Aztec Wallet Development Proposal

Title: ZKWallet - Your Gateway to Private Transactions

Contact Details

- Email: blinkztyler@gmail.com
- Discord: Mahmudsudo
- Telegram : olayinksbello

Summary

ZKWallet aims to revolutionize the user experience for Aztec network participants by providing a sleek, intuitive, and secure browser-based wallet. Our solution will leverage Aztec's unique features, including private and public state management, native account abstraction, and seamless composability between private and public transactions. ZKWallet will prioritize user privacy, offering a streamlined onboarding process, robust key management, and an elegant interface for interacting with the Aztec ecosystem. By focusing on user experience and security, we aim to lower the barrier to entry for privacy-preserving blockchain interactions and foster wider adoption of the Aztec network.

Estimated Start and End Date

- Start Date: November 15, 2024
- End Date: March 15, 2025 (with functional version for testnet by December 2024)

About Us

Our team consists of three experienced blockchain developers and one UX designer:

1. Mahmud Bello (Lead Developer): 5+ years of experience in Ethereum development, specializing in smart contracts and wallet infrastructure. github username : mahmudsudo
2. Macbobby Precious (Privacy Specialist): 3 years of experience working on privacy-focused blockchain projects, with expertise in zero-knowledge proofs. github : theghostmac
3. Ganiyu Olamide (Full-stack Developer): 4 years of experience in web3 development, proficient in React and Typescript.
4. David stephens (UX Designer): 6 years of experience designing user interfaces for fintech and blockchain applications.

Together, we bring a strong mix of technical expertise, privacy-focused development experience, and user-centric design skills to the project.

Details

Technical Architecture

ZKWallet will be implemented as a browser-based application using React and TypeScript. The wallet will interact with the Aztec network through the PXE (Private eXecution Environment) and will be designed with a modular architecture to allow for easy updates and feature additions.

Key components:

1. Key Management Module

: Securely generates and stores signing keypairs, nullifier keypairs, and viewing keypairs using a combination of browser's Web Crypto API and custom encryption libraries.

1. Account Contract

: We will implement a flexible account contract in Aztec.nr that supports:

- Secp256r1 signing scheme

- Authwit management (adding, spending, cancelling, and validity checking)
- Upgradability for future improvements
- Secp256r1 signing scheme
- Authwit management (adding, spending, cancelling, and validity checking)
- Upgradability for future improvements
- Transaction Manager

: Handles the creation, signing, and submission of both private and public transactions.

1. State Synchronization

: Efficiently syncs the wallet state with the PXE, including note discovery and management.

1. Privacy-preserving RPC Proxy

: Implements a server-side proxy to forward transaction calldata to the mempool, enhancing user privacy.

1. Multi-Account Support

: Ability to manage multiple Aztec accounts within a single wallet interface.

1. Passkey-based Onboarding

: Streamlined user onboarding using passkeys for enhanced security and usability.

Grant Milestones and Roadmap

Phase 1: Foundation (October 20 - November 30, 2024)

1. Set up development environment and integrate with Aztec Sandbox
2. Implement core key management and account contract functionality
3. Develop basic UI for wallet operations (send, receive, view balances)
4. Create privacy-preserving RPC proxy

Phase 2: Testnet Ready (December 1 - December 15, 2024)

1. Integrate with Aztec testnet
2. Implement transaction batching and fee management system
3. Develop and test Wallet Connect integration
4. Launch beta version of ZKwallet for testnet

Phase 3: Enhanced Features (December 16, 2024 - February 15, 2025)

1. Implement advanced sync and backup solutions
2. Develop intuitive authwit management interface
3. Create and integrate educational components
4. Develop contract verification tool

Phase 4: Polish and Launch (February 16 - March 20, 2025)

1. Conduct thorough security audits and implement fixes
2. Optimize performance and user experience
3. Prepare comprehensive documentation and user guides
4. Official launch of ZKwallet v1.0

Future Roadmap (Post-Grant)

- Develop mobile wallet version
- Explore hardware wallet integrations
- Contribute to Aztec ecosystem by developing SDKs and developer tools
- Implement advanced privacy features (e.g., stealth addresses, private NFTs)

Grant Amount Requested

We are requesting a grant of $75,000 to support the development of ZephyrZK.

Grant Budget Rationale

- Developer Salaries (3 developers, full-time for 5 months): $45,000
- UX Designer (full-time for 5 months): $10,000
- Infrastructure and Testing Costs: $10,000
- Security Audit: $10,000

This budget allows our team to dedicate full-time efforts to developing a high-quality, feature-rich wallet while covering necessary infrastructure and security costs. The timeline and milestones are structured to deliver a functional wallet by the testnet launch in December, with continued development and refinement through Q1 2025.

Questions

1. Are there specific security standards or best practices we should adhere to when implementing the privacy-preserving RPC proxy?
2. Can you provide more details on the expected integration points between the wallet and the upcoming browser-based PXE?
3. Are there plans for standardizing wallet interfaces or features across the Aztec ecosystem that we should be aware of or contribute to?
4. What level of integration should we expect between the wallet and potential future Aztec-native DeFi protocols?

We are excited about the opportunity to contribute to the Aztec ecosystem and look forward to your feedback on our proposal. Our team is committed to creating a wallet that not only meets the current needs of Aztec users but also pushes the boundaries of what's possible in privacy-preserving blockchain interactions.

User Interface Design

We've created a mockup of the main wallet interface to showcase our design philosophy:

[

svgviewer-png-output

1000×750 19.5 KB

](https://europe1.discourse-cdn.com/flex013/uploads/aztec/original/2X/6/6173f3ad40fa0626746f1323451b35746041e64b.png)