SoK: Liquid Staking Tokens (LSTs)

Abstract—**Liquid Staking Tokens (LSTs) - tradable representations of staked Ether (ETH) with accruable staking rewards - became the preferred method of staking. With over 10 million ETH staked, LSTs contribute 37% of the total staked ETH at the Ethereum blockchain. This Systematization of Knowledge (SoK) presents the architecture, peg mechanisms, and risk implications of various LST designs, including node operator selection, staking distribution models, and a taxonomy for LSTs. An empirical analysis of the major LSTs, and their deviations from the staking rate, is conducted. The paper investigates potential threats posed by LSTs to Ethereum network security. It presents Distributed Validator Technology (DVT) and assesses its impact on Ethereum and LSTs resilience.**

Index Terms—**Decentralized Finance, Liquid Staking, Blockchain, Ethereum, Proof-of-Stake**

I. Introduction

Throughout 2022 and 2023, Ethereum [32] successfully migrated to a Proof-of-Stake (PoS) consensus mechanism in an upgrade process called The Merge [18]. The Merge increased the transaction throughput of the Ethereum network, reduced the electricity consumption [16] and made it possible to stake and unstake Ether (ETH). Staking - participation in Ethereum's transaction validation - is considered a relatively safe method of token allocation that generates consistent returns[33]. However, from the user's perspective, locking ETH at the validator is seen as a disadvantage, as it reduces the token liquidity. The staked ETH cannot be traded nor used in other applications. Until the Shanghai upgrade, it was not possible to unstake ETH.

Decentralized Finance (DeFi) quickly addressed these drawbacks by introducing Liquid Staking Tokens (LSTs) - tokenized representations of staked ETH. While accumulating staking rewards, LSTs can be transferred anytime or freely traded at Decentralized Exchanges (DEXs). LSTs can be also used in DeFi for liquidity provisions at Automated Market Makers (AMMs), or be leveraged to multiply the staking rewards. The leveraging process involves proving LST as collateral to the lending protocol to borrow ETH. The borrowed ETH is used to purchase LSTs at DEXs. The process is repeated multiple times, or executed with a flashloan. LSTs became the dominant form of collateral in DeFi lending [25], and recently they can serve to mint decentralized stablecoins.

With the possibility of unstaking ETH after the Shanghai upgrade, the risk of staking and liquid staking significantly decreased. With 10mn staked ETH, LSTs become the preferred form of staking among the user, representing 37% of total staked ETH, followed by Centralized Exchanges (28%) and Staking Pools (15%) [12]. Consequently, Lido[1], the first protocol that offered LST, has become the largest DeFi protocol with $14bn Total Value Locked (TVL) [4] and liquid staking has emerged as the largest DeFi category ($20bn TVL [4]). However, the concentration of staked ETH at a single protocol - 31% at Lido - raised the question about LSTs' impact on the Ethereum network's security.

Protocols that issue (mint and burn) LSTs are referred to as Liquid Staking Protocols (LSPs). LSPs vary in many areas, with major differences in distributing staking rewards, governing the protocols, and operating validators. Notably, the latter aspect can range from a more centralized approach to a permissionless and decentralized one. LSPs rely on node operators to manage validators, and diverse processes exist to select node operators. The number of node operators varies significantly, such as 30 for Lido and over 3000 for Rocket Pool [13]. With the emergence of permissionless and decentralized LSPs, it became possible to run a validator with just 4 or 8 ETH of own collateral, while LSPs provide the remaining ETH to meet the 32-ETH requirement. Distributed validator technology (DVT) [15] is the recent advancement in LSPs that improves protocol security by distributing validators' keys to multiple node operators. DVT ensures that no single node operator has direct control over any validators, increasing LSPs resilience.

This work begins with the background information about the staking mechanism at the Ethereum blockchain. Next, it establishes a taxonomy for LSTs based on the node operators, staking reward distribution, and governance mechanism and introduces DVT solution. It is shown that the LSTs are pegged tokens, similar to stablecoins, and their market price (at DEXs) converges over time to the protocol price (based on reserves of staked ETH). The subsequent chapter presents the overview of Ethereum attacks and examines how LSTs can be applied to perform such attacks. In a series of simulations, DVT solution is evaluated in the context of preventing the attacks. The second part of this work empirically studies the ten largest LSTs regarding the market share of staked ETH. The divergence from the staking rates is measured for each LSTs and compared. Based on the historical data, de-pegs are observed and explained.

Methodology and Contribution

This paper systematically organizes knowledge around LSTs and examines their impact on the security of the Ethereum network. It establishes an LST taxonomy and its relations with tokens' performance and risk. More precisely, this study presents how various architectural decisions and decentralization levels impact i) the Ethereum security thresholds and ii) the convergence of LSTs to the Ethereum staking rate. These goals are achieved with DVT simulations and empirical studies of the on-chain LST data. Subsequently, LSTs' market and protocol prices are compared and studied. The market price is the price of LST at CEX or DEX, whereas the protocol price is the price for minting or burning LSTs directly at LSPs.

This study analyzed whitepapers, technical documentation, and implementation of the ten largest LSTs in terms of staked ETH that represent over 96% of the liquid staking market [4]. Lido with stETH and wstETH tokens [1] represent 75% of the liquid staking market. Other analyzed tokens include Binance's bETH and wbETH [8], Coinbase's cbETH [3, 10], Rocketpool's rETH [26], Stader's ETHs [28], Frax's sfrxETH [20], lcETH by Liquid Collective [24], Ankr's ankrETH [5], Swell's swETH [30], stakewise's sETH and rETH2 [29] and DIVA's divETH, wdivETH [11]. This study found that:

- LSTs are pegged tokens that operate a similar mechanism to stablecoins and wrapped (bridged) tokens to maintain the peg. Market prices of studied LSTs tracked the staking rewards with a similar accuracy.
- Market price of LSTs at DEX temporarily de-pegs following extreme market events such as FTX insolvency, or Terra/Luna crash. Decentralized (permissionless) LSTs de-peg (upwards) when no sufficient node operators to run validators are provided.
- Arbitrage opportunities existed between the market price at DEX and the protocol price (based on reserves of staked ETH) following extreme market events.
- LSTs, especially with the DVT solution implemented, do not pose a direct security risk for the Ethereum network. However, the growing dependence of DeFi on LSTs might affect the Ethereum network security.

II. Background

This section provides background information about the Proof-of-stake (PoS) consensus mechanism, calculations of staking rewards, and Ethereum migration to the PoS consensus mechanism in the process called the Merge.

A. PoW and PoS

PoW and PoS are two different consensus mechanisms used in blockchain networks to achieve agreement on the state of the ledger and validate new transactions. In Proof-of-Work (PoW), introduced by Bitcoin[38], miners compete to solve complex mathematical puzzles to validate and add new blocks to the blockchain's ledger. To achieve this, they must spend computational power and energy in the process called mining. The first miner to solve the puzzle and find the correct solution is rewarded with newly minted cryptocurrency and transaction fees. This miner's block is then added to the blockchain, and other nodes in the network verify its validity. PoW assumes that the majority of the network's computational power is honest, preventing double-spending and tampering with the blockchain's history.

Proof-of-Stake is an alternative consensus mechanism that aims to address the limitations of PoW, primarily its high energy consumption. In a PoS blockchain, validators create new blocks, attest proposed blocks and secure the network based on their stake: the amount of blockchain native tokens they hold and "stake" as collateral. Validators are selected to create or attest blocks on a random schedule. Whereas in PoW network, miners compete with each other in a race to produce a block, in a PoS blockchain, validators are guaranteed to receive a reward over a period of time, assuming they perform their duties. Validators are penalized, in a process called *slashing*, for being offline, missing attestation or a block proposal, or any mischievous activity.

B. Ethereum PoS

Staking of Ether (ETH) refers to the process of participating in the Ethereum network's PoS consensus mechanism by locking and holding a certain amount of ETH as collateral at the validator. When staking ETH, validators lock ETH in a smart contract for a specified period of time, during which they actively participate in block validation and other consensus activities. The amount of ETH staked by validators can vary, but it requires a minimum threshold of 32 ETH to be eligible for staking. By staking ETH, validators contribute to the network's security, as the PoS consensus mechanism relies on the assumption that most participants act honestly to protect their stake. Validators are incentivized to act in the best interest of the network by following the protocol rules. They can earn indigenous or exogenous rewards. Figure 1 presents the historical (average) staking rewards at the Ethereum blockchain.

1) Indigenous Staking Rewards: Indigenous rewards are specific to the Ethereum PoS and validators are guaranteed to receive them, on condition that they perform their duties. There are five different types of indigenous rewards: attestation, block proposal, sync committee, slashing reward, and priority fees [26]. Ethereum PoS specifies the calculation of these rewards based on the participation rate, total staked ETH, epoch length, and network inflation [19].

Participation Rate: The participation rate, also known as the effective balance, is the amount of ETH actively staked by a validator in the network. Validators with a higher stake have a higher chance of being chosen to validate blocks and earn rewards.

Total Staked ETH: The total amount of ETH staked across the entire network is considered when calculating staking rewards. This helps determine the validator's proportion of the overall stake and their probability of being selected as a validator.

Epoch Length: Ethereum operates in epochs, which are specific time intervals within the staking process. The length of each epoch can vary but is typically several minutes (ca 6.4m minutes). The duration of an epoch is essential in determining the frequency of reward distribution, as staking rewards are distributed at the end of the epoch.

Network Inflation: Ethereum's staking rewards are influenced by the network's inflation rate. The inflation rate determines the number of new ETH tokens minted and distributed as rewards to validators. This rate can change dynamically based on network parameters and consensus rules.

