial for both NOs and stakers due to better performance and lower risks, Ethereum would move towards a higher degree of decentralization.

Stader plans to leverage DVT into its ETHx offering. Stader will have a DVT pool which will have the following characteristics:

- Cluster size of 4 & 7: Each validator will be run by a group of either 4 or 7 node operators. This setup will allow the validator to perform its duties even if 1 or 2 of the nodes are offline/unavailable respectively.
- Lower bond of ~2 ETH: Participation for node operators will be easier with lower bond requirements of as low as 2 ETH.
- Higher performance and security for stakers: With DVT, the risks of the validator being offline or getting slashed are reduced. Also, the chances of NOs stealing MEV are reduced significantly.

In our pilots done with DVT clusters, attestations for size 4 and size 7 clusters were 99.1% and 99.1% respectively vis-a-vis 97% for solo-staked node. Also, proposals were at 100% for both size 4 and size 7 clusters.

| 2

Introduction

Ethereum staking is an important aspect of the network as it defines the resilience of the network. A higher number of node operators leads to better decentralization and better network security. The staking ecosystem is growing significantly and currently stands at about $40 bn. Despite staked ETH being about 20% of the overall market cap, there are several challenges with regard to decentralization.

Permissionless NOs play an important role in decentralizing Ethereum. A higher number of permissionless node operators leads to better censorship resistance. So, it is important to reduce barriers to entry for permissionless NOs to join the network.

With Stader's ETHx, we are taking a step in this direction, making it easier for permissionless NOs to join the network with ~80% lower capital vis-a-vis solo staking. With thorough analysis, risk assessments, and simulations, we have been able to bring down the bond amount for NOs to 4 ETH. As part of ETHx, we also ensure that the capital efficiency is higher and the rewards generated for NOs are better than anywhere else in the staking ecosystem.

Even with ETHx having lower bonds and high rewards for NOs, at Stader, we believe that there could be further optimizations that would make it easier and more rewarding for NOs to join Ethereum staking. At Stader, we're excited to leverage Distributed Validator Technology (DVT), a solution designed to enhance Ethereum's resilience and tackle crucial challenges
In this lite paper, we will discuss DVT, its importance, and how both ETHx stakers and node operators can benefit from it.

But before that, let us dive into some of the challenges/issues of Ethereum staking in more detail.

| 3

The current state of the ETH staking ecosystem

The Ethereum network has $40B worth of staked ETH. However, there still are challenges associated with staking on Ethereum:

1. Single-point failure risk

With individual node operators running a validator, if there is any issue with the machine, the validator goes offline and faces penalties.

Any malicious activity done by the node operator (like double signing or double proposal), can lead to the slashing of validators, putting the staked ETH at risk.

