ClayStack Ethereum Liquid Staking: Decentralized, Secure, and Highly Scalable

Mohak Agarwal, ClayStack

Abstract

The ClayStack protocol is a dedicated proponent of the growth and progression of the Ethereum liquid staking industry. ClayStack endeavors to establish an inclusive, secure, scalable, highly decentralized, and censorship-resistant architecture that will catalyze liquid staking adoption and propel it into the mainstream of the ecosystem. We posit that the Ethereum ecosystem is presently bereft of the requisite resources to onboard the next billion users, primarily due to the centralization of stake. Albeit with the activation of withdrawals, the majority of ETH stake has not been redeposited, instead, there has been a marked rise in the number of validator nodes on Ethereum and an increase in the amount of ETH that is being channeled into available liquid staking solutions. Sadly, however, due to the lack of promising liquid staking protocols that uphold security and decentralization, users' options for liquid-staking their assets are highly limited. One of the main reasons why most existing protocols aren't able to solve these burning problems is because of the billions of dollar's worth of ETH that is already staked with them. This inability creates an exponential amount of technical debt on the protocols to change their existing systems. We contend that this poses huge centralization risks to Ethereum and - unless this is solved immediately - it hinders its growth. ClayStack introduces a novel liquid staking architecture for Ethereum that upholds the highest standards of security and decentralization, while offering an intuitive user experience. It offers an unparalleled solution to users by enabling the running of a validator node on Ethereum with a much lower barrier to entry, while upholding the highest standards of security. Moreover, it aspires to assist stakers by maintaining the most stringent standards of decentralization and security for csETH, the liquid staking token (LST). In this paper, we undertake an analysis of ClayStack 's Ethereum liquid staking protocol to comprehend how it advances the Ethereum staking ecosystem, and endows it with the necessary tools to onboard the next billion users.

Reflecting on Ethereum staking

Currently, the amount of staked stands at a 17.66%, which is a marked increase from the amount of ETH that was staked prior to withdrawals being enabled. Clearly, prior to the upgrade, a wide spectrum of users were likely to refrain themselves from participating in staking because it wasn't possible for them to withdraw their assets.

Even the Shapella upgrade had a wide spectrum of users prophesying the fate of Ethereum once it happens. While there were people on both spectrums, we took particular interest in those who predicted a mass exit of ETH and validators from the ecosystem post the upgrade. Unsurprisingly, however, all of them were proven wrong. While there were certainly outflows from the network, the fact that the Entry Queue ballooned while the Exit Queue dried up proved to be testaments to users' evolving attitudes towards Ethereum. The enabling of withdrawals marked a crucial closure to Ethereum's transition to PoS and unlocked the possibility for users to truly partake in the benefits of a PoS network. We assert that this upgrade was a good litmus test to examine how users' liquid staking preferences have changed over time. Now, there is an abundant emphasis on decentralizing stake to keep the network secure; while earlier, users flocked to protocols that were the most-well-known.