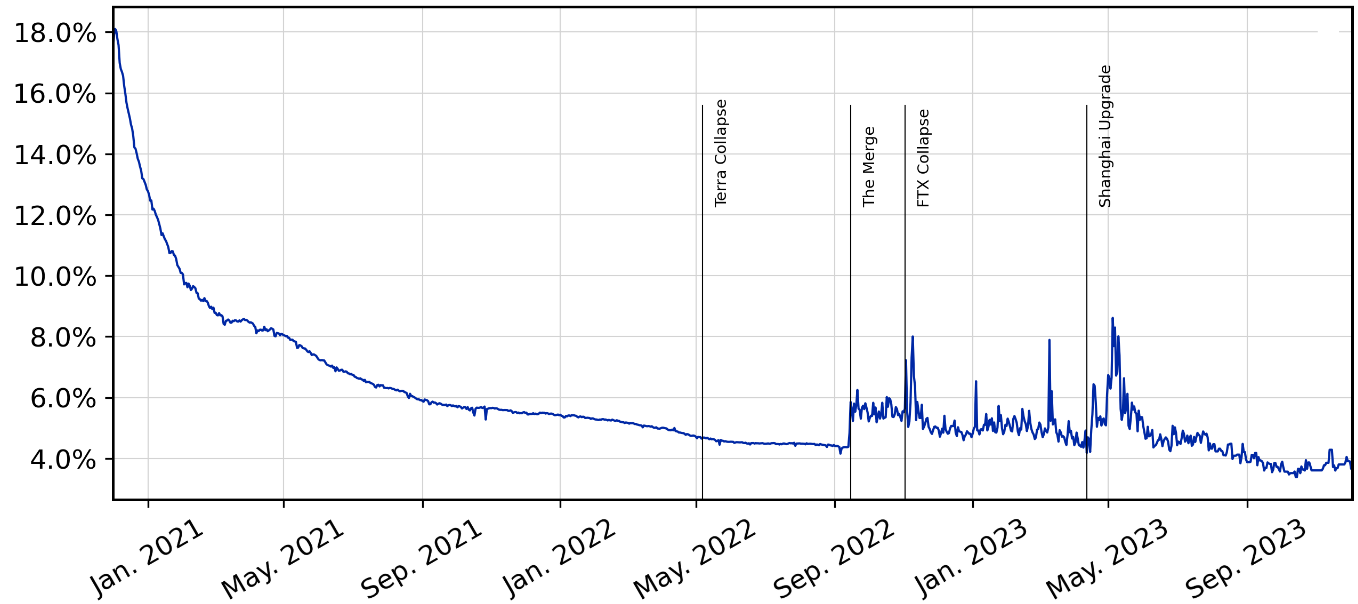

Fig. 1. Average (annualized) staking rewards at the Ethereum blockchain

2) Exogenous Staking Rewards: An additional source of revenue for validators is Maximal Extractable Value (MEV). MEV refers to the re-ordering transaction in the block by the validator to generate profit. Various forms of MEV exist e.g. front-running and back-running, and the revenue comes from the arbitrage opportunities at DEX, liquidations at lending protocols, or sandwich attacks [34, 37]. Validators participate in MEV auctions and compete with other validators to win the MEV rewards. These rewards are not deterministic and independent of the Ethereum PoS mechanism and, consequently, are referred to as exogenous rewards.

3) Staking and Unstaking Queues: In order to security the network stability, Ethereum PoS introduces staking and unstaking queues for validators. The length of the activation and exit queues is based on the number of validators joining or exiting, the total number of active validators in the network, and the churn limit. Up to 16 validators per block can partially withdraw staked ETH. The full withdrawal is a multi-step process comprising an exit queue and withdrawal delay. In the best-case scenario, the shortest time to clear the exit queue is 5 epochs (ca 32 minutes) [17].

C. The Merge

Throughout 2022 and 2023 Ethereum transitioned from the PoW to a PoS consensus mechanism [18]. This upgrade, also known as Ethereum 2.0 or the Merge was designed to enhance the network's scalability, security, and sustainability. With the Merge, the Beacon Chain, which represents the PoS component of Ethereum 2.0, has been successfully integrated into the existing Ethereum mainnet. The Beacon Chain was initially launched as a separate PoS chain and has now been unified with the main Ethereum network.

PoW and PoS differ in several aspects. PoW is resource-intensive, requiring significant computational power and energy consumption for mining, whereas PoS is more energy-efficient as validators are chosen based on their stake. In terms of block validation, PoW involves miners competing to solve puzzles, while PoS selects validators based on their stake to propose and validate blocks. Unlike PoW miners, PoS validators are guaranteed to receive the rewards over a period of time. The security models also contrast, with PoW relying on computational work and the assumption of honest computational power, while PoS relies on the assumption that stakeholders act in the network's best interest due to the risk associated with their stake. PoS has the potential for greater scalability compared to PoW, as it is not limited by hardware and energy requirements.

III. Liquid Staking Tokens

Liquid Staking Tokens (LSTs), also known as Liquid Staking Derivatives (LSDs), are tokenized representations of staked tokens [39]. In the PoS blockchains, the staked tokens are locked within validators, limiting their accessibility and liquidity. Liquid Staking Protocols (LSPs) address this drawback by minting LSTs, which not only preserve the benefits of staking but also add a new layer of versatility. LSTs can be freely traded and accumulate staking rewards, making them a valuable asset that can be utilized in various ways within the DeFi ecosystem. The following section examines the architecture of LSPs, introduces the taxonomy, and presents LST applications on layer-2 blockchains (L2s) and within the DeFi protocols.

A. Architecture

The architecture of LSP, as illustrated in Figure 2, comprises validators, node operators, and the staking pool. In the case of LSPs operating with staked ETH, they also manage a network of oracles to harmonize the state between Ethereum's Beacon Layer and Execution Layer.

Validators ensure the consistency and security of the PoS blockchain. Their responsibilities involve monitoring incoming transactions, attesting to new block proposals, and confirming the legitimacy of the transactions within these blocks. Periodically, validators themselves propose new blocks. In contrast to PoW miners who must compete for block rewards and may not secure one unless they discover the next block, validators are guaranteed to receive rewards as long as they fulfill their duties. Failure to meet their obligations, such as missing an attestation or block proposal, results in penalties - *slashing*.

The staking pool manages user deposits and withdrawals to the LSP, and the distribution of staking rewards. Whenever a new user mints LST within the LSP, he must deposit ETH into the staking pool. Similarly, the staking pools facilitate the withdrawal (burning) of LSTs by users in exchange for ETH. The LSP allocates ETH for staking among node operators in a random manner.

Node operators are responsible for managing the infrastructure required to run a validator. This includes overseeing the hardware, performing software updates, monitoring performance and security, and, in return, receiving staking rewards as recognition for their contributions. Staking rewards are directly transferred from validators to the staking pool in a process known as *skimming*.

Oracle operators are entities tasked with synchronizing the state from Ethereum's Beacon Layer to Ethereum's Execution Layer within the protocol. Given the absence of native communication between these two networks, LSPs rely on a network of oracles to ensure regular synchronization.

1) Distributed Validator Technology: Distributed Validator Technology (DVT) [15] is a new technique designed to enhance the security and resilience of validators by dispersing key management and signing responsibilities among multiple node operators. Its primary objective is to reduce the risks associated with a single point of failure, a scenario in which one node operator possesses the private keys for a validator. In the DVT model, the complete private key is never concentrated on a single machine but is instead distributed across multiple node operators organized into a cluster. As a result, this approach ensures that the validator can continue to operate even if certain nodes within a cluster go offline - *liveness*, or some node operators act maliciously - *fault tolerance*.

Validators generate two sets of public-private key pairs: keys for participating in consensus protocols and withdrawal keys for accessing funds. While withdrawal keys can be securely stored in cold storage, validator private keys must remain continuously online. Compromising a validator's private key could lead to an attacker gaining control of the validator, resulting in slashing penalties or the loss of staked ETH. DVT provides a solution to this vulnerability. With DVT, LSPs' node opearators can participate in staking while safeguarding the validator's private key in cold storage. This is achieved by encrypting the original complete validator key and dividing it into key shares. These key shares are maintained online and distributed across multiple nodes, enabling the distributed operation of the validator. The full, original master validator key is securely stored offline.

When a validator's management is distributed across numerous operators and machines, it becomes resilient to individual hardware and software failures, reducing the risk of downtime. Additional resilience can be achieved by using diverse hardware and software configurations across the nodes within a cluster. In the event of a failure within a node operator in a cluster, the other nodes ensure the continuous operation of the validator. LSPs determine the policy for distributing key shares among node operators, considering factors such as random allocation and prioritizing smaller nodes. The potential risks associated with these policies are examined in Section IV.

2) Node Operators Selection: LSPs vary in their approaches to approving new node operators. The primary methods include whitelisting and requiring collateral for each validator managed by the node operator. In the whitelisting model, the protocol only adds trusted node operators to its network. For example, in the case of Lido[1], a new node operator is added through a DAO vote. In the collateral-based approach, the network of node operators is permissionless, but each operator must post collateral to ensure the performance of its validators, as seen in projects like Rocket Rocket Pool[26], Stader[27].

3) Token Model: Another significant aspect that distinguishes LSTs is the mechanisms used to distribute staking rewards. LSPs typically employ one of three standard token models for this purpose [2]: rebase tokens, reward-bearing tokens, and the dual-token model. These models are further described in detail.

