Grant Proposal: PillarX - Modular Abstraction Wallet

Contact: tg: aldin4u / aldin@pillar.fi

Summary:

We propose the development of a modular wallet for the Aztec ecosystem, featuring social logins, transaction batching, gas abstraction, token swaps, bridging, PXE privacy, and a dApp store-like UI. The wallet will offer seamless onboarding, delayed account contract deployment, private transaction handling, and news feed integration, providing a user-friendly, privacy-focused experience.

[

1600×1041 247 KB

](https://europe1.discourse-cdn.com/flex013/uploads/aztec/original/2X/2/2d80c40b0e550f82a1db67f36908bb3349857ef1.jpeg)

About us:

Our team has been deeply involved in account abstraction and smart wallet design since 2018, contributing significantly to the development of one of the first smart wallets in the form of Pillar Wallet (https://www.pillar.fi/) and more recently PillarX (https://pillarx.app/) a 7579-based modular abstraction wallet which is currently in beta testing.

Estimated Start and End Dates

- Start Date: October 7, 2024
- End Date: January 31, 2025

Grant Timeline and Milestones:

Milestone 1: Initial Wallet Functionality and Setup (End of October)

- Onboarding and Account Creation

: Implement passkeys support andcreate a user-friendly onboarding process with automatic keypair generation (signing, nullifier, viewing keys).

- Token Balances, Transfers and Transaction History

: Display private and public token balances, enabling basic token transfers, and transactions history (explorer integration).

- Delayed contract deployment

: Account contracts are deployed only when the user initiates their first public transaction.

- Wallet Connect

: enable wallet connect functionality for the aztec ecosystem.

- PXE Integration

: Enable interaction with the Private Execution Environment (PXE) for private transaction execution if this is available via a browser-based PWA.

Milestone 2: Modular Architecture & Account Sponsorship (Mid-November)

- Modular ERC-7579-inspired Design

: Build the wallet’s modular architecture, supporting multi-sig and authwit (authorization witnesses).

- Account Sponsorship

: Sponsor user’s first transactions and account creation fees.

Milestone 3: Transaction Batching (End of November)

- Transaction Batching

: Allow users to submit multiple transactions in a single batch, compatible with PXE for private execution.

- Gas Abstraction:

Implement gas abstraction using ERC-20 tokens and initial paymaster support.

Milestone 4: Swaps, Bridges, & Contract Interactions (End of December)

- Token Swaps & Bridges:

Implement basic token swap and bridging functionality to enable cross-chain transfers.

- Paymaster Sponsorship

: Allows for projects to sponsor contract interactions like token Swaps.

Milestone 5: dApp Store UI and News Feed Integration (End of January)

- dApp store UI

: provide projects an easy path to leverage the account abstraction functionality through inclusion inside the PillarX ecosystem.

- Aztec Ecosystem News Feed

: Integrate a news feed to display updates and educational content about the Aztec ecosystem.

Milestone 6: Privacy and Security Enhancements (Mid-December)

- Zero-Knowledge Proofs (zk-Proofs) Integration

: Ensure all transactions use zk-proofs for private data verification without exposing sensitive details. This includes the privacy-first transaction flow where balances, transaction history, and user data are protected.

- Data Privacy Measures

: Implement API request management and IP anonymization to prevent data leakage. Ensure no logs or analytics are collected to maintain privacy across all wallet interactions.

- Privacy Alerts

: Incorporate user notifications for any potential privacy risks (e.g., when interacting with APIs or external nodes).

Milestone 7: Account Migration & Backup (Early January)

- Encrypted Key Backup & Recovery

: Integrate an encrypted backup system for all keypairs (signing, nullifier, viewing). This will ensure users can securely recover their accounts in case of device loss or transition.

- Account Export/Import Functionality

: Implement the ability for users to export and import their accounts, allowing seamless migration between devices or platforms without data loss.

- Compliance with Aztec Account Standards

: Ensure compatibility with other Aztec-compliant wallets, enabling smooth migration and interaction across the ecosystem.

Milestone 8: Syncing and Data Management Optimization (End of January)

- Snapshot Syncing for PXE

: Implement snapshot syncing to quickly retrieve user data when migrating to new devices, reducing the need for full data resynchronization.

- Fast Syncing on New Devices

: Enable quick synchronization for existing accounts, ensuring users have up-to-date account status immediately upon logging into a new device.

- Encrypted Data Management

: Ensure all synchronization and data transfers happen over secure, encrypted channels, maintaining the privacy and integrity of user information during syncing operations.

Contract Interactions

Future:

- Chrome Extension

: in the future we plan to expand the wallet as a chrome extension that can handle interactions with the wider ecosystem.

Grant Amount Requested: $95,000

Budget Breakdown

Item

Unit Price

Quantity

Amount

Blockchain Engineer

$2,200/week

12 weeks

$26,400

Full-Stack Engineer

$2,200/week

12 weeks

$26,400

Front-End Engineer

$1,800/week

12 weeks

$21,600

UX/UI Designer

$2,500 (one-time)

1 time

$2,500

Infrastructure Costs

-

-

$4,100

Testing & QA

$1,500/week

4 weeks

$6,000

Total

$95,000