Tenderize v2: Solution Prospectus in the Current State of Centralized Liquid Staking
(-as of September 2023)

The Cambridge Labs at TRGC

Part 1: Introducing Tenderize v2 for Staking Decentralization

Tenderize v2 claims to be "a new liquid staking protocol that delivers liquidity for staked assets without centralizing of the underlying validator set". As staked assets are locked until satisfaction of a smart contract condition, the introduction of liquid staking became a solution to offer value upon those assets in the form of proxy tokens. This is liquid staking, in which derivative tokens representing staked holdings are made tradeable or even useable as collateral on existing applications, including lending. Centralization of liquid staking tokens (LSTs), which function as certificates of digital asset ownership, is a commonly observed phenomenon in crypto. For example, currently Lido controls nearly a third of the staked ETH volume with Coinbase and Binance following at 9.3% and 4.9% market share, respectively[1]. Disproportionate plurality controls pose an economic risk by what is dubbed the "cartelization of block space"[2] as the wider Ethereum community is dissuaded from participating in the network. Even whilst a staking contract may be acceptable, the lack of options becomes evident in the long run. As a centralized provider, the assets staked are within their control, even though the flexibility advantage is that tokens may be readily staked/unstaked. The fintech layer being satisfied, it is possible that future application layers may be bounded to incumbent protocols and limited. Of course, this may not be a problem so long as the smart contracts are acceptable, and incumbent companies can continue to formulate new provisions and agreements to satisfy needs. Tenderize's solution is to allow free entry & exit of validators and delegators with validators able to automatically issue TenderTokens (tToken) pegged to their respective nodes in return for the staked asset. Thus, it does away with validator whitelists associated with centralized protocols. Next, the values of the LSTs are tied to the performance of their respective nodes, eliminating socialization of risk as slashing penalties become isolated. Finally, by allowing 1:1 swap of tTokens with underlying staked tokens, it solves the problem of fragmented liquidity in which clearing arrangements are unmet between traders and contributors because of data availability differences between platforms/networks. In blockchain, this notoriously causes complications such as spurring the proliferation of liquidity aggregator protocols. While their data availability, analytics programmability, and deal screening efficiency is beneficial, it requires them to take in greater liquidity that reduces staking sector diversification. Currently, Tenderize supports MATIC, GRT and LPT tokens but is expanding to include ETH as well, offering a direct alternative to centralized liquid staking solutions. The Tenderize v2 architecture's advantages/risks against centralized solutions and economic outlooks are deliberated.

AUGUST 2023 –

Most recently, Tenderize v2 was launched as an open-source protocol intended to bolster decentralized finance. For instance, at this time, Lido controls over 32% of staked ETH, incurring the concerns formally associated with centralized assets control in the blockchain space. The fundamental departure for Tenderize v2's method is its open-source protocol in which validators are individually certified by their LST tTokens, which enables stake flow to validators as opposed to a company. This decentralizes staking on the individual level and, when performed efficiently, is purported to reduce the value of centralized services in the staking economy. From the user side, this allows immediate swapping of staked/unstaked assets, additional yields, and borrowing. While this does seem to retain the virtues of transparency, self-custody, and permissionless processing, it trades off specific economic advantages inherent to centralized muscle in financial management. For the user, however, this kind of non-custodial system enables greater competition and free market as individual nodes will need to improve quality and affordability in order to process stakers' interests.

1.1 The State of Affairs in the Liquid Staking Economy

$7 billion ETH becomes the largest staked asset, indicative of the aforementioned expectations. According to CoinMarketCap, it comes as no surprise, given the illiquid and inaccessible nature of conventional staking, that liquid staking derivatives The value of a liquid staking token(LST)/liquid staking derivative(LSD) is pegged to that of the original asset, which in accordance with other smart contract protocol effects, acts as a certification of ownership. Proof-of-Stake (PoS) networks will be advantaged by having crypto assets locked up as collateral in return for token compensation to the staker. The blockchain is awarded financial support to drive transaction validation throughout the network. This boost in liquidity on can further attract more stakers and validators, essentially creating a pot of accessible funds upon which more robust services can be offered and managed. The overall security and application streamlining of the blockchain is thereby bolstered, seen as especially advantageous to Ethereum given its L1 mainnet guarantees. As multiple blockchains establish staking, it becomes easier to interface even a cross-chain decentralized application (DApp) as a result of increased financial backing

for services. Essentially, applications and indeed, even Layer 2 infrastructure for other solutions, can be optimized due to the bottom-up fertilization of the network.

Staking-as-a-Service (STaaS) have the advantage of collating computational muscle and providing reliable support and even monetary compensation, especially when sustained by greater sums of staked assets. This makes them centralized as they are intermediaries who conduct custodial services on behalf of the user. Fundamentally, the ability to amass nodes in one STaaS company generates an efficiency buffer to the entirety of DeFi, but as an ecosystem. This allows there to be a reduced barrier to entry for stakers from both a user-friendly point of view, as well as for resource management and providable service capabilities. The problem comes when governance is influenced by the nucleation of validation nodes working towards as one intermediary. (https://messari.io/report/what-s-at-stake-in-staking-as-a-service)

Total value locked (TVL) for liquid staking rose 292% to well over $20 billion, since 2022 (Bloomberg; CoinDesk). The democratization of staking that results from liquid staking is largely beneficial to Ethereum, in particular, whose mainnet security guarantees DApps leverage. As more L2 infra and middleware are built, these guarantees become more vital. As a result, Ethereum is seen as a safer alternative to lenders in the space, especially when centralized lenders, such as Gemini Earn or Celsius, have fallen. From this August 2023 update, staking revenue has concurrently grown 19% Q/Q to $88 million, assuming only 13% of the net. now make up $18 billion of the total share, with a recent TVL of $21 billion for these protocols. The ability to trade or put up collateral against staked assets is a definitive game changer in DeFi.

Concurrent with the market expansion surrounding liquid staking derivatives, institutionalization of providers, aggregators, and validators has occurred as a means to providing better services. As a result, risk diversification has been significantly reduced as incumbents monopolize layers on the blockchain. As of 6th August 2023, Lido DAO controls 31.73%[3] of the total staked ETH volume. This makes Lido by far the largest holder of staked ETH. Coinbase and Binance follow Lido at 9.3% and 4.9% market share respectively (See Fig. 1). Lido stands to gain further as US regulatory authorities crack down on staking services offered by centralized exchanges, despite commodities and securities law debates ongoing. In February 2023, centralized exchange Kraken was made to cease crypto asset staking services for US users and pay legal penalties to the tune of $30 million under settlement with the Securities and Exchange Commission (SEC)[4]. In the last 6 months, Kraken has seen a 35% drop in its staked ETH volume. The SEC has hinted at the possibility of a similar settlement with Coinbase and Binance in June 2023[5]. This comes at a time when Lido's staked ETH volume has already grown at a whopping rate of 65% in the last 6 months, compared to 4% and 23% for Coinbase and Binance respectively[6]. *Figure 1* presents the state of market share for the leading ETH staking intermediaries.

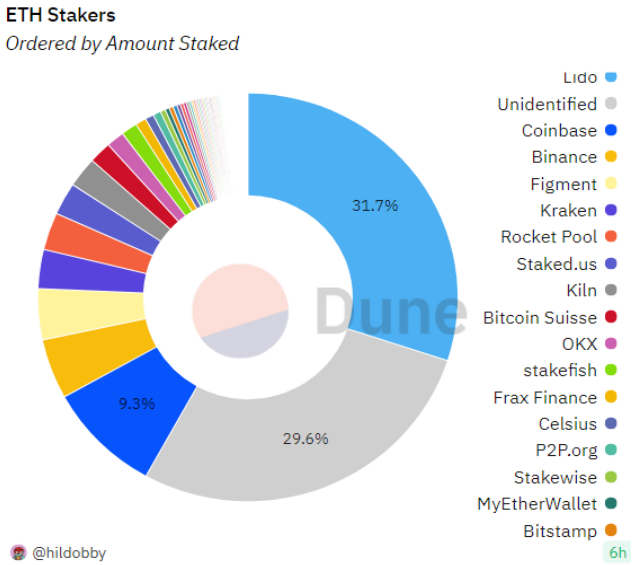


Figure 1 ETH stakers market share

(https://dune.com/hildobby/eth2-staking)

It was assumed that the "Shapella" upgrades to Ethereum will temper the market dominance of Lido. However, since withdrawals have been enabled, the market share of Lido has marginally increased from 31.4% to 31.73%[7]. Any single protocol's market dominance can be seen as a dire situation for PoS chains hoping to preserve decentralization. Centralized staking protocols need to decide which node operators they wish to include in their validator set. In this post a post by GitHub user 'djrtwo' titled "The Risks of LSD", the author has outlined two ways this can be achieved:

i. Governance by token holders;
ii. Economic selection (and removal) of node operators.

Part 2: Discussion – Hazards of Centralization in Liquid Staking

The Faults of Centralization:

Staking in the decentralized finance (DeFi) sphere has experienced centralization quirks driven by liquidity providers and aggregators due to either incumbency or preference for their primitive. Projections entail significant risk for DApp development, downstream, and financial security. The most relevant areas of risk discussed here are governance, validators, and market risk/economic sustainability.

2.1 Governance:

i. Community Democracy: Governance token holders decide on node operator inclusion/removal through a simple vote based on their share of the token supply. This might seem like a democratic measure to validator whitelisting but this is only possible if the token holders' sets are sufficiently diverse and decentralized. Unfortunately, DAO vote distribution often suffers from large concentrations of votes in a few hands, or governance whales. Even if token distribution itself is not concentrated, DAO governance votes often get concentrated through delegations, since small holders are unable and/or unwilling to participate in the process. Time and energy constraints to construct informed opinions and proposals are less within the average operational capacity of more casual, small-time holders in the community. While not necessarily the fault of the system and well within the fundamental moralities of the free market, this does create disparities which serve some more than others. This is not inherently bad- the "WAGMI" idea works when all partaking in the ecosystem benefit, even if due to the choices of a few; however, when liquid staking itself is centralized to a few intermediary services, then it is possible to take advantage of the more diversified service provider portfolio against other pockets of the ecosystem. This becomes a cross-platform disparity in the hands of the few and compartmentalizes the ecosystem, itself. As is known, the most foremost example of token concentration is Lido DAO where out of more than 37,000 LDO holders, the top 10 control more than 50% and the top 100 more than 85% of token volume respectively (See *Figure 2*).[8]

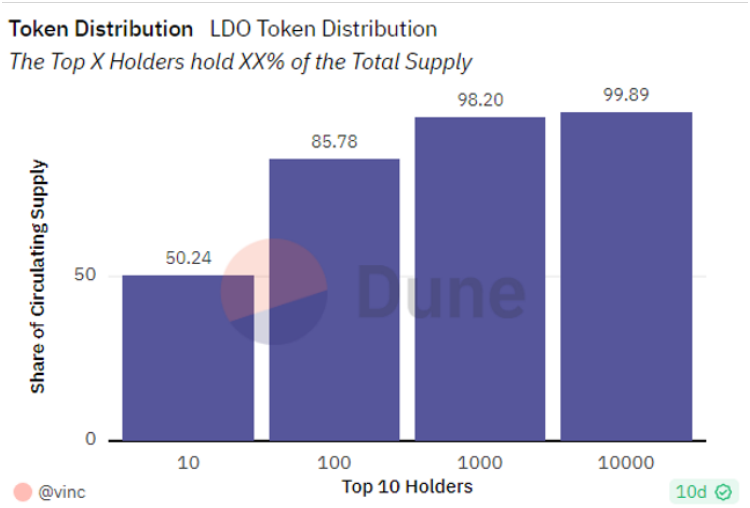


Fig. 2: LDO Token Distribution

(https://dune.com/vinc/lido-dao)