Rebase Tokens: Rebase-LST maintains a 1:1 peg to ETH, and the protocol periodically increases the token supply to reflect the rewards obtained from staking. An example of a rebase LST is stETH, which is minted by Lido. Lido regularly increases the balance of stETH for its holders to mirror the additional ETH earned as staking rewards. The advantage of rebase LSPs lies in their straightforward functionality. However, their drawbacks include limited compatibility with most DeFi protocols, especially decentralized exchanges (DEXs) and lending protocols, and the inability to bridge to other blockchains, which is explained in further subsections.

Reward-bearing Token: Reward-LST continuously increases in value to reflect the accumulation of staking rewards. Consequently, they are not pegged 1:1 to ETH, but instead, their value grows relative to ETH. Reward-LSTs are fully compatible with DeFi and can be bridged to other blockchains. Many LSTs follow this design, including projects like RocketPool[26], Stader [27], CoinBase Wrapped Staking [3], and others. Some LSP offer reward-LST in addition to rebase tokens, as seen in projects like Lido, DIVA[11], Binance[8].

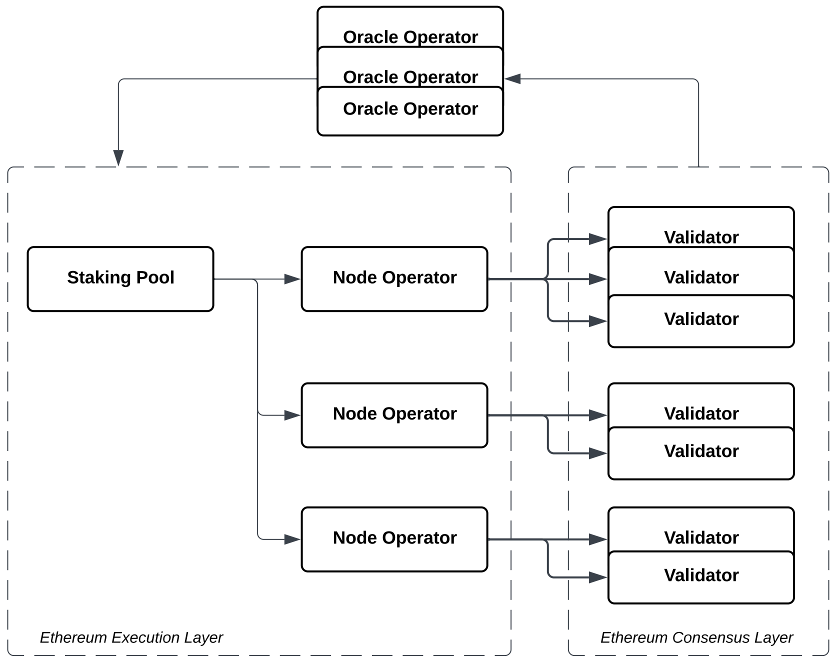

Fig. 2. The Architecture of Liquid Staking Protocols

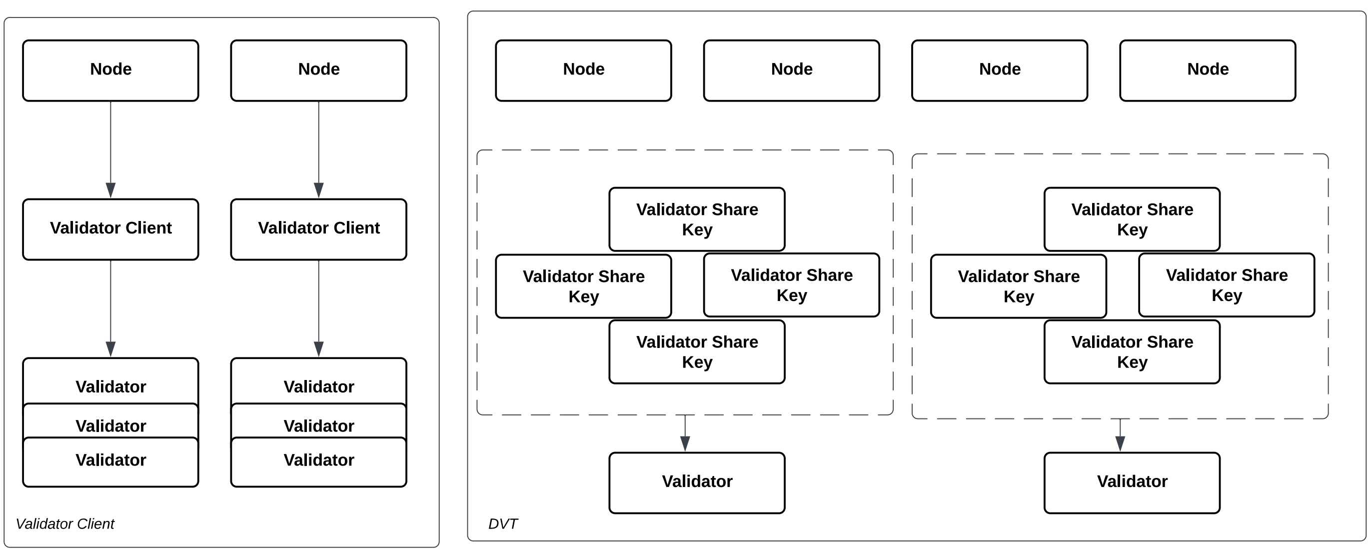

Fig. 3. Comparison of Validator Key Management with and without Distributed Validator Technology

Dual Token: In the dual token model, the asset token is separated from the staking rewards it generates. For instance, StakeWise [29] operates two tokens: sETH2, which maintains a 1:1 peg to ETH, and rETH2, which accumulates in value based on staking rewards. The drawback of this model is fragmented liquidity between two separate tokens.

B. Peg Mechanism

Every LST has associated with it the *protocol value*, often referred to as fair value, peg value, or reserve value. This fair value is determined by dividing the value of the reserves, which include staked ETH and protocol reserves, by the number of tokens in circulation. The *market value* of LST is the value at which tokens are traded on DEXs or CEXs. Discrepancies between fair and market values can arise from market inefficiencies and may create arbitrage opportunities. There are two primary methods to acquire LSTs:

- purchase LSTs on a DEX or CEX at the market price,
- mint LSTs directly from LSP for a fair price

The minting and burning LSTs are explained by algorithms 1 and 2, respectively. The user who mints LSTs is known as the Depositor or Staker, as they deposit their ETH into the staking pool of LSP in exchange for LSTs. The value of the newly minted LSTs is equivalent to the value of the

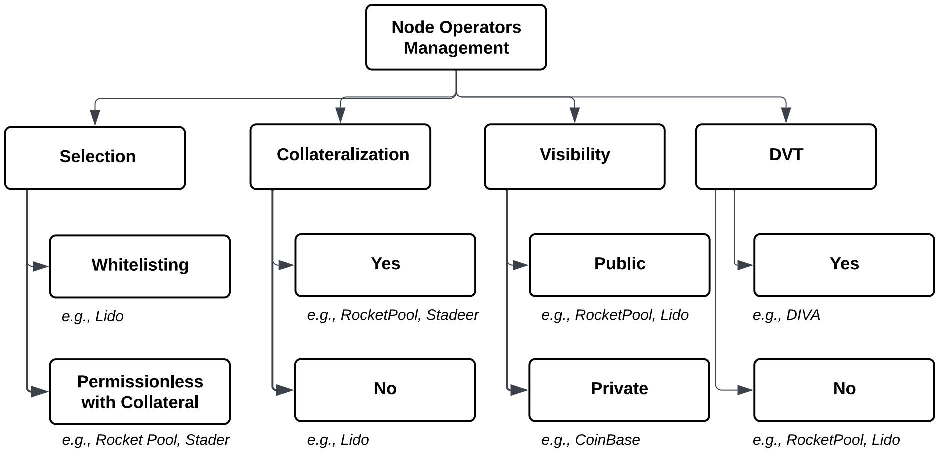

Fig. 4. Liquid Staking Protocols' collaboration models with validators[36]

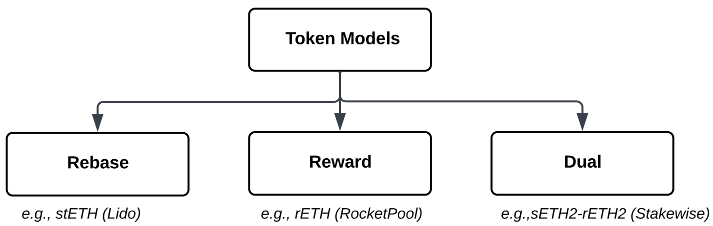

Fig. 5. Token models in use by Liquid Staking Protocols[36]

tokens deposited, thereby keeping the fair value unchanged. Once there is enough ETH in the staking pool to create a new validator, the LSP distributes ETH to randomly selected node operators. The node operator creates a new validator and stake ETH. When LSP operates permissionless set of node operators, each node operator must provide a collateral to create a new validator. e.g. 4ETH or 8ETH. The remaining ETH for the required 32 ETH threshold is provided from the staking pool. In the circumstances when there is no new node operators willing to provide the collateral, LSTs for Depositors are acquired at DEXs. The implementation of LSP determines since when Staker received the staking rewards. In case of Lido, the the staking rewards are being collected withing 24 hours from depositing ETH, regardless whether deposited ETH is staked or not. In this approach, the risk of waiting queues is spread among all LST holders.

Algorithm 1 Minting LST by LSP

1: **Collect** ETH from the Depositor in the staking pool.
2: **Mint** new LSTs, with the value of deposited ETH, and provide these LSTs to the Depositor.
3: Once the amount of ETH in the staking pool is sufficient for the node operator to set up a new validator, distribute the ETH to a random node operator for **staking**.

