Rest Finance: Ethereum Liquid Restaking Protocol

Abstract. Rest Finance issues restETH – the first liquid derivative of restaked ETH on EigenLayer. Rest allows users to earn restaking rewards without maintaining restaking infrastructure or locking up their assets.

EigenLayer is a set of smart contracts on Ethereum that allows consensus layer ETH stakers to opt in to validating new software modules built on top of the Ethereum ecosystem. Ethereum, when compared to other blockchain networks, remains a highly desirable place to transact and store wealth – not because of its efficient and low-cost nature, but because of its robust security. Stakers opt-in by granting the EigenLayer smart contracts the ability to impose additional slashing conditions on their staked ether, enabling an extension of Ethereum's crypto-economic security to new platforms. This results in an opportunity for validators to earn an increased return, but is not without tradeoffs. EigenLayer restaked ether is completely illiquid and, therefore, cannot be utilized across DeFi, unlike the highly liquid market for standard LSTs.

Rest's liquid restaking protocol is a complementary staking protocol to EigenLayer solving for these drawbacks. Users deposit EigenLayer-approved LST (stETH, cbETH, or rETH) into the Rest smart contracts and receive restETH – an ERC20 token representative of restaked ether – while the underlying assets are deposited into EigenLayer smart contracts. restETH is free from all the drawbacks of natively restaked ether, being fully transferable and liquid. The community of contributors surrounding Rest Finance will work to integrate restETH across as many DeFi protocols as possible – as a lendable and borrowable asset, as margin for perpetual futures, as a pair token for decentralized exchanges, and much more.

1. Staking and Restaking

In September 2022, Ethereum upgraded its consensus layer from proof-of-work to proof-of-stake in a process called The Merge. This transformation replaced miners with validators as the ones responsible for participating in the consensus protocol. In proof-of-stake, validators stake thirty-two ETH and are incentivized to participate honestly in securing the network by performing certain duties, or risk forfeiting a varying portion of their staked deposit. Maximizing the yield of a validator requires minimizing the chances of this forfeit, which is referred to as slashing.

1.1 Proof-of-Stake Validator Rewards

Validators that participate in securing the network by executing their key functions are rewarded by the new issuance of ETH, priority fees paid by users, and optionally MEV[1]. These rewards are derived from running both Execution clients, which bundle and execute transactions, and Consensus clients, which grab transactions and block hashes from the execution client and add them to the beacon block. The following are the validator rewards derived from both the consensus and execution layers of Ethereum[2]:

Type	Layer	Frequency	Amount
Attestation	Consensus	Once per Epoch (every 6.4 minutes on average)	0.000014 ETH
Block Proposal	Consensus	Every 2 months on average	0.02403 ETH
Sync Committee	Consensus	Every 2 years on average	0.11008 ETH
Slashing Reward	Consensus	Very rarely included in Block Proposals	Up to 0.0625 ETH
Priority Fees	Execution	Included in all Block Proposals containing transactions	0.01+ ETH
MEV Rewards	Execution	Included in Block Proposals when using MEV-boost	0.01+ ETH

1.2 Restaking on EigenLayer

EigenLayer enables Ethereum validators to deposit to their smart contracts and opt into validating new software modules atop Ethereum – enhancing the crypto-economic security of new Actively Validated Services (AVS). Restaking requires operators to set their beacon chain withdrawal credentials to the EigenLayer smart contracts, which enables them to opt into new AVS and earn fees. Earning fees requires downloading each AVS' off-chain container, a package of additional node software that validators must run. The modules have the ability to impose slashing conditions on the underlying staked ether, thereby preventing adversarial behavior

[1] Maximum Extractable Value, obtainable through mev-boost
[2] Estimations derived from RocketPool returns

against the AVS – the staked ETH represents the cost of corruption for interfering with module security or otherwise misbehaving.

Each EigenLayer restaked validator can choose which software modules they wish to opt into, thus determining which slashing conditions they are subject to. The more AVS' one opts into, the more risk they take on – as they are subject to increased slashing risk. However, the reward is also greater. As different combinations of modules result in differing slashing risks, Rest Finance depositors cannot individually decide which modules to opt into – this task is instead delegated to the DAO.

For users who don't stake ether to the Beacon Chain themselves, EigenLayer permits a variety of ETH liquid-staked tokens (LST) to be deposited into the restaking smart contracts, acting just like Beacon Chain staked ether in the sense that it acts as a cost of corruption for mismanaging the AVS containers.

While restaking is a powerful primitive that comes with an array of new yield opportunities, it is not without opportunity cost. LST such as Lido's stETH, RocketPool's rETH, and Coinbase's cbETH all have some degree of integration within DeFi, giving their users a greater variety of opportunities to choose from. Consequently, restaking with EigenLayer comes with a great deal of opportunity cost, as ETH restaked does not natively issue a fungible token, nor is it liquid across any secondary markets. Additionally, fees associated with restaking and claiming fees can be costly, to the point of being prohibitive for smaller actors.

