Title:

Zenith Wallet

Contact Details:

- Email:

saurishdarodkar@gmail.com

- TG:

@IMSaurish

@NadeemBhati

- Signal

@nadeem.14

Summary

Zenith Wallet

aims to provide seamless user interaction within the Aztec ecosystem by offering a privacy-focused, secure, and user-friendly wallet solution. Aztec's unique features such as native account abstraction, private and public execution, and advanced cryptographic capabilities will be used by Zenith Wallet will simplify onboarding, facilitate seamless transactions, and integrate advanced functionalities like authwit support. Our mission is to become the primary gateway for users to interact with privacy-preserving blockchains, enhancing accessibility without compromising security or privacy.

Estimated Start and End Date

- Start Date:

October 8, 2024

- Functional Testnet Version:

December 15, 2024

- Final Version Release:

March 31, 2025

About Us

Our team comprises four seasoned professionals with extensive experience in blockchain technology, full-stack development, and UI design.

- Nadeem Bhati
- Blockchain Engineer
- 7+ years in Web3 development
- Currently part of the Status.im team
- Former CTO at Virtual Labs and Protocol Engineer at Composable Finance
- Specializes in zero-knowledge proofs (ZKPs) and cryptography
- Proficient in Rust and Solidity
- LinkedIn:

linkedin.com/in/nadeem-bhati

- 7+ years in Web3 development
- Currently part of the Status.im team

- Former CTO at Virtual Labs and Protocol Engineer at Composable Finance
- Specializes in zero-knowledge proofs (ZKPs) and cryptography
- Proficient in Rust and Solidity
- LinkedIn:

linkedin.com/in/nadeem-bhati

- Saurish Darodkar
- Blockchain Engineer
- 4+ years in Web3 development
- IIT-B postgraduate
- Experience with wallets and decentralized exchanges (DEXs)
- Expert in TypeScript and Go
- LinkedIn:

linkedin.com/in/saurish-darodkar

- 4+ years in Web3 development
- IIT-B postgraduate
- Experience with wallets and decentralized exchanges (DEXs)
- Expert in TypeScript and Go
- LinkedIn:

linkedin.com/in/saurish-darodkar

- Ekant Kapgate
- Fullstack Engineer
- 5+ years in fullstack development
- Expertise in React, TypeScript, and Web3 integration
- Previously worked on multiple blockchain-based projects
- LinkedIn:

linkedin.com/in/ekant-kapgate

- 5+ years in fullstack development
- Expertise in React, TypeScript, and Web3 integration
- Previously worked on multiple blockchain-based projects
- LinkedIn:

linkedin.com/in/ekant-kapgate

- Shumaila Chini
- Designer
- 4+ years in UI/UX design
- Expert in Figma and Adobe Creative Suite
- Focused on creating intuitive and engaging user interfaces
- LinkedIn:

linkedin.com/in/shumaila-chini

- 4+ years in UI/UX design
- Expert in Figma and Adobe Creative Suite
- Focused on creating intuitive and engaging user interfaces
- LinkedIn:

linkedin.com/in/shumaila-chini

Details

Technical Overview

Zenith Wallet will be a browser-based wallet extension

. The wallet will interface directly with Aztec's Private Execution Environment (PXE) and support both private and public transactions. Secure communication protocols will be established to interact with PXE, ensuring all sensitive data remains encrypted and secure.

Key Features

1. User-Friendly Onboarding

- Seedless Authentication

: Implement passkeys or biometric authentication to eliminate traditional seed phrases.

- Key Generation

: Automatically generate required keypairs behind the scenes.

- Delayed Account Deployment

: Deploy account contracts only when necessary to optimize gas fees.

- Token Bridge Integration

: Seamless in-wallet bridging of tokens using the Token Bridge API.

- Fee Payment Mechanisms

: Provide options for fee payment, including paymasters and dedicated fee tokens.

2. Account Contract Implementation

- Aztec.nr Contracts

: Write account contracts using Noir.

