Umbra - Browser Extension Wallet for Aztec

Contact Details

Satyam Bansal

Gmail: satyamsgsits1994@gmail.com

Telegram: Telegram: Contact @satyambnsal

Summary

Umbra is a browser extension wallet designed specifically for the Aztec network, focusing on intuitive user experience. Initially developed during Alpha build 1, Umbra was awarded the Best UX prize, demonstrating our commitment to user-centric design. With a basic version already live and ready to try, we've laid a strong foundation for future development.

Our wallet aims to provide a user-friendly interface for managing accounts, executing private and public transactions, and interacting with dApps on the Aztec network. Umbra's goal is to create an intuitive wallet that abstracts away the complexities of Aztec's privacy-preserving technology while empowering users with full control over their privacy settings.

Building upon our successful alpha version and prioritizing both technical excellence and user-friendliness, Umbra seeks to become the preferred wallet for engaging with the Aztec ecosystem.

Estimated Start and End Date

- Start: October 15, 2024
- End: March 15, 2025 (with a functional version ready for testnet in December 2024)

About You

Our team consists of three talented individuals with diverse skills and experiences in blockchain development, UI/UX design, and open-source contribution:

1. Satyam Bansal
2. Full stack developer and open source contributor
3. Kernel community fellow
4. 8 years of experience building applications
5. Currently working as Developer at Nethermind
6. GitHub: https://github.com/satyambnsal
7. Participated in Previous alpha build and builtaztec uniswap v2
8. Full stack developer and open source contributor
9. Kernel community fellow
10. 8 years of experience building applications
11. Currently working as Developer at Nethermind
12. GitHub: https://github.com/satyambnsal
13. Participated in Previous alpha build and builtaztec uniswap v2
14. Yash Mittal
15. UI developer
16. Created the UI for Umbra wallet extension during Alpha build 1
17. GitHub: https://github.com/yassmittal
18. UI developer

19. Created the UI for Umbra wallet extension during Alpha build 1
20. GitHub: https://github.com/yassmittal
21. Ankita Dixit
22. UX designer
23. 3 years of experience creating UI designs for web3 applications
24. Winner of multiple hackathons
25. UX designer
26. 3 years of experience creating UI designs for web3 applications
27. Winner of multiple hackathons

Our team combines deep technical expertise, proven UI/UX skills, and a track record of success in the web3 space. With our diverse backgrounds and complementary skills, we are well-positioned to deliver a high-quality, user-friendly wallet for the Aztec ecosystem.

Details

We have developed a preliminary version of the Umbra wallet as a browser extension, compatible with major browsers such as Chrome, Firefox, and Brave. You can view our initial UI design and implementation here. The source code for this basic version is available in our GitHub repository. current version runs with hosted aztec sandbox and can be connected with local sandbox by changing the RPC url.

Building upon this foundation, we have created a comprehensive technical system design for the full-featured Umbra wallet. The design incorporates the following key features:

- Seamless onboarding process with optional passkey support
- Management of multiple Aztec accounts
- Support for both private and public transactions
- dApp interaction support
- Integration with Aztec's PXE for client-side proof generation
- Built-in privacy controls and educational resources
- Support for authwits and account abstraction features
- Intuitive UI for managing tokens, fees, and contract interactions
- WalletConnect Integration
- Modular code structure for reusability across Aztec projects

To illustrate the interactions between these components and the overall architecture of the Umbra wallet, we have created the following system design flowchart:

[

flowchart

2866×1564 304 KB

](https://europe1.discourse-cdn.com/flex013/uploads/aztec/original/2X/9/9baf9d754cd6c01287f6326fa68422faa9d6939d.png)

This flowchart provides a visual representation of how the various modules within the Umbra wallet will interact. It showcases the flow of data and actions, from user interactions through the browser extension interface to the underlying Aztec network operations.

Grant Milestones and Roadmap

1. October-November 2024: Enhanced Wallet Functionality and Devnet Integration

We will continue with existing codebase from Alpha Build 1 which includes

- Basic wallet UI implementation
- Account creation and deployment
- Token transfer functionality
- Transaction history viewer

As part of this Milestone we plan to achieve

- Custom Account Contract: Deploy and integrate custom account contract
- Token Bridge Integration: Integrate token bridge for asset porting
- Fee Management: Implement fee juice functionality
- Devnet Connection experiment: Establish connection with Aztec devnet instance(current version connects to sandbox running remotely). at the same time extension will support connection with sandbox running locally by changing the RPC url.

Note: We will make sure not to release devnet connection app or share details without Aztec team permission.

- Balance Display: Add fee juice balance display to the UI
- Refinement: Improve existing UI and functionality from Alpha Build 1

2. December 2024: dApp Integration and Authwit Support

(Expanding wallet functionality for ecosystem interaction)

- Authwit Implementation: Develop and integrate authwit support
- Wallet Connector Methods: We have already done the POC of injecting connector methods on windows

object and now we will Enhance existing POC (umbra/chrome-extension/src/background/index.ts at main · satyambnsal/umbra · GitHub) with comprehensive connector methods like: * Account connection

- Balance checking
- Transaction signing and sending
- Account connection
- Balance checking
- Transaction signing and sending
- dApp Integration Interface: Create a user-friendly interface for connecting to and interacting with Aztec dApps
- Developer Documentation: Publish minimal guide for dApp developers on integrating Umbra wallet

This milestone focuses on making the wallet fully interactive with the Aztec ecosystem, enabling seamless dApp interactions and laying groundwork for developer adoption.

3. January 2025: Advanced Features and Privacy Enhancements

- Passkey support
- Syncing and Backup: Develop snapshot/quick syncing feature for efficient PXE information export and backup
- Fee Payment Options: Create interface for selecting fee payment methods (fee juice or Devcoins)

Management of authorization scopes

-Optional analytics with clear disclaimers

- Enhanced Token Transfers: Develop QR code-like protocol for easy private token transfers

4. February 2025: Ecosystem Integration and advanced Authwit

- WalletConnect Integration: Implement WalletConnect protocol for broader dApp compatibility
- Advanced Authwit Management: Develop interface for adding, spending, cancelling, and checking validity of authwits
- Transaction Management: Add support for canceling pending transactions and setting tx.max_block_number
- Explorer Integration: If there is an explorer in the ecosystem, embed it within the wallet interface

4. March 2025: Polish, security audits, feedback, UI improvements

materials about Aztec and privacy features

- Community Feedback: Incorporate final round of community feedback and suggestions
- Basic Security audit of our custom account contract and overall codebase
- UI/UX Refinement: Polish user interface and experience based on accumulated feedback
- Ecosystem Readiness: Coordinate with key Aztec ecosystem projects for seamless integration at launch

5. Continuous improvements, Preparation for mainnet

As we approach the potential mainnet launch, our focus will shift towards ensuring Umbra is fully prepared for widespread adoption. While the exact steps may evolve based on the Aztec ecosystem's development and user needs, our primary goals will be enhancing reliability and incorporating user feedback. We'll conduct rigorous testing to ensure the wallet's stability and security under various conditions. User experience will be at the forefront, with continuous refinements based on accumulated feedback

Grant amount requested

$70,000

Grant budget rationale

The requested amount of $70,000 will cover development costs for our team of 3 members over the 6-month period, including:

- Core Development: $38,000
- Integration with Aztec's PXE
- Implementation of privacy features and account abstraