Pirex ETH: Ethereum Liquid Staking Token Powering the Dinero Protocol

sami@redacted.finance, never@redacted.finance, funky@redacted.finance

Abstract

In this whitepaper, we propose a new type of Liquid Staking Token ("LST") for Ether ("ETH"), called Pirex ETH or pxETH. pxETH is built on top of the Redacted DAO's Pirex platform and forms an integral part of the Dinero protocol, a protocol which aims to vertically integrate ETH staking, block proposal and building, a Remote Procedure Call ("RPC"), leverage, and yield stripping into one synergistic ecosystem comprising pxETH, the Redacted Relayer RPC, and the DINERO stablecoin. pxETH provides users with a liquid and fungible tokenized staked ETH which benefits from Ethereum staking rewards and other revenue forms such as maximal extractable value ("MEV") tips and block rewards. Future pxETH yield and pxETH withdrawals can be tokenized and used within decentralized finance ("DeFi").

Keywords: ethereum, liquid staking, MEV, stablecoin, relayer

1 Introduction

1.1 Motivation

As the Ethereum ecosystem evolves, the demand for innovative solutions that enrich the user experience in DeFi is accelerating. Notably, a challenge facing users is the lack of liquidity and flexibility in staking ETH, which discourages many from participating in Ethereum's proof-of-stake system and staking rewards. Additionally, the lack of competition in the liquid staking vertical has led to monopolization, which poses its own set of risks to the Ethereum network.

In response to these challenges, we designed pxETH to bring Ethereum staking to DeFi in a way that allows users to make better use of their ETH holdings. By vertically integrating this functionality into the Dinero protocol, we hope to deliver a holistic solution that combines several useful tools under one, easy-to-use protocol.

1.2 Overview

The Dinero protocol vertically integrates ETH staking, block proposal and building, RPC,[1] leverage, and yield stripping into one synergistic ecosystem comprising pxETH, the Redacted Relayer RPC, and the DINERO stablecoin.

pxETH is a liquid and fungible receipt token for ETH deposited into the Dinero protocol. Nearly all of this ETH is staked by the Dinero protocol, which is used to run validator nodes on the Ethereum network, which in turn power the Redacted Relayer RPC. The remaining marginal amount of ETH, known as the ETH buffer, is kept unstaked to facilitate: (i) pxETH liquidity; (ii) ETH staking and unstaking; and (iii) self-sufficient meta transactions via the Redacted Relayer RPC.

1.3 Leveraged yield

The pxETH token itself does not earn any rewards. However, pxETH can be deposited into an auto compounding rewards vault in exchange for apxETH, a vault share token. This vault benefits from Ethereum staking rewards and other rewards such as MEV[2] tips and block rewards generated by the Dinero protocol (minus fees), which are compounded into pxETH. As rewards are earned by the vault over time, the amount of pxETH underlying each apxETH increases.

With the Redacted DAO incentivizing pxETH (and not apxETH) liquidity on decentralized exchanges ("DEXs") through its treasury holdings, not all pxETH is expected to be deposited in the rewards vault, as a portion of it will be in incentivized LPs. This scenario creates a leverage effect on the rewards, with 1 pxETH in the rewards vault linked to rewards from more than 1 ETH staked within the Dinero protocol.

1.4 Yield stripping

Yield from the apxETH vault can be tokenized through yield stripping. For example, if a user wants to tokenize 1 year of yield for 1 pxETH deposited in the rewards vault, they can exchange 1 pxETH for:

- 1 pxETH principal semi-fungible token which can be exchanged for 1 pxETH in one year; and
- 1 pxETH yield semi-fungible token for each rewards period in the next year, which can be exchanged for the rewards earned by 1 pxETH in the rewards vault in one rewards period.

Users have the ability to choose how many rewards periods they wish to tokenize. These yield and principal NFTs are semi fungible, composable within DeFi, and can be traded (e.g. on the Pirex Marketplace).

Yield stripping provides users the ability to leverage, hedge, and speculate on future pxETH price and future yield. The trading of future yield and future pxETH could

---

[1]RPC (Remote Procedure Call) allows local systems to execute functions, like sending transactions or fetching data, on a remote Ethereum node.

[2]Maximal extractable value (MEV) refers to the maximum value that can be extracted from block production in excess of the standard block reward and gas fees by including, excluding, and changing the order of transactions in a block. See https://ethereum.org/en/developers/docs/mev/.

be a large market, especially considering the various liquidity mechanisms available to pxETH which are designed to keep the pxETH:ETH peg tight, therefore providing access to the futures market of the second largest crypto asset, ETH.

