Faro: Liquid Staking Protocol for Decentralized Layer-2 ZK-Rollups

Tal Derei, Xinhao Liu, Steve Ye

July 2022

Abstract

Proof-of-Stake (PoS) is a consensus mechanism used by blockchains to achieve distributed consensus. In PoS blockchains, staking is the process of locking up tokens to ensure the security of the underlying network. Staking ultimately exposes the end-user to an inherent feature built into its design: locked liquidity. Staking includes a minimum lock up period, ranging on average a few weeks, where user funds are locked and inaccessible. In more extreme cases, for instance on Ethereum 2.0 beacon chain, user staked deposits represent frozen assets that cannot be withdrawn until post-merge. This further introduces price risks, where the price of your deposited asset is lower compared to when you deposited it. Liquid staking addresses these concerns by allowing users to earn staking rewards without lock up periods or maintaining staking infrastructure. **Faro** serves as a liquid staking protocol for decentralized, layer-2 ZK-Rollups. Faro means "*lighthouse*" and aims to be the beacon for layer-2 staking. We motivate the technical specifications in further detail below.

1 Motivation

As of the publication of this whitepaper, all major ZK-Rollups are still centralized. Their current setup consists of a single non-censorship resistant node operator. They plan to progressively decentralize their sequencers and release the open-source software for running sequencers and provers in the coming year. Facilitating their decentralization also involves launching a native token to compensate node operators for actively operating staking infrastructure and securing the network through consensus participation. This will unlock a new wave of protocols like liquid staking on Layer-2s.

Liquid staking is an alternative to locking up staked assets, allowing users to access their funds while they're staking them. **Faro** is a liquid staking protocol for ZK-Rollups. Faro

offers liquid staking services for everyone, without withdrawal lockups or minimum deposit requirements commonly seen in self-staking or custodial exchange staking. The staking process involves depositing layer-2 tokens in Faro smart contracts deployed on the Ethereum mainnet and receiving "*stToken*" -- a tokenized version of staked deposits -- in return. stToken represents a staking derivative token backed 1-to-1 to a user's initial stake. It can be freely exchanged and used across the DeFi ecosystem to compound their yield on top of the staking rewards, ultimately leading to greater capital efficiency and utility. Liquid smart contracts controlled by the Faro DAO then allocate user funds by staking them with node operators.

Faro incorporates a hybrid liquid staking model that will undergo two phases in its protocol roadmap:

- **Phase 1:** Faro maintains an initial set of trusted node operators responsible for running validator software and managing a stable staking infrastructure on Layer-2s. These node operators are professional staking providers, thoroughly vetted to ensure the safety of protocol funds and maximal uptime. Each node operator manages multiple validator nodes, known as sequencers and provers, and their respective private keys. Node operators perform actions to maintain the health of the network such as validating signatures, packaging transactions into blocks, and generating proofs on the network. The Faro DAO will initially be permissioned, governed by the founding team and set of node operators.
- **Phase 2:** Phase 2 will begin as soon as Faro can maintain baseline stability and security. With the ethos of progressive decentralization in-mind, Faro plans to decentralize the DAO and validator set and allow anyone to become a node operator. This means anyone with the proper hardware requirements will be able to run their own node with Faro. This hybrid system prioritizes a high degree of network security for proof-of-stake systems on ZK-Rollups upon their initial decentralization.

Faro's staking pool initially applies a 10% service fee as a percentage of the rewards from the staked principle by minting a proportional amount of stToken. This fee is evenly split between Faro node operators and the DAO's treasury account. The DAO also maintains a slashing insurance fund to compensate for slashing penalties. The remaining staking rewards go to stToken holders through a rebasing mechanism that increases their stToken balances. These fees are adjustable by the DAO and are fully auditable and transparent.

2 Liquid Staking Protocol

2.1 Faro DAO

We foresee competition from centralized exchanges as well as other decentralized protocols like Lido in time. The DAO is a logical compromise between centralization and decentralization. Our protocol is highly dependent on the designs and specs of the various Layer-2 chains, which may change at any time. Therefore, our protocol should be upgradeable to stay competitive. The DAO allows us to perform upgrades with the speed of centralized exchanges, without full centralization or custody. The DAO treasury will accumulate a portion of platform fees, which will be used to fund public goods such as development work and slashing insurance. It further determines key protocol parameters and executes Faro network upgrades appropriately.

The Faro DAO will initially be governed by the founding team and full node operators. Governance will eventually open up to the public by launching the FRO governance token through a ERC-20-compliant token smart contract during **Phase-2**. The base layer of the protocol will integrate core DAO functionality to ensure that token holders have full control over core governance decisions of the platform. FRO will also integrate core DeFi functionality (staking rewards and liquidity pool) to capture the value generated by the platform to redistribute to FRO token holders. FRO will act as the DAOs governance token for on-chain voting for network related modifications. DAO voting ultimately acts as a publicly verifiable form of decentralized participation, allowing community members to participate in the state of our network.