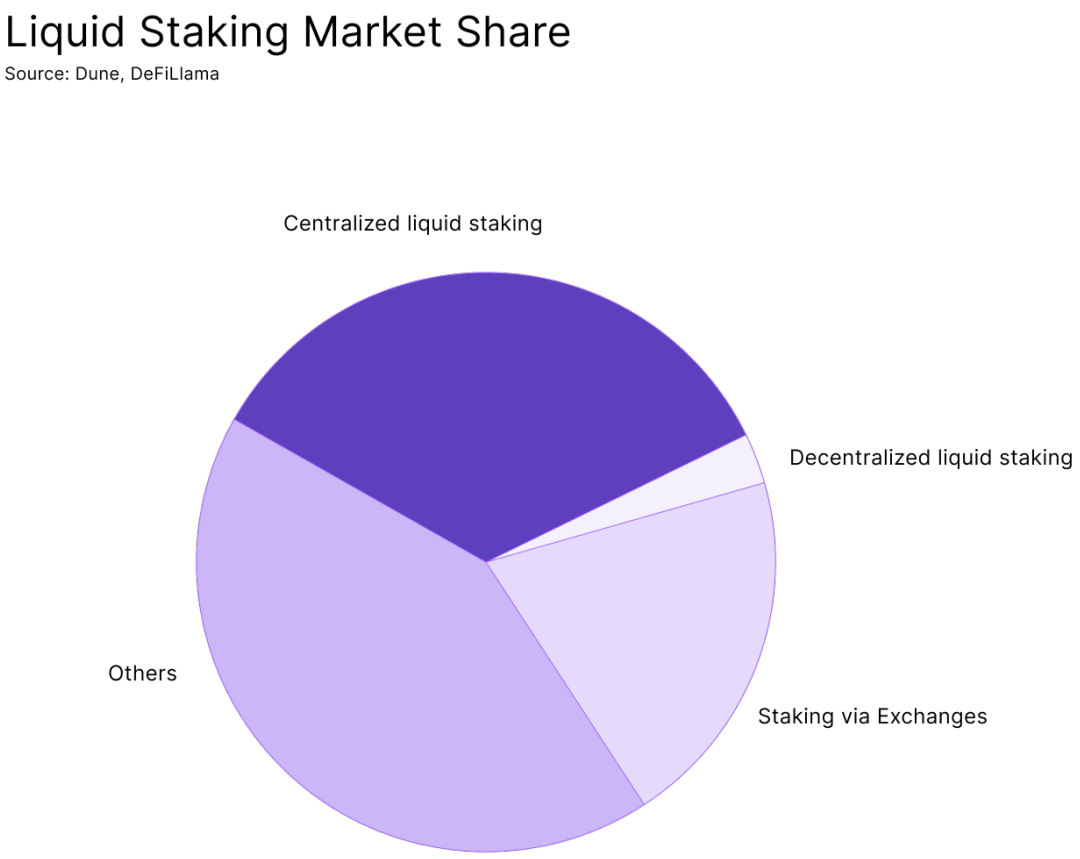
Most of the Ethereum that was withdrawn (either as rewards or even the principal) has now flown back into the network - either as stake into liquid staking protocols or users have spawned new validators nodes on the network. While the resilience of the network is certainly increasing as the number of validators increase consistently, there is an alarming trend of stake flowing back into centralized entities (such as centralized liquid staking protocols).

LSD	Inflow	Principal Outflow	Rewards outflow	Net inflow
Lido	593,056	0	-280,805	312,251
Rocket Pool	206014	-29247	-14906	161861
Frax Finance	69312	-384	-1492	67436
Stafi	160	-448	-254	-542
Harbour	800	0	-195	605
Swell	13312	0	-15	13297
Stakewise	3264	0	-2696	568

CEX	Inflow	Principal Outflow	Rewards outflow	Net inflow
Coinbase	224672	-298784	-163762	-237874
Kraken	83136	-562783	-114934	-594581
OKX	113792	-9824	-5758	98210
Huobi	32448	-59616	-11414	-38582
Binance	319904	-203648	-93953	22303

Staking Pools	Inflow	Principal Outflow	Rewards outflow	Net inflow
StakeFish	32384	-25248	-24507	-17371
Staked.us	161888	-59710	-30211	71966
Figment	147200	-82304	-14825	50071
P2P	126432	-2176	-382	123,874
Kiln	267264	-288	-1181	265795
MyEtherWallet	1664	-5726	-2035	-6098
InfStones	3840	-6976	-647	-3783

This is pernicious to the entire ETH staking ecosystem. The following chart perfectly captures the existing state of stake distributed across the Ethereum network via different entities.



*Note: The figures for the above chart were updated as of writing this litepaper. Please refer to the sources mentioned for real-time updates.

It’s not just the limited centralized entities through which stake gets deposited is the concern. The problem lies in the limited set of node operators that these entities have. The largest liquid staking protocol on Ethereum also has just a limited set of node operators. Not only does this create systemic risks for Ethereum, but it also creates problems around censorship. A limited node operator set creates problems for the entire DeFi ecosystem. Let’s understand how.

Systemic risks to Ethereum

One of the biggest persistent risks with a centralized staking ecosystem is the systemic risk to the entire DeFi ecosystem. This is particularly felt when a single protocol is dominant over the entire DeFi ecosystem. Any risk that isn’t mitigated at the protocol level would then spill over to the entire network leading to huge systemic risks - this can even reduce the amount of ETH staked within the network in a crisis. This can further induce a lot of bank-run scenarios where several users panic-exit the system. The impact of such an event would domino into the whole of DeFi, causing a cataclysm that would damage all the applications where the LST tokens are being utilized.

