Dinero Protocol, a litepaper

sami@redacted.finance, never@redacted.finance,
fahad@redacted.finance

Abstract

The rise of Layer 2 networks, MEV, and Flashbots has led to the notion of "premium" block space on Ethereum's ledger. This new form of ledger access promises users privacy and protection from malicious actors exploiting economic activity. However, as more power users become attracted to premium blockspace, knowledge of its potential issues – such as monopolization or censorship – grows. As Ethereum matures into the settlement layer for programmable finance, democratizing the ability to operate, capture, and monetize its rich and crowded blockspace should pave the way for new forms of decentralized money.
In this litepaper, we present "DINERO", a permissionless stablecoin backed by user-owned blockspace on Ethereum mainnet.*Users with Ether ("ETH") can utilize the Dinero protocol to stake their ETH and access a premium decentralized remote procedure call ("RPC") that revolves around a stablecoin as a medium of exchange.

Keywords: ethereum, staking derivative, stablecoin, relayer

1 Introduction

Blockspace has emerged as a valuable commodity on the Ethereum network, with its value skyrocketing after the introduction of EIP-1559,[1]which turned blockspace into a stable and predictable fee market. Consequently, transactions with larger tips are more likely to appear earlier in each block, as validators (formerly miners under proof-of-work consensus) are incentivised to prioritize them.

When transactions are submitted to the Ethereum blockchain, they enter multiple memory pools ("mempools") to await confirmation. Validators, responsible for adding these transactions to the next block(s), sort and distribute the transactions and their associated blockspace bids across a peer-to-peer network among all nodes' mempools.

* "Dinero" refers to the Dinero protocol. "DINERO" refers to the stablecoin issued by the Dinero protocol.

[1] https://github.com/ethereum/EIPs/blob/master/EIPS/eip-1559.md

Due to the ordered execution of transactions within a block and the Ethereum network's limitation on the total size of transactions which can be included in each block, blockspace possesses time value. This presents countless opportunities for market participants to capitalize on Maximal Extractable Value ("MEV"),[2] including front-running and sandwich attacks, making unconfirmed transactions susceptible to exploitation.

As blockspace is a limited resource that cannot scale with demand, users needing swift transaction validation must be willing to pay more than other mempool participants. Determining the value of blockspace at any given moment is challenging, leading to continuous fluctuations in bids and, consequently, gas prices for each block.

Dinero is an experimental protocol which capitalizes on the premium blockspace market by introducing: (i) a public and permissionless RPC for users; (ii) a decentralized stablecoin (DINERO) as a medium of exchange on Ethereum; and (iii) an ETH liquid staking token ("LST") which benefits from staking yield and the Dinero protocol.

2 Pirex ETH

The Dinero protocol utilizes an ETH liquid staking token built on top of Redacted's Pirex offering,[3] known as Pirex ETH or pxETH. When users deposit ETH into the Dinero protocol it is tokenized as pxETH, and the underlying ETH is staked to validate transactions. Eventually, Dinero protocol validators will power the Redacted Relayer (as defined below) premium RPC.

Dinero validators will operate a custom Ethereum execution client, which integrates with decentralized smart contracts for key management. To bootstrap pxETH liquidity, a ETH/pxETH pool will be bootstrapped using Redacted's governance power. The upcoming Ethereum Shanghai upgrade will allow staked ETH to be unstaked. This mechanism will allow pxETH to be redeemable for ETH, allowing for peg arbitrage and reduced liquidity provider maintenance costs.

3 DINERO

Learning from previous stablecoin iterations, three issues stand out: (i) centralization risks, (ii) liquidity challenges, and (iii) a lack of product market fit.

DINERO is a collateralized debt position ("CDP") stablecoin primarily backed by ETH, the most decentralized collateral available in the decentralized finance ecosystem. Initially, DINERO will function like a typical CDP stablecoin (e.g. DAI). However, the ultimate goal is to use the underlying ETH collateral to enable a decentralized RPC (the "Redacted Relayer") and a block builder which protects Dinero users from MEV attacks.

DINERO will be the currency of the Dinero protocol as a whole, which will enable users to interact with it. Redacted DAO's governance power (e.g. CVX, CRV) will help bootstrap DINERO liquidity on decentralized exchanges.

[2] https://ethereum.org/en/developers/docs/mev/
[3] https://pirex.io/

3.1 Technical specifications

3.1.1 Collateralization

DINERO will be primarily backed by pxETH and ETH. Additionally, the Peg Stability Module ("PSM") will accept USDC as collateral to alleviate upward price pressure and maintain peg (see below).

