PRIVATE WALLET

by Legba

A Private Execution Layer for Digital Assets

1. Problem Statement

Cryptocurrency systems are transparent by default. Wallet software leaks metadata through RPC providers, browsers expose persistent identifiers, and infrastructure providers correlate timing and volume long before a transaction reaches the chain.

Most privacy tools address only a single layer. Consequently, users obscure on-chain data while remaining identifiable through network or application-level correlation. Privacy that depends on user discipline fails under realistic conditions.

Legba Private Wallet is designed for adversarial environments where observation is assumed.

2. Design Objective

The objective of the Legba Private Wallet is to prevent reliable linkage between a user's identity and their digital asset activity. This requires suppressing attribution at the point of execution, not retroactively at settlement.

Privacy is structural, not configurable.

2.1 Strategic Definition: Execution vs. Speculation

Legba is strictly an **execution environment**, not a portfolio management tool. It is designed for the secure, private movement and interaction of capital. It is **not** designed for price discovery, trade optimization, or market timing.

3. Threat Model

The system assumes adversaries with access to:

- Blockchain analytics and clustering tools
- RPC request logs and timing correlation
- Browser fingerprinting techniques
- Behavioral data collected by dApps and infrastructure providers

The system does not attempt to defend against endpoint compromise or physical coercion. It prevents network- and application-level attribution under normal operation.

4. System Constraints and Non-Negotiable Principles

The following constraints are architectural invariants. Any feature or integration that violates one is out of scope.

- No public execution paths
- No optional privacy modes
- No persistent execution identity
- **No custody or intermediation of funds**
- No protocol changes
- No new chains introduced by Legba
- No aggregation or pooling
- **No persistent identifiers or behavioral telemetry designed to identify users**

Privacy cannot be disabled, downgraded, or misconfigured.

5. Architecture Overview

The Legba Private Wallet is composed of three core components and a strict asset-role model.

5.1 Shielded Transfers (Zcash)

Zcash provides mature shielded pools using zero-knowledge proofs. The wallet supports shielded addresses only. Transparent addresses are not exposed to the user interface. Zcash functions as a privacy rail, not a core asset.

5.2 Private Smart Contract Execution (Ethereum)

Ethereum interaction is performed exclusively through Railgun.

- Public Ethereum addresses are never exposed
- Public contract approvals are not supported
- Execution occurs through zero-knowledge paths

Public rails are used for ingress and egress only. Execution and interaction are performed exclusively through private paths.

5.3 Isolated Execution Runtime

All wallet logic, dApp interaction, and network communication occur within an isolated execution environment. This environment:

- Suppresses browser fingerprinting
- Suppresses network identifiers
- Prevents persistent execution state

Each session operates with a fresh execution identity destroyed at termination. Wallet state and cryptographic keys persist independently of execution identity and are never exposed as execution, network, or application identifiers.

5.4 Asset Role Separation

Assets are not treated symmetrically.

- **BTC and Stablecoins** are Capital Anchors
- **ZEC and Railgun** are Privacy Rails
- **ETH and SOL** are Execution Surfaces

Legba is the boundary between identity and activity.

6. Split Execution Model

Legba Private Wallet is built on a split execution model. Application execution occurs inside the isolated runtime. Cryptographic keys remain local to the user.

The runtime performs routing, dApp interaction, session isolation, and network suppression. It requests transaction signatures but cannot generate them. The system cannot initiate transactions autonomously.

7. Bitcoin Integration

7.1 Bitcoin as Capital Anchor

Bitcoin is treated strictly as a store of value and a capital ingress and egress asset. It is not an execution environment and is never used interactively.

7.2 BTC Ingress

Users fund the system from a standard BTC UTXO.

- Each ingress UTXO is single-use.
- **Bitcoin is only observed at ingress and egress and is never used interactively.**

Immediately upon ingress, BTC crosses into the private environment through **user-initiated, external conversion paths selected and executed outside of Legba**. Legba does not intermediate trades, quote prices, or route orders. The original UTXO is burned from behavioral relevance.