2.2 System Architecture

2.2.1 Stack

Faro's core protocol smart contracts will be deployed on Ethereum as we suspect most networks will manage their staking logic on Ethereum's mainnet. Faro is therefore implemented as a set of base-layer Ethereum smart contracts governed by the Faro DAO. The DAO will bootstrap the protocol by initially deploying the protocol smart contracts and undergoing key important events before assigning an initial set of node operators to the DAO:

- Selecting participants for the BLS based m-of-n threshold signature scheme represented by the initial staking providers.
- Facilitate the multi-party computation (MPC) ceremony to create the threshold signature withdrawal account to service withdrawals.

Faro is a hybrid liquid staking model split into two phases. The system architecture for **phase 1** consists of multiple modular parts for maximal composability. The key protocol components are described below.

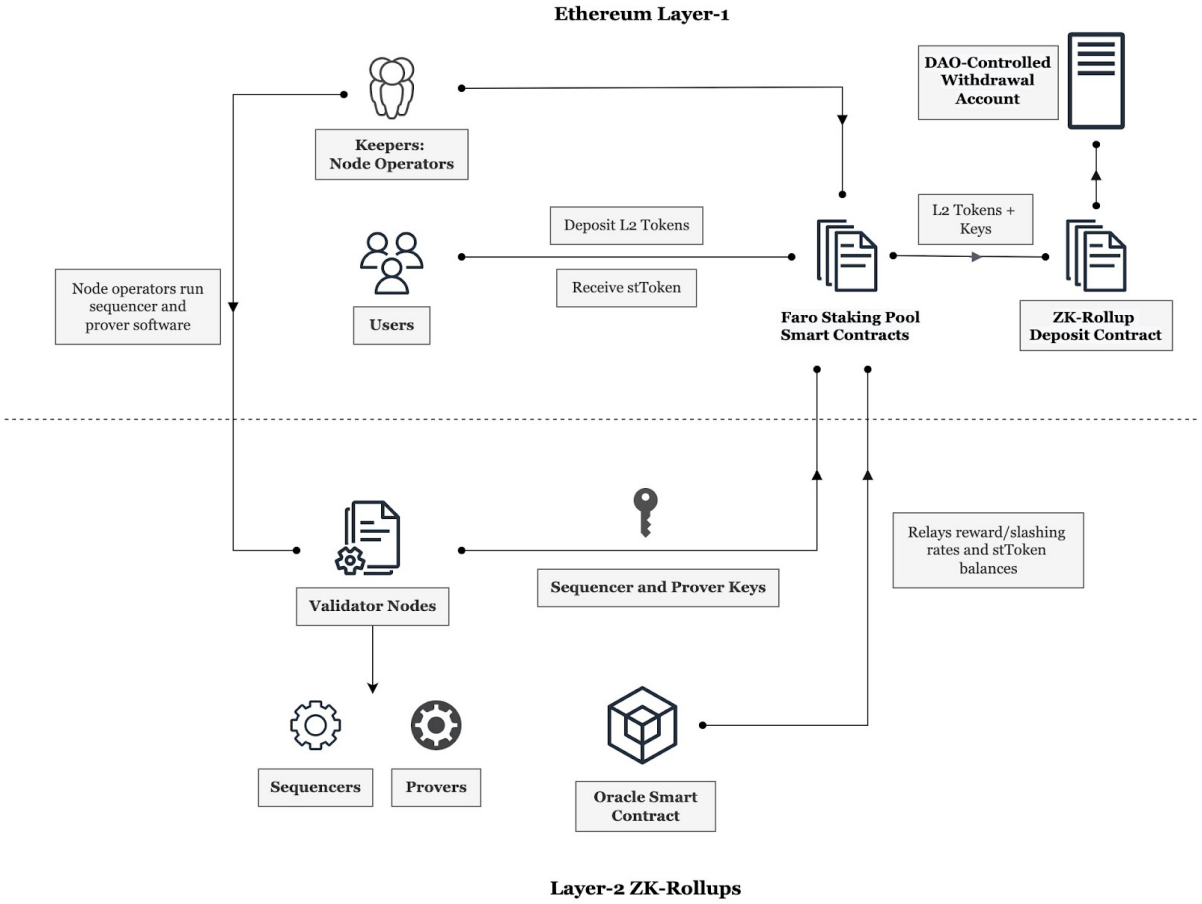

Figure 1: Phase 1 of the Staking Design Flow

1. **Liquid staking pool deposit contracts:** responsible for token deposits/withdrawals, minting/burning of stToken derivative tokens, delegating user funds to node operators, and applying fees to staking rewards.

