ETHANE: An Efficient Liquidity Locker and Universal Gasless Experience For ERC-20 Tokens

The Ethane Team
info@ethane.app

June 2023

Abstract

Ethane allows for a simple gasless user experience by outsourcing transactions involving ERC-20 tokens to an intermediary smart contract that is then called by a Relayer. The Relayer consumes the gas fee and in exchange for this service, the user will compensate with the ERC-20 token(s) involved in the transaction. In addition, Ethane also provides a cost-efficient liquidity locker solution allowing a user to approve and lock their Uniswap liquidity tokens in one transaction.

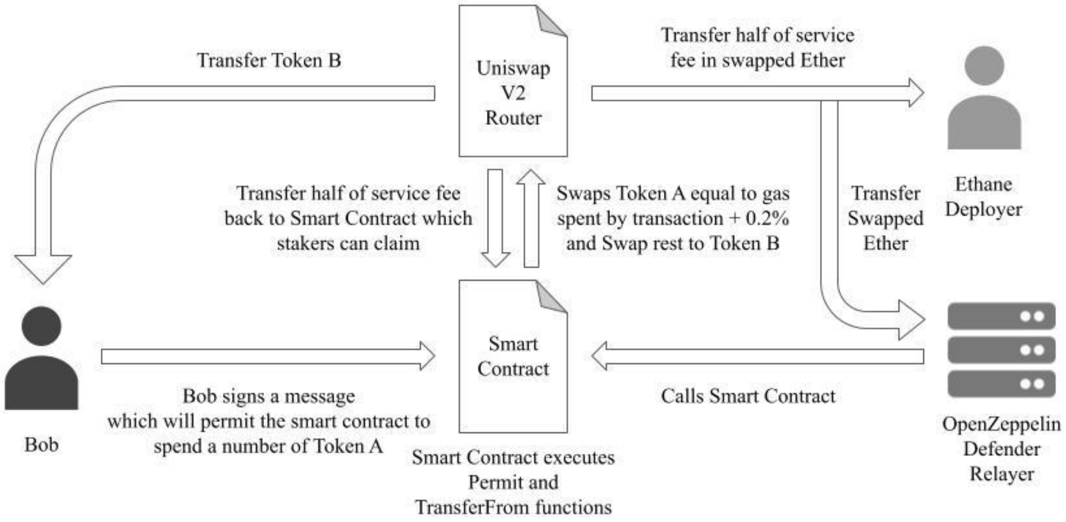
1 INTRODUCTION

The majority of ERC-20 tokens on the Ethereum Blockchain lack the ERC-20 Permit functionality which is a recent initiative that implemented EIP-712 allowing for typed-structured data hashing and signatures. Traditional ERC-20 tokens rely on an owner-first initiative where the owner is required to send a transaction to the blockchain allowing a designated spender to use them. This process is inefficient and requires extra time and gas to be spent. With the ERC-20 Permit extension, token owners can now save time and gas by simply signing a message through their Web3 wallet provider allowing the spender to use their tokens. The spender can now submit approval known as the "permit" and any transfer functionalities in the same transaction.

Now suppose that the owner signs a message permitting a smart contract access to a designated number of ERC-20 tokens. The smart contract can utilize the $transferFrom$ function to transfer the owner's tokens to a designated receiver. The entity calling the smart contract to perform this transaction is called the Relayer. Ethane uses the OpenZeppelin Defender Relay service which serves as the Relayer for the transactions. Since the Relayer is handling the transaction, the token owner and the receiver which the smart contract is transferring tokens to from the owner, do not pay any gas. The owner has only signed a message and no action is needed from the designated receiver. The Relayer is responsible for the gas required by the transaction it sent to the blockchain. With the use of a Relayer, a token owner can now send tokens to a designated receiver without needing any Ethereum to pay gas.