Therefore, there exists a strong possibility of a small minority in centralized staking protocols being able to coerce the token holders to engage in monopolistic behaviour, like coordinated MEV extraction and censorship with non-alignment inviting punishment through removal*. There is also the possibility of regulatory authorities like the SEC more easily able to target the cartel and capture the network instead of a set of decentralized node operators. The SEC's willingness to prevent US users from engaging in staking may make this possible.

ii. 'Dual Governance': In response to concerns regarding the risks for LST governance from centralization, Lido itself recently proposed the concept of 'dual governance' (July 2023) (https://hackmd.io/@lido/BJKmFkM-i). The goal is to enable a democratic veto power to avoid the possibility of Lido unilaterally adjusting the terms between the protocol and stakers. The first steps are obvious, such as upgrading the LST smart contract, adjusting the manner in which stake is distributed between nodes under Lido's management, and dictating acceptable fees. The mechanisms required for this governance design are described according to staker community availability against a timelock in `CRITICAL_DECISION_TIMELOCK_DURATION` seconds, a window during which the community is able to deliberate the effects of their decision and adjust subsequent actions. By introducing the **Veto Escrow** smart contract, the LST is locked in escrow and used as estimation of community concurrence to gauge preliminary decision making. Depending on a margin of disagreement to be decided upon, the **Veto Voting** state is enacted to block execution of the command, allowing the wider community to then participate. This process and essential protocol parameters are illustrated in *Figure 3*:

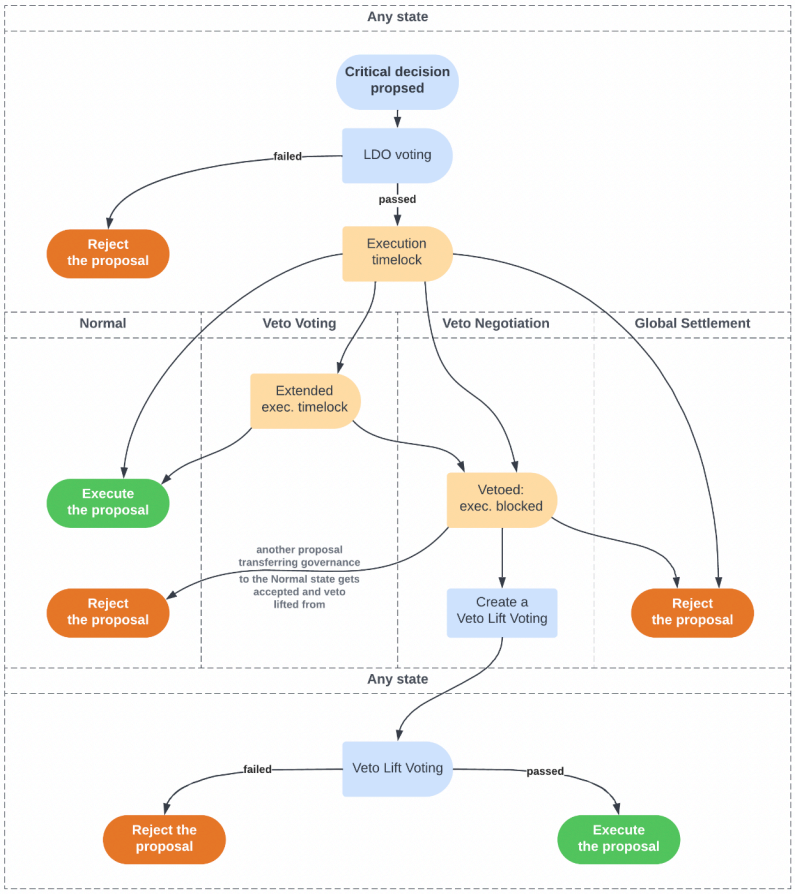


Figure 3: Lido's proposal for a 'dual governance' strategy to pacify concerns of governance authority overstep by their centralized service. It works with certain assumptions regarding the availability and willingness of their client body to be involved and has a multi-tier, as well as a step revision protocol (https://hackmd.io/@lido/BJKmFkM-i).

CRITICAL_DECISION_TIMELOCK_DURATION
Duration of a timelock following a successful LDO vote for a critical governance decision during which the decision cannot be executed.
Reference value: 1 week.

FIRST_SEAL_THRESHOLD
Percentage of total stETH supply required to be locked into the Veto Escrow in order for the veto voting to be started.
Reference value: 3%.

VETO_VOTING_MIN_DURATION
Minimum duration of veto voting.
Reference value: 1 month.

VETO_VOTING_DURATION_INC_PER_STETH_PCT
How much veto voting duration is extended with each additional 1% of the total LDO supply locked into the Veto Escrow.
Reference value: 1 week.

VETO_NEGOTIATION_THRESHOLD
Percentage of total stETH supply required to be locked into the Veto Escrow by the time veto voting ends in order for the Veto Negotiation governance state to be activated.
Reference value: 15%.

VETO_NEGOTIATION_MIN_DURATION
Minimum duration of the Veto Negotiation phase.
Reference value: 1 month.

GLOBAL_SETTLEMENT_TIMEOUT
For how long governance should be in the Veto Negotiation state in order for the Global Settlement to be activated.
Reference value: 1 year.

GLOBAL_SETTLEMENT_THRESHOLD
Percentage of total stETH supply required to be locked into the Veto Escrow for the Global Settlement to be immediately activated.
Reference value: 70%.

VETO_LIFT_VOTING_DURATION
Duration of a Veto Lift voting.
Reference value: 1 week.

VETO_LIFT_VOTING_MIN_QUORUM
Percentage of veto voting power required to participate in a specific veto lift voting in order for this voting to succeed.
Reference value: 15%.

Problems: As of September 2023, the 'dual governance' proposal by Lido is the most novel strategy put forth to quell governance abuse fears by centralized liquid staking entities. Unfortunately, there are inherent problems:

- The protocol assumes that a *small* but active portion of stakers will react to controversial governance actions by the company with the ability/willingness to escalate.

- A medium tier larger subset is alerted to the reaction of the former group, requiring a dependence on the veto protocol.

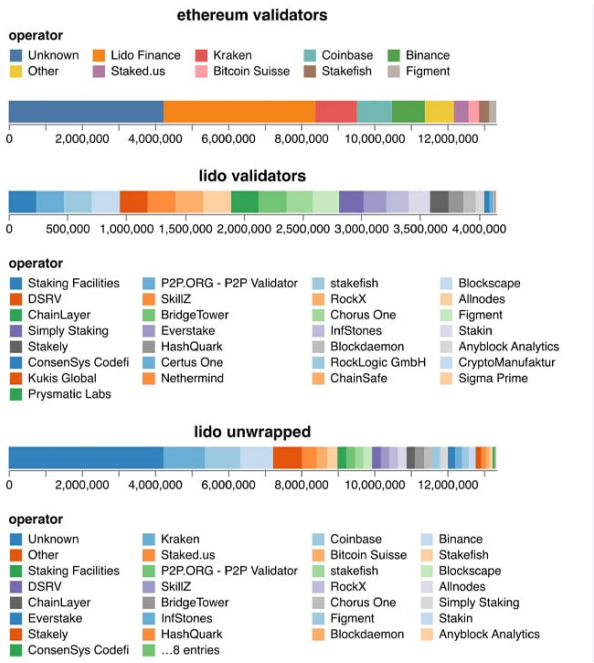
- The largest possible subset is activate after dormancy to finally respond.

The chief purpose, it would seem, is to corral as much of the staker base as possible, made successful by incrementing awareness of governance process in a step-wise fashion led by whoever is immediately attentive.

Unfortunately, this most recent attempt of mitigating centralization detriments to governance comes with technical complications which may not yet prove workable or, indeed, adequate to maintain robustness of operation of the LST sector. The amount of funds placed into escrow may be changed according to the dictate of the company. Voting time may not suffice to gain an adequate proportion of the staker base's votes. Democratic process is enabled but the civic principle of voter turnout has never been easily gauged by Web3 networks, since it at least requires that not only do all voting parties vote, but that all at least are receptive to the situation. The only way this can be monitored, in any degree, is by confirming wallets are accessed on the blockchain, which even then does not necessarily mean that the specific alert to a governance prospect has been read. Time constraints on voting process itself are arbitrary and may/may not suffice to allow all interested stakers to comfortably participate. In turn, the `VETO_LIFT_VOTING_MIN_QUORUM` applies a prerequisite voting power to be successful. Somehow, this will need to be enforced as voter turnout always runs the risk of not meeting necessary thresholds, as well. As an aside, the reiterative nature of voting settlement inviting subsequently larger bodies of stakers is a promising method of gaining commendable viewership and participation. Fundamentally, however, stakers being the explicit stewards of their own funds by delegating to truly decentralized nodes guarantees 100% involvement on governance at the time of staking and encourages personal responsibility. This remains true.

2.2 Validator Regime Centralization:

The service providers dominating the liquid staking sub-sector are able to deploy the brunt of the most efficient validator nodes due to the centralization of their financial and technical support assets. This form of Node Hosting Infrastructure comes with various risks. The distribution of the Ethereum validation pluralities, as of September 2022, is described in the following *Figure 4*. It is further considered that certain markets can be muscled in or out depending on the local geographic presence of the validator nodes in promising regions. This has not been confirmed in any quantifiable manner but is a note on the point of 'collusion'. This is the concept that the nodes of centralized LST intermediaries, as well as local government and finance bodies, can cartelize data availability. This would contribute to data fragmentation by colluding to operate in illicit ways that are not transparent to the user community.