Challenges with current LST implementations

One of the biggest challenges with staking via the existing liquid staking protocols is the economic (along with that of having the requisite technical knowledge) barrier to entry (the amount of ETH bond they must deposit) to run a validator node. There have been attempts at reducing the minimal capital required to participate in Ethereum network as a validator: for instance reducing it from 32 to 8 ETH, we contend that that is still a sizeable amount for a majority of validators. This means that a majority of the ETH is then staked via a limited/centralized set of institutional node operators, further leading to centralization of the stake itself. The centralized set of node operators that operate for a variety of liquid staking protocols thus reduce the censorship-resilience of the underlying network.

Censorship resistance

The under-discussed aspect that significantly contributes to the centralization debate revolves around the presence of a centralized group of node operators. When top staking entities share common node operators, it creates an additional vulnerability. Consider the scenario where multiple node operators collude or are compelled to cease operations by their respective governments. A clear instance of this occurred when Kraken, a centralized exchange, was compelled to halt its staking services. While one may view this incident favorably, given that it affected a centralized exchange, it serves as a reminder that this situation can impact node operators across various protocols.

One of the biggest risks with centralized exchanges offering staking services is the storage of both validator and withdrawal keys. One assumption behind that is the storage of these keys are determined by an agreement between the exchanges and the node operators. The top centralized exchanges are expected to undertake the highest security measures to ensure that the keys are stored securely. That said, these secure storage options are also highly centralized, which reintroduces these risks. In an instance where the node operators' keys are compromised, it jeopardizes the entire staked balance, rendering the exchange incapable of fulfilling users' redemption requests.

The second risk pertains more to the regulatory risks associated with such exchanges offering staking services. This is a ubiquitous concern that results out of the regulatory ambiguity around staking.

It is crucial to differentiate a staking account from a deposit account, as the former lacks a debt relationship and does not involve the immobilization of funds. Banks directly finance interest payments in deposit accounts. In contrast, PoS consensus mechanisms distribute rewards to validators based on their stake, which is subsequently shared among all stakers. Furthermore, staking differs from lending or borrowing arrangements since it does not involve a counterparty. One perspective is to view them as managing pooled assets on behalf of the node operators, who, in this case, could be centralized exchanges. However, this could be countered by the fact that validators solely adhere to the protocol's rules. The question then arises: do node operators possess control over staked funds due to their custody of validator keys?

Consequently, regulators can exert pressure on centralized entities to comply with laws, with non-compliance potentially resulting in forced shutdowns, similar to the situation with Kraken. This reduces the fault-tolerance of the overall architecture and opens users to additional risks of censorship - depending on the geography of the node operator.

Moreover, there is uncertainty regarding whether staking risks, such as slashing, are adequately addressed in this context. Consider the potential consequences of a slashing event. Who bears the financial burden in the case of a centralized exchange?

The answers to most of these questions always remain enveloped in intrigue because of the ambiguity around how these exchanges operate their staking services

Ethereum lacks the fuel to onboard the next billion validators

If the current state of Ethereum is stretched out into perpetuity, then it lacks the firepower to onboard the next billion users. We contend that this is because of a lack of superior liquid staking architecture that can compete with the centralized options that exist today. Moreover, the existing liquid staking protocols will find it challenging to make significant changes in favour of decentralization and scalability because of the billions of dollars of ETH that are already staked with them. Thus, while the existing decentralized liquid staking protocols do make attempts at scalability and the centralized protocols make attempts at decentralization – none of these protocols can achieve both at the same time.

While finding a one-size-fits-all solution for all the staking problems of Ethereum is near-impossible, there is a strong need for constant reiteration to solve the existing problems of stake centralization and lack of censorship-resistance.

This is where ClayStack's Ethereum liquid staking comes in.