- secp256r1 Key Scheme

: Utilize the secp256r1 signature scheme for enhanced security.

- Authwit Support

: Implement support for authorization witnesses (authwits) for advanced authorization mechanisms.

- Upgradability

: Ensure account contracts are upgradable to adapt to future requirements.

- Nonce Abstraction & Replay Protection

: Implement secure transaction management.

3. Privacy and Security

- Secure PXE Communication

: Establish secure communication with PXE to prevent unauthorized data access.

- No Data Collection

: Avoid logs or analytics that could compromise user privacy.

- User-Controlled Features

: Allow users to disable features that might leak personal data (e.g., currency conversion APIs).

4. Contract Interactions

- Intuitive Interface

: Provide a seamless experience for private and public token transfers.

- QR Code Protocol

: Develop a protocol to facilitate private transactions using QR codes.

- Batch Transactions

: Support batching multiple actions into a single transaction.

- Real-Time Information

: Display account and network status (e.g., synced block number, balances).

5. Ecosystem Integration

- WalletConnect Integration

: Enable interaction with dApps using WalletConnect.

- Community Collaboration

: Work with the Aztec community to establish standards (e.g., for account contracts, authwits).

System Design Diagrams

Diagram 1: Onboarding and Transaction Processing

Sequence Diagram

[

Screenshot 2024-10-04 at 4.39.42 PM

2444×1870 355 KB

](https://europe1.discourse-cdn.com/flex013/uploads/aztec/original/2X/7/77258c7042622013a1eb9ce44d27a764c5e5103f.png)

Diagram 2: Account Management, dApp Interaction, and Privacy

Sequence Diagram

[

Screenshot 2024-10-04 at 4.54.29 PM

3086×1842 415 KB

](https://europe1.discourse-cdn.com/flex013/uploads/aztec/original/2X/2/24354c2bb5ebbf54ff1e8b533f9b6844d05161f3.png)

Grant Milestones and Roadmap

Milestone 1: Core Development Setup (Oct 8 - Oct 31, 2024)

Week 1 (Oct 8 - Oct 14):

- Tasks:
- Set up development environments and repositories.
- Define architecture and detailed system design.
- Begin preliminary UI/UX design sketches (to be developed later).
- Set up development environments and repositories.
- Define architecture and detailed system design.
- Begin preliminary UI/UX design sketches (to be developed later).
- Team Involved:

Nadeem, Saurish, Ekant, Shumaila

Milestone 2: Feature Development (Nov 1 - Nov 30, 2024)

- Weeks 2-5:
- Tasks:
- Develop the Key Management Module.
- Implement seedless authentication mechanisms.
- Develop the Transaction Module for private and public transactions.
- Establish secure communication protocols with PXE.
- Start account contract development in Aztec.nr.
- Integrate delayed account contract deployment logic.
- Set up Aztec Node (Server) infrastructure.
- Develop the Key Management Module.
- Implement seedless authentication mechanisms.
- Develop the Transaction Module for private and public transactions.
- Establish secure communication protocols with PXE.
- Start account contract development in Aztec.nr.
- Integrate delayed account contract deployment logic.
- Set up Aztec Node (Server) infrastructure.
- Tasks:
- Develop the Key Management Module.
- Implement seedless authentication mechanisms.
- Develop the Transaction Module for private and public transactions.
- Establish secure communication protocols with PXE.
- Start account contract development in Aztec.nr.
- Integrate delayed account contract deployment logic.
- Set up Aztec Node (Server) infrastructure.
- Develop the Key Management Module.
- Implement seedless authentication mechanisms.