2. Capital requirements

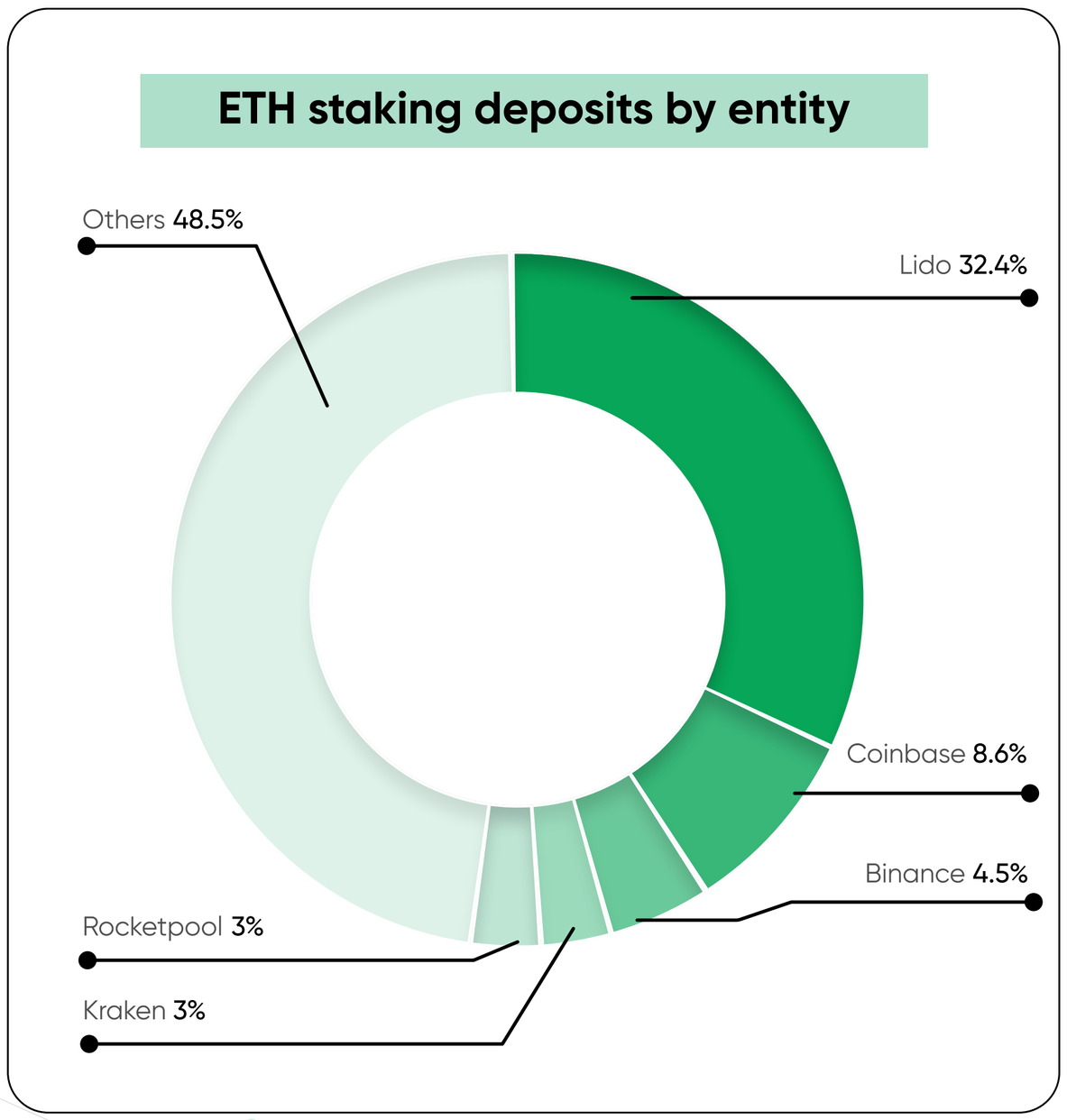
One of the critical challenges permissionless node operators face is a high bond requirement that isn't capital efficient. Along with a barrier to entry, it also creates scenarios where operators earn less than the optimal rewards.

The lowest entry point now is at 4 ETH provided by Stader's ETHx. This is still high and prohibitive for smaller operators.

3. Decentralization

The ideal scenario for Ethereum is to have as many independently operated validators as possible.

However, a few staking providers have become very popular and account for a substantial portion of the total staked ETH on the network. More than 50% of the entire staked ETH volume is still with just 5 entities as described below.



| 4

Solution: Stader's ETHx

ETHx offers the lowest entry point to run a node with only 4 ETH + 0.4 ETH worth of SD bonding requirement. Reducing capital barriers considerably allows for many operators to join Ethereum staking.

More details are available in the **ETHx lite paper.** The liquid staking solution can be checked out on the **ETHx dApp.**

ETHx 2 month round-up

Node operators	Validators	Node operator bond
140	**550+**	**$4.9M**

Despite ETHx's advantages, there are several other challenges that need to be addressed like reducing single-point failure risks, lowering capital entry barriers further, etc. This would in turn encourage more operators to join Ethereum staking and help in further decentralizing the network.

We believe DVT will play a crucial role in solving these issues. Let's understand DVT in more detail.

| 5

DVT explained

Distributed validator technology (DVT) is a primitive that improves validator security and resiliency. A validator key, unique for every validator, is distributed in parts called key shares and given to a group of node operators. Now, this group of NOs, collectively called a cluster, will perform all the duties of the validator like block proposals, attestations, etc. This way, the responsibility of each validator is distributed across the entire cluster instead of residing with just one node. In case any node in a cluster cannot perform its duties, the validator's duties are still performed with the help of other NOs in the cluster.