Similarly to acquiring LSTs, there are two options for redeeming them:

- sell LSTs on a DEX or CEX at the market price,
- burn LSTs directly within the LSP for a fair price.

On the assumption that there is a sufficient amount of ETH in the staking pool, there is no necessity to unstake ETH, as described in algorithm 2. After burning LSTs, the equivalent value of ETH from the staking pool is paid to the Depositor. In the opposite circumstances, LSP randomly selects a node operator to unstake ETH. The unstaked ETH is allocated to the staking pool to pay the Depositor. Depending on the implementation, LSPs might be able to force node operators to unstake ETH, or not. The exit queues to unstake ETH might further extend the waiting period for the Depositor burning LST.

Algorithm 2 Burning LST by LSP

1: **Collect** LSTs from the Depositor and provide from the staking pool equivalent value of ETH in exchange, if there is enough balance.
2: **Burn** the collected LSTs.
3: If there is not enough ETH in the staking pool, **unstake** ETH with the value of collected LSTs by requesting it to node operators.

C. Arbitrage Opportunities

Market inefficiencies can create disparities between the protocol and market values of LSTs. Algorithms 4 and 3 outline arbitrage strategies that aim to profit from the price differences and equalize the protocol and market values of

LSTs. Transaction costs at DEX, gas fees, queues to stake or unstake ETH contribute to discrepancies persisting between the protocol and market values, as studied empirically in the further sections of this work.

In the case of the protocol value of LSTs higher than the market price, arbitrageurs seize the opportunity to buy LSTs on a DEX at the market value and then proceed to burn them within the LSP, receiving the fair value in return.

Algorithm 3 Arbitrage Strategy when market price < protocol price

1: **Buy** (undervalued) LSTs at DEX for the market price.
2: **Burn** LSTs at LSP for the protocol price.

Conversely, in the case of the market price exceeding the protocol price, arbitrageurs mint LSTs within the LSP at the protocol price and sell them on a DEX at the higher market price.

Algorithm 4 Arbitrage Strategy when market price > protocol price

1: **Mint** LSTs at LSP for the protocol price.
2: **Sell** LSTs at the DEX for the market price.

D. Liquid Staking Tokens on L2s

Layer-2 blockchains (L2) are gaining popularity, as they operate on the Ethereum security but offer lower gas fees compared to the Ethereum mainnet [35, 41]. LSTs, available on L2s, are bridged tokens from the Ethereum mainnet. Typically, the bridge locks LST tokens on the Ethereum mainnet and mints equivalent wrapped tokens on the L2 chain. This approach is prone to hacking attacks on the bridge and functions only with reward-based LSTs [22].

The alternative approach of cross-chain liquid staking adopts a native, also referred to as canonical, token on L2 networks. Native LST tokens on L2s differ from wrapped tokens in that they directly represent tokenized staked assets on the Ethereum mainnet without wrapping. Achieving native LST tokens on L2s involves proof-of-storage protocols that provide information to L2s about the state of assets on the Ethereum mainnet, ensuring a seamless and efficient connection between the two layers [9].

E. Liquid Staking Tokens in DeFi

Unlike staked ETH, LSTs can be freely transferred between users, or serve multiple purposes in DeFi. Reward-based LSTs dominate DeFi, as rebase tokens are incompatible with most DeFi protocols. This section describes the major use cases of reward-based LSTs in DeFi that are not feasible with native staking and explains the reasons for rebase-tokens DeFi-incompatibility.

Trading on DEX or CEX: LSTs can be exchanged on decentralized exchange (DEX) and centralized exchange (CEX) at market prices. The market price may differ from the protocol price. Most AMM-based DEX platforms do not support the trading of rebase LSTs, with Uniswap being an example [22]. Rebase LSTs can be traded at Curve v2 [22].

Collateral in Lending: LSTs can be used as collateral in DeFi lending protocols to borrow other tokens. As reward-LSTs' value appreciates over time thanks to staking rewards, these tokens become the primary collateral in DeFi, surpassing ETH [25]. Rebase-LSTs are not used as collateral in DeFi lending because the staking rewards would be divided between the borrower and the lender. In contrast, in the case of reward LSTs, all staking rewards are accrued by the collateral provider.

Collateral for Stablecoins: Similar to their advantages in DeFi lending, LSTs serve as collateral for minting decentralized stablecoins. As the value of LSTs increases, thanks to stake rewards, the liquidation risk of the collateral decreases over time.

Leveraging: LSTs can be leveraged at the lending protocols through a process known as *looping*. In this process, LSTs serve as collateral to borrow ETH, which is later used to buy new LSTs. Another approach to leveraging LSTs involves flash loans. A flash loan is used to purchase LSTs, then lock LSTs as collateral in the lending protocol to borrow ETH and repay the flash loan.

Providing Liquidity to AMM-DEX: LSTs can be utilized in liquidity provisions to AMM-based DEXs. Nevertheless, as AMMs convert part of LSTs to ETH in the case of LST-ETH liquidity pools, only part of the liquidity pool is allocated to LST and earns staking rewards. Only sufficient trading volumes and corresponding swap fees can compensate for the missed staking opportunities. As the future pricing of LST can be estimated based on the current staking rate, LSTs are often traded in AMM with concentrated liquidity such as Uniswap v3.

Operating a validator with less than 32ETH: To operate an Ethereum validator, 32 ETH must be deposited. With LSPs, it is possible to operate a validator with 4ETH or 8ETH, while LSPs provide the remaining ETH to the operator from the staking pool.

The risks associated with LST-based DeFi, especially in the case and LST de-pegs and DeFi liquidations, are discussed in Section VI.

IV. Impact on Ethereum Security

Within the Ethereum blockchain, malicious actors with dishonest intentions constantly seek vulnerabilities. This selection presents the potential attack vectors on Ethereum's security and outlines the minimum defensive thresholds of staked ETH to guard against these threats.

A. Attackers Objectives

It is a common misconception that a successful attacker can mint a new ETH token or steal it from any account. These attack options are impossible due to the requirements imposed on transactions by the Ethereum blockchain. Each transaction must meet specific criteria, such as being signed by the sender's private key and having a sufficient balance; otherwise, it is rejected. Attackers primarily focus on reorganizations of blocks (reorgs), double finality, and finality delay [14, 40].

Reorg refers to the reordering of blocks, occasionally adding or removing blocks from the canonical chain. There are two types of reorgs: ex-ante and ex-post. In the ex-ante reorg, the attacker replaces a block from the canonical chain while it has not yet been created. In the ex-post reorg, the attacker removes a verified block from the canonical chain. The attacker must control over 2/3 of stake ETH to conduct ex-post reorg. The ex-ante reorg, on the other hand, involves the manipulation of blocks to be included or excluded, enabling double-spending or exploiting transaction reordering in the block from MEV. The most extreme form of ex-ante reorg, finality reversion, becomes possible when an attacker can control more than $\frac{1}{3}$ of the total staked ETH, a threshold known as *economic finality*.

Finality delay requires the attacker to control at least 1/3 of staked ETH and aims to disrupt Ethereum operations by hindering the network from finalizing portions of the chain. In Ethereum PoS, each new block must be attested by 2/3 of the staked ether. If 1/3 or more of the staked ETH is maliciously attesting or failing to attest, then a 2/3 supermajority cannot exist. However, if the chain fails to finalize for four epochs, validators failing to attest or attesting contrary to the majority are gradually slashed until they represent less than 1/3 of the total staked ETH, and supermajority exists. This attack does not directly benefit the attacker unless financial incentives are tied to the chain disruption.

Double finality arises when two forks reach finality simultaneously, leading to a permanent split in the chain. This is theoretically achievable for an attacker risking 34% of the total staked ETH, as the attacker's validator would be double-voting simultaneously and finally slashed with the highest possible penalty. Resolving such chain splits would require off-chain coordination within the community.

Attackers controlling over 51% of total staked ETH can split the Ethereum blockchain into two forks of equal size and control the fork choice algorithm. The attacker cannot change history but controls the future by applying their majority votes to favorable fork, enabling censorship of transactions and reordering of blocks for MEV rewards.

Attackers controlling over 66% of staked ETH can vote for the preferred fork and then finalize it with the dishonest supermajority. The attacker can perform ex-post reorgs (change the history) and do finality reversions (control the future).

The more staked ETH the attacked controls, the more influence over new blocks he has. Table I summarizes the threshold amounts of staked ETH required for specific attacks. The defense against the attacks is the associated cost to perform them. The majority of staked ETH used by the attacker would eventually be slashed after the social layer adopts the honest minority fork. The subsequent sections explain how liquid staking might reduce these attack thresholds by allowing the attacker to control part of the staked ETH from Liquid Staking Protocols.

TABLE I
THE MINIMUM THRESHOLD AMOUNTS OF STAKED ETH REQUIRED FOR THE ETHEREUM ATTACKS [14]

Staked ETH	Attack Type
33%	delay finality
34%	cause double finality
51%	censorship, control over blockchain future
66%	censorship, control over blockchain future and past

TABLE II
THE MINIMUM THRESHOLD AMOUNTS OF STAKED ETH REQUIRED FOR THE ETHEREUM ATTACK. LSP'S COLLATERAL REQUIREMENTS TO OPERATE A VALIDATOR ARE 16ETH, 8ETH, 4ETH, 1 ETH, AND THE THE PROTOCOL PROVIDES THE REMAINING ETH FROM THE STAKING POOL TO OPERATE A VALIDATOR. THE DVT MODE ASSUMES THAT THE 2/3 OD KEY SHARES ARE REQUIRED TO OPERATE A VALIDATOR, AND THE NODE OPERATOR CAN SELECT SHARE KEYS.