7.3 BTC Inside the Private Environment

Inside Legba, Bitcoin exists only as value exposure. There is no addressable Bitcoin wallet, no interactive BTC execution, and no public RPC interaction.

7.4 BTC Egress

When exiting:

- BTC exits through a fresh UTXO.
- Route Sanitization is applied.
- **No prior execution behavior is observable at settlement.**

Bitcoin never touches dApps, user-side RPCs, or browser execution paths. **Bitcoin is only observed at ingress and egress.**

8. Stablecoin Integration

8.1 Stablecoins as Execution Fuel

Stablecoins are treated as transient execution liquidity. They are temporary, mobile, and stateless inside the system. They are not accounts, balances, or financial products.

8.2 Shielded Stablecoin Handling

All stablecoins entering the system:

- Immediately enter a private balance
- Never appear as public ERC-20 transfers
- Never require public approvals
- Never persist as visible addresses

8.3 No Stablecoin Accounts

There is no stablecoin wallet address, balance history, or public representation. Stablecoins exist only as spendable private liquidity.

8.4 Permitted Uses

Stablecoins may be used for Ethereum dApp execution, Solana execution funding, temporary hedging, and capital rotation. They are not parked long-term, off-ramped by Legba, pooled, or intermediated.

8.5 Stablecoin Exit

Stablecoins exit directly or are converted externally by the user.

9. Solana Integration

9.1 Solana as Execution Surface

Solana is treated as a high-velocity execution target, not a resident chain. Legba does not expose public Solana addresses, persistent Solana accounts, or user-visible Solana wallets.

9.2 Isolated Solana Execution

All Solana interaction occurs inside the isolated execution runtime using ephemeral session identities destroyed after execution. Keys remain user-controlled and are never reused across sessions.

9.3 Funding Solana Execution

Solana execution is funded via private stablecoin conversion or private ETH to SOL paths. Fee funding for ephemeral execution identities is handled inside the isolated runtime **in a manner that avoids reuse and minimizes correlation to the user's capital anchor.** Users do not bring public Solana wallets into the system.

9.4 Risk Posture

Solana execution is disabled by default and explicitly activated.

10. Crossing the Boundary

10.1 The Reality of Off Ramps

There is no fully private fiat off ramp. Banks, exchanges, and payment networks operate under compliance regimes that require identity and reporting. Legba does not attempt to eliminate this boundary.

10.2 Exit Philosophy

Privacy is enforced structurally inside the system. Privacy degrades only at the user's chosen exit point. The counterparty sees a transaction. They do not see a user.

10.3 Route Sanitization

Before funds leave the private environment, they undergo Route Sanitization. Legba provides **sanitization tooling, not automated settlement.**

Route Sanitization leverages the **native anonymity sets of the underlying privacy rails** to disrupt transaction-graph linkage. Users retain agency over the specific timing and sizing of exits. Legba does not aggregate flows across users.

10.4 Exit Paths

Users may exit through multiple paths without Legba intermediating any of them:

- Centralized exchanges
- External transfers and spending
- Crypto-native custody rotation

Compliance occurs at the counterparty.

11. Hole-Proofing Checklist

The system is considered compromised if any of the following occur:

- **A public chain observes the same externally visible address twice**
- A dApp sees a stable user fingerprint
- A stablecoin balance persists across sessions
- Solana RPC metadata leaks
- Bitcoin UTXOs are reused
- Users can opt out of privacy

The architecture **is designed to prevent these conditions.**

12. Scope Limitations

The wallet deliberately excludes features that introduce attribution risk, including fiat integration, public execution modes, and identity-linked services.

13. Manifesto

Most crypto wallets optimize for convenience. In doing so, they expose users to surveillance through layers outside the blockchain.

Legba treats visibility as the primary failure mode and removes it at the execution layer. This is not a privacy feature added to an existing wallet model. It is a private execution system designed for adversarial environments.

Legba is invisible by design.