1.5 pxETH liquidity

In addition to the DEX liquidity for pxETH incentivized by Redacted DAO, the Dinero protocol has additional mechanisms to improve pxETH liquidity and support the pxETH:ETH peg in both normal and adverse market conditions allowing for greater pxETH DeFi composability.

ETH can be withdrawn from the Dinero protocol in exchange for pxETH, either from the ETH buffer or ETH unstaking. A novel incentivized withdrawal pool facilitates quicker pxETH withdrawals especially when there is an ETH unstaking queue and/or adverse market conditions.[3]

These mechanisms increase the capital efficiency of liquidity, allow for DEX peg arbitrage, reduce the reliance on expensive DEX liquidity, and crucially, provide vital liquidity during adverse market volatility — a critical component for DINERO vaults. The DEX liquidity bootstrapped by Redacted DAO and the aforementioned liquidity mechanisms should provide important pxETH liquidity in both favorable and unfavorable market conditions, which should allow pxETH DINERO vaults to support lower collateral ratios than other LST stablecoins.

1.6 Pirex ETH in Dinero Protocol

The Dinero protocol vertically integrates ETH staking, block proposal and building, an RPC, leverage, and yield stripping into a synergistic ecosystem offering. pxETH plays a foundational role in the Dinero protocol. ETH underlying pxETH is used to operate validators on the Ethereum Network, which power the operations of the Redacted Relayer RPC, including block proposal and building. apxETH, which users receive when they deposit pxETH into the rewards vault, can act as collateral for DINERO stablecoin loans. DINERO is the currency of the Redacted Relayer RPC, with all MEV tips being paid in DINERO. pxETH and its underlying ETH not only powers this ecosystem but also reaps benefits from the value generated within.

Tokens within the Dinero protocol such as pxETH, apxETH, pxETH yield, pxETH principal, DINERO, etc. are composable within DeFi, allowing for an array of DeFi primitives to be built atop them.

---

[3]There are limits on the rate at which validators can enter and exit the Ethereum network, based on the number of validators there are in total. See https://hackmd.io/@ghosts0301/rkmOjqY7t.

Fig. 1 Overview of pxETH within the wider Dinero protocol
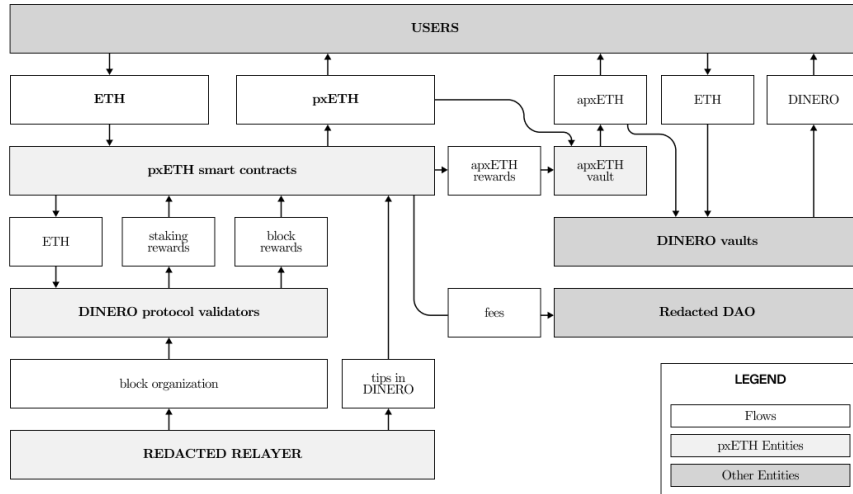

1.7 Omnichain (Cross-Chain)

Tokens such as apxETH and DINERO will be completely omnichain, allowing for greater composability across various chains and protocols.

2 System Architecture

2.1 pxETH deposits

ETH is deposited into the Dinero protocol on-chain via immutable pxETH smart contracts. pxETH, an IOU token, is minted 1:1 for deposited ETH. The majority of the ETH is staked by Dinero protocol validators and used to validate transactions. The remainder is kept unstaked and is referred to as the "ETH buffer".