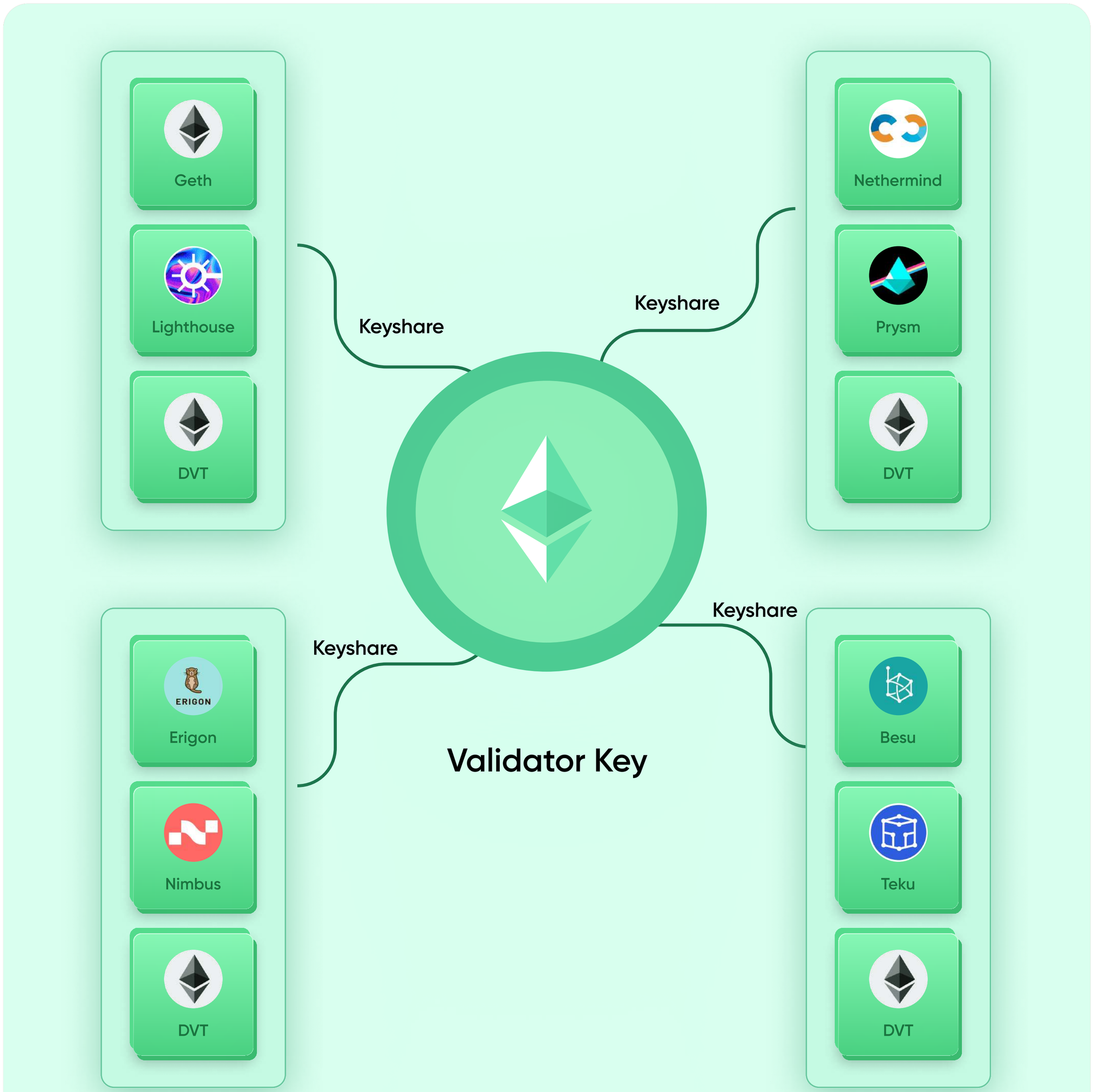


image: www.ethereum.org/en/staking/dvt

Benefits of DVT

Distributed validators are fault-tolerant and will continue running even if some nodes go down. So, the cluster is resilient even if some nodes are malicious or offline.