Country	SUM of Validators	% of Validators
Germany	17,082	13.1%
Switzerland	14,390	11.1%
US	13,392	10.3%
Cayman Islands	11,159	8.6%
Korea	7,391	5.7%
BVI	7,391	5.7%
Singapore	7,390	5.7%
Netherlands	7,390	5.7%
France	7,390	5.7%
Canada	7,188	5.5%
Malta	6,500	5.0%
Ukraine	6,000	4.6%
Hong Kong	6,000	4.6%
Estonia	5,664	4.4%
UK	5,208	4.0%
Gibraltar	209	0.2%
Austria	209	0.2%
Australia	187	0.1%
Grand Total	**130,140**	

Figure 4: Ethereum validators per key staking operator, as of September 2022. Lido Finance assumes a sizable plurality of validators and maintains a healthy distribution around the world with their highest numbers in key Western financial hubs (-originally shared by Banteg (left) and Alex Svanevik (right).) https://news.bitcoin.com/proof-of-work-proponents-question-validator-censorship-as-59-of-staked-ethereum-is-held-by-4-companies/TTTdasdffd

Specifying a pre-defined criterion could be used to determine the composition of the validator set. It is suggested that profitability of a node operator is the only trust-less (automated) measure of a node operator's usefulness to the protocol. It could then be argued that participation in the protocol is dependent on falling under a certain percentage of profitable node operators. This may be akin to governance coercion, the only difference being its automation. This is because there are significant economic incentives to be had from capture of MEV and block space censorship. Non-participation as an independent validator renders a validator unprofitable compared to the cartel. This eventually leads to automatic removal from the validator set. On Ethereum, if the cartel gains 1/3rd of the staked volume, they can stop blocks from finalizing. If they gain 2/3rd control of the staked ETH volume, they can start creating and finalizing blocks, the access to which they can easily censor. One of Ethereum's core principles of having off-chain governance is compromised as an entity is now able to govern Ethereum on Ethereum itself. Since we already have established that this could be a minority of the number of Ethereum participants, such a situation is bound to invite a hard fork of the network. The 'sliding scale' of cartelization of stake, therefore, not only poses protocol risks but also "risks to capital"[9] as the delegators to a cartelized staking solution will eventually run the risk of losing their stake altogether. This firmly establishes that stake centralization is not only harmful to the network but also individual stakers who might benefit initially from cartelization. The solutions to the 'sliding-scale problem' is for centralized staking protocols to either place self-imposed limits on the stake they control or to completely do away with validator whitelists, that is decentralizing their protocols. Since there is no way for the network to ensure the self-imposed limits are followed apart from simply trusting the protocol, it runs counter to the spirit of trust-less networks. Decentralization, therefore, is the only viable solution to ensure protocol robustness and staked capital security in the long run.

i. Censorship and manipulation: The economic model for compensation of validators can be tuned to enable theoretical extremes. This manipulation is especially robust where smart contracts dictate price fluctuation goalposts between joint parties after which withdrawal of staked funds is possible. When a service provider, including an aggregator facilitating deals, is able to hedge on behalf of clients, the network or deal flow can be censored. Force-liquidation clauses can be triggered unilaterally. Contributor regimes, such as validators, can also

be barred from diversifying the compensation economics of staking pools or transactions, resulting in consensus collusion. As put by The Ethereum Foundation, prevention of open source transaction data availability, like this, at windows critical to smart contract executions, makes it possible to "privatize the profits and socialize the losses." While governments are yet to fully levy financial securities laws on crypto assets and blockchain platforms, there is increased possibility that centralization of staking providers and aggregators can warrant censorship enforcement on the protocol level. Though users would inevitably argue against it, they too would be technically unable to dictate the arrangements of the centralized service. The two exceptions to this would be DAOs pre-programmed against data censorship and collusive behaviours, or validators changing their activities. The latter can be argued less likely, given that a centralized service may be inclined to compensate further to maintain the infrastructure. Indications of staking share are provided in Figure 5). In the situation that censorship does occur, by whatever means, there does seem to be qualitative evidence for many validators willing to fork a blockchain in order to renew transparent work.

- The Principal-Agent Problem: Governance affects stake delegation directly due to the mass fungibility of readily tradeable crypto "securities" offered as LSTs. ('The Principal-Agent Problem in Liquid Staking' -Tzinas and Zindros. May 2023.). In the case of any security compromise or detection of illicit behaviour by a validator, the slashing of the stake is possible. This possibility is fundamentally hampered when validators are centralized due to the possibility of collusive scheming. Thus, it is important to mitigate illicit practices on part of the validator ('The Agent') that would affect the working capital of the delegating user ('The Principal'). This is known as the "Principal-Agent Problem" (Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure -Michael C. Jenson and William H. Meckling). As is seen in *Figure 5*, the simplest form of attack takes the form of capital manipulation behind the scenes strategized for a specific unbonding period for withdrawal of stakes. Since this information is open, despite the presence of smart contracts adding a measure of defense, in the presence of liquid staking, the possibility of immediate withdrawal expands the scope for capital manipulation. The earned equivocation by the validator is not proportional to the economic processes of the network. This kind of thing is

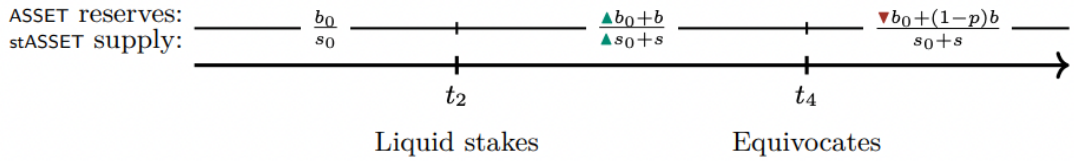


Figure 5: 'Timeline of the simplistic attack' by Jenson and Meckling. All stakers are affected across the community as a result of selling fungible, pegged value assets. These are socialized losses and can occur according to newly quoted prices between time t_2 and t_4, after which equivocation is earned illegitimately by the Agent.

akin to the recent behaviour of the Silicon Valley Bank (SVB) fiasco, in which deregulation of centralized entities enabled stewards of users' funds to take increased risks against long-term holdings ('The Silicon Valley Bank (SVB) Collapse and Implications for Business' –The Conference Board, 15 May 2023.). The ability to sell assets with proportional representation of a fund holding causes this. This problem can in fact be exacerbated in domains such where the current climate, such as the SEC hunting of crypto asset staking under the pretense of unregistered securities, becomes standard. Here, judicially enforced pay-outs by indicted actors further uproot the stability of the crypto economy and diminish users' holdings value. The encouraged outcome is then LST oversight and potential future corruption by state governments, even after reducing malicious validator behaviour.

In counter, punishment of nodes can be a limiter upon illegitimate practice by agents, such as slashing. Unfortunately, in deregulating centralized entities, this is under-enforced. When enforced, "fair punishment" of nodes is difficult to argue, since slashing stops the progression of the behaviour. This means effectively hiding transaction data can avoid slashing, something which is easier within centralized bodies of validators.

iii. Network resilience & long-term sustainability: Network resilience is at its highest, able to shield against technical malfunction, adversarial attacks, and illicit collusion when the validator regime is well distributed, which includes digitally/professionally decentralized nodes, and even their geographical separation (https://messari.io/report/evaluating-validator-decentralization-geographic-and-infrastructure-distribution-in-proof-of-stake-networks). To gauge the resilience of a network to compromising activity tied to centralized infrastructure or process, it becomes to quantify decentralization itself. This is determinable via a Lorenz curve according to a certain value of Nakamoto Coefficient, or the minimum number of entities in a subsystem that can achieve 51% capacity. A subsystem is the infrastructural parameter facilitating centralization/decentralization of the resource.

Multiple subsystems exist in any given situation, creating complex intersectionalities that collectively, either reduce or increase their Nakamoto Coefficient. Therefore, more may be able to operate together at a higher Coefficient, depending on the capacity or properties of each subsystem. Examples of such properties and their compromise thresholds are presented in *Figure 6*):

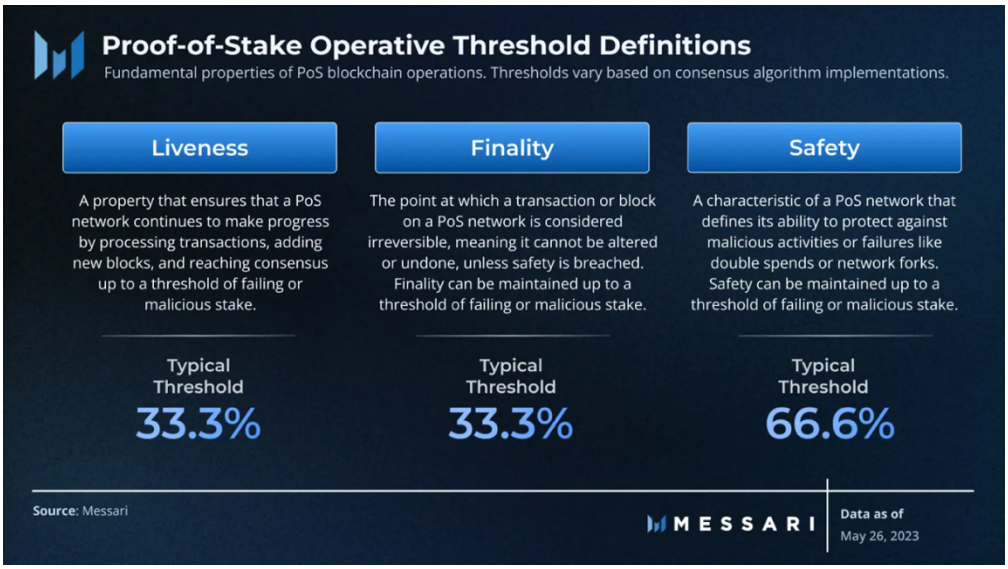


Figure 6: Proof-of-Stake properties and their typical thresholds against failing or malicious staking behaviours. These properties of a network decrease or increase in response to the influence of subsystems number.

Operational decentralization for network resilience is most impacted by the following subsystem characteristics:

i- Node Hosting Infrastructure: Chief focus is the presence of validation nodes operating for intermediary LST providers and their associated risks.

ii- Geographic Location: Geographic jurisdictions, node hosting infrastructure, technical fortitude, and resources can bias the manner in which network layers operate, or their robustness.

iii- Node Software (Client): Software diversities can improve the ease of access of users and validators, providing different operational interfaces or hardware compatibilities which allow for heterogeneity in network abilities and resource availability. Centralization counteracts this and can standardize lower quality performance.

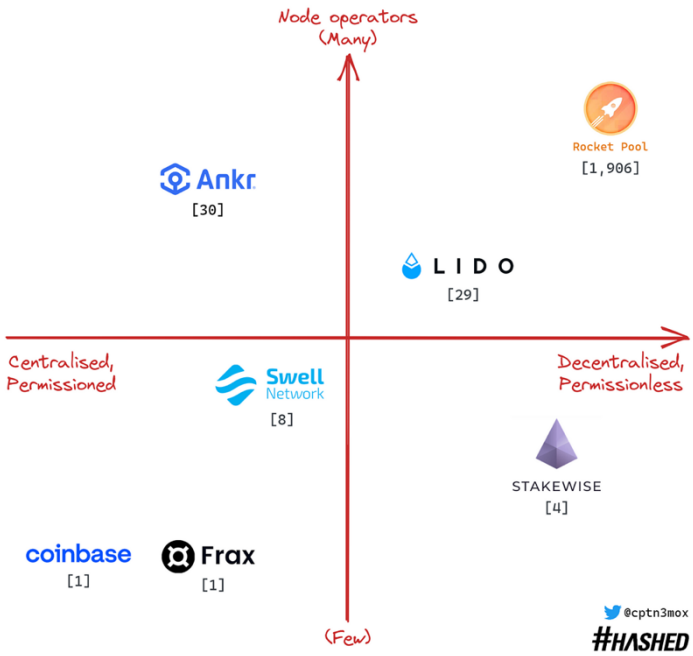


Figure 7: Qualitative comparison of the dominant liquid staking entities in terms of relative centralization/decentralization and the permissionless/permissioned nature, not considering specific operational differences. (https://medium.com/hashed-official/a-dive-into-eth-liquid-staking-node-operators-shanghai-future-innovations-and-dvt-523e275a467c)