2. Design Ethos

The goal of Rest Finance is to provide a complementary product to EigenLayer that makes up for any trade offs incurred in the process of restaking while maximizing benefits for the end user. The primary objectives of Rest are:

- To enable users to earn boosted staking rewards through restaking without losing immediate liquidity.
- To make it possible for smaller-size users to take advantage of restaking without incurring high costs.
- To reduce the risk of slashing or the otherwise loss of a staked deposit due to software bugs or malicious actors.
- To establish the restETH token as quality collateral within DeFi and introduce it as a building block for other applications and protocols to use in a permissionless fashion.
- To establish the most liquid restaked token available, using algorithmic collateral management systems. We refer the reader to Section 4 for more information.

restETH fulfills our design ethos as a fully liquid, transferable token that gives its holder exposure to restaking rewards without the drawbacks of natively restaking with EigenLayer. It is

integrated with cross-chain messaging rails, and natively functions across multiple blockchains without incurring third-party bridge or wrapper risks. It is designed to maximize user flexibility and developer composability alike.

3. System Architecture

Rest Finance is a collection of smart contracts that work together to facilitate rewards tracking on EigenLayer, account for slashing costs and computing costs, and relay the correct reward rate to the user through the restETH token.

3.1 Rest Deposit Contract

Responsible for withholding capital for the Algorithmic Collateral Manager (ACM), minting restETH for the user, and depositing user assets to EigenLayer for restaking.

3.2 Algorithmic Collateral Manager (ACM)

The ACM mints restETH to pair in a Uniswap v3 LP position alongside withheld ether from the rest deposit contract, essentially creating a debt between the ACM and the protocol. When users withdraw, a portion of the withdrawn ether is derived from the ACM, which then burns restETH from the LP to settle the debt with the protocol (see Section 4).

3.3 EigenLayer Rewards Oracle

The EigenLayer rewards oracle is responsible for tracking the accrual of rewards within the EigenPods and relaying data accordingly to facilitate distribution of restETH rewards.

3.4 restETH

The restETH token is a tokenized version of restaked ETH. When users send ether into the Rest deposit contract, the user receives the corresponding amount of restETH tokens. The restETH token represents user deposits and the corresponding restaking rewards and slashing penalties. The restETH token is a liquid alternative for restaked ether: it can be transferred, traded, used in integrated DeFi applications, and natively moved across multiple blockchains. Rest makes the restETH token balance track the balance of rewards pending in the EigenPod. A user’s balance of restETH tokens corresponds one to one with the amount of ether a user could receive if withdrawals were instant on EigenLayer.

4. Collateral Management

Rest Finance differs from standard liquid staking products, and other restaked ETH products, through its Algorithmic Collateral Management (ACM) system. Maintaining deep liquidity is one of the primary aspects of any liquid-staked token protocol. Deep liquidity allows

users to bypass the restaking queue and minting fees while enabling low slippage exits and the avoidance of the usual seven-day unstaking period enforced by EigenLayer. Additionally, the greater the concentration of liquidity a protocol can maintain around the price of the native LST, the more effectively that LST can be used as collateral across DeFi. While most liquid-staking products are purely wrappers for the underlying Beacon Chain staked ETH, Rest differs as it is partially collateralized by restaked ETH and partially by ETH deposited within a DEX liquidity pair. Let's go through an example:

> Vitalik deposits 100 ETH to the Rest Deposit Contract and receives 100 restETH in exchange. The deposit contract restakes 90 ETH immediately and deposits 10 ETH to the ACM. The ACM then mints another 10 restETH and deposits them along with the 10 ETH already collected from Vitalik's deposit into a Uniswap v3 Concentrated Liquidity Position. The yield Vitalik earns from his 100 restETH is a combination of the restaking yield from EigenLayer, and the yield generated by the liquidity position.

