

Ethane: Quasi Account Abstraction Wallet and Token Exchange Protocol

The Ethane Team

info@ethane.app

April 2024

Abstract

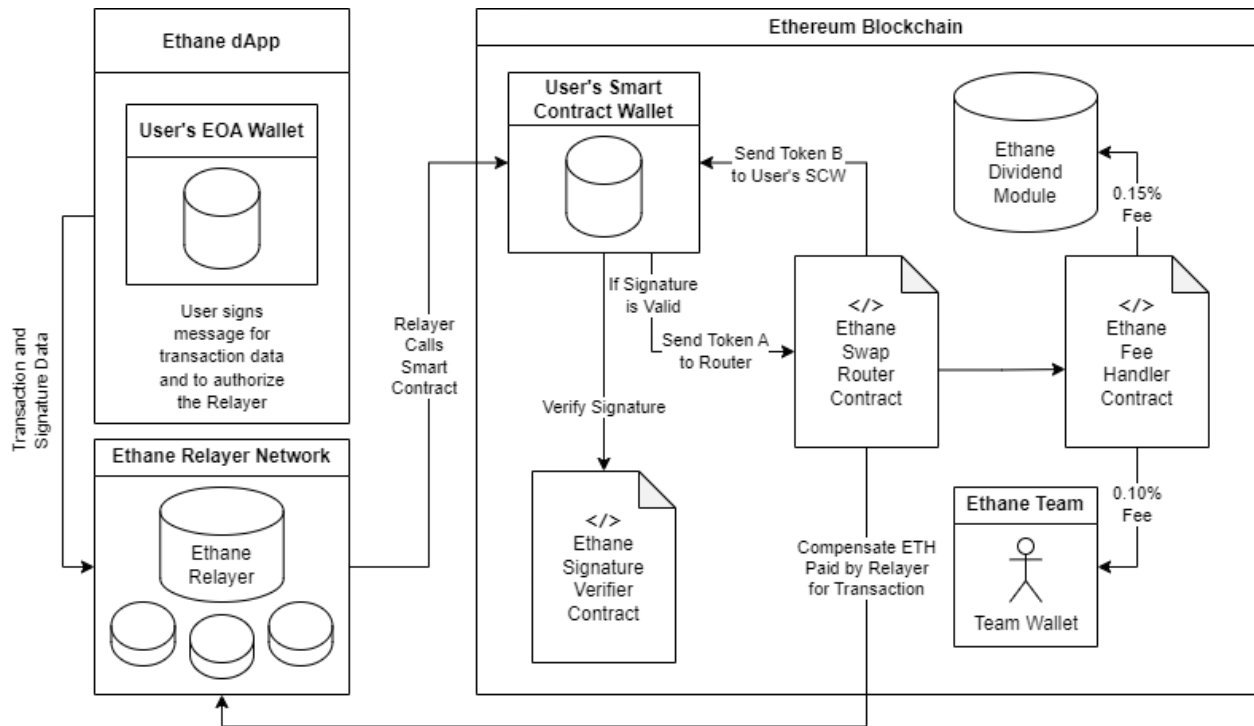
The Ethane platform provides its users with Smart Contract Wallets, which allow for the convenience of exchanging their ERC-20 tokens without being obligated to spend their Ethereum upfront for network fees. Instead of the user expending their Ethereum balance to submit the transaction, a Relayer will cover the network fee on behalf of the user and in exchange for this service, the user will compensate the paid network fee with the ERC-20 token(s) involved in the transaction.

1 INTRODUCTION

The majority of the users that submit transactions to the Ethereum blockchain use some form of an EOA (Externally Owned Account) Wallet such as MetaMask or TrustWallet. When submitting transactions from their EOA wallet, the user is required to hold an adequate Ethereum balance to be able to pay the network fee. Without this fee, the transaction cannot be submitted. In the context of this document, if the user does not hold enough Ethereum for network fees, they will not be able to purchase or sell their ERC-20 tokens. This can be time consuming for the common user who simply wants to exchange Token A for Token B but is prevented until they transfer in adequate funds to be able to submit this transaction. Additionally, it is a steep learning curve for the average layman who is new to the world of cryptocurrency. But what if the network fee could be offset to a

third party Relayer so the user would not need to worry about their Ethereum balance? This is what the Ethane platform accomplishes.

With Ethane, a user can generate a special type of wallet called a “Smart Contract Wallet” or SCW¹. This SCW is fully under the control of the user deploying it. It is linked to the EOA wallet that they use so even in the event of the Ethane platform experiencing downtime, the user will be able to interact with their SCW but at the expense of the relaying service. This is because the Ethane platform is essentially providing the relaying service to be able to perform transactions on behalf of the users. In other words, in the unlikely event of downtime, the user can still perform transactions with their SCW through their EOA wallet, but they will need to pay network fees to do so. The takeaway is that the SCW and all its assets are in full



1.1: A Breakdown Model of the Transaction Process

custody of the user who deployed it and therefore the user can be at ease knowing they have not lost access to their assets.