Collateral	Threshold	Threshold DVT
32 ETH	33%	22%
16 ETH	16.5%	11%
8 ETH	11%	7.3%
4 ETH	4.13%	2.75%
1 ETH	1.03%	0.69%

B. Liquid Staking in Ethereum Attacks

LSPs do not directly manage validators but establish a network of node operators responsible for validator operations. In the permissioned model, these node operators are whitelisted by the protocol, often through a DAO vote, which effectively prevents the inclusion of malicious actors. In the permissionless model, node operators are required to deposit collateral to operate a validator, with the remainder of ETH provided from the staking pool of the LSP. Consequently, attackers on the Ethereum network no longer need to provide the full 32ETH to operate a validator but only a portion covering the collateral requirements of the LSP. This results in a decreased attack threshold, as represented in table II. Further reductions in the attack threshold are possible with Distributed Validator Technology (DVT). Assuming that only 2/3 of the key shares are required to operate a validator and a node operator can select share keys, attack thresholds are further diminished by 2/3. Nevertheless, LSPs can prevent this circumstance by randomly distributing the key shares to private keys of validators among node operators.

C. Simulation

Assuming that LPS protocols have n node operators and m validators, and each validator key is split into k shares. There are mk key shares distributed randomly to node operators. At least π of key shares are required to control a validator. Each node operator must provide a collateral of $\frac{32ETH}{\pi}$ to receive one key share. The probability that one node operator receives at least l share key to one validator is

$$P(m,k,l) = m * \frac{k}{mk} * \frac{k-1}{mk-1} * ... * \frac{k-l+1}{mk-l+1}$$
$$= \frac{k!}{(mk)!} * \frac{(mk-l)!}{(k-l)!}$$

The probability that one node operator receives π of key shares of one validator significantly decreases as a function of the signature threshold π and number of validators m (see Figure IV-C).

V. Comparison of Liquid Staking Protocols

Liquid staking, with \$20bn TVL, is the largest category among DeFi protocols, and the preferred method of staking among users The overall 37% of staked ETH is staked by LSTs. Table III lists major Liquid Staking Protocols (LSPs), their respective value locked, market share in the general ETH staking market, and other respective metrics. Lido is undeniably the biggest LSP, with over 31% of staked ETH (and 14.44b\$ TVL) operated by 29 node operators. These node operators manage 276k validators - 9.5k validators (1.07\$ of total staked ETH) on average per Lido node. In comparison, RocketPool has 3088 node operators, each of which manages, on average, eight validators. In the next paragraphs, we analyze the design decisions behind LSPs, and empirically study peg stability to the ETH staking rewards. The section ends with a comparison of the historical performance of LSTs with native staking.

A. Major Liquid Staking Protocols

This section discusses the architecture of the major LSPs. The protocols were selected based on the value of staked ETH [4], and represent all previously described mechanisms. A summary of LSPs's design decisions can be found in table IV. Only RocketPool, Stader, and DIVA maintain the permissionless network of node operators, each of them requiring collateral from the node operator to manage validators. Consequently, RocketPool and Stader have the highest number of node operators, over 3000 and 100, respectively, followed by Lido - 29 nodes. Lido approves node operators in the DAO vote. Another important differentiation between LSPs is the private key management. Only DIVA already supports the Distributed Validator Technology (DVT) model, in which each private key to a validator is spread between various node operators. Consequently, none of the node operators has full control over a single validator. In the case of RocketPool, Stadler, Lido, and other LSPs each node fully controls a set of validators.

Lido Protocol was launched in December 2020, as the first LSPs. The protocol operates as a decentralized autonomous organization (DAO) governed by Lido governance token holders. Key decisions regarding the protocol, such as fee structures, staking parameters, and upgrades, are determined through community voting. Lido approved its network of node operators based on their track record and reputation in DAO vote. The protocol provides real-time monitoring of its validator performance and staking metrics. Lido issued two LSTs on the staked ETH: stETH, which distributes the staking rewards in the rebase model and wstETH, which operates in the reward model. The token stETH is the 8th largest in terms of market capitalization crypt-currency, according to CoinGecko. The market share of Lido (31%) in the total staked ETH raises questions about its impact on the Ethereum blockchain security, which is discussed in the next section.

Rocket Pool, founded in 2016 and officially launched in 2021, provides rETH: reward-based token. The protocol is permissionless in a way that any node operator can join the network to manage validators on the condition that it provides the necessary collateral. After the Atlas upgrade in 2023, the node operators can choose between 8ETH and 16ETH collateral for each validator. The remaining 24ETH or 16ETH, respectively, is provided by RocketPool from its staking pool. The additional deposit is equal to 10% of the ETH from the pool and is provided in the RocketPool governance tokens.

Stader is an example of LSPs with the premissionless set-up of node operator. The required collateral is just 4th, compared to 8ETH in the case of RocketPool.

Stakewise is the only LPSs that operates two tokens: sETh2, which is pegged to ETH and rETH2, which accumulates staking rewards. According to Stakewise, the dual model is planned to be replaced with the reward-LSTs.

Frax offers reward-based LST - sfrxETH, which is minted after depositing frxETH - an ETH wrapper with a value equal to 1 ETH. The frxETH token is not a rebase-based LST, but is the ERC20 representation of ETH.

Liquid Collective, by providing transparency around the node operators of the validator, focuses on the institutional customers. Mandatory anti-money laundering (AML) checks for users and operators facilitate regulatory compliance.

DIVA Protocol uses Distributed Validation Technology (DVT) to operate Ethereum validators. Node operators use DVT Key Shares instead of validators' private keys. Each validator is run by 16 DVT Key Shares, and the node operator must lock one divETH collateral per Key Share. The remaining 16ETH required to run Ethereum operators is provided from DIVA staking pool. Key shares are generated by the network with Multi-Party Computation (MPC) technology. Consequently, private keys never come together, eliminating single points of failure.

Binance and *Coinbase* are the leading CEX that on top of the native staking services they provide to their customers, launched their own LSTs. The selection of node operators is a centralized process without a DAO vote. DAO vote governs the Lido's node operators network.

B. Historical Performance

We examine the performance of LSTs compared to native staking of ETH. To determine the daily performance of LSTs, we obtained market price data directly from UniSwap[31]. The analysis considers the allocation of one ETH, either to LSTs or to staking. For the calculation of staking rewards, we make the assumption that rewards are claimed and re-staked

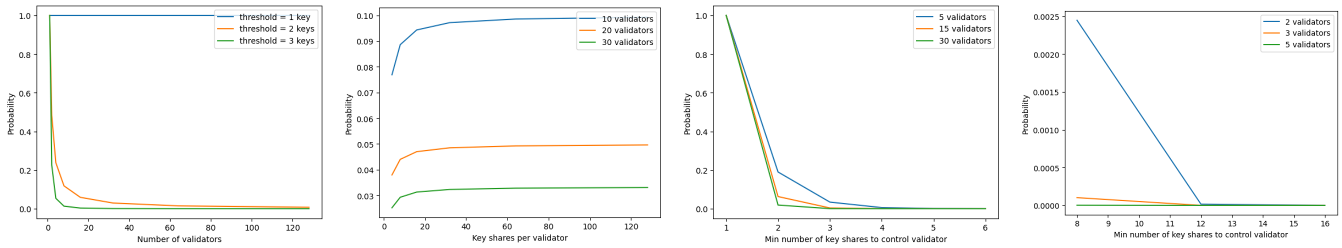

Fig. 6. Probability that one node operator controls a validator as a function of a number of validators, key shares per validator, and minimum signature threshold. Each validator key is divided into 16 key shares with 2-share signature threshold, unless marked otherwise

TABLE III
MAJOR LIQUID STAKING PROTOCOLS (LSPS) IN TERMS OF TOTAL VALUE LOCKED (TVL) AND % MARKET SHARE OF THE TOTAL STAKED ETH

Protocol		**TVL ($)**	**Market(%)**	**LSTs**	**Governance Token**	**Nodes**	**Validators**	**Fees**
Lido	[1, 21]	14.44b	31	stETH, wstETH	LDO	29	276k	10%
Rocket Pool	[26]	1.774b	3.89	rETH	RPL	3088	25k	20%
Binance Staked ETH	[7, 8]	983.7m	2.16	bETH, wbETH	-	-	-	10%
Frax Ether	[20]	451.72m	0.99	sfrxETH	-	-	7k	10%
CoinBase Wrapped Staked ETH	[3, 10]	327.28m	0.72	cbETH	-	-	-	25%
StakeWise	[29]	159.63m	0.35	sETH2, rETH2	SWISE	4	3k	10%
Stader	[27, 28]	94.89m	0.21	ETHx	SD	109	718	10%
Swell	[30]	79.77m	0.18	swETH	SWELL	8	-	10%
Liquid Collective	[23, 24]	57.55m	0.13	lcETH	-	-	-	10%
Ankr	[5]	51.36m	0.11	ankrETH	ANKR	-	-	10%
DIVA	[11]	28.18m	0.06	divETH, wdivETH	DIVA	-	-	10%

TABLE IV
COLLATERAL REQUIREMENT TO OPERATE A VALIDATOR FOR LIQUID STAKING PROTOCOLS (LSPS) WITH A PERMISSIONLESS SET OF NODE OPEARATORS

Protocol	**Permissionless**	**Collateral**
Lido	No	-
Rocket Pool	Yes	8ETH or 16ETH
CoinBase Wrapped Staked ETH	No	-
Binance Staked ETH	No	-
Staked Frax Ether	No	-
Ankr	No	-
StakeWise	No	-
Stader	Yes	4ETH
Swell	No	-
Liquid Collective	No	-
DIVA	Yes	1ETH

on a daily basis. Staking yield rates fluctuate daily and vary among validators, as depicted in figure 1. To ensure accuracy, we utilize historical staking rates sourced from the Ethereum Explorer.

Rebase-LSTs maintain the 1:1 peg to ETH. Historically, their market values, presented in Figure 9, temporally de-peg from the target, especially in times following the market turmoil. Historical performane of reward-LSTs is depicted in Figure 10. The analysis presents the compounded daily returns of reward-LSTs in comparison to staking ETH directly.

Dispersion Analysis of ETH LSTs is presented in Figure 7 and 11. It illustrates the distribution of the difference between the daily returns of LSTs and the daily staking rewards for the reward LST, and the deviation from the target value of 1 ETH for the rebase LSTs. As seen in Figure 11, the inclusion of fees charged by LSPs results in a negative shift in the distribution. Additionally, the incorporation of MEV rewards leads to a rightward shift in the distribution. As a result, the overall returns of the LSPs tend to be slightly negative, as indicated by a negative median return. When examining the daily return basis, it is observed that cbETH exhibits the lowest tracking error among the LSTs. Conversely, ankrETH tokens demonstrate the highest deviation. The deviations from the staking rate significantly decreased after the Shanghai upgrade, which allowed to unstake ETH.

Terra and FTX collapses— In 2022, the crypto market experienced significant disruptions due to adverse market conditions. One of the major events was the crash of the algorithmic stablecoin USDT, which resulted in the collapse of the Terra blockchain and its associated ecosystem of protocols on May 7, 2022. This event had a widespread impact on the market. Subsequently, the centralized exchange FTX faced insolvency on November 2, 2022, leading to the freezing of

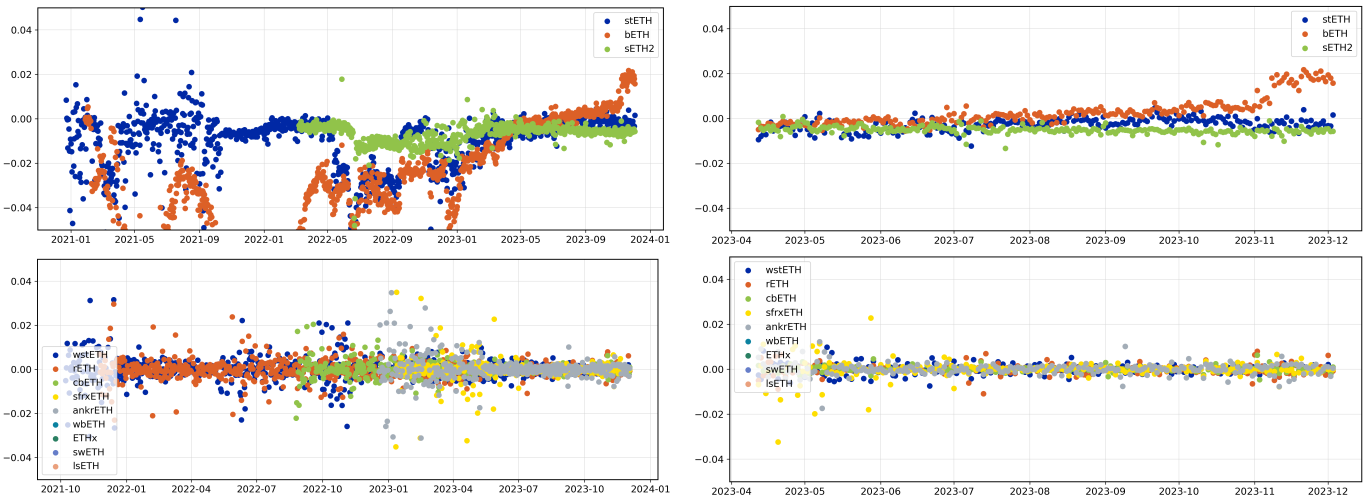

Fig. 7. Distribution of differences between the market price of rebase LST and target value of 1 ETH (top row) and between the daily reward-LST return and daily staking rate (bottom row), since the token inceptions (left column) and after the Shnaghai upgrade (right column)

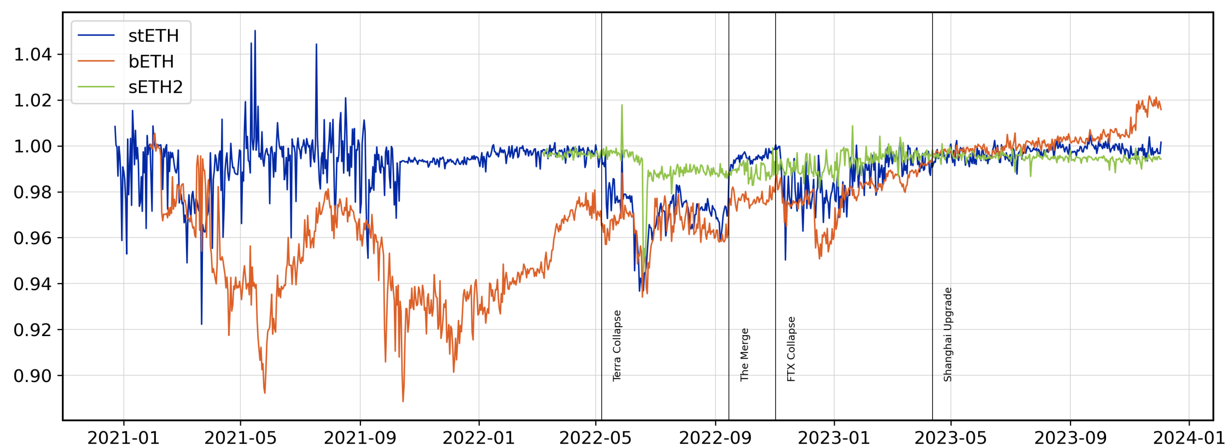

Fig. 8. Historical market values of rebase LSTs - stETH from Lido, bETH from Binance, and sETH2 from StakeWise since the token inception, with ETH as a reference currency.

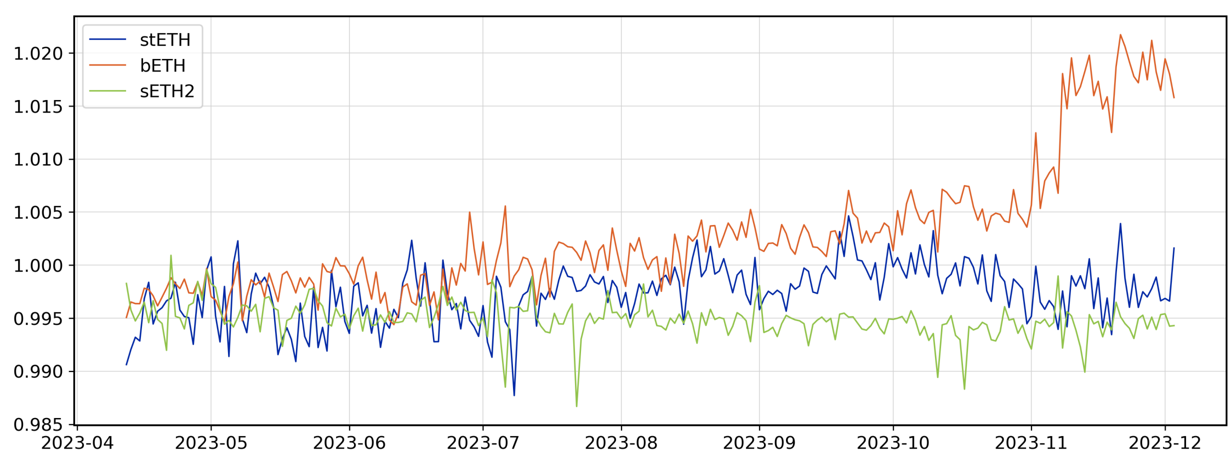

Fig. 9. Historical market values of rebase LSTs - stETH from Lido, bETH from Binance, and sETH2 from StakeWise, after the Shanghai upgrade, with ETH as a reference currency.

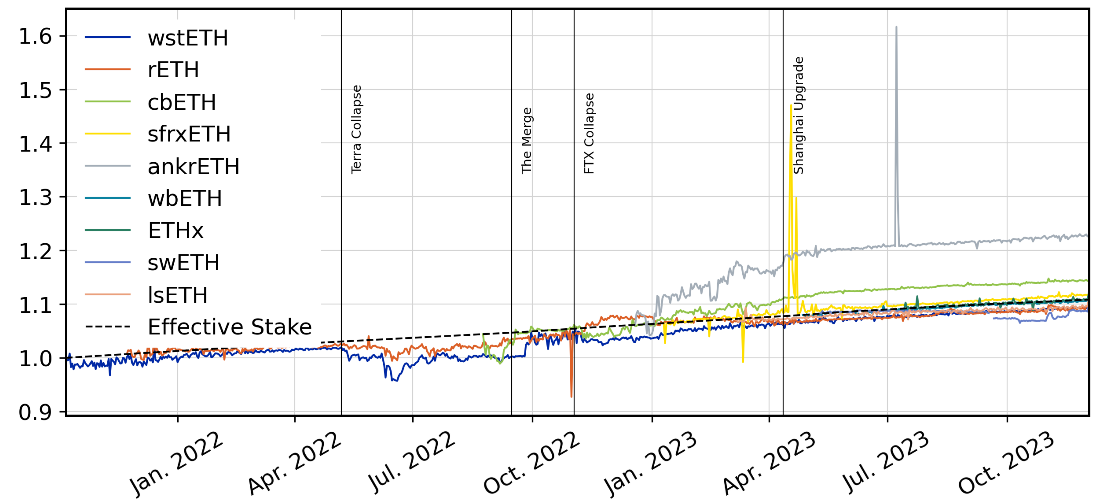

Fig. 10. Historical market value of major reward-based LSTs since their inception. The dotted line represents the accumulative staking rewards.

digital assets held by its customers. During the period between the collapse of Terra and the insolvency of FTX, both stETH and rETH tokens performed worse than traditional staking. However, following the FTX collapse, the rETH token demonstrated better performance compared to staking. This can be attributed to investors' reluctance to engage with centralized protocols. Rocket Pool, known for its permissionless selection of validators, is considered more decentralized than the Lido protocol, which follows a whitelist approach via DAO vote.