Cluster sizes can be defined by using the formula 3n+1, where n is the number of faulty nodes the cluster can tolerate.

So, for n=1, the cluster will be formed of [(3*1)+1] = 4 nodes. There can be 1 faulty or malicious node and at least 3 nodes must be online to perform the duties of the validator

Risks & challenges with DVT

1. In a completely permissionless DVT cluster, if a single entity controls the threshold number of key shares, it gains the influence to represent the validator. This situation could potentially lead to slashable offenses, risking stakers' ETH.

2. MEV theft: In a permissionless setup, although difficult, a cluster can steal the MEV of the validators it is running. So, the EL rewards are susceptible to misappropriation.

Given this information, Stader has come up with a solution that leverages the benefits of DVT and addresses its challenges.

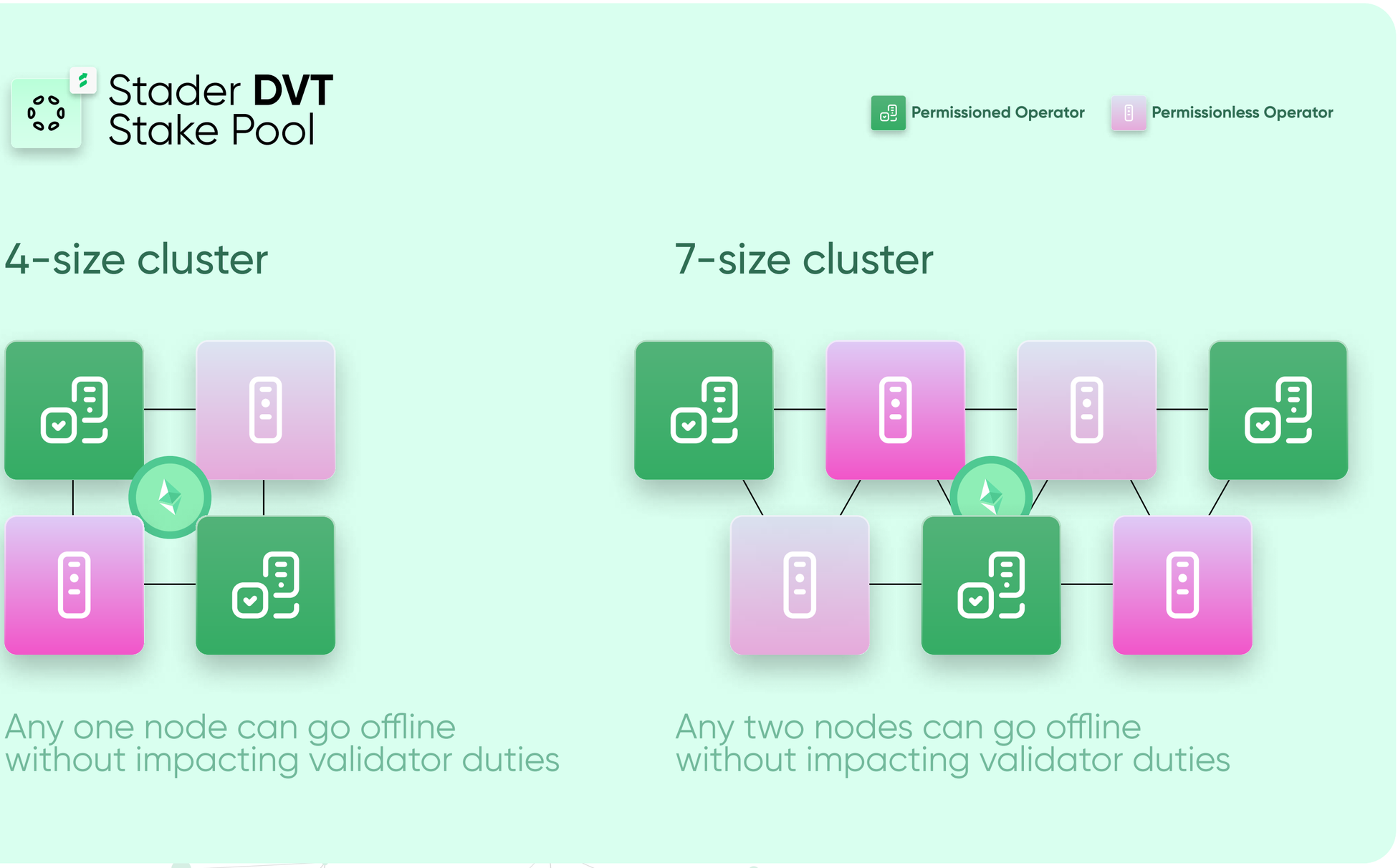
Stader's proposed DVT solution

Stader proposes that in ETHx, along with permissionless and permissioned staking pools, we have a 3rd pool that runs validators on the DVT cluster. Each cluster of this 3rd DVT pool will have the following properties:

- Each validator key will be split into a 4-size or 7-size cluster where up to 1 or 2 nodes respectively can be offline without impacting validator duties.

- Each cluster comprises disparate parties, some KYC'ed and the rest permissionless.
  - 2 permissionless node operators in the case of a 4-size cluster and 4 permissionless node operators in a 7-size cluster. Anyone can become a permissionless node operator.
  - 2 different permissioned node operators in a 4-size cluster & 3 different permissioned node operators in a 7-size cluster. Each permissioned operator is KYC-ed and DAO approved after due diligence.

- The above setup will help ensure that all the influence does not reside with a single entity, as at least 3 operating entities in case of 4-size & 5 operating entities in case of 7-size have to come together to act maliciously.



Added safety for staked funds

1. Validator ownership risk