Fig. 2 Overview of pxETH system architecture
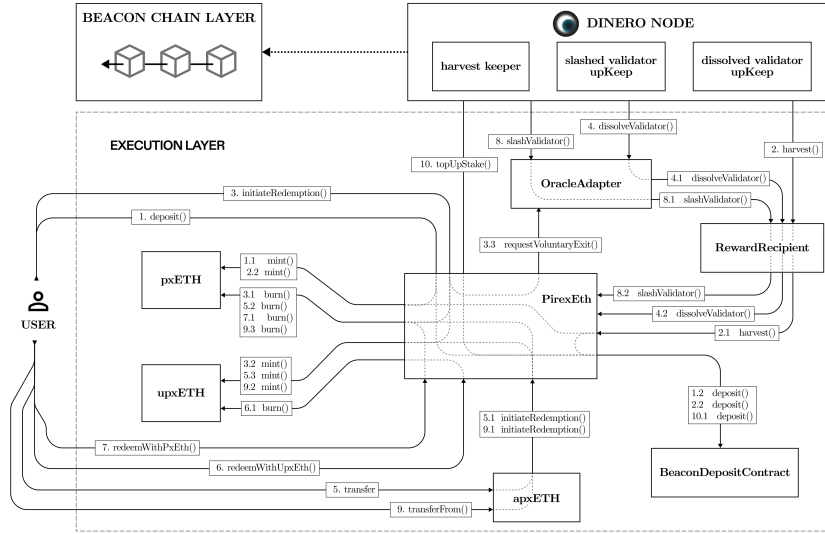
2.2 Validators

Nearly all of the ETH deposited into the Dinero protocol is staked on the Ethereum network by validators. These validators will use a custom Ethereum execution client integrated with Dinero smart contracts for validator and withdrawal key management. At first the validators will be primarily operated by Dinero protocol itself, however, in the future it will be possible for outside parties to operate validators.

The validators will be used to secure the Ethereum network and also operate the Redacted Relayer RPC once enough ETH is staked to allow for consistent successful block proposals.

Validators are spun up when the pending deposits are larger than the deposit size of 32 ETH plus the buffer.

2.2.1 ETH buffer

A small percentage of the ETH deposited into the Dinero protocol is kept unstaked. This helps to facilitate staking and unstaking, which occurs in 32 ETH increments, while also allowing for some ETH withdrawals from the Dinero protocol and self-sufficient meta transactions via the Redacted Relayer RPC. The Redacted DAO's policy arm will adjust the ETH buffer and other pxETH variables following a transparent process approved by the DAO.

2.2.2 pxETH withdrawals

ETH can be withdrawn from the Dinero protocol in exchange for pxETH. This ETH either comes from the ETH buffer (if there is ETH available) or from the spinning down of validators and the unstaking of ETH. In cases where the withdrawal requires

spinning down validators, a user will receive upxETH, issued as an ERC-1155 token, in exchange for their pxETH, which can be redeemed for ETH once the relevant validator(s) has been spun down.

A withdrawal fee is levied on withdrawals, with a larger fee for withdrawals from the ETH buffer, reflecting the greater ease of withdrawal. These withdrawal mechanisms allow for ETH:pxETH peg maintenance and for greater liquidity, especially during times of market volatility.

2.2.3 Withdrawal pool

There are limits on the rate at which validators can enter and exit the Ethereum network, based on the number of validators there are in total. Therefore, if there is a significant ETH unstaking queue, this can hamper the timeliness of ETH withdrawals from the Dinero protocol from the spinning down of validators.

In these circumstances, an incentivized withdrawal pool can be used to improve pxETH liquidity from ETH unstaking. Users can deposit ETH into a pool and receive rewards whilst they provide liquidity to that pool. Where there is an unstaking queue and ETH from the spinning down of validators is not readily available, ETH from this pool is provided to users in exchange for pxETH, with the exchange rate or price being determined by demand for ETH from the pool. As pxETH is redeemed and validators are spun down, ETH is replenished in the pool. Depositors into the withdrawal pool therefore receive rewards in exchange for potential ETH illiquidity.

As pricing depends on the demand for ETH in the pool, rewards on deposited ETH increase during periods of high demand, allowing the pool to scale when demand is high. This makes liquidity provision more efficient and cost effective.