Peg Analysis— Prior to the Shanghai upgrade, there was no possibility to unstake ETH, resulting in market value deviations from the fair value. Figure 12 showcases the market and fair (peg) values for the rETH token of RocketPool. Between the collapse of Terra-Luna on May 7, 2022, and the FTX collapse on November 2, 2022, rETH was undervalued compared to its peg value. If unstaking ETH had been possible during this period, arbitrageurs could have equalized the market and peg values of rETH. After the FTX crash and until January 2023, rETH tokens were overpriced, creating an opportunity for an arbitrage strategy as outlined in Algorithm 4. Arbitrageurs could mint rETH at the Rocket Pool Protocols for the protocol value and sell it at a DEX such as UniSwap for a market price that exceeded the protocol price. The overpricing of Rocket Pool's LSTs can be attributed to the aversion towards centralized protocols following the FTX collapse.

Before the Atlas upgrade in early 2023, RocketPool required 16 ETH of collateral from the node operators to set up a new validator [26]. The lack of possibility to set up enough new validators contributed to the (upward) de-peg of rETH price in 2022 and 2023.

VI. Discussion

With over 10mn ETH staked via LSTs, LSTs emerged as the preferred method of staking ETH (37%) and the largest category within DeFi in terms of capital (27bn USD). Lido, as the first LSP, established itself as the major protocol with 31% of the entire staked ETH [13] raising concerns about risks to the Ethereum blockchain security. Lido's share of staked ETH approaches the economic security threshold of 1/3 staked ETH which would allow the attacker to delay the network's finality. Although Lido employs 30 node operators, each managing ca 1% of the staked ETH, each node operator relies on Lido's software that can be hacked. Such a hacking attack would give an attack control over 1/3 of the staked ETH required for finality delays and temporary transaction censorship.

RocketPool introduced measures to enhance the decentralization of node operators and currently operates with over 3000 nodes. Historically, RocketPool was not able to attract enough node operators to stake ETH from Depositors, leading to its LST's market price (upwards) de-peg. In the permissionless of RockePool, node operators deposit collateral of 16 ETH to 8ETH to run a validator (4ETH at Stader protocol). With just 8ETH or 4ETH, instead of 32ETH, to operate a validator, the economic security threshold of Ethereum decreases to 11% and 4.13 %, respectively.

Distributed Validator Technology (DVT) aims to mitigate risks associated with a single point of failure and allows LST and node operators to coexist while preserving the network's decentralization. By distributing the validator keys across multiple machines, DVT increases the difficulty of malicious actions. Nevertheless, DVT also increases the complexity of managing LSP infrastructure and requires the right policies for distributing key shares to node operators. Without such policies, attack thresholds could be further diminished by a factor of signature thresholds, e.g. 2/3, if a malicious actor can select a key share to a certain validator. As the simulations showed, the random distribution of key shares decreases the risk that an attacker can possess a signature threshold necessary to control a validator. DVT approach, once implemented by Lido, RocketPool, and other protocols issuing LSTs will significantly increase the resilience of LSTs, decreasing the

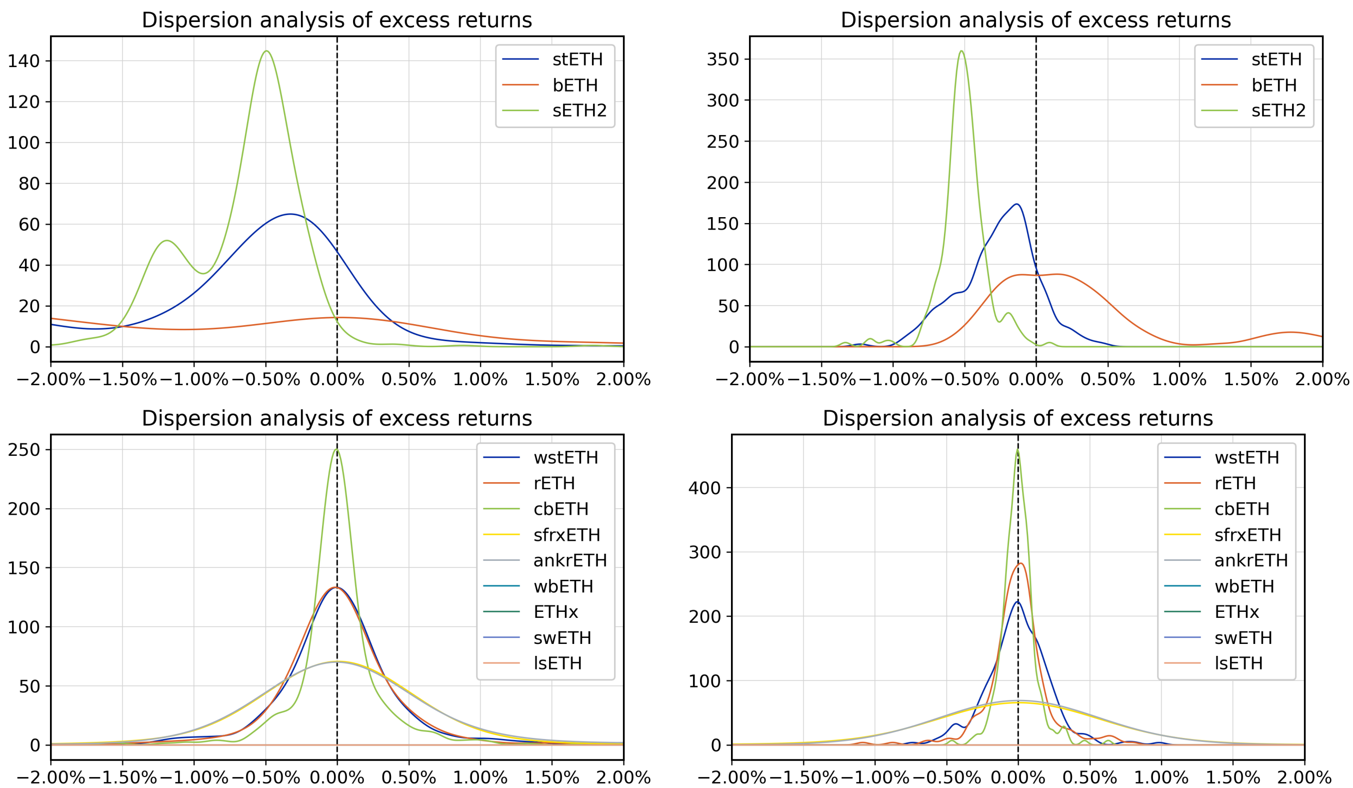

Fig. 11. Dispersion analysis of rebase LST (top row) and reward LSTs (bottom row), since the token inceptions (left column) and after the Shnaghai upgrade (right column). For rebase LSTs the difference between the LST market price and the target value 1 ETH is calculated. For reward-LSTs, the difference between the daily LST return and staking rate is analyzed

probability of a sucessful attack on Ethereum via LSTs.

Another challenge in the LSP design is the enforcement of ETH unstaking and unstaking queues. While some centralized protocols can control the withdrawal keys of validators, certain protocols lack the means to compel node validators to unstake ETH. This situation and unstaking queues may result in prolonged de-peg periods for LST market values. LSTs are already the major collateral in DeFi lending [25], often leveraged to multiply the staking rewards. The potential de-peg, higher than the liquidation threshold, would lead to the cascade liquidations of the lending positions, further decreasing the token value. Consequently, LSPs would be forced to unstake ETH to restore the token peg. The sudden increase in unstaked ETH might undermine the security of the Ethereum blockchain.

To mitigate the risk of single LST de-pegging, index protocols have emerged, such as Asymmetry Finance [6]. These protocols create a basket comprising LSTs from various providers. Institutional liquid staking providers, such as Liquid Collective, cater to corporate investors rather than retail stakers and entail a Know Your Customer (KYC) process for all node operators and depositors.

While this work focuses on staking as an integral part of PoS blockchain, other forms of staking mechanisms are present within DeFi. Some protocols enable users to stake their governance or LP-tokens, locking them for a specific period of time to accumulate additional rewards. The liquid staking framework can be extended to accommodate these alternative staking methods as well.

VII. Related Work

Liquid staking and its risk have not been vastly studied in the literature. Scharnowski et al. [39] conducted the first economic analysis of LSTs, focusing on the price disparity between LSTs and their corresponding native tokens. The work [36] differentiated three staking distribution models - reward, rebase, and dual and observed discrepancies between the protocol and market prices for LSTs on Ethereum before the Merge.

Building upon these studies, this research established LST taxonomy that includes the key technical aspects: the validators' management mechanisms. It examines and discusses its implications on the LST performance and risk, especially the resistance to de-peg in the aftermath of extreme market events. By analyzing the token designs and implementation limitations, it is explained under which conditions the discrepancies between market and protocol prices of LST lead to arbitrage opportunities. This is the first work that evaluates the impact of LSTs on Ethereum security.