a. With only 2 permissionless operators in a cluster and 3 operators required to reach a consensus in a 4-size cluster, even if a single entity owns all the permissionless operators, a slashable offense or MEV misappropriation cannot happen. Similar logic applies for a 7-size cluster.

b. By similar logic, even the permissioned operators cannot do a slashable offense or MEV appropriation.

2. Single-point failure

Since there is fault tolerance in both 4-size & 7-size clusters, the chances of a validator going offline reduce drastically. If a solo node has an uptime of 95%, a cluster of 4 with the nodes having the same performance will have an uptime of 98.56% as shown below. This is a significant improvement. With similar computations, the uptime for a cluster of 7 nodes will be ~99.5%.

Detailed calculation is available in **Appendix**

3. MEV theft

a. Any single node operator of the cluster will not control the withdrawal and EL rewards addresses. So, individual operators cannot steal MEV.

b. Even if permissionless operators decide to collude and change the address, they will not be able to do so as they will not be able to reach a consensus due to lack of majority.

Reduced security collateral

Since the risk of slashing and penalties is almost negligible in DVT, we plan to also pass on the benefits to the Permissionless node operators.

We have defined a bond amount of 2 ETH per validator in a combination of ETH and SD.

This will reduce the barrier to entry into the ecosystem even further for home stakers and add to the decentralization of the Ethereum ecosystem.

Detailed analysis is provided in the **Simulation** section.

Better returns for node operators

With the benefits of DVT and the reduced bond amount, NO rewards will be ~47% and 9% higher vis-a-vis solo staking and ETHx respectively for a size 4 cluster. Similarly, for a size 7 cluster, NO rewards will be ~54% and ~14% higher vis-a-vis solo staking and ETHx respectively.

Below is the comparison of returns for a permissionless node operator as a solo NO v/s ETHx NO v/s DVT NO.