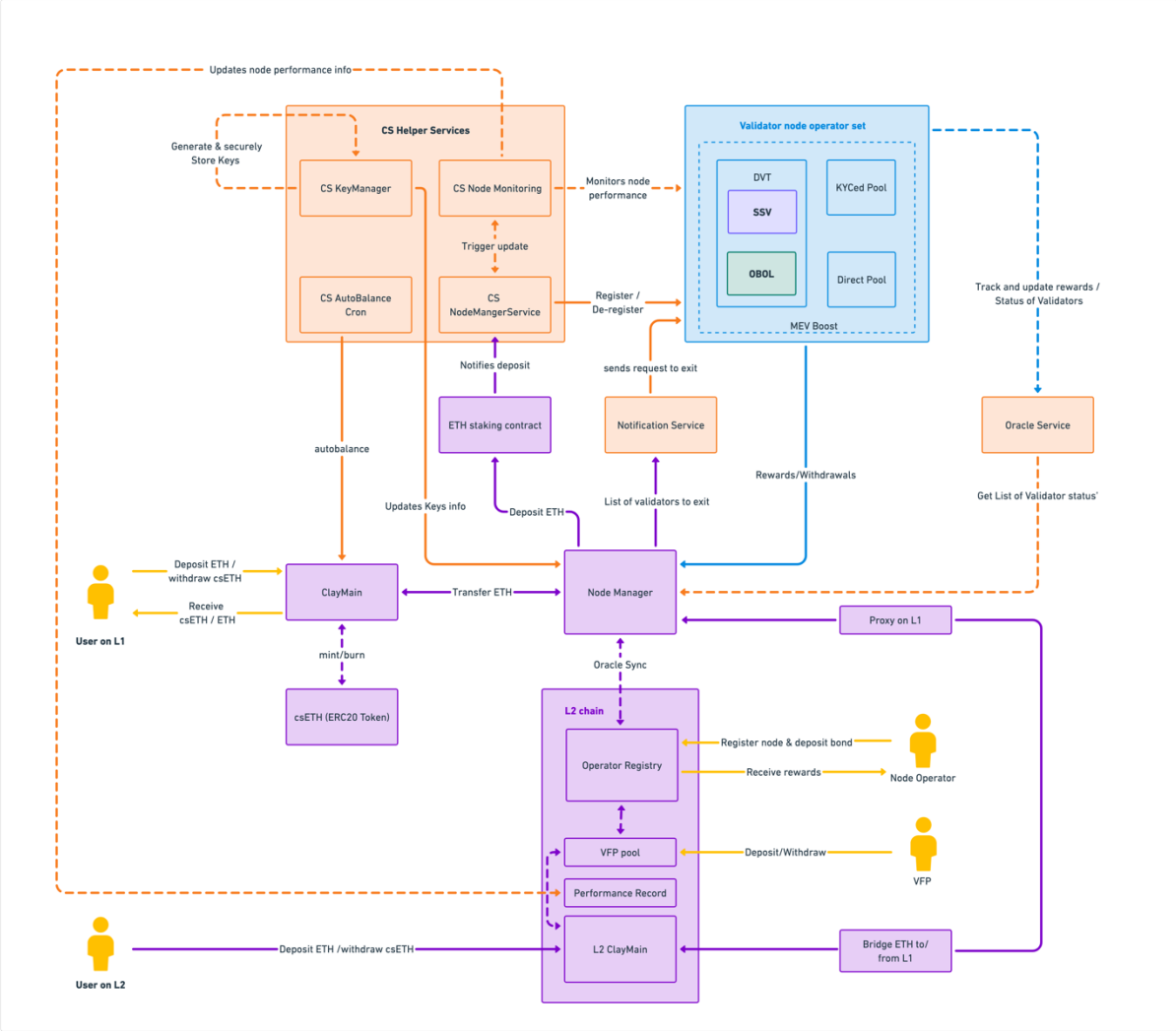
Enter ClayStack

ClayStack has been devotedly aligned with the core ethos of Ethereum i.e., of building a highly decentralized and secure architecture. The ClayStack Ethereum protocol introduces modularity to the liquid staking ecosystem to incentivize accelerated stake diversification. ClayStack's csETH (the liquid staking token) is the product of years of effort of finding a viable solution for Ethereum that offers decentralization and security at the same time, while offering highly superior returns to both validators and stakers.

Our vision with Ethereum liquid staking is to transition the bond requirement for joining the Ethereum to so low that anyone with the technical understanding and will can join and secure the network. This is an extension of our long-term vision to keep the Ethereum network decentralized and censorship-resistant.