2 ECONOMICS

In order for a token exchange transaction to be economically viable, the ERC-20 tokens involved in the transaction are required to have liquidity on Uniswap². 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 involved in the transaction will be swapped into Ethereum using the Uniswap v2 Core smart contracts. The transaction must yield an adequate amount of swapped Ethereum to compensate for the network fee 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 Relayer will not sponsor and submit a transaction if the number of tokens being exchanged cannot yield the adequate Ethereum to compensate. In addition to compensating the Relayer, a micro 0.25% service fee is accounted for when tokens are swapped to Ethereum using Uniswap. 60% of this fee (or 0.15% of the transaction volume) will serve as dividends for Ethane token owners who have opted into receiving dividends through the Ethane decentralized app. The remaining fee will be transferred to the Ethane Team. Refer to *Diagram 1.1* above to gain a visual understanding of the transaction process.

3 TRANSACTIONS

Ethane Smart Contract Wallets can perform any transaction, similar to many other

cryptocurrency wallets. Additionally, users are able to batch multiple transactions in one transaction. This is only possible via Smart Contract Wallets and not through a typical EOA wallet. An example of this would be how an EOA wallet must perform two separate transactions to successfully swap a desired token. They must approve their tokens first and then they are able to perform the swap transaction. This process not only wastes time, but gas as well.

What if you could combine the approval and swap transactions in just one transaction? This is possible through Smart Contract Wallets. When a user wants to exchange their tokens, they're simply prompted to sign a message to authorize the Relayer and then proceed to submit their swap transaction. This allows the exchange of tokens to happen much faster.

4 RELAYER NETWORK

In order for transactions to be relayed to the blockchain in an efficient and timely manner, it is imperative that multiple sponsor wallets be prepared to submit these transactions. If only one sponsor is available in the Relayer network, the transactions being processed during times of high volume may not succeed. The solution to this problem would be to distribute the load of transactions across multiple relayers. To maximize the number of relayers that can be available to accept transactions, incentives are offered to attract potential clients who are interested in relaying transactions. When calculating the fee for the transaction, the estimated gas will be slightly higher than the actual gas used during execution. The discrepancy between the two gas numbers is what the sponsor

gets to keep for themselves. Additionally, there is no risk of wasted gas on failed transactions for an individual interested in becoming a relayer since the node being utilized in the Relayer Network will not submit transactions that will fail to the blockchain. The node will only submit the transactions that succeed to the blockchain.

5 SOCIAL NETWORK LOGINS

Users will also have the option to generate their Smart Contract Wallets after signing up to the platform with their social media account like Google. When a user selects the option to login with Google, they will be prompted to the commonly used Google OAuth screen allowing the user to sign into their Google account or select an account if logged in already.

At face value, this option simultaneously comes with several benefits and drawbacks. Giving the user the ability to login with their Google account eliminates the need for a third-party browser extension like MetaMask to be used since the Smart Contract Wallet (SCW) being utilized is tied to the user's Google account on the database. This means that, if the user chooses to, they will not even be prompted to sign a message. Rather they will be able to simply click the "Swap" button and have their transaction submitted immediately. The data required for the swap is sent to the server where then the SCW is called and executes the desired transaction. An immediate drawback that may come to mind is the concern of custody of the assets in the SCW and the centralized nature of this application. To alleviate these concerns, the user will be able to have non-custodial control over their Google SCW. This is

accomplished by utilizing the Web3Auth³ service, which is a reliable industry-leading platform that provides developers with the ability to integrate social network logins into their blockchain applications with the utmost security kept in mind. By utilizing this service, the user will be able to recover their account in the event of losing their seed phrase or the Ethane platform experiencing downtime. The goal is to allow the user to have non-custodial access to their SCW even if they're using social network logins.

6 EVM-BASED BLOCKCHAINS

The Ethane platform will also be supported on multiple EVM-based Blockchains like Base, Polygon, Arbitrum, Binance Smart Chain, and other Layer 2 EVM Blockchains. For blockchains like Polygon and Layer 2 chains, the entire gas fee will be sponsored on behalf of the user rather than the gas in the native token being deducted from the swap transaction.

In contrast to the Ethereum blockchain, the gas fees on Layer 2 chains have significantly improved since the implementation of the Dencun Upgrade⁴ which added proto-danksharding and blobs to Ethereum. This allows for fees on Layer 2s to be worth virtually nothing and ultimately allows the Ethane platform to sponsor the entire transaction.

7 REFERENCES

- [1] John Gilbert. March 2023. What Are Smart Contract Wallets? A Beginner's Guide <https://blockworks.co/news/what-are-smart-contract-wallets>
- [2] Uniswap. <https://github.com/Uniswap/v2-core>
- [3] Web3Auth. <https://web3auth.io/>
- [4] Omkar Godbole. March 2024. Layer 2 Blockchains Become Cheaper After Ethereum's Dencun Upgrade <https://www.coindesk.com/markets/2024/03/14/layer-2-blockchains-become-cheaper-after-ethereums-dencun-upgrade/>