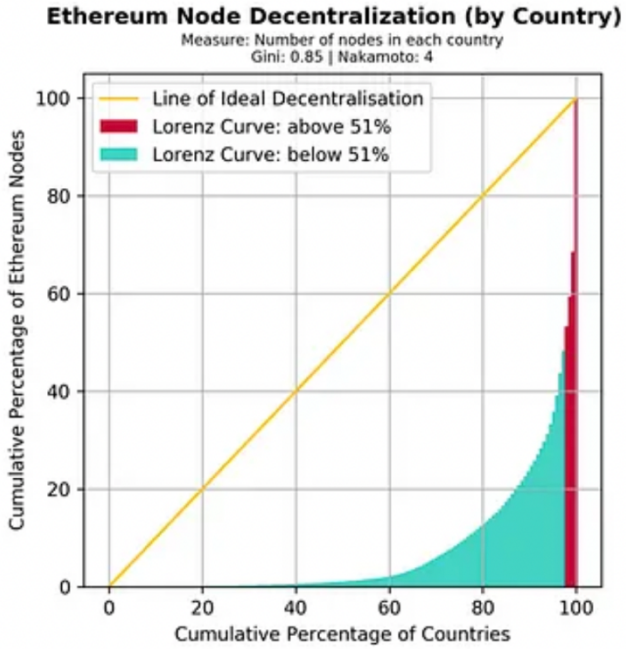


Figure 8: Decentralized presence of Ethereum nodes by country in staking. 51% of total supply is assumed by 4 entities. ('Quantifying Decentralization' -Balaji S. Srinivasan)

i. Recap of Node Hosting Infrastructures and their distribution among incumbent actors in staking:

The focus *throughout this report* has been Node Hosting Infrastructure in the form of the centralization of nodes by concentration under incumbent LST providers. *Figure 7* provides an indication of the incumbency of nodes centralized vs. decentralized and permissioned vs. permissionless operation:

As of April 2023, Lido has only 29 nodes, as opposed to Rocket Pool, whose 1906 nodes occupy a much more decentralized and permissionless protocol. Lido, Swell, and Ankr further only periodically open their operator slots to the nodes, which are facilitated by an internal committee (https://medium.com/hashed-official/a-dive-into-eth-liquid-staking-node-operators-shanghai-future-innovations-and-dvt-523e275a467c). On the extreme, Frax and Coinbase validators are run in-house by internal employment. It is worth reiterating that the best validator performance comes with the centralized, permissioned processes accommodated by these players, and resource management is granted extra time to ensure returns are competitive for their stakers.

ii. Geographic Location:

Because the hardware infrastructure nucleates in specific states or economic zones, security is weakened as legal infringements can hamper the network. (https://zkvalidator.com/why-does-the-location-of-your-validator-matter/#:~:text=A%20high%20concentration%20of%20validators,gain%20control%20over%20the%20network.) Coercive steps by governments or technical complications, such as electricity grid or internet connectivity failure, can become acutely concentrated issues, increasing the chances of the entire network malfunctioning or being breached. The United States is currently running investigations and executive ceasing orders of staking movements led by concerns that crypto assets could be designated as securities. The fear is that formal regulatory proceedings may begin which subject liquid staking assets to the procedures which govern traditional stocks. As opposed to this, the European Union instead approved Markets in Crypto-Assets (MiCA) legislation on April 2023, which does impose some regulation but focuses on establishing more reliable frameworks for token issuers and asset managers in the space. There has yet been no move made on the staking sector. Given that 47% of Ethereum nodes are located in the United States vs. 12% in Germany, it is easy to see how geographic distribution is vital to the global network operation of the liquid staking sector. Meanwhile, Solana's validators place 20.4% in the United States with 21% in Germany. In this case, the Coefficient, assuming a same number of subsystems, would potentially be lower for Ethereum, posing greater risk for compromise of the system due to centralization.

As has been noted in *Figure 4*, validation nodes find themselves most concentrated in certain countries where global financial institutions are prevalent. In the context of staking, here described in terms of cumulative Ethereum nodes against cumulative percentage of countries (*Figure 8*).

iii. Node Software (Client):

Clients are software that run processing of transactions between validator nodes and the blockchain. Liquid staking derivatives' transactions are handled by companies through these tools and are provided security

depending on the nature of the client. Each client's architecture speaks to the robustness of its security and the efficacy of the operations that must be handled.

Client Architecture: At its simplest, multiple validator keys are used to access the verification layer. A validator client is connected to a beacon node, through which validators flow transaction duties in exchange for ETH remuneration. This comprises the basic security level.

. Problems:

. The keys must be constantly online, running expenses high and leaving the system potentially open to cybersecurity risks.

. Each validator client is accessible by a unique key set, without which slashing is automatic. If the client malfunctions, there is no back-up to reboot the process.

. The infrastructure is centralized.

. Network Resources:

- Hardware and Upfront Capital: Nodes require adequate hardware and economic margins ascertained by the amount staked through each in order to remain profitable.

- Ongoing Operational Expense: Resource consumption and maintenance of the node will incur operational costs which must be tabulated within profit margin.

- Stake Delegation: The ability to pitch more stake to existing validators is essential, governed by the efficacy of the network, the robustness of their own client, and their availability.

- Validator Set Caps: An imposed cap can limit blocks processed to validators with competitively stakes.

Distributed Validator Technology on Ethereum: The use of Distributed Validator Technology (DVT) is an important means by which Ethereum aims to improve decentralization, fault tolerance, and security. Another tool for LST companies to use, multiple validator keys, both public and private, allow the operator to earn rewards. A validator client is connected to a beacon node which runs the validation. A schematic of this architecture is provided in *Figure 9*:

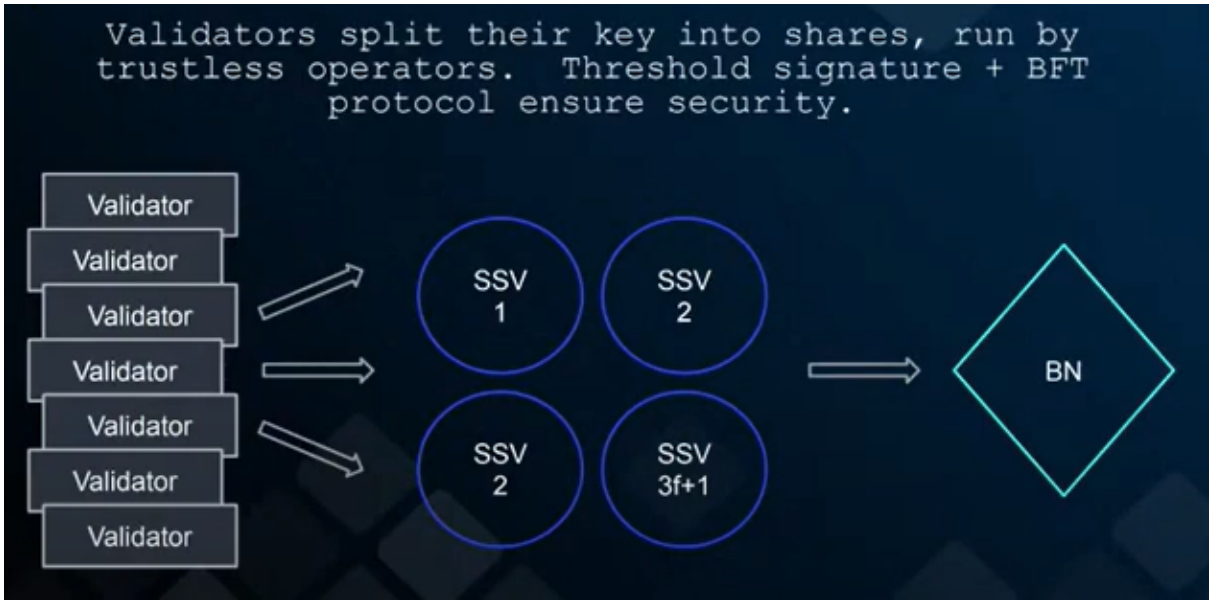


Figure 9: An example of SSV Network's DVT with multi-sig formalization of jobs to be passed onto the beacon chain, or slashed. (https://docs.ssv.network/learn/readme/tech-overview)

In this situation, all nodes are engaged in trustless protocols and are independent, meaning truly decentralized. Jobs are verified and processed in tandem with secondary, assistant nodes, notified by the job-receiving validator. The recipient node initiates the duty and opens an opportunity for other nodes to join in the verification. In the case that the validity of the transaction stands and slashing does not occur, each node signs into the multi-sig construct with their own unique KeyShare, certifying passage onto the beacon chain. This is known as distributed key generation (DKG). In this case, the shared public and private keys constitute a set constructed by the operators running that instance on the SSV network. Since nodes carry a portion of the collective private key, operators cannot coerce the validation unilaterally (https://docs.ssv.network/learn/readme/tech-overview). Secure multi-party

computation (MPC) of this kind enables operators to rapidly be granted novel keyshares and perform decentralized validator work without a single point of failure.

There are still, however, problems even with this. Additional components are introduced which may have diminished security or are more vulnerable. The only solution that has been voiced thus far is multiple implementations of a DVT node for a multitude of clients. This does create resource overstretch and increase the number of potential faults present, however. Operational costs concurrently increase as the validator is distributed with the DVT mechanism to multiple parties. This is because multiple nodes are recruited to perform a single task. Finally, increased latency is inevitable as the consensus between multiple nodes can induce lag in the system. Furthermore, the presence of multiple layers of smart contracts introduces new potential vulnerabilities which can cascade down-path to compromise a transaction. (https://ethereum.org/en/staking/dvt/#:~:text=Potential%20drawbacks%20of%20using%20DVT,-Additional%20component%20%2D%20introducing&text=Potentially%20increased%20latency%20%2D%20since%20DVT,can%20potentially%20introduce%20increased%20latency).

All decentralization methods described still deserve observation and subsequent analysis. While some reduce the possibility or inclination of collusion, they do not necessarily eliminate them. What is clear is that the nature of their infrastructure is still quite centralized. Network resilience is reduced as a result and leaves open to cybersecurity risk. Even where erosion of trust in a company's internal practices may be alleviated, systemic faults may end up becoming the trade-off. Ironically, it may become difficult to confirm whether illicit practices by a validator regime are to blame, should something occur, or if it is due to system integrity. Where the former is ascertained, it may actually serve favorable momentum to much more decentralized LST solutions, such as Tenderize v2. In truly decentralized architectures, it is possible to cultivate an culture amongst nodes that values longterm sustainability via competitiveness. As stated by Messari: "Validator operators should aim to self-host nodes when feasible, switch to a non-dominant server solution, or at the very least when economically feasible run validators on data centers in different geographical locations with the same hosting provider. Doing so will help mitigate risks associated with political or corporate hostility, infrastructure failure, and natural disasters impacting a specific region."