- Develop the Transaction Module for private and public transactions.
- Establish secure communication protocols with PXE.
- Start account contract development in Aztec.nr.
- Integrate delayed account contract deployment logic.
- Set up Aztec Node (Server) infrastructure.
- Team Involved:

Nadeem, Saurish, Ekant

Milestone 3: Testnet Preparation (Dec 1 - Dec 15, 2024)

- Weeks 6-7:
- Tasks:
- Finalize account contract with authwit support.
- Ensure compatibility with Aztec testnet.
- Conduct comprehensive testing and debugging.
- Release functional testnet version by December 15, 2024.
- Finalize account contract with authwit support.
- Ensure compatibility with Aztec testnet.
- Conduct comprehensive testing and debugging.
- Release functional testnet version by December 15, 2024.
- Tasks:
- Finalize account contract with authwit support.
- Ensure compatibility with Aztec testnet.
- Conduct comprehensive testing and debugging.
- Release functional testnet version by December 15, 2024.
- Finalize account contract with authwit support.
- Ensure compatibility with Aztec testnet.
- Conduct comprehensive testing and debugging.
- Release functional testnet version by December 15, 2024.
- Team Involved:

Nadeem, Saurish, Ekant, Shumaila

Milestone 4: Feature Enhancement (Dec 16, 2024 - Jan 31, 2025)

- Weeks 8-12:
- Tasks:
- Implement multi-account support and quick syncing.
- Develop backup and migration tools.
- Enhance contract interaction functionalities (batch transactions, QR codes).
- Collaborate with Aztec community to establish standards.
- Optimize wallet performance and security.

- Begin preparations for mainnet launch.
- Implement multi-account support and quick syncing.
- Develop backup and migration tools.
- Enhance contract interaction functionalities (batch transactions, QR codes).
- Collaborate with Aztec community to establish standards.
- Optimize wallet performance and security.
- Begin preparations for mainnet launch.
- Tasks:
- Implement multi-account support and quick syncing.
- Develop backup and migration tools.
- Enhance contract interaction functionalities (batch transactions, QR codes).
- Collaborate with Aztec community to establish standards.
- Optimize wallet performance and security.
- Begin preparations for mainnet launch.
- Implement multi-account support and quick syncing.
- Develop backup and migration tools.
- Enhance contract interaction functionalities (batch transactions, QR codes).
- Collaborate with Aztec community to establish standards.
- Optimize wallet performance and security.
- Begin preparations for mainnet launch.
- Team Involved:

Nadeem, Saurish, Ekant

Milestone 5: Finalization and Mainnet Launch (Feb 1 - Mar 31, 2025)

- Weeks 13-17:
- Tasks:
- Finalize all features.
- Shumaila integrates UI components.
- Conduct third-party security audits.
- Prepare user guides and educational materials.
- Release final version by March 31, 2025.
- Finalize all features.
- Shumaila integrates UI components.
- Conduct third-party security audits.
- Prepare user guides and educational materials.
- Release final version by March 31, 2025.
- Tasks:
- Finalize all features.

- Shumaila integrates UI components.
- Conduct third-party security audits.
- Prepare user guides and educational materials.
- Release final version by March 31, 2025.
- Finalize all features.
- Shumaila integrates UI components.
- Conduct third-party security audits.
- Prepare user guides and educational materials.
- Release final version by March 31, 2025.
- Team Involved:

Nadeem, Saurish, Ekant, Shumaila

Grant Amount Requested

Total Grant Requested:

$88,000

Grant Budget Rationale

Personnel Costs

Role	Rate	Duration	Total
Blockchain Engineer (Nadeem)	$2,000/week	12 weeks	$24,000
Blockchain Engineer (Saurish)	$1,750/week	12 weeks	$21,000
Front-End Engineer (Ekant)	$1,500/week	12 weeks	$18,000
Designer (Shumaila)	$1,500/week	5 weeks	$7,500

Further Development and Support Funds

-

-

$17,500

Total

$88,000

Questions

1. Standards Alignment:
2. Are there any specific standards or protocols under development for account contracts and authwits that we should align with? Guidance on this will help us maintain compatibility and interoperability within the Aztec ecosystem.
3. Communication Channels:
4. What are the preferred channels for ongoing communication and feedback during the development process? Knowing the best way to reach out—whether via email, dedicated forums, or scheduled meetings—will help us coordinate effective