ClayStack aims to encompass a host of product features and integrate with several fundamental protocols to facilitate wider staking adoption and accelerate the decentralization of Ethereum. Below are some of the core features that the protocol includes.

Technical Architecture/Design



Modularity

The ClayStack Ethereum protocol introduces modularity to liquid staking and enables the validation of the Ethereum network via an algorithmically managed node operator system. It allows us to combine SSV, Obol, KYC-fulfilled as well as public pools of nodes. The modularity of the protocol enables it to have a plug-and-play mechanism with L2s and fellow DeFi and/or other LST-based protocols.

Decentralisation

Any permissionless node operator with the requisite technical knowledge can validate on the Ethereum network. The ClayStack Ethereum protocols aims to significantly reduce the barrier to entry for anyone to join, thereby bolstering the network's security and decentralization.

Scalability

ClayStack facilitates the Ethereum network to have higher scalability while retaining its properties of security and decentralization. It achieves that by lowering the minimum capital required to run a

validator node. The protocol aims to make the bond as ubiquitously low as is needed for anyone to join the Ethereum network and start validating. This allows for infinite scalability for the network.

Layer 2 Node Operator Management System

The Layer 2 Node Operator Management System is a ground-breaking node management system that incentivizes optimal validator performance by storing all validator-related information on Layer 2 networks. This is an extension of the modularity of the ClayStack Ethereum protocol and offers the ability to users to stake via L2s. The scalability and efficiency of L2 chains allow for large-scale operations that would be cost-prohibitive on the base layer. With this system, node operators can claim their rewards on L2s, submit proposals, and optimize for maximal validator perforamance.

Distributed Validator Technology (DVT)

ClayStack protocol employs DVT implementation to ensure higher censorship-resistance of its liquid staking architecture by distributing the validator responsibilities across a host of node operators. This reduces the single-point-of-failure problem with traditional architectures and greatly increases the fault-tolerance of the system. Furthermore, the integration of multiple DVTs catalyzes a more diverse and inclusive validator ecosystem and incentivizes greater participation from different types of operators ranging from home stakers to major institutions.

Algorithmic Node Balancing

ClayStack employs an Algorithmic Node Balancing (ANB) system that incentivizes optimal validator performance by a proportional distribution of staked ETH across the highest-performing node operators. This process is entirely automated and renders additional resilience to the network by delegating to the highest-performing operators. ANB facilitates in the underlying network’s ability to remain highly transparent, decentralized, and censorship-resistant.

Validator Funding Provider (VFP)

The Validator Funding Provider (VFP) module implements a new market of Direct Delegators (DD) and Validators. Through this module, the Direct Delegators can interact with the node operators and delegate their funds to generate superior returns. By participating in this module, both the VFPs and the DDs can partake in superior returns and continuously generate much higher returns.

Censorship-resistance

The ClayStack Ethereum protocol integrates with SSV and Obol to increase the censorship-resistance of the protocol. This ensures that the network has the highest liveness and uptime coming from ClayStack validators, while being highly resilient to any geographical/political crackdowns on validator nodes in certain regions.

MEV Extraction & Flash Exit

The ClayStack protocol integrates the popular MEV relayer MEV-Boost to maximize the rewards that both stakers and validators get. The Flash Exit functionality obliterates the traditional shackles of waiting for the customary unbonding duration or fretting over the perils of slashing while awaiting the readiness of claims. Through this groundbreaking feature, ClayStack holders are empowered to expeditiously exit their positions in return for a nominal fee. This fee, in turn, undergoes equitable distribution among the persisting csETH holders, thereby imparting a surge in the overall yield they get.

Integration with Sonic

The ClayStack protocol also partners with Sonic, opening up an efficient market for both stakers and unstakers. This ensures that users can enter and exit their csETH positions efficiently without needing to either pay an additional fee for Flash Exit or waiting for the unbonding period to get over.

Closing Thoughts

At ClayStack, our goal is aligned with the core ethos of Ethereum, which is to decentralize and securely scale the network. We strongly believe that the existing liquid staking solutions are limited in offering the same security, decentralization, and scalability that Ethereum needs to onboard the next billion users. We at ClayStack are focused on helping Ethereum achieve that goal. Join us as we revolutionize the world of Ethereum liquid staking.