2.3 Market Risk and Economic Sustainability:

i. Pooled Stake and Network Costing:

The reason that PoS ecosystems are inherently more prone to centralization and monopoly is due to the fact that staking maximizes the importance of capital. As a result of this, all that is needed to obtain control of a pool is for an incoming party to allocate funds matching the total original stake. In doing so, the operations of the network and their total net worth are steerable to the new delegate authority, akin to an investment whale. (https://river.com/learn/proof-of-work-pow-vs-pos-proof-of-stake/#:~:text=Proof%2Dof%2DStake%20systems%20are,than%20labor%20and%20cheap%20energy.) Naturally, where intermediaries begin to host pools and validators, the inevitable outcome is that their respective LSTs, in this new age, become the governance stranglehold over the rest of the network. (https://www.coindesk.com/layer2/2022/04/20/is-ethereum-staking-pool-lidos-growth-an-omen-of-centralization/) Similar to a bank operation, if the contract enables the free liquidation of staked funds from a pool managed by the intermediary, there is suddenly expendable capital that is usable on/off-chain outside the sphere of the stake itself. The only promise here is that there are funds remaining to accommodate stakers' withdrawals, should the need arise.

When LSTs revolutionized staking, the sudden ability to peg representative transactable token pegged to staked assets during 'Shapella' enabled dramatic fluidity in value exchange and circulation. While this does benefit validators and stakers, there is now more opportunity for centralized services to act on the leveraged capital over which they preside to compromise the mainnet's ability to self-regulate. (https://dataalways.substack.com/p/endgame-perils-of-restaking) In order to garner yields on staking, there are operational costs that must be taken into consideration, such as fees which may be levied either by the network and/or exacerbated through 3rd party centralized services. Refer to *Figure 10* which shows the profiles of projected staking yields as a result of costing:

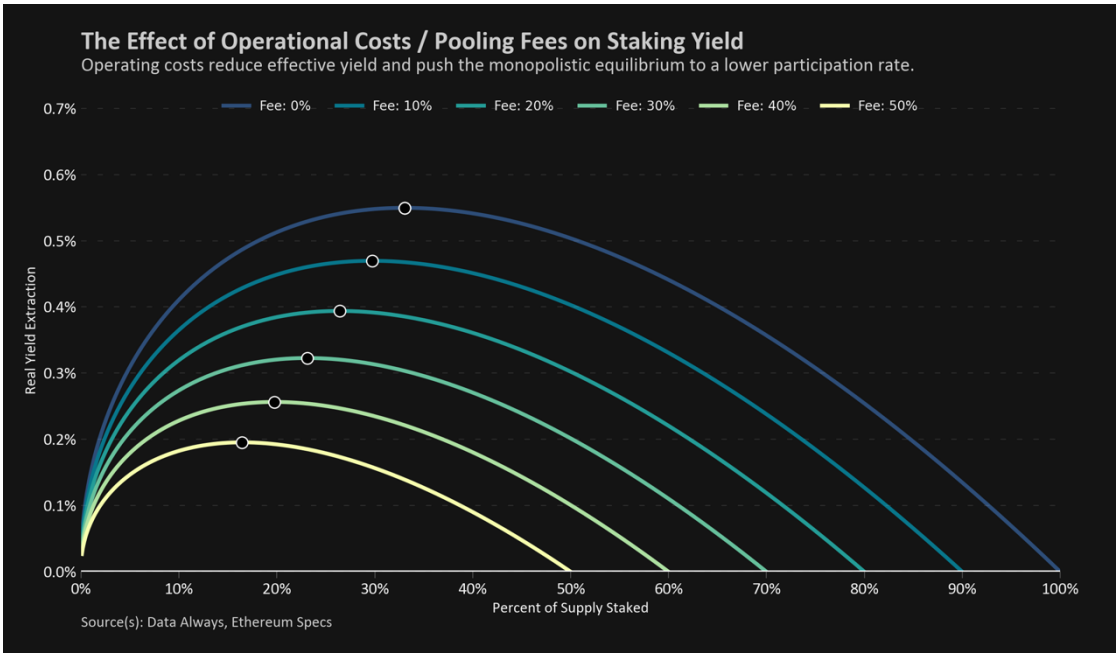


Figure 10: Fee rates' effects (and extrapolated secondary operational costs) on the staking yield. (https://dataalways.substack.com/p/endgame-perils-of-restaking)

In restaking via LSTs, the new mechanic introduced is the ability to feed back staking yields into the ecosystem to increase the validator count. In doing so, accelerated future returns might be ensured in short-term forecast as the staked yields can be compounded. This is successfully managed when the validators are hosted by a delegating protocol. Secondary network operational costs, however, are concurrently elevated due to increased transaction activity, bouncing between smart contracts for restaking/slashing. This congestion can exacerbate the mainnet-derived gas fees, which becomes a global inflationary damp on all individuals attempting to stake. Centralized pools can also compete for limited block spaces, resulting in even greater gas fees. The secondary costing is manageable when processes are streamlined with centralized services, but the increased competition in the latter further means that only they are able to benefit from the priority delegation from higher value jobs. This results in a positive reinforcement cycle which may encourage further centralization.

External yield sources, which are derived from middleware services which award restaking, can shift the management monopoly of real staking yields by centralized providers, such as Lido. As evident in *Figure 11(a.)*, external yield has a margin of effect, dependent on the amount of token supply staked, within which staking yields can be increased. Increased external yield sources result in decreased real extractable yield of the pool, the internal yield, which deviates reliance on centralized providers and tends to break the reinforcement cycle. (https://dataalways.substack.com/p/endgame-perils-of-restaking).

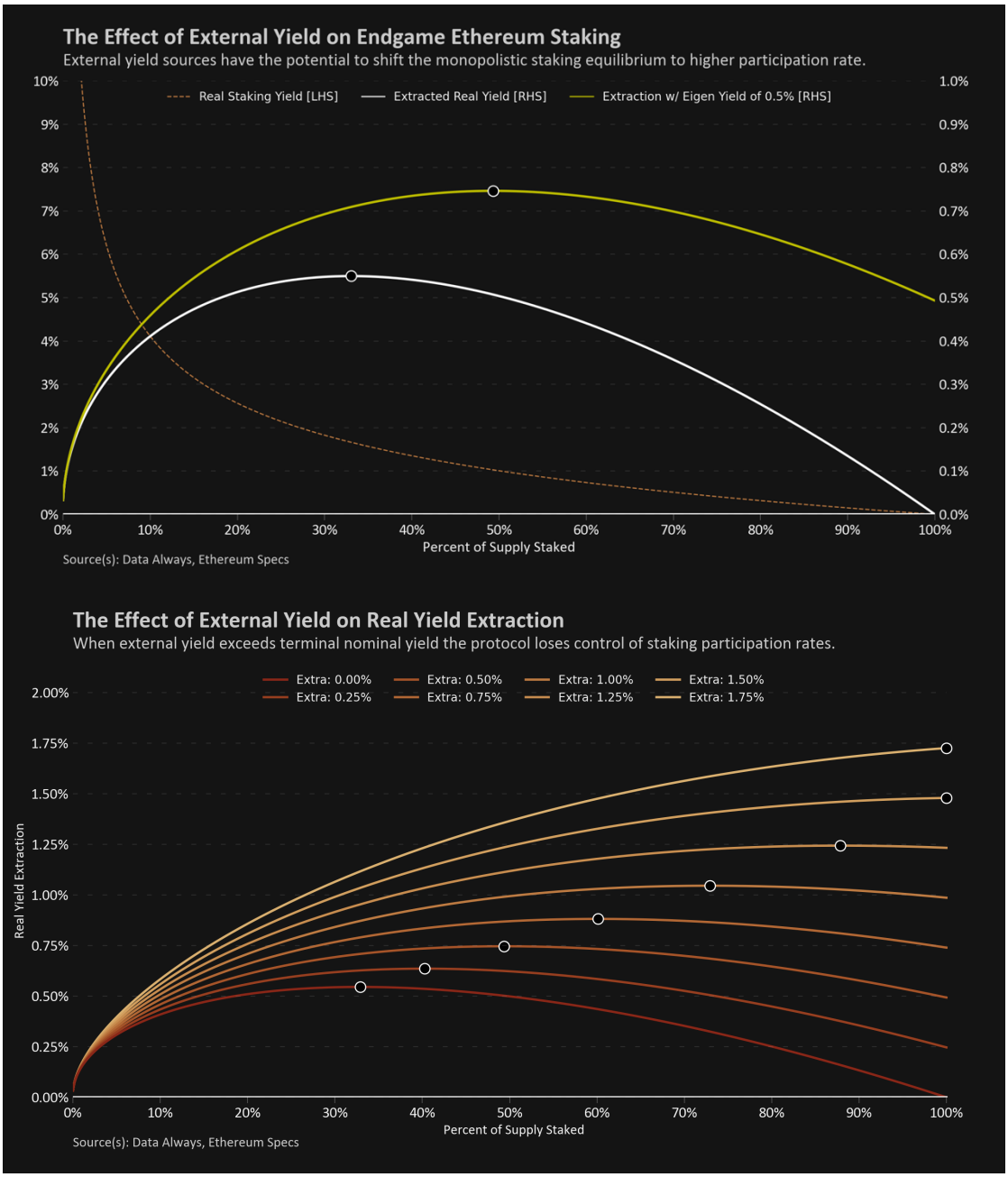


Figure 11: (a.)Real staking yield is stabilized to a lower staking supply against increasing external yield sources, which encourages higher participation rate by shifting staking pool dominance away from centralized monopolies. (b.) The staking equilibrium shifts as external yield surpasses the value of the terminal nominal yield, at which point participation drops. (https://dataalways.substack.com/p/endgame-perils-of-restaking)

The protocol charges fees for staking at 'nominal' terms which may be based on a host of operational costs occurring within the network. As a result of this, there is a disconnect which, when accounting for increased staking participation and concurrently, higher fees, drops the real staking yield. This causes the equilibrium due to monopolistic entities to shift towards lower participation to break even on returns from staking.

ii. Liquidity constraints and volatility:

Liquidity constraints can bottleneck the system as a consequence of stakers attempting to access their funds against a small party of validators or providers. The problem also affects secondary markets as the users constitute the consumer or contributor base of other Web3 applications, especially those which are built on the network in which funds are staked.

Liquidity Fragmentation:

Liquid staking derivatives (LSD) mirroring the value of underlying staked assets currently form an important component of major staking protocols. LSDs allow stakers to earn yield on their staked capital

whilst being able to simultaneously use the derivative assets in DeFi. Centralized protocols like Lido and Coinbase have successfully launched their own LSDs in the past: stETh and cbETH with market cap of $14.6B and $1.3B respectively[10]. The ability to issue LSD could be a major differentiating factor for staking protocols as delegators are disincentivized from delegating to protocols that simply lock up their capital to stake. At the same time, we know that individual node operators or even small staking protocols don't have the requisite liquidity to issue LSDs. In fact, even the biggest protocols often face liquidity crunches (see here). For example, Lido incentivizes liquidity provision through monthly "liquidity and marketing incentives", of which it paid more than $100M in 2022 and is expected to pay $14M in 2023[11]. Deep liquidity is necessary to maintain the peg to the staked asset. Once we establish that decentralization is desirable, we are left with the problem of ensuring individual validators and/or small groups of validators are able to issue LSDs. Without LSDs, users would not have much of an incentive to move towards decentralized solutions. Simply ensuring more and more stakers stake to individual validators to increase their liquidity is not possible since liquidity would be fragmented between thousands of pools. Each pool would also require an equal amount of a paired asset (e.g. ETH) to be used for swaps on DEXs which would be suboptimal as those assets will be locked up in thousands of pools with minimal liquidity. Effective decentralization, then, would require being able to pool the collective liquidity of all the pools to ensure viability of individual validators. Here is where Tenderize steps in.