Reward distribution logic is available in the **Appendix**

ETHx: Low bond, high yield for home stakers

	Solo NO	ETHx	DVT (size 4)	DVT (size 7)
Min ETH bond per NO	-	4 ETH	0.8 ETH (per key share)	0.4 ETH (per key share)
Total bond per validator	-	4 ETH	1.6 ETH	1.6 ETH
Staker stake per validator	32 ETH	28 ETH	30.4 ETH	30.4 ETH
Rewards for ETH bonded by NO	1.92 ETH	0.167 ETH	0.033 ETH	0.017 ETH
Rewards to NO for ETH staked by stakers	0 ETH	0.058 ETH	0.016 ETH	0.009 ETH
Rewards	4.17%*	5.63%*	6.15%*	6.43%*

Note:

1. Returns have been calculated basis last 30 days average return from Ethereum
2. The bond per key share for DVT clusters is applicable to Permissionless NOs. Accordingly, Permissionless NOs will be earning the rewards on that bond which are listed under the 'Rewards for ETH bonded by NO' section in the table above.
3. The rewards earned by NOs on ETH staked by stakers have been equally distributed between permissionless and permissioned NOs. We are still assessing the right proportion and the final proportion of rewards between permssionless and permissioned NOs will be defined

So, a DVT cluster gives higher returns than a solo node and ETHx node at a much lower barrier to entry.

Current state of DVT implementation

Stader is working with SSV & Obol to run pilots and implement DVT with ETHx.

The integration of ETHx and SSV's DVT is in final stages. Various modules like Operator onboarding, keyshare generation, keyshare registry and rewards distribution through smart contracts among others are already live on JATO V2 (SSV's latest testnet). We also plan to launch the DVT pool with few validators on mainnet soon.

With Obol, we are working to be part of their Alpha launch where we will be running a cluster with 1 mainnet validator using Obol's DVT solution.
We have also been hard at work in testing out the DVT technology over the past few months. Let's dive into the details of how well DVT delivers on its promise.

| 7

Stader's DVT pilot

To understand the technology and its impact on staking better, we conducted several pilots to validate several hypotheses related to the benefits of DVT.

We investigated the following:

1. Performance comparison of a DVT cluster with a solo node
2. Performance comparison of different sizes of DVT clusters to define the ideal size

Pilot setup

Node/cluster type	Threshold	Participants
Solo node	-	Node run by Stader
DVT cluster of size 4	3/4	SSV: 1 node by Stader, 3 non-Stader nodes Obol: 4 nodes by Stader
DVT cluster of size 7	5/7	SSV: 1 node by Stader, 6 non-Stader nodes Obol: 7 nodes by Stader

| 8

DVT pilot insights

Validator performance on DVT cluster of size 4 v/s size 7 v/s solo node

	% attested	Proposed blocks	Missed blocks	Validator
Solo node	97%	**0**	**0**	Link 1
Size 4	**99.1%**	**1**	**0**	Link 1 Link 2
Size 7	**99.1%**	**3**	**0**	Link 1 Link 2

The performance of size 4 and size 7 clusters are at par with each other while being higher than a solo node.

| 9

Appendix

A1. Slashing probability for solo node validator v/s DVT cluster validator

A2. Simulation for bond amount

A2.1 Slashing network conditions

A3. Rewards distribution mechanisms

A4. Probability data for validator liveness

Slashing probability for solo node validator v/s DVT cluster validator

From a probability standpoint, the chances of a DVT validator getting slashed in an epoch is ~10^{16} times less than the chances of a solo validator getting slashed. Let's deep dive.

Slashing is observed to be a low-probability event on Ethereum. Only about 279 validators have been slashed so far.

Based on historical data, the probability of a solo validator getting slashed is $5.1*10^{-9}$

Now, for a DVT Validator being run by a Size 4 cluster, the chances of slashing can be calculated by considering these cases:

1. 3 nodes in the cluster agree to commit a slashable offense for the validator
2. 4 nodes in the cluster agree to commit a slashable offense for the validator

That gives us the slashing probability of a validator in an epoch as:

	Solo validator	DVT validator
Probability of a slash	5.10E-09	8.02E-25

Simulation for bond amount

We recommend a bond amount of **1.6 ETH + 0.4 ETH of SD.** This bond will cover the scenario where - 1920 validators are being slashed together, and there is an Inactivity leak of 3 days.

Slashing Network Conditions

Let’s get into how we came about this number. For the simulation, we have considered the following network conditions:

1. **Isolated slashing event:** When no other validator has been slashed within 36 days of our validator getting slashed

2. **Non-isolated slashing event:** When other validators have been slashed within 36 days of our validator getting slashed. For this, we have considered the scenario of the largest slashing event in 2021, where 96 validators were slashed.