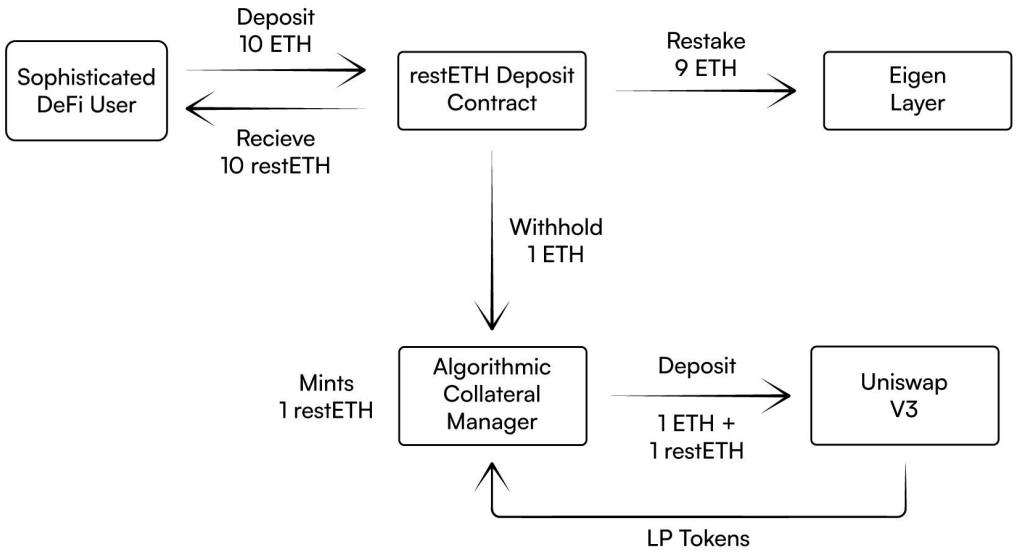

Figure 1: Restaking Deposit Flow

At this stage, the total supply of restETH exceeds the total number of ETH, restaked or otherwise, in the system. This does not, however, indicate bad debt or insolvency in any way. The entirety of the surplus restETH is contained within the ACM's LP position, meaning that it can be removed and burnt at any time, thereby eliminating the debt. Let's look at an example of the ACM reducing the supply of restETH:

Vitalik has accrued 10% yield[3] on his restETH thus far and seeks to exit, redeeming 110 restETH for ETH. Accordingly, the withdrawal contract redeems 99 ETH restaked on EigenLayer, which is a seven-day process. It also redeems 11 ETH from the ACM's liquidity position. In exchange, Vitalik's 110 restETH are burnt, along with 11 restETH from the liquidity position. In sum, the protocol has released 110 ETH but burnt 121 restETH, thus rebalancing the total supply of restETH with the number of ETH deposited in the system.

As illustrated, upon withdrawal the surplus restETH is burnt, thus restoring supply parity. At any point in time if the system becomes overweighted with restETH compared to ETH, the ACM is able to burn surplus debt to restore this parity. This ACM system is inspired by the Algorithmic Market Operations Controller (AMO) v2 system employed by Frax in the design of frxETH, which is a relatively battle-tested system. Their implementation in frxETH have been consistently profitable, and the system has remained fully solvent since inception.

The ACM varies in the sense that it does not rely on emissions from Curve to incentivize liquidity but instead employs more aggressive strategies on Uniswap V3 combined with peg arbitrage to generate yield for liquidity providers. With new incentive layers being built atop concentrated liquidity DEXs, the moat Curve once held for stable-pair swaps is now rapidly diminishing. Additionally, the "Curve Wars" are filled with incumbents – innovation lies on the frontier of more customizable liquidity positions, with more effective liquidity provision per dollar provided.

5. Risks and Mitigations

5.1 Smart Contract Security

Smart contract security has to be the highest priority for the community of contributors surrounding restETH. restETH will launch with multiple audits by leading firms, and maintain a bug bounty program to incentivize community participation in security.

5.2 EigenLayer Technical Risk

Rest is built atop experimental technology. The failure of this underlying primitive would spell the end for Rest Finance, and the destruction of the value that backs restETH. The largest source of risk for EigenLayer, apart from smart contract security, is the lack of active risk mitigation by module developers. EigenLayer's whitepaper details how, in some instances, when

[3] Let's assume that the 10% APR was generated equally by restaking rewards and returns from the liquidity position, for the sake of this example.

multiple modules accept validation from the same party, profit from corruption can rise far beyond the cost of corruption and thus leave the system open to attack[4].

5.3 Slashing Risk

EigenLayer restaked ether is subject to greater slashing risks than standard Beacon Chain staked ether. This is because computational requirements and slashing conditions snowball as the user opts into more modules. Rest Finance mitigates these risks by carefully selecting the AVS it opts into. Rest only secures modules that have been admitted by EigenLayer's veto committee, which has the ability to rollback slashing. The set of new AVS that EigenLayer enables is quite broad, encompassing new blockchains, middleware, data availability layers, and much more. Accordingly, the potential for software error can be high, especially as these new systems become battle-tested. The veto committee exists to protect user assets in the case of system errors or malicious slashing, thereby reducing smart contract risk for EigenLayer-based protocols such as Rest.

5.4 restETH Price Risk

It is possible that at times, the restETH price may not be at par with the value of its underlying assets. This could be indicative of market sentiment or unusual market behavior. Rest Finance mitigates this risk through the ACM system, which enables constantly deepening liquidity and automated arbitrage to protect the peg.

[4] EigenLayer: The Restaking Collective, 3.4.1