For a decentralized staking protocol, merely ensuring that provided liquidity is not fragmented is not enough, the problem of mercenary capital needs to be tackled by putting in place proper incentives for liquidity providers to retain their capital in the protocol. The foremost solution to the mercenary capital problem in DeFi is Protocol Owned Liquidity (POL) pioneered by Olympus DAO[12]. Under POL, the protocol sells zero-coupon bonds denominated in the treasury token in the open market to incentivize liquidity provision to the protocol. The bonds are later redeemed at a premium, ensuring LPs are sufficiently rewarded for not moving their capital out of the protocol. This works well in practice; however, POL depends exclusively on external market forces.

Volatility:

There is an inverse between participation in staking and the price of the concerned asset. The motivation behind stakers to flock to more robust, centralized providers has already been discerned to reduced yields long-term, but price change is unaffected directly. In increasing the number of individual investing in an asset, there is a possibility of price increase as purchases grow. Unfortunately, if these purchases are disproportionately facilitated towards staking, observance of the lack of utility is magnified. The direct repercussions of 'Shapella' may also reduce the economic scarcity of an asset in the short-term. Long-term volatility is more evident in the context of staking, while other vectors affect short-term price volatility. By reducing the short-term scarcity further by enabling immediate withdrawals, price volatility short-term is bolstered even further. (https://medium.com/coinmonks/how-to-unlock-the-potential-of-liquid-staking-derivatives-lsds-1e28015008fb)

Part 3A: Tenderize v2 – Infrastructure and Solutions: Tenderize has the potential to remove the very real risks in *Part 2: Hazards of Centralization in Liquid Staking*. Even in the extreme unrealism that such hazards do not come to pass, their motive philosophy aligns closely with the values of the Web3 space and operates pragmatically from the grassroots level.

Tenderize's core architecture is composed of two components, TenderVault and TenderSwap. The two components aim to solve the aforementioned problems of stake centralization and fragmented liquidity, respectively. The Tenderize LST is the WAGYU token, whose value is pegged to the assets staked via growth and adoption of their ecosystem. BeefBank further secures loans via stablecoins by minting BeefBuck tokens in exchange for freezing stake holdings. The Tenderize ecosystem is as follows (*Figure 13*):

3.1A TenderVault:

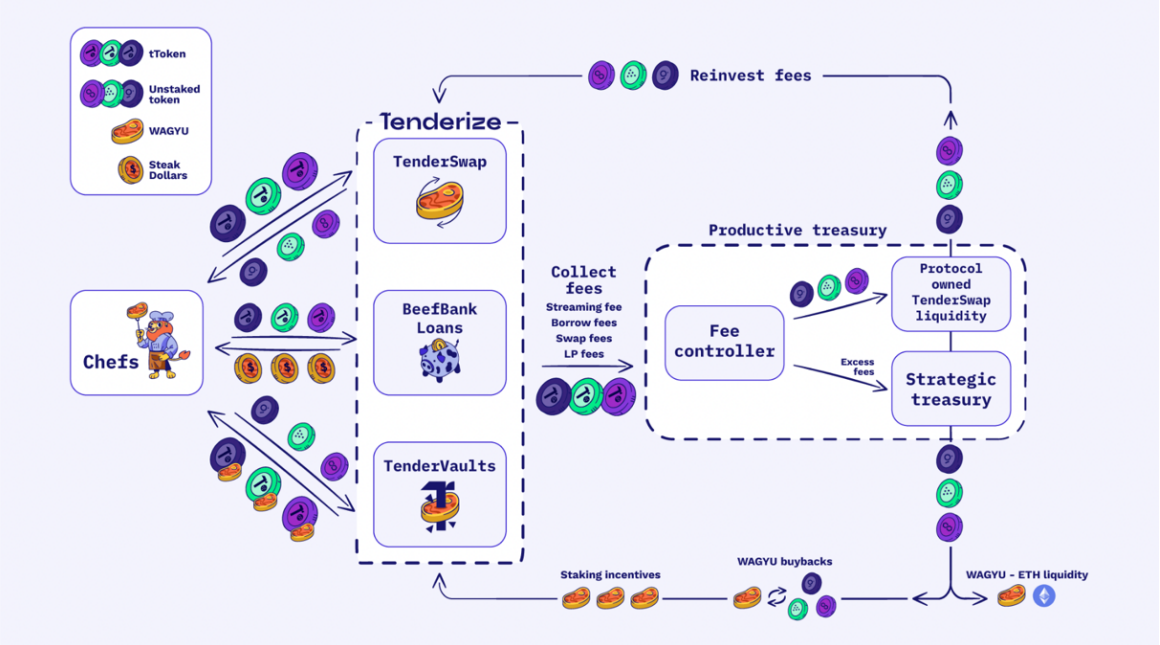


Figure 13: Schematic of Tenderize v2's digital infrastructure for liquid staking across staking for tTokens (TenderVaults), swapping LSTs for immediate unstaking (TenderSwap), and borrowing stablecoins via collateralized LSTs and repayment via derivative rewards(BeefBank).

Tenderize v2 allows free entry of node operators onto the protocol, eliminating the need for validator whitelists that the centralized alternatives require. Delegators are also allowed free entry and exit and can choose to stake to any validator of their choice. The user deposits are staked with the validator, following which the protocol mints an LST equivalent in value to the staked amount. The LST, called TenderTokens (tTokens) are specific to the validator and are similar to Aave's aTokens in that their supply maps the supply of the staked asset to that particular validator 1:1. Supply increases with additional stake and staking rewards and decreases with slashing penalties and/or withdrawal of stake. By allowing every single node operator to issue their own LST, Tenderize bridges the disparity between large, centralized staking protocols and small groups of validators operating independently. Most importantly, Tenderize claims to solve the problem of the socialization of risk in LSDFi. Centralized staking protocols can be thought of as a middleware layer funnelling staked assets from delegators to whitelisted node operators on their network. Stakers to centralized staking protocols exercise no choice over the exact node operator they delegate their stake to. If a node operator engages in malicious behaviour and ends up getting slashed, the whole network bears the brunt of the slashing as the stake is delegated collectively to the whole protocol and not assigned to individual operators. This is what is termed the 'socialization of risk'. Tenderize does away with the socialization of risk. Delegators are offered granular choice of choosing validators they trust with their stake, enhancing not only their agency but also the responsibility of individual validators as slashing drives down their tToken to zero and they cannot divide responsibility amongst the entire validator set.

3.2A TenderSwap:

Tenderize v2 also ensures liquidity split amongst the large number of tTokens is pooled together to enable effective decentralization. This, it achieves through a novel protocol-specific AMM architecture called TenderSwap (See Fig.14). Unlike Uniswap where assets need to be paired (LST and staked asset), TenderSwap functions on a Metapool architecture where sub-pools for every single tToken is paired with the sub-pool for the underlying staked asset. Since assets can be un-staked at any time, Tenderize treats tTokens and the underlying asset as the same, always maintaining a 1:1 peg. tTokens can be swapped in and out of the sub-pools freely. This

way, the protocol ends up with very deep liquidity as the entire Metapool becomes one liquidity pool. Since all the assets are treated as the same, liquidity provision doesn't require providing paired assets and capital can be more efficiently used elsewhere. Tenderize claims this benefits both staking service providers and individual stakers as the former don't have to incentivize liquidity provision whereas the latter enjoys exit liquidity.

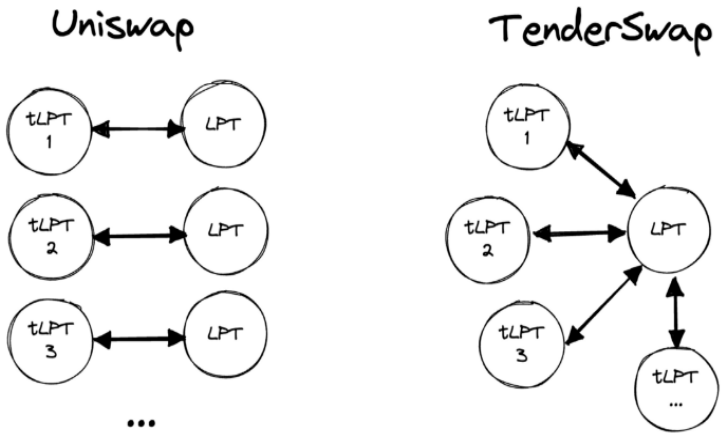


Figure 14: Uniswap vs. TenderSwap architectures.

At any given point, a sub-pool's state can be defined by the record of its assets and liabilities – the available capital to swap and tokens owed to the liquidity providers, respectively. The states of the sub-pools regularly change as assets move in and out. The state of the metapool is defined collectively by the states of every sub-pool. A sub-pool is said to be balanced if its assets exceed the liabilities. Whenever a swap causes an imbalance in a pool whilst the other remains balanced, the metapool is said to move away from optimal state. On the other hand, when a swap restores imbalance in a pool whilst the other remains balanced, the metapool is said to move towards optimum. To ensure the protocol stays close to this optimal state, swappers are charged (the rewards) slippage fees (arbitrage profit) based on whether or not the metapool deviates from optimum. Slippage fees and arbitrage profit are determined by a 'distance compensation function'. For example, if a user swaps 10 tETH for ETH, they receive 8 ETH, paying 2 tETH as a slippage fee. The protocol then must incentivize replenishment of the ETH. The 2 tETH function as arbitrage profit is had, in this case, as a user can deposit 8 ETH to replenish the pool in return for 10 tETH. To this, TenderSwap creates an automated mechanism to ensure constant access to deep liquidity, minimizing the need for central governance.

3.3A BeefBank:

Whilst not integral to the staking protocol itself, Tenderize v2 introduces BeefBank, a borrowing program for depositing tTokens, which act as collateral for minting the stablecoin pegged to USD, known as SteaksDollar.

Part 3B: Solutions Deliberated:

3.1B Solution to Liquidity Fragmentation:

Tenderize has come up with a solution akin to POL, which it has termed 'Autonomous Liquidity Provision' (ALP), which combines both market participation and automated liquidity provision through accrual of fees into the protocol's treasury. The fees that the protocol earns through swaps and as a share of the staking rewards is funnelled directly into the protocol treasury to ensure that there is always a steady stream of liquidity regardless of market dynamics. Holders of Tenderize's treasury token WAGYU would be able to decide on the target liquidity ratio (TLR) they want to maintain. This is the ratio between the amount of the underlying asset as a fraction of the amount staked on Tenderize for that underlying asset.

$$LiquidityRatio = \frac{Tokens_{tenderSwap}}{Tokens_{staked}}$$

A higher liquidity ratio needs to be maintained for volatile market conditions as more people are likely to sell their assets and demand for liquidity of the underlying asset is high. WAGYU holders can respond to lesser volatile conditions by reducing the TLR. The TLR determines which bonds the protocol would need to sell to provision liquidity. When the liquidity ratio is less than TLR, they can sell discounted tToken bonds in return for the underlying asset. Since fee accrual also leads to added liquidity for the underlying asset, this would suffice in most cases. However, the protocol might also sell WAGYU-denominated bonds on the open market to achieve the TLR. In the opposite case of the liquidity ratio being higher than TLR, inverse bonding will occur with the protocol selling bonds denominated in the underlying asset. This would allow WAGYU holders to capture a profit whilst increasing the capital efficiency of the underlying asset, otherwise locked up in the protocol.