2 ECONOMICS

In order for the transaction model described in the previous section to be economically viable, the ERC-20 token involved is required to have liquidity on Uniswap. When a Relayer sends a transaction to the blockchain, their Ethereum balance will decrease as a result of paying gas. If they continue to sponsor transactions, the Relayer will lose all its Ethereum and will fail to continue to sponsor transactions. In order to prevent such a scenario, a certain number of the ERC-20 token


Transfer Token B
Uniswap V2 Router
Transfer half of service fee in swapped Ether
Transfer half of service fee back to Smart Contract which stakers can claim
Swaps Token A equal to gas spent by transaction + 0.2% and Swap rest to Token B
Transfer Swapped Ether
Ethane Deployer
Smart Contract
Bob
Bob signs a message which will permit the smart contract to spend a number of Token A
Smart Contract executes Permit and TransferFrom functions
Calls Smart Contract
OpenZeppelin Defender Relayer

1.1: A Breakdown Model of the Transaction Process

involved in the transaction will be swapped into Ethereum using Uniswap v2 Core smart contracts. The transaction must yield an adequate amount of swapped Ethereum to compensate for the gas paid by the Relayer. This Ethereum is transferred to the Relayer and thus it can continue to sponsor transactions while maintaining a stable balance. The smart contract will prevent a user from transferring their tokens if the number of tokens cannot yield the adequate Ethereum to compensate. In addition to compensating the Relayer via ERC-20 tokens, a micro 0.2% service fee is accounted for when tokens are swapped to Ethereum using Uniswap. Half of this 0.2% fee will serve as dividends for Ethane token owners who have staked through the Ethane decentralized app. The remaining half of the fee will be transferred to the Ethane Team.

3 GASLESS WRAPPED ETHER

The current Wrapped Ether contract deployed on Ethereum also lacks the ERC-20 Permit extension. Ethane has deployed a modified version of the Wrapped Ether contract called “Gasless Ether” with symbol $gETH$ which includes Permit functionality to seamlessly integrate into the Ethane ecosystem. This will allow the smart contract to utilize the permit functionality while also unwrapping into regular Ethereum to use when appropriate.

4 GASLESS SWAPS

The use of swaps introduced in the Economics section will also be available to users. Since the smart contract has the ability to transfer tokens from the user without the owner paying gas, it can execute any logic written within it. By utilizing Uniswap’s smart contract, tokens will be swapped to the designated token desired by the user. Refer to *Diagram 1.1* to gain a visual understanding of the transaction process.

5 LIQUIDITY LOCKER

Ethane also utilizes the ERC-20 Permit functionality for locking liquidity tokens. The common approach to lock such tokens is to first send a separate approve transaction followed by sending the actual lock transaction to the blockchain. Instead of this two-step time and cost inefficient model, Ethane combines the process in a single transaction. Similar to what was discussed earlier in the Introduction section, the user signs a message permitting the Locker smart contract to spend a designated number of the user’s Uniswap Liquidity Provider tokens (UNI-V2). Then the user pays 0.04 ETH to call the lock function which first transfers the tokens from themselves to the smart contract and then locks it until the designated deadline. Of the fee paid to lock the liquidity provider tokens, 75% goes to Ethane token holders that are staking and the rest of the fee is transferred to the Ethane deployer.

6 STAKING

Staking serves as a method to reward Ethane token holders by distributing 75% of the locker fees to stakers. Rewards are calculated each time a holder interacts with the Locker smart contract via the stake, unstake, and claim functions. The following equation depicts how the reward of a user is calculated:

$$F(u,c,l) = r\left(\sum_{n=0}^{l}\frac{1}{L(n)} - \sum_{n=0}^{c}\frac{1}{L(n)}\right)$$

Let a function $F(u,c,l)$ represent the rewards for a user u, inclusively between the $lockEventIndex\ c$ which represents the number of times locks have occurred and $lastLockEventIndexUpdate\ l$ which represents the lock index of the last time a stake, unstake, or claim function was called. Let $L(n)$ represent the total number of Ethane tokens staked at $lockEventIndex\ n$. Let r represent the reward rate of $0.03\ ether$ which is the 75% fee from every time there is a lock event.