The protocol will implement at least two vault types: one for ETH and one for pxETH. Since pxETH will have lower liquidity than ETH, the pxETH vault will enforce more stringent risk parameters.

3.1.2 Peg Stability Module

Like other CDP stablecoins, DINERO will employ a Peg Stability Module (PSM) to help maintain its target price of USD1.00 when its price exceeds USD1.00. Although this increases the centralization of DINERO, the Dinero Protocol aims to reduce reliance on a PSM for price stability once a reliable alternative emerges. While the Dinero protocol relies on a PSM, it will not be married to USDC and the use of other stablecoins will be explored.

3.1.3 Interest Rates

When users mint DINERO against the assets deposited to their vaults, interest (payable in DINERO) will start to accumulate. The Redacted DAO's policy arm will adjust Dinero's interest rates, which are specific to each vault type (e.g. ETH and pxETH vaults), following a transparent process approved by the DAO.[4]

3.1.4 Oracles

Dinero's oracle design, inspired by Liquity,[5] relies on two oracles for its ETH-USD and pxETH-USD price feeds: Chainlink as a primary oracle and a second oracle to be determined by the DAO that serves as a fallback if Chainlink's price feed goes down.

3.1.5 Liquidations

DINERO vault liquidations will be carried out via Dutch auctions. If a vault drops below its minimum collateral requirement, a keeper initiates the liquidation by submitting a transaction to Dinero's smart contracts. The collateral is then removed from the vault and put up for auction.

Dutch auctions begin with a high price, then decrease the price as a function of time. When a bid is submitted, the auction is instantly settled. This enables Dinero's collateral auctions to settle in one block – improving their efficiency for keepers and the protocol alike.

---

[4] This process will be similar to how Maker DAO changes its Stability Fee: https://forum.makerdao.com/t/impact-analysis-lowering-steth-b-stability-fee-to-0/18122

[5] https://www.liquity.org/blog/price-oracles-in-liquity

4 Redacted Relayer

The Redacted Relayer is the final building block of the Dinero protocol. It allows for meta transactions, value capture opportunities for pxETH, and eventually private transactions.

4.1 Meta Transactions

Meta transactions allow users to interact with the Ethereum blockchain without requiring them to pay for network transaction fees in ETH (the native gas token).

Meta transactions allow one transaction to execute within another, such that the creator of the original transaction is not the one executing it and paying the network fee. Rather, the user creates and signs the transaction for authentication. Then, the data is sent to an operator or relayer who publishes it on chain with the help of a second party. For example:

- Users sign a request with their private key, with information needed to execute smart contract logic and send it to a relayer.
- Relayer wraps the request and submits a transaction to a contract.
- Contract unwraps the transaction and executes it on a chain with their own ETH.

The Redacted Relayer will enable DINERO holders to transact on Ethereum using meta transactions, removing the need for ETH. Instead, they'll simply tip the Redacted Relayer with their DINERO.

4.2 Searchers Ethereum Reserve

pxETH will power the Redacted Relayer and the Dinero protocol. The majority of the ETH underlying pxETH will be staked and used for validation, while the remainder will cover ETH transaction fees through the burning of DINERO tips received by the Redacted Relayer. DINERO from the originator is split into two parts: one for paying the transaction fee or validator tip and the other to pay a fee to the pxETH vault.

4.3 Private Transactions

Once the protocol is large enough to process transactions and construct blocks, DINERO will become a gateway token, unlocking access to pxETH's block space, enabled by the underlying staked ETH. This will enable the protocol to ensure private transaction flows pass through the mempool and facilitate additional use cases, such as payment for order flow.

5 Conclusion

Dinero protocol is a manifestation of Redacted DAO's move away from the application layer to the consensus layer. The Dinero protocol comprises of:

- **pxETH** - a new liquid staking solution that offers ETH staking and will enable meta transactions for Dinero protocol users

- **DINERO** - a decentralized and over-collateralized stablecoin with a new approach to collateral utilization and stablecoin use cases
- **Redacted Relayer** - the glue of the system, a permissionless and transparent relayer that lets pxETH and Dinero communicate in order to execute its intrinsic use-case

By combining these three primitives Dinero will offer unprecedented access to Ethereum's blockspace. Dinero will give stablecoins a new use case that serves an untapped segment of the crypto-economy.

This litepaper represents the first iteration of the Dinero protocol. Further details will be made available in future whitepaper(s) and some details are subject to change by the DAO and relevant contributors. The Dinero protocol will continue to iterate further, remaining agile as the ecosystem evolves.