Interactive Wallet For Immediate Transactions

Dor Malka, Maya Deshe

December 31, 2025

1 Interactive Wallet Design

The goal of this project is to design an interactive wallet that allows users to perform immediate transactions while ensuring the security of their digital and physical assets. Currently, transactions are executed over the blockchain only after being admitted to the mempool and selected by block producers according to fee-based prioritization, which may delay execution by minutes or hours.

We propose an interactive wallet architecture composed of two optional parallel execution layers, designed to support both standard and immediate transaction execution while preserving strong security guarantees. This wallet will leverage advanced authentication mechanisms, including continuous credentials, to provide a seamless and secure user experience.

1.1 Layer 1: Standard Interactive Execution

The first layer follows the conventional interactive wallet model. Transactions executed through this layer are:

- Explicitly approved by the user
- Signed using the user's private key
- Broadcast directly to the blockchain mempool
- Executed according to standard fee-based block inclusion mechanisms.

This layer prioritizes cost efficiency and conservative execution and serves as the default mode for non–time-critical transactions.

1.2 Layer 2: Immediate Execution Layer

The second layer is an optional fast-path execution mechanism intended for time-critical transactions. When a user opts into this layer:

- The transaction is approved with higher priority fees
- The approved amount is immediately deducted from the user's wallet balance
- The transaction is placed into a wallet-managed transaction pool, distinct from the public mempool

- The wallet actively transmits the transaction from this pool to the blockchain mempool using aggressive fee escalation and replacement strategies.

Unlike standard wallets, this layer does not rely on passive broadcasting. Instead, it assumes responsibility for transaction execution, guaranteeing that the transaction will be mined within a bounded time window.

1.3 Receiver Assurance Mechanism

Upon approval via the immediate execution layer, the receiver (e.g., a seller or merchant) is notified instantly that:

- The transaction amount has been authorized
- The corresponding funds have been locked and deducted from the sender's wallet
- Blockchain settlement is guaranteed and pending.

This notification enables the receiver to safely release goods or services prior to on-chain confirmation, thereby bridging the gap between user authorization and blockchain finality.

1.4 Enhanced Security via Multi-Credential Authentication

To compensate for the increased risk associated with fast execution, transactions approved through the immediate execution layer require stronger authentication. Specifically, authorization in Layer 2 is gated by:

- Possession of the private key (discrete credential).
- Continuous biometric authentication (e.g., face recognition).

This dual-credential model ensures that authorization reflects both cryptographic key ownership and live user presence. Consequently, possession of a compromised private key alone is insufficient to trigger immediate execution, decreasing the risk of rapid, large-scale asset theft.

2 Timetable

- **27.11.2025** – Discussion of multiple project ideas and formulation of the interactive wallet concept.
- **31.12.2025** – System design of the interactive wallet for immediate transactions.
- **10.01.2026** – Implementation of the wallet user interface and the two-layer execution architecture.
- **18.01.2026** – Development of the multi-credential authentication mechanism and the interactive wallet protocol.
- **22.01.2026** – Testing and evaluation of the interactive wallet, including preparation of the final presentation.
- **26.01.2026** – Final presentation of the interactive wallet.