3. **Inactivity leak of 3 days:** Ethereum stops finalizing in an inactivity leak. An inactivity leak of 3 days should be enough time to fix most issues that might be causing the inactivity leak. Historically, there have only been 2 periods, lasting less than 2 hours combined.

Scenarios	Validator balance	ETH lost
Normal Network Conditions	32.000	0
Isolated Slashing Event	30.935	1.065
Non-Isolated Slashing Event of 96 validators	30.921	1.079
Inactivity Leak for 3 days	31.563	0.436
Isolated Slashing Event + Inactivity Leak for 3 days	30.386	1.614
Non-Isolated Slashing Event + Inactivity Leak for 3 days	30.374	1.626

Considering a scenario where validators getting slashed are in **multiples of the worst case scenario: '96 validators getting slashed'**

	Balance	ETH lost
Non-Isolated Slashing of 96 validators	30.920	1.079
Non-Isolated Slashing of 192 validators	30.907	1.092
Non-Isolated Slashing of 480 validators	30.869	1.130
Non-Isolated Slashing of 960 validators	30.805	1.194
Non-Isolated Slashing of 1920 validators	30.678	1.321
Non-Isolated Slasing of 192 validators + 3D Inactivity Leak	30.360	1.639
Non-Isolated Slashing of 480 validators + 3D Inactivity Leak	30.323	1.676
Non-Isolated Slashing of 960 validators + 3D Inactivity Leak	30.262	1.737
Non-Isolated Slasing of 1920 validators + 3D Inactivity Leak	**30.138**	**1.861**

This bond amount is considered to safeguard the risks for stakers. At the time of writing, only 279 cases of slashing have been observed with a maximum of 96 getting slashed together. And, the mentioned bond covers a scenario 20X worse than the above scenario which creates a lower risk for stakers.

There are additional options available for insurance of staked funds. Please reach out to Stader team to get more information.

Rewards distribution mechanisms

1. For solo stakers:
    a. All the rewards generated for the 32 ETH will be of solo NO

2. For ETHx:
    a. 100% of the rewards generated on the bond amount will be given to the NO
    b. 5% of the rewards earned on Staker’s stake will be given to the NO

3. For DVT:
    a. 100% of the rewards generated on the bond amount will be given to the permissionless NOs
    b. 5% of the rewards earned on Staker’s stake will be distributed to the entire cluster, which includes both permissioned & permissionless NOs. So, each NO in the cluster will get 1/4th or 1/7th of the 5% rewards depending on the cluster size.

Probability data for validator liveness

For nodes that perform the same, theoretically, a DVT node will perform validator duties at 98.56% vis-a-vis 95% of a solo node.

Here is the calculation:

The performance of a solo node is assumed to be at 95%. This means that there is a 5% chance that the solo node does not perform

Applying the same principle to all the nodes in a DVT cluster.

Probability of duties performed	Node 1	Node 2	Node 3	Node 4	Probability
All nodes performed duties	95%	95%	95%	95%	81.4%
Nodes 1, 2, 3 perform but Node 4 does not	95%	95%	95%	5%	4.29%
Nodes 1, 2, 4 perform but Node 3 does not	95%	95%	5%	95%	4.29%
Nodes 1, 3, 4 perform but Node 2 does not	95%	5%	95%	95%	4.29%
Nodes 2, 3, 4 perform but Node 1 does not	5%	95%	95%	95%	4.29%
				Total	**98.56%**

| 10

Conclusion

With the DVT pool, Stader aims to lower the entry barrier for node operators and increase capital efficiency by giving them higher rewards.

For stakers, the goal is to provide an extremely secure way of staking on Ethereum and reducing the risk of their Ethereum getting slashed or the MEV getting stolen.

Stader’s vision is to further the decentralization of Ethereum and bring out the best of this ecosystem for both stakers and node operators alike.

We are focusing on launching a staking pool with DVT that will help us evaluate the performance of DVT and our offering on mainnet. After assessing all the information, we plan to roll out a permissionless offering for everyone who wants to be a part.

We would love to hear thoughts, comments, and opinions from the community. Dive into the discussion and tell us what you think

Stader