VIII. Conclusions

Liquidity Staking Tokens (LSTs) emerged as the preferred staking method among users, contributing 37% of staked ETH today, and grew into the largest category within DeFi in terms of capital (27bn USD) within a year. This paper systematically organizes knowledge around LSTs and examines their impact on the security of the Ethereum network. It establishes a taxonomy including node validator selection and token model to distribute staking rewards to users. Employing the proposed taxonomy, major LSTs were assessed, providing insights into their performance, security, and decentralization. This work investigated the effectiveness of tracking staking rewards and compared peg stability among different LSTs.

We found that following the Shanghai upgrade, which allowed to unstake ETH, the tracking of daily staking rewarding by LSTs significantly improved. The tokens with a permissionless set of node operators, such as rETH from RocketPool, de-peg (upwards) when the demand for LSTs exceeds the node operator capacity to set up new validators.

Lido, with 31% of staked ETH, approaches the economic security threshold of Ethereum. However, with 30 node operators and DVT solution being implemented, the simulations showed that the probability of a successful attack is below 0.001%. Similarly, while other protocols like RocketPool and Stader - with permissionless node operators - may decrease the security economic threshold, with the DVT approach implemented, the probability of a successful attack on Ethereum is very low. To conclude, LSTs, especially with DVT approach implemented, do not pose a direct security risk for the Ethereum network. However, the growing dependence of DeFi on LSTs, might affect Ethereum's security.

Future research into LSTs in DeFi can build upon this systematization of knowledge, particularly liquidity provision of LSTs in AMMs and the utilization of LSTs as collateral in lending protocols and stablecoins. These avenues for research can leverage the presented taxonomy to contribute to the development of a more robust and secure LST-based DeFi ecosystem.

References

[1] Lido: Ethereum Liquid Staking Whitepaper, 2020. URL https://lido.fi/static/Lido:Ethereum-Liquid-Staking.pdf.

[2] A wrap-up on designing liquid staking protocols:, 2022. URL https://twitter.com/FigmentCapital/status/1567324278906933250.

[3] CoinBase cbETH Whitepaper, 2022. URL https://www.coinbase.com/cbeth/whitepaper.

[4] DeFi Llama, 12 2022. URL https://defillama.com/.

[5] Ankr Liquid Staking Documentation, 2023. URL https://www.ankr.com/docs/liquid-staking/overview/.

[6] Asymmetry Finance, 2023. URL https://www.asymmetry.finance/.

[7] Binance ETH Staking Documentation, 2023. URL https://www.binance.com/en/eth2.

[8] Binance Wrapped Beacon ETH Documentation, 2023. URL https://www.binance.com/en/wbeth.

[9] Chainlink Documentation: Cross-chain liquid staking derivatives, 2023. URL https://blog.chain.link/cross-chain-liquid-staking-derivatives/.

[10] CoinBase cbETH Documentation, 2023. URL https://www.coinbase.com/cbeth.

[11] DIVA Documentation, 2023. URL https://docs.staking.foundation/.

[12] Dune Analytics - Ethereum Staking, 12 2023. URL https://dune.com/hildobby/eth2-staking.

[13] Dune Analytics - Ethereum Beacon Chain Deposits, 11 2023. URL https://dune.com/jackjin/lsd.

[14] Ehtereum Technical Documentation: Ethereum Proof-of-Stake Attack and Defense, 2023. URL https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/attack-and-defense/.

[15] Ehtereum Technical Documentation: Distributed validator technology, 2023. URL https://ethereum.org/de/staking/dvt/.

[16] Ethereum Foundation - Ethereum's energy expenditure, 2023. URL https://ethereum.org/en/energy-consumption/.

[17] Ethereum PROOF-OF-STAKE (POS), 2023. URL https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/.

[18] Ethereum Roadmap, 2023. URL https://ethereum.org/en/roadmap/merge/.

[19] Ethereum PoS Rewards and Penalties, 2023. URL https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/rewards-and-penalties/.

[20] Frax Ether Documentation, 2023. URL https://docs.frax.finance/frax-ether/frxeth-and-sfrxeth.

[21] Lido: Ethereum Liquid Staking Whitepaper, 2023. URL https://docs.lido.fi/.

[22] Lido Technical Documentation: Lido Token Integration Guides, 2023. URL https://docs.lido.fi/guides/lido-tokens-integration-guide.

[23] Liquid Collective Documentation, 2023. URL https://docs.liquidcollective.io/v1/.

[24] Liquid Collective Whitepaper, 2023. URL https://liquidcollective.io/litepaper/.

[25] Messari Report - State of L1s Q2 2023, 11 2023. URL https://messari.io/report/state-of-l1s-q2-2023.

[26] RocketPool Technical Documentation, 2023. URL https://docs.rocketpool.net/guides/staking/overview.html.

[27] Stader Documentation, 2023. URL https://www.staderlabs.com/docs-v1/intro.

[28] Stader Lightpaper, 2023. URL https://www.staderlabs.com/docs/eth/Stader%20ETH%20Litepaper.pdf.

[29] StakeWise Documentation, 2023. URL https://docs.stakewise.io/.

[30] Swell Documentation, 2023. URL https://docs.swellnetwork.io/swell/what-is-swell.

[31] Hayden Adams, Noah Zinsmeister, Moody Salem moody, uniswaporg River Keefer, and Dan Robinson. Uniswap v3 Core. Technical report, 2021.

[32] Vitalik Buterin. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. Technical report, 2014.

[33] Sylvain Carré and Franck Gabriel. Security and Credit in

Proof-of-Stake DeFi Protocols *. Technical report, 2022. URL https://ssrn.com/abstract=4307207.

[34] Tarun Chitra and Kshitij Kulkarni. Improving Proof of Stake Economic Security via MEV Redistribution. 2022.

[35] Ankit Gangwal, Haripriya Ravali Gangavalli, and Apoorva Thirupathi. A survey of layer-two blockchain protocols, 2022.

[36] Krzysztof Gogol, Benjamin Kraner, Malte Schlosser, Tao Yan, Claudio Tessone, and Burkhard Stiller. Empirical and Theoretical Analysis of Liquid Staking Protocols. 2023.

[37] Lioba Heimbach and Roger Wattenhofer. SoK: Preventing transaction reordering manipulations in decentralized finance. sep 2022. doi:10.1145/3558535.3559784. URL https://doi.org/10.1145%2F3558535.3559784.

[38] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. Technical report, 2008. URL www.bitcoin.org.

[39] Stefan Scharnowski and Hossein Jahanshahloo. Liquid Staking: Basis Determinants and Price Discovery. Technical report, 2022. URL https://ssrn.com/abstract=4180341.

[40] Caspar Schwarz-Schilling, Joachim Neu, Barnabé Monnot, Aditya Asgaonkar, Ertem Nusret Tas, and David Tse. Three attacks on proof-of-stake ethereum, 2021.

[41] Bennet Yee, Dawn Song, Patrick McCorry, and Chris Buckland. Shades of finality and layer 2 scaling, 2022.

APPENDIX

TABLE V

OVERVIEW OF LIQUID STAKING TOKENS (LSTS) ON STAKED ETH, THEIR STAKING DISTRIBUTION MODELS, AND SUPPORTED BLOCKCHAINS, ACCORDING TO THE PROTOCOLS' OFFICIAL DOCUMENTATION.

Protocol	**LST**	**Model**	**Blockchain**
Lido	stETh	rebase	Ethereum
Lido	wstETH	reward	Ethereum, Arbitrum, Optimism, Polygon
Rocket Pool	rETH	reward	Ethereum, Optymism, Arbitrum
CoinBase Wrapped Staked ETH	cbETH	reward	Ethereum
Binance Staked ETH	bETH	rebase	Ethereum
Binance Staked ETH	wbETH	reward	Ethereum
Frax Ether	sfrxETH	reward	Ethereum
Ankr	ankrETH	reward	Ethereum
StakeWise	sETH2, rETH2	dual	Ethereum
Stader	ETHx	reward	Ethereum
Swell	swETH	reward	Ethereum
Liquid Collective	lcETH	reward	Ethereum
DIVA	divETH	rebase	Ethereum
DIVA	wdivETH	reward	Ethereum

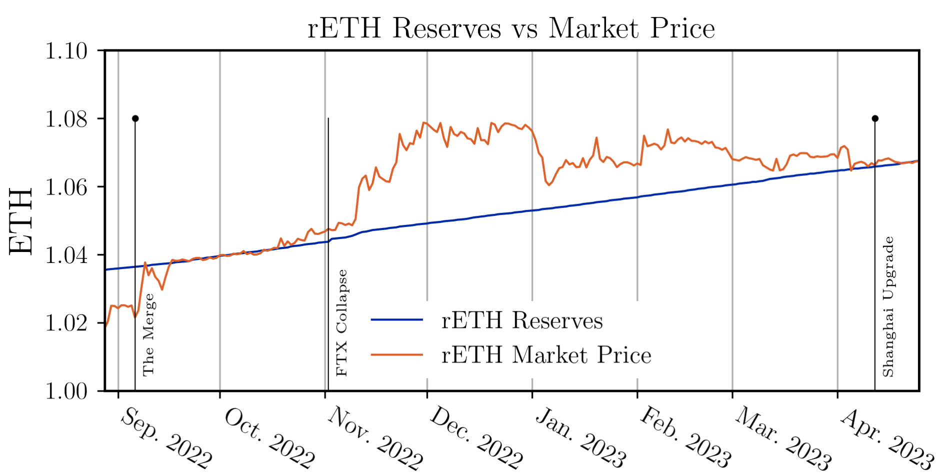

Fig. 12. Divergane of rETH market price from its reserve value in a period between FTX insolvency and the Shanhei upgrade.