Fig. 3 Overview of withdrawal pool
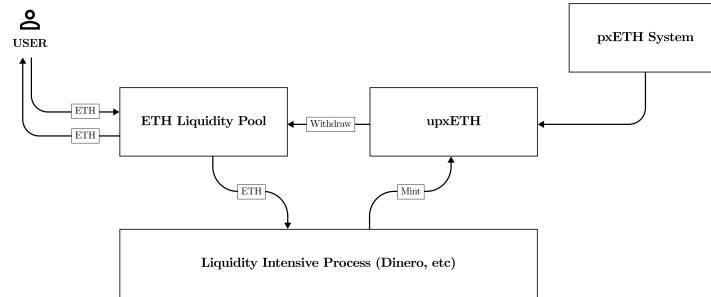
2.3 Validator reward distribution

Validators will receive rewards in the form of Ethereum staking rewards, block rewards, MEV, and tips generated by the Redacted Relayer RPC. These rewards, less variable fees based on the type of reward, are distributed.

Consensus Layer Rewards: In Ethereum, at least 66% of nodes agree on the global state of the network. Consensus layer provides incentives for participating in proposing or validating blocks, voting for their view of head of chain and participating in sync committees.

- **Block proposal reward** - Rewards for proposing blocks as well as whistleblowing rewards for providing evidence of dishonest validators.
- **Attestation Reward** - Every epoch or 6.4 minutes, a validator proposes an attestation to the network. The voting from all the validators are compiled to reach consensus regarding the state of the Ethereum blockchain. Validators vote for a source checkpoint for Casper FFG, target checkpoint for Casper FFG and chain head block for LMD-GHOST.
- **Sync committee reward** - Sync committee is a group of 512 validators. Every 27 hours or 256 epochs, 512 validators are randomly assigned by the Ethereum network to a sync committee. The committee continually signs block header. Validators in the sync committee can get significantly more rewards by serving light clients. The purpose of this committee is to allow light clients to verify a block (i.e. authenticate block signature) without needing to connect to an external provider.

Execution Layer Rewards: Execution layer rewards are available to validators for validating a block (group of transactions). These rewards are paid directly to the Pirex ETH validator contract.

- **Transaction priority tips** - Transaction priority tips are associated with each transaction where the sender would include them to incentivize Dinero validators for processing transactions faster.
- **MEV tips** - Dinero nodes come with MEV-boost enabled. MEV searchers might tip the Dinero validators for processing bundles of transactions quickly.

2.3.1 apxETH

The pxETH token itself does not receive any rewards. However, pxETH can be deposited into an auto compounding rewards vault in exchange for apxETH, a ERC-4626 vault share token. This vault benefits from validator rewards (less fees), which are compounded into pxETH. As rewards are earned by the vault over time, the amount of pxETH underlying each apxETH increases. apxETH is fungible and composable within DeFi and can be used as collateral for DINERO stablecoin loans.

The Redacted DAO will incentivize DEX pxETH liquidity using its treasury and BTRFLY emissions. DEX's with good levels of bribe efficiency will be targeted, so as to make best use of these treasury assets, boost yields on LP positions, and increase pxETH TVL. With not all pxETH being deposited in the rewards vault (some being in liquidity positions), this scenario creates a leverage effect on the rewards, with 1

pxETH in the rewards vault linked to rewards from more than 1 ETH staked within the Dinero protocol.

2.3.2 Yield stripping

Yield from the apxETH vault can be tokenized through yield stripping. When yield stripping, users exchange their pxETH in exchange for ERC-1155 NFTs representing future pxETH and future rewards earned by pxETH in the rewards vault. Users have the ability to choose how many rewards periods they wish to tokenize. These yield and principal NFTs are semi fungible, are composable within DeFi and can be traded (e.g. on the Pirex Marketplace).

The tokenization of future pxETH and future returns provides users the ability to leverage, hedge, and speculate on pxETH and future returns. The trading of future yield and future pxETH could be a large market, especially considering the various liquidity mechanisms available to pxETH which are designed to keep the pxETH:ETH peg tight, therefore providing access to the futures market of the second largest crypto asset, ETH.