3.2B Enabling DeFi Use Cases:

Liquidity provision bereft of fragmentation and secured by backstops opens up DeFi use-cases for delegators. Although not integral to the staking service itself, Tenderize v2's stablecoin lending solution BeefBank aims to take advantage of the deep liquidity it expects to procure. BeefBank allows users to deposit tTokens as collateral to avail over-collateralized loans denominated in Tenderize's own stablecoin termed 'Steak Dollars' (SD). Tenderize claims SD to be "the first of a kind decentralised stablecoin backed by a basket of various liquid staked assets". Users are able to open Collateralized Debt Positions (CDP) which increases the SD supply to the tune of the borrowed amount and which contracts the supply once the loan is repaid. Stablecoin lending could initially drive users to the protocol as Tenderize offers a clear advantage over other small-cap LSDs which cannot be used as collateral in DeFi. In addition, as the collateral is itself earning yield, the yield can be programmed to enable further use-cases. A potentially useful case is that of yield-bearing stablecoins as the collateral above the required ratio or the risk appetite of the borrower can be used to mint SD which is paid to the borrower. The yield generated in tTokens can also be swapped with SD to create auto-repaying loans. A final use-case is that of flash repay – similar to Aave's flash loan liquidations allowing arbitrageurs to borrow the required capital to pay off the loan, receive the collateral in return and sell the required repayment amount for the borrowed asset to complete the flash loan, all in a single transaction. This allows arbitrageurs to profit whilst the protocol avoids bad debt.

3.3B Risks:

The primary risk associated with Tenderize is that while it allows decentralized, small-scale node-operators to onboard onto the platform and avail the benefits of pooled liquidity, it doesn't prevent node operators from colluding to operate like a cartel. In simple terms, while decentralization is possible through Tenderize, centralization is not deemed impossible.

To identify the potential risks to the protocol, we first need to make some reasonable assumptions. Let us assume that there already exists a centralized entity, CEN, which controls more than a third of the total staked volume of a token that Tenderize offers. Let us term the token, STK. The threshold of 1/3 is chosen because it is a significant threshold in PoS chains like Ethereum as the centralized entity can collude to prevent blocks from finalizing and therefore exert indirect censorship control. This is possible, for example, through refusing to finalize blocks which include transactions of certain kinds, a virtual veto that the entity holds. Now let us assume that the vast majority of the delegators prioritize yield generation over respect for decentralization. This can certainly be held true up until the point cartelization doesn't initiate a demand for a hard fork of the Ethereum protocol. Finally, we can assume that the vast majority of the delegators do not have knowledge about trustworthiness of individual validators beyond the yield they are able to generate.

Tenderize claims that the individualization of risk it offers is an advantage it has over CEN. Individual delegators on Tenderize do not get punished for the malicious activity of nodes they do not delegate their stake to. However, as it is extremely difficult for any delegator to establish the trustworthiness of an individual node operator (it requires time and effort and sufficient information about the operator might not even be public), there isn't much of an actual difference between CEN and Tenderize on this front. From a delegator's perspective, delegating its stake to a validator through a centralized entity is largely the same as 'choosing' the validator to stake to through Tenderize. Socialization of risk, then, becomes a positive as the risks are spread across the validator set; however, in Tenderize, delegators who cannot establish credibility of its validator lives in constant fear of staked assets being zeroed.

In such a situation, let us assume that CEN offers a 5% APY to its delegators. Since our assumptions lead us to conclude CEN outcompetes Tenderize on the capital risk front and delegators do not care about the decentralization of the protocol as long as they are compensated with yield on their stake, it can be argued that Tenderize can only support validators which offer a higher yield than CEN. Moreover, since CEN can engage in indirect censorship driving yields up, the 5% APY would be higher than yields for the vast majority of individual or small groups of validators. Therefore, Tenderize would only be able to support a very small number of node operators on its platform.

The components of higher yield can either be more efficient MEV-extraction or lower fees that the delegators charge since it is extremely difficult to outperform a centralized entity able to censor the blockchain. MEV-extraction is a very competitive market and the improved techniques can be caught on by CEN to drive the difference between CEN and Tenderize validators down. Fees charged for validating seems to me to be the only viable way this could be achieved. At the same time, Tenderize protocol can only support staked assets that the collective node operator infrastructure is able to support. Since they are generating higher yields, there will be demand in the market to delegate more staked assets to Tenderize's validator set. Consequently, validators would want to enhance their infrastructure capabilities to fulfil the demand.

Therefore, we have a small group of node operators charging minimal fees from delegators each wanting to expand their node operation. In this case, let us assume that there is a minimum fee level for this set of operators. If one node operator starts charging lesser fees than the previous minimum level, it can generate the highest yield for the delegators, driving the demand for it to expand its infrastructure capabilities to accommodate more stake. This node operator can avail credit from the market to do so in the hope of the liquidity getting concentrated on its nodes. If the node operator is somehow able to capture enough liquidity to generate its required level of profit with the minimum fees it charges, it could become a centralized Tenderize since it would be the only viable node operator on the protocol. This situation is however unlikely, since other node operators will also start charging lesser fees if one of them does. If multiple nodes were to follow what a single node did, they would end up in a worse situation than if only the single node lowered its fees. That is because liquidity will again be fragmented between multiple nodes, which will most likely not be able to amortize the loss inflicted by lowering fees. Also, the terms of credit will be relatively unfavourable as chances of a single node succeeding reduce with the number of competitors.

Therefore, it would not make sense for node operators to lower the fees below the 'minimum level'. The only way for the node operators to continue to profit is for all of them to charge the same fees. As we have assumed the node operators are decentralized, it is not an easy objective. Coordination, however, could still be achieved as there exists strong incentives to do so. More favourable credit terms for improving infrastructural capabilities can be availed by a group of validators than individuals separately. The group could also split other fixed capital costs using their collective bargaining power in the open market. Since we have already established the group comprises of a very small number of node operators, coordination is a real possibility. Finally, the long-run viability of even this cartelized version of Tenderize as an alternative to CEN depends on whether they are able to operate with lower fees in the long run, failing which Tenderize would end up duplicating CEN.

Part 4: Tenderize Business Development

4.1 Venture Seed

As of 7th July 2022 (*CryptoRank*) Tenderize has a total raise of $3 million across 7 investors in 1 seed round. Formally founded in 2020, Tenderize Labs Ltd. is funding led by Eden Block, signed by partner Dermot O'Riordan on the 7th August. His partner investments number nine and his focus has been primarily on the DeFi and data infrastructural development of Web3. The ethos of Tenderize may be benefited by his additional focus in improving governance systems for digital communities, including via DAOs. As has been iterated earlier, DAOs may indeed pave the way forward for anti-censorship boundaries in centralized staking networks, not only in contract, but in alienation from governmental overstep. Other investors include Figment and Encode Club (most recent), preceded by TRGC, Omni, Livepeer, and Daedalus Angel Syndicate (*CrunchBase*). A year has passed since this funding round concluded, during which the Tenderize v2 launch has been prepared. It's updated liquid staking protocol is set to go live on Arbitrum and Ethereum, this October 2023.

4.2 Competitors

Tenderize is in competition with 42 currently active companies and ranks 6th among them (*Tracxn*). Of these competitors, 9 have undergone funding and pose the greatest rivalry. The top 3 are Lido (Finland), P2P (George Town, USA), and Swell Network (Sydney, Australia). Lido has been funded $72 million, after which it has succeeded in managing over 32% of staked ETH. The Lido DAO Token itself holds a market cap of $1.38 billion, indicating a high degree of competitive control. Collectively, the listed competitors are funded $121 million from 10 funding rounds, with 3 of the top 10 occupying Series A. Tenderize is labelled with a growth score of 94/100, overtaking all except Lido, whose score is 97/100 even at its current state of incumbency.

4.3 Initial Projections

From a business point of view, Tenderize may be considered disruptive enough, given its individual-level decentralization, to potentially siphon a sizable proportion of the market's validator nodes, including those currently centralized by Lido and others. This may be achievable from purely the philosophical merit of Web3 decentralization, so long as the efficacy of Tenderize v2 matches or surpasses that of its competitors. It is worth waiting to observe the October roll-out on Arbitrum and Ethereum, finishing an analysis of Q4 2023 so as to evaluate its performance. If a robust bull market were to take place, may be that new incoming stakers will produce an influx that continues to approach centralized solutions, given their lower barrier to entry and ease of use. Despite this, it may be likely that such an influx will also include a fair share of new stakers who would be willing to approach Tenderize. Given the banking failures and crypto exchange fiascos of 2020 – 2022, the aforementioned philosophical credence to veer from centralized solutions may work in Tenderize's failure. This sense is generally stronger in a Web3 bull market as many believe that reduced faith in centralized systems is what has led to current upturn in Web3. CEO of Tenderize, Alec Shaw, said this: "Tenderize empowers users to stake their assets with confidence, knowing that they retain custody and are making the underlying network more

decentralized. Users join a grassroots movement which values decentralization and security in parallel with financial returns."

The mechanics of settlement are impacted in most centralized systems as the intermediary adds multiple layers of internal processing before connecting the user to the buyer/seller. In staking, settlement insurances can therefore be pinned on the whims or abilities of the entity, which reduces confidence in the possibility that transaction attempts will not bounce back. Meanwhile, delegated Proof-of-Stake alternatives allows validator selection based on the parameters of their staking pool. That differentiation increases competitiveness and increases diversification of the staked portfolio. In centralized systems,

Staking Revenue

	TVL	Gross Staking revenue	Steaming Fee	Tenderize revenue
Launch	$20,000,000.00	$1,355,450.00	0.5%	**$6,777.25**
Year 2	$450,000,000.00	$31,054,500.00	0.5%	**$155,272.50**
Year 3	$4,500,000,000.00	$303,030,000.00	0.5%	**$1,515,150.00**
Year 4	$14,000,000,000.00	$780,030,000.00	0.5%	**$3,900,150.00**

CDP Revenue

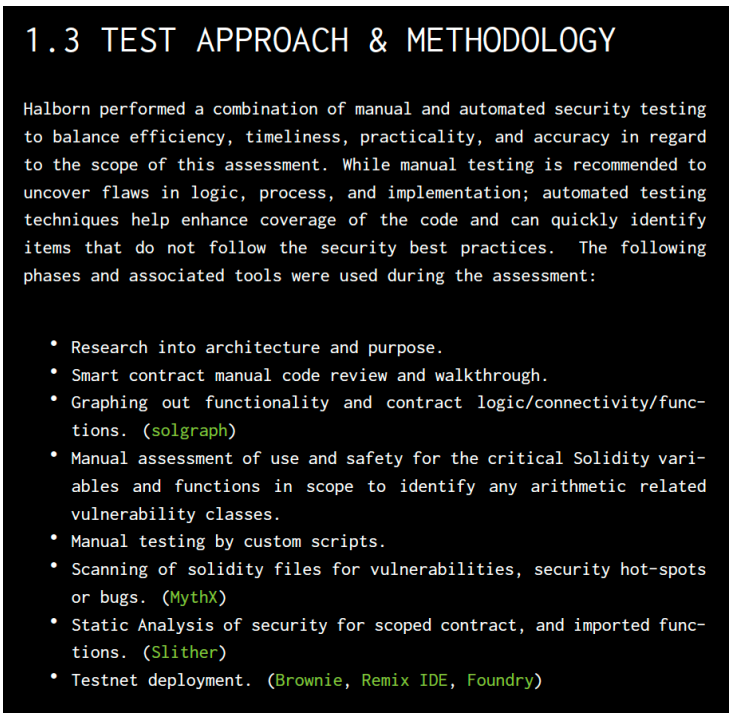
	TVL	Borrow Fee	Loan To Value	Tenderize Revenue
Year 2	$450,000,000.00	0.5%	30%	**$675,000**
Year 3	$4,500,000,000.00	0.5%	30%	**$6,750,000**
Year 4	$14,000,000,000.00	0.5%	30%	**$21,000,000**

Figure 15: Revenue generated by Tenderize has shown marked increase across all areas.