2. **Keepers (Node Operators):** manage validators (sequencers and provers) that are responsible for achieving network consensus, validating transactions and packaging them into blocks, and generating zero knowledge proofs.
    a. **Light Keepers (Sequencers)** are equivalent to full nodes on Ethereum: ordering transactions, executing transactions, and batching multiple transaction executions into blocks.
    b. **Heavy Keepers (Provers)** generate the computationally heavy zero-knowledge proofs that are posted on Layer-1, alongside the call-data for data availability. Then optimized precompiled smart contracts on Ethereum perform the lightweight proof verification on-chain.
3. **Layer-2 oracles:** monitor node operator accounts and relay reward/slashing rates to determine stToken balances.
4. **Faro DAO:** responsible for governing protocol parameters through FRO ERC-20 governance token.
5. **stToken derivative token:** ERC-20 earning staking rewards minus slashing penalties.

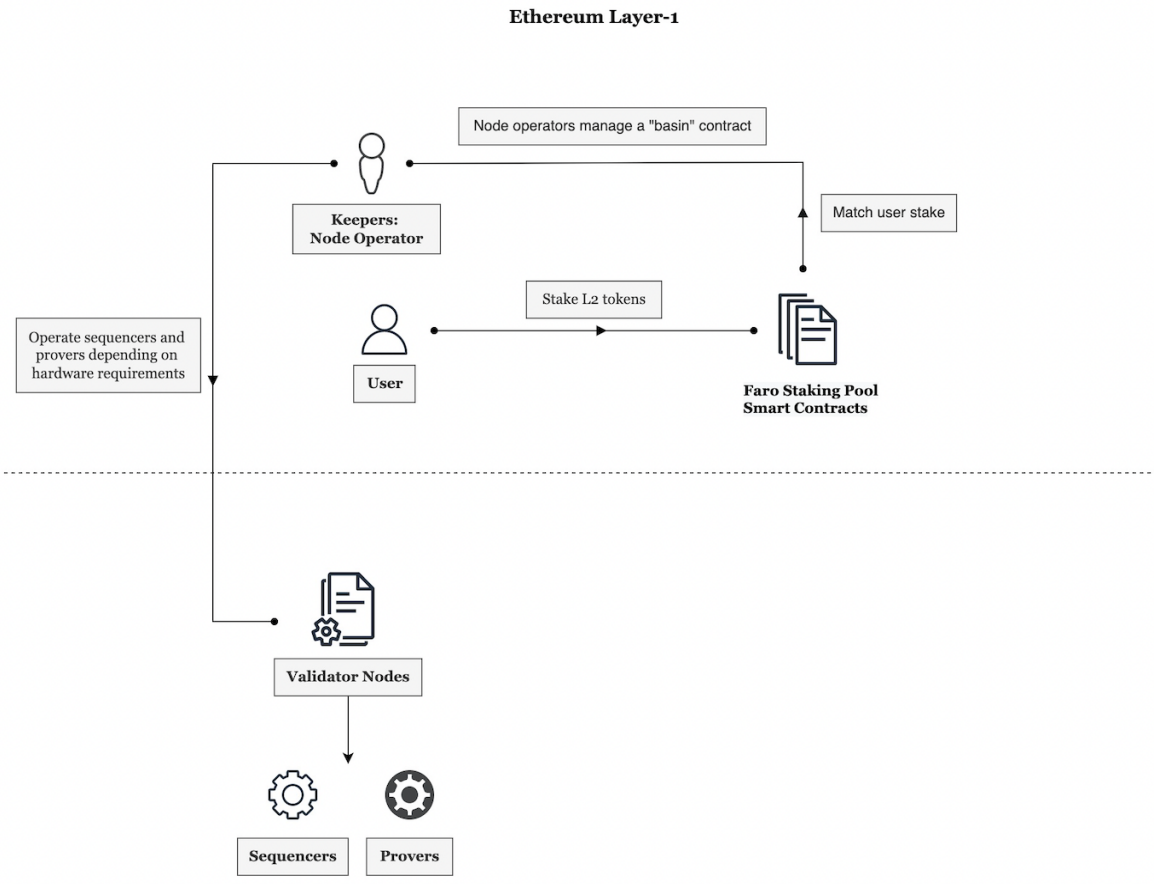

Figure 2: Phase 2 of the Staking Design Flow

Phase 2 will expand this architecture by introducing **"basins"**, representing a smart contract instance on Ethereum that an individual node operator manages. This allows them to create a validator and set up their own staking infrastructure. They can choose between running Light Keepers (Sequencers) and/or Heavy Keepers (Provers), each having drastically different hardware requirements. Staking rates will therefore be dynamic and incur different network fees. With Faro, running a node will require staking a minimum of half of the staking requirement yet to be determined by ZK-Rollups. Faro will then proportionally match the user's stake from other user deposits.

