CIP:

To be assigned upon advancement to Phase 2

Title:

Delegated Trading Smart Contract Wallet with Dual-Key Security for CoW Swap

Author:

mookow4eva

Status:

Draft

Created:

2024-12-26

Requires:

N/A

Replaces:

N/A

Simple Summary

This proposal suggests the development of a CoW-specific smart contract wallet featuring two distinct keys with separate roles: one designated for trading and the other for withdrawals. This dual-key system enhances security by allowing users to delegate trading activities to a hot wallet while safeguarding withdrawal capabilities within a cold wallet. The solution is tailored for trading on CoW Swap, leveraging its unique characteristics and needs.

Motivation

The primary objective is to bolster user security and operational efficiency within the CoW Protocol ecosystem. By introducing a wallet with delegated trading capabilities, users can engage in frequent trading on CoW Swap without exposing their assets to unnecessary risk. This setup resolves several key issues:

- Enhanced Cold Wallet Security:

The current user experience with cold wallets is fraught with risk and confusion because users often have no idea what they are signing. This undermines the security and purpose of using cold storage. Delegated trading eliminates this problem by confining signing operations to the hot wallet's trading key.

- Separation of Duties:

Users can delegate trading while keeping withdrawal permissions isolated, greatly reducing the attack surface for unauthorized withdrawals.

- Competing with Uniswap:

By enhancing security and convenience for users, CoW Swap can attract market share away from competitors like Uniswap, especially among users who prioritize security in their trading operations.

- Trusted Implementation:

While the concept might seem orthogonal to CoW Swap, it needs to reside in a trusted ecosystem—and CoW Swap is a natural home for such innovation.

- Improved Security for Bots:

Bots, which necessarily operate using hot wallets connected to the internet, would benefit significantly from delegated trading. By utilizing this system, bots can confine their operations to trading activities while ensuring that withdrawal permissions remain protected. This dramatically reduces the risk of losing funds due to a bot's hot wallet being compromised.

User "mfw78" outlined an achievable approach involving a Safe, a transaction guard, and a Safe module (permalinkforum link). This insight underscores the feasibility of implementing this proposal using well-established tools and practices.

Specification

The proposed smart contract wallet will incorporate the following features:

1. Dual-Key Management

- Withdrawal Key:
- Capabilities:
- Transfer funds to external wallets.
- Add ERC-20 tokens to a whitelist for trading.
- Update the trading key.
- Transfer funds to external wallets.
- Add ERC-20 tokens to a whitelist for trading.
- Update the trading key.
- Storage Recommendation:
- Kept in cold storage to minimize exposure to external threats.
- Kept in cold storage to minimize exposure to external threats.
- Capabilities:
- Transfer funds to external wallets.
- Add ERC-20 tokens to a whitelist for trading.
- Update the trading key.
- Transfer funds to external wallets.
- Add ERC-20 tokens to a whitelist for trading.
- Update the trading key.
- Storage Recommendation:
- Kept in cold storage to minimize exposure to external threats.
- Kept in cold storage to minimize exposure to external threats.
- Trading Key:
- Capabilities:
- Execute trades exclusively among whitelisted ERC-20 tokens on CoW Swap.
- Execute trades exclusively among whitelisted ERC-20 tokens on CoW Swap.
- Storage Recommendation:
- Stored in a hot wallet to facilitate active trading operations.
- Stored in a hot wallet to facilitate active trading operations.
- Capabilities:
- Execute trades exclusively among whitelisted ERC-20 tokens on CoW Swap.
- Execute trades exclusively among whitelisted ERC-20 tokens on CoW Swap.
- Storage Recommendation:
- Stored in a hot wallet to facilitate active trading operations.
- Stored in a hot wallet to facilitate active trading operations.

2. Token Whitelisting

- Only tokens explicitly approved by the withdrawal key can be traded. This ensures controlled and secure trading on CoW Swap.

3. Allowance Management

- Allowances for token spending are granted concurrently with the addition of tokens to the whitelist by the withdrawal key. This guarantees that trades can only occur within user-approved parameters.

4. Integration Components

- Safe and Modules:

The solution will leverage a Safe, a transaction guard, and a Safe module as described by user “mfw78” to implement the dual-key architecture.

- Transaction Guard:

Ensures that the trading key operates strictly within its permissions, adding an additional layer of security.

5. Security Measures

- The trading key’s permissions are tightly scoped, preventing unauthorized withdrawals even if the key is compromised.
- Regular audits and security assessments will be conducted to ensure the integrity of the smart contract.

6. Cow-Themed User Interface

To enhance user experience, the wallet will feature a CoW-themed interface and wallet creation wizard. By adopting a “less is more” philosophy, the design will be custom-tailored specifically for CoW Swap users. Expanding beyond the scope of CoW Swap could detract from the streamlined experience and potentially introduce improperly configured security measures or unnecessary complexity, undermining the wallet’s core purpose. Therefore, the focus will remain on simplicity, usability, and alignment with the CoW Swap ecosystem.

Rationale

The dual-key architecture addresses critical security concerns in delegated trading on CoW Swap. By segregating duties between two keys, users can confidently delegate trading activities to a hot wallet while retaining full control over withdrawals with their cold wallet. This approach:

- Solves the Cold Wallet Dilemma:

Users no longer need to risk their funds by signing ambiguous transactions with their cold wallet, preserving its purpose as a secure store of assets.

- Tailored for CoW Swap:

The proposal is explicitly designed for trading within the CoW Swap ecosystem, ensuring seamless integration and user experience.

- Competing with Uniswap:

Providing enhanced security and usability gives CoW Swap a competitive edge against platforms like Uniswap, particularly for security-conscious traders.

- Leveraging Trusted Infrastructure:

By using Safes, modules, and transaction guards, the proposal builds on robust and proven technologies.

- Bot Security:

Bots are integral to the DeFi ecosystem but face heightened security risks due to their always-online nature. Delegated trading mitigates this risk by limiting bots’ permissions to trading activities, ensuring that funds remain secure even if a bot’s hot wallet is compromised.

- User Experience:

A cow-themed interface reinforces CoW Swap’s branding and provides a seamless experience tailored specifically for its users. The custom wallet creation wizard will simplify onboarding while maintaining high security standards.

Although the concept might seem tangential to CoW Swap's primary mission, it provides an essential utility for its users and must be hosted in a trusted environment—making CoW Swap the ideal home for this innovation.

Safe Transaction Data

To be provided upon finalization of the smart contract implementation.

Tenderly Simulation

A link to the Tenderly simulation will be included once the smart contract is developed and tested.

Snapshot

A link to the corresponding CoW DAO Snapshot poll will be added when the proposal advances to Phase 2.

This proposal addresses a critical need for secure delegated trading within the CoW Protocol ecosystem. By implementing a dual-key smart contract wallet tailored for CoW Swap, users can trade actively and securely without compromising the integrity of their assets. For further details and community discussions, please refer to the original forum thread: forum link.