As of Q3 2023, the Top 35 PoS assets have a market capitalization of over $279 billion, $71 billion of which are staked. Staking yield has decreased by 100bps to 10.6%, even as the average staking rate increased by 460 bps to 49.3%. There does indeed seem to be a grassroots momentum to staking despite steady decrease in yield. Much of this has been attributed to the drop in MEV and transaction activity operations, the former of which has come to be seen as another example of centralization in Web3. Despite decreases in yield, Ethereum-based annualized rewards in staking increased 800 bps, assimilating 44% of the Proof-of-Stake market. The demand has naturally been bolstered following Ethereum's 'Shapella' Upgrade in Q2, for which withdrawal functionality has been enabled.

4.4 Technical Audit of Tenderize v2:

In August 2023, Halborn released the 'Tenderize - v2 Smart Contract Security Assessment', identifying potential security issues with architecture. Few concerns were identified and all were fully resolved by Tenderize. Test approach and methodology: ('Tenderize - v2 Smart Contract Security Assessment' -Halborn (August 1st – 29th, 2023):



1.3 TEST APPROACH & METHODOLOGY

Halborn performed a combination of manual and automated security testing to balance efficiency, timeliness, practicality, and accuracy in regard to the scope of this assessment. While manual testing is recommended to uncover flaws in logic, process, and implementation; automated testing techniques help enhance coverage of the code and can quickly identify items that do not follow the security best practices. The following phases and associated tools were used during the assessment:

- Research into architecture and purpose.
- Smart contract manual code review and walkthrough.
- Graphing out functionality and contract logic/connectivity/functions. (solgraph)
- Manual assessment of use and safety for the critical Solidity variables and functions in scope to identify any arithmetic related vulnerability classes.
- Manual testing by custom scripts.
- Scanning of solidity files for vulnerabilities, security hot-spots or bugs. (MythX)
- Static Analysis of security for scoped contract, and imported functions. (Slither)
- Testnet deployment. (Brownie, Remix IDE, Foundry)

Due diligence on part of TRGC and fellow portfolio company Halborn was completed in the form of the complete technical audit, from which minimal risk was discovered. These risks founded in Tenderize v2's programming robustness were immediately resolved, maintaining its promise. It's current technical outlook is sound and it is believed that its security and ability to execute smart contracts will be both compliant and reliable, operationally.

SECURITY ANALYSIS	RISK LEVEL	REMEDIATION DATE
(HAL-01) ONLY ONE UNLOCK OR WITHDRAW IN EVERY UNLOCK PERIOD ALLOWED	Critical (10)	SOLVED - 09/07/2023
(HAL-02) REGISTRY INITIALIZATION CAN BE FRONTRUN	Low (4.1)	RISK ACCEPTED
(HAL-03) INCONSISTENT PARAMETER NAMING CONVENTION	Low (2.5)	SOLVED - 09/07/2023
(HAL-04) CONTRACT PAUSE FEATURE MISSING	Low (2.5)	RISK ACCEPTED
(HAL-05) INCOMPLETE NATSPEC DOCUMENTATION	Informational (0.0)	ACKNOWLEDGED
(HAL-06) INCORRECT METADATA KEY	Informational (0.0)	SOLVED - 09/07/2023
(HAL-07) THE UNLOCK() FUNCTION DOES NOT RETURN TOKENID	Informational (0.0)	ACKNOWLEDGED

Part 5: Conclusion

To reiterate Tenderize's goal - "a new liquid staking protocol that delivers liquidity for staked assets without centralizing of the underlying validator set". The statement needs to be qualified in light of the above discussion. Tenderize does contain inherent risks which can lead its validator set to become centralized. However, going back to our assumption that delegators will move away from high-yield centralized services if the threat of a hard fork is real, we can say that the scope of the centralization is limited. If CEN or a cartelized version of Tenderize gains control over a quantity of STK above a critical consensus threshold and chooses to act maliciously to drive up profits, liquidity could move to lower-yield node operators on Tenderize. This would not be reasonably expected from delegators in any other situation. Thus, to conclude, Tenderize can be thought of as a circuit breaker in LSDFi which through its incentives for decentralized node operators, prevents the blockchain secured by the underlying stake from hard forking and user-deposited capital to dissipate. Centralization that doesn't pose such threats is not only possible but highly likely.

*The risks and vulnerabilities are not attributed specifically to Lido or any particular staking protocol. Instead, the general case of a centralized staking protocol has been discussed.

CITATIONS:

1. https://dune.com/hildobby/eth2-staking
2. https://github.com/djrtwo/writing/blob/main/docs/2022-05-30_the-risks-of-lsd.md
3. See 1.
4. https://www.sec.gov/news/press-release/2023-25?ref=bankless.ghost.io
5. https://www.bankless.com/sounding-the-lido-alarm
6. See 1.
7. See 5.
8. https://dune.com/vinc/lido-dao
9. See 2.
10. https://coinmarketcap.com
11. https://research.lido.fi/t/lido-v2-may-1-2023-december-31-2023-lido-ongoing-grant-request/4476
12. https://docs.olympusdao.finance/
13. 'The State of Staking' – Q3 2023 report at staking.staked.us
14. https://hackmd.io/@lido/BJKmFkM-i
15. https://messari.io/report/evaluating-validator-decentralization-geographic-and-infrastructure-distribution-in-proof-of-stake-networks
16. 'Quantifying Decentralization' -Balaji S. Srinivasan (published: https://news.earn.com/quantifying-decentralization-e39db233c28e)
17. https://medium.com/hashed-official/a-dive-into-eth-liquid-staking-node-operators-shanghai-future-innovations-and-dvt-523e275a467c
18. https://zkvalidator.com/why-does-the-location-of-your-validator-matter/#:~:text=A%20high%20concentration%20of%20validators,gain%20control%20over%20the%20network.
19. https://docs.ssv.network/learn/readme
20. https://ethereum.org/en/staking/dvt/#:~:text=Potential%20drawbacks%20of%20using%20DVT,-Additional%20component%20%2D%20introducing&text=Potentially%20increased%20latency%20%2D%20since%20DVT,can%20potentially%20introduce%20increased%20latency.
21. 'U.S. Federal Securities and Commodity Law Analysis of Liquid Staking Receipt Tokens' – Proof of Stake Alliance
22. 'The economics of liquid staking derivatives: basis determinants and price discovery' -Scharnowski and Jahanshahloo. Feb. 2023
23. 'The Principal-Agent Problem in Liquid Staking' -Tzinas and Zindros. May 2023.
24. Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure -Michael C. Jenson and William H. Meckling
25. 'The Silicon Valley Bank (SVB) Collapse and Implications for Business' –The Conference Board, 15 May 2023.
26. 'Liquid Staking Research Report: Implications of Proof-of-Stake Assets in Decentralized Finance' -Chorus One (2023).
27. https://medium.com/coinmonks/how-to-unlock-the-potential-of-liquid-staking-derivatives-lsds-1e28015008fb
28. https://coinwire.com/tenderize-launching-live-on-polygon-to-unlock-liquidity-for-web3-staked-assets/
29. https://inc4.net/staking-as-a-service-explained-pros-cons-and-popular-platforms/
30. https://messari.io/report/what-s-at-stake-in-staking-as-a-service

31. https://www.forbes.com/sites/emilymason/2021/07/01/jpmorgan-says-ethereum-upgrades-could-jumpstart-40-billion-staking-industry/?sh=2bd4077c1512
32. https://www.crunchbase.com/organization/tenderize
33. https://cryptorank.io/ico/tenderize
34. https://menafn.com/1106780800/Introducing-Tenderize-V2-Addressing-Centralization-Challenges-In-Liquid-Staking
35. https://menafn.com/1106780800/Introducing-Tenderize-V2-Addressing-Centralization-Challenges-In-Liquid-Staking
36. https://www.coindesk.com/consensus-magazine/2023/09/05/explaining-ethereums-risk-free-rate-of-return/
37. https://www.forbes.com/sites/tomerniv/2023/08/21/4-liquid-staking-startups-that-are-unlocking-ethereums-potential/?sh=2835e4aa7793
38. https://www.bitcoinmarketjournal.com/sector-report-liquid-staking/
39. https://www.nasdaq.com/articles/liquid-staking-in-crypto%3A-how-it-transforms-defi-investments
40. https://blog.ethereum.org/2015/06/06/the-problem-of-censorship
41. https://cointelegraph.com/news/how-liquid-staking-can-potentially-harm-the-ethereum-ecosystem-hashkey-report
42. https://news.bitcoin.com/proof-of-work-proponents-question-validator-censorship-as-59-of-staked-ethereum-is-held-by-4-companies/
43. Parma Bains, Blockchain Consensus Mechanisms: A Primer for Supervisors, International Monetary Fund (Jan. 2022), available at https://www.imf.org/-/media/Files/Publications/FTN063/2022/English/FTNEA2022003.ashx.
44. 'Digital Assets: Consultation Paper" – Law Commission (2022).
45. https://consensys.net/blog/news/liquid-staking-needs-clear-tax-rules-the-uk-shows-a-possible-way-forward/
46. 'Tenderize - v2 Smart Contract Security Assessment' -Halborn (August 1st – 29th, 2023).
47. REGULATION (EU) 2023/1114 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937
48. Consultation Paper Technical Standards specifying certain requirements of the Markets in Crypto Assets Regulation (MiCA) – European Securities and Markets Authority(12 July 2023)
49. 'Staking Pool Centralization in Proof-of-Stake Blockchain Network', (2020). -Ping He, Dunzhe Tang, and Jingwen Wang. https://ssrn.com/abstract=3609817 or http://dx.doi.org/10.2139/ssrn.3609817
50. https://river.com/learn/proof-of-work-pow-vs-pos-proof-of-stake/#:~:text=Proof%2Dof%2DStake%20systems%20are,than%20labor%20and%20cheap%20energy.
51. https://www.coindesk.com/layer2/2022/04/20/is-ethereum-staking-pool-lidos-growth-an-omen-of-centralization/
52. https://dataalways.substack.com/p/endgame-perils-of-restaking
53. https://ethresear.ch/t/circulating-supply-equilibrium-for-ethereum-and-minimum-viable-issuance-during-the-proof-of-stake-era/10954
54. 'The economics of liquid staking derivatives: Basis determinants and price discovery', (2022). -Scharnowski and Jahanshahloo. http://dx.doi.org/10.2139/ssrn.4180341