In summary, ZK-Rollup networks are currently in the process of formulating their decentralization designs. The network logic implemented in Faro smart contracts is subject to change depending on how these decentralization protocols are structured and released. Other network aspects like the type of proof-of-stake systems and MEV also need to be considered.

2.2.2 POS designs

The proof-of-stake (PoS) network for decentralized sequencers can take on several design choices. The following are the two most likely PoS systems for ZK-Rollups.

- **Permissionless PoS with Leader Election**: Byzantine Fault Tolerant (BFT) based Proof-of-Stake design with a leader election that rotates the sequencers. If some sequencers are faulty, it will require a Byzantine Consensus (honest majority) to successfully publish the state.
- **Permissionless PoS with MEV Auctions:** auction model that replaces a specified leader election mechanism, with sequencer duties awarded to the highest bidder.

2.2.3 Miner-Extractable Value (MEV)

ZK-Rollups currently maintain a single node operator, enabling them to frontrun transactions and extract MEV in-theory. Upon their decentralization, MEV will be opened to the community of stakeholders. One approach is to remain neutral and opt out of MEV altogether as validators don't have the option to extract MEV unless it's explicitly enabled by the protocol. Another approach is to prioritize MEV and pass on the rewards to users. The way Faro DAO approaches MEV is subject to change.

2.3 Tokenomics

2.3.1 FRO Governance Token

FRO represents the governance token used in the Faro DAO. FRO voting power is proportional to the amount of staked FRO in the voting contract. A token distribution will be decided in the future.

2.3.2 stToken

stToken is the derivative token that represents a claim to the underlying asset that's been staked. In Faro's context, an stToken is an ERC20 liquid derivative token of the native staking token of a supported ZK-Rollup.

When a user stakes their underlying token with Faro, an equivalent amount of stToken will be minted in their wallet. Conversely, anyone may burn stTokens through Faro to redeem the underlying token. This redemption process is subject to any unbonding period specified by the ZK-Rollup's native staking design. stTokens are backed 1:1 with the underlying tokens staked with Faro, which means there is no risk of a bank run.

stToken's value is related to the future expected price movements of the underlying asset. It is the team's duty to ensure the initial liquidity of the stToken derivative token and make it available on major decentralized exchanges. Faro will further prioritize liquidity integrations on DeFi protocols like Curve.

2.4 Risks

Decentralized ZK-Rollups are an experimental technology under active development. There's no guarantee these networks will be free of errors/bugs. New chains and proof-of-stake systems are always subject to systematic risks and potential attack-vectors. These risks will slowly mitigate as the network matures and the sequencer/prover software is better understood.

Additionally, staking incurs the risk of losing the face value of the token. Irrespective of the staking APY rates, the volatility of crypto assets is concerning and can affect staking volume. For example, investors tend to stake their assets less in a bear market for this very reason. This can lead to an imbalance in the exchange rate between stToken and the native layer-2 token as a result. Therefore, risk management in times of downward network fluctuations is necessary.

On the validator side, there's a risk for sequencers and provers to incur slashing penalties for going offline and double signing transactions. Faro onboards reputable node operators with previous experience in maintaining staking infrastructure in response. Faro also maintains a slashing insurance fund to protect against sizable slashing events.

2.5 Unknowns

Until ZK-Rollups decentralize their sequencers and open-source the software for running sequencers and provers, there are currently several unknowns in the implementation details of these networks:

- Networks have not fully finalized their decentralization roadmaps and decentralization may not be a priority right now;
- How staking will work with multiple full nodes (sequencers and provers) and their dynamic fee structures;
- New risks in the liquid staking space related to running sequencers and provers and on Layer 2;

2.6 Conclusion

As ZK-Rollups continue with their accelerated growth, the security of these networks will depend on the amount of staked tokens and their level of decentralization. Locked withdrawals and minimum staking requirements will result in some users not being able to afford self-staking. For many users, they will either have to stake with a centralized custodial exchange or pass on staking altogether. We do not expect exchange staking to offer rewards comparable to self-staking. Additionally, this scenario presents a tangible risk of network centralization as these exchanges will likely end up with very large stakes.

Liquid staking offers a viable alternative to both self and exchange staking. Faro provides a balance of risk, reward, and convenience. It allows users to quickly enter or exit staking positions of any size. Smaller wallets may stake without losing access to a significant portion of their funds, while larger entities will be able to hedge against price volatility.

Faro is ultimately committed to opening the liquid staking space to ZK-Rollups. As the broader ecosystem and user adoption of these networks grows, Faro will be well positioned to service their staking needs.