Fig. 4 Yield stripping example
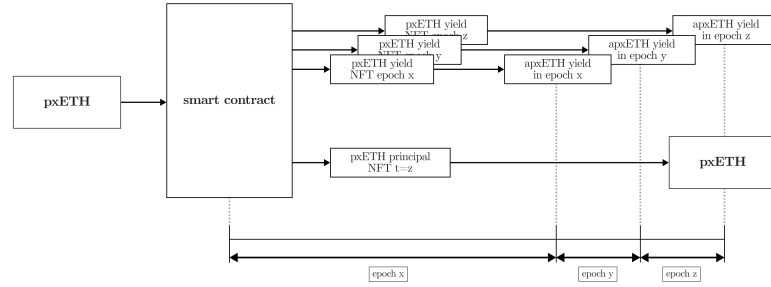
2.3.3 Omnichain (Cross-Chain)

pxETH will be completely omnichain, allowing for greater composability across various chains and protocols. The Dinero protocol is exploring cross chain solutions from providers such as Layer Zero and Chainlink CCIP. This will allow for easy cross chain transfers where users can take advantage of providing liquidity and/or leveraging their pxETH elsewhere.

The concept of the Dinero protocol can be extended to multiple chains, including experimental zones (such environments could include a zkSYNC instance focused on MEV-minimization powered by their Custom Paymaster module, and a Berachain instance, focused on IBC and interchain security) for implementing new parameters and controllers. The immediate focus will be on acquiring market share on the Ethereum mainnet, complemented by occasional liquidity incentivization programs in collaboration with L2 partners of the Redacted Protocol.

3 Risks

3.1 Slashing

Slashing occurs when validators make attestations or block proposals that violate specific protocol rules, often linked with potentially harmful behavior to the network. Getting slashed means losing a significant amount of the stake and being ejected from the protocol.

Although Dinero protocol validators will do their utmost to avoid getting slashed, there remains a slashing risk. Should slashing occur, the Dinero Protocol Insurance Fund, supported by a portion of the protocol's fees, absorbs initial losses, followed by using validator rewards to cover losses. These protective measures aim to maintain a 1:1 backing of all pxETH with ETH within the Dinero protocol, however this may not be possible in adverse circumstances.

In the event of slashing, the keepers will notify the reward recipient about the same amount of ETH that was released from the beacon chain. The keeper will also pass an array of accounts with corresponding amounts that would face the burn of pxETH equal to the sum of amounts. This array of account addresses will be approved by governance.

3.2 Peg Stability

The ETH:pxETH ratio on DEXs may deviate from the desired 1:1 ratio, especially during adverse market conditions. However, Ethereum's Shanghai Upgrade enables liquidity mechanisms that will facilitate the arbitrage of this peg, thereby helping to maintain stability short and long term.

3.3 Multisig Keys / Validator Keys

Dinero leverages a non-custodial key management platform to secure the protocol. Cryptographic keys are managed using HSM-sealed Nitro enclaves in AWS, where both key generation and signing occur.

3.4 Smart Contract Risks

pxETH will employ immutable smart contracts. The Redacted DAO prioritizes smart contract security, subjecting all code to extensive audits and testing. Despite these measures, no amount of security is infallible. Users should be aware of the risks associated with smart contracts.

4 Conclusion

pxETH is an ETH LST which powers the Dinero protocol, a protocol which aims to vertically integrate ETH staking, block proposal and building, an RPC, leverage, and yield stripping into one synergistic ecosystem comprising pxETH, the Redacted Relayer RPC, and the DINERO stablecoin. pxETH uses immutable smart contracts and a non-custodial key management platform to secure the protocol.

pxETH can be deposited into an auto compounding rewards vault in exchange for apxETH. This vault benefits from Ethereum staking rewards and other rewards such as MEV tips and block rewards generated by the Dinero protocol (minus fees), which are compounded into pxETH. With the Redacted DAO incentivizing pxETH liquidity on DEXs' through its treasury holdings, not all pxETH is expected to be deposited in the rewards vault. This scenario creates a leverage effect on the rewards, with 1 pxETH in the rewards vault linked to rewards from more than 1 ETH staked within the Dinero protocol.

In addition to the DEX liquidity for pxETH incentivized by Redacted DAO, the Dinero protocol has additional mechanisms to improve pxETH liquidity and support the pxETH:ETH peg in both normal and adverse market conditions allowing for greater pxETH DeFi composability.

Yield from the apxETH vault can be tokenized through yield stripping. Users have the ability to choose how many rewards periods they wish to tokenize. These yield and principal NFTs are semi fungible, composable within DeFi, and can be traded (e.g. on the Pirex Marketplace). Yield stripping provides users the ability to leverage, hedge, and speculate on future pxETH price and future yield. The trading of future yield and future pxETH could be a large market, especially considering the various liquidity mechanisms available to pxETH which are designed to keep the pxETH:ETH peg tight, therefore providing access to the futures market of the second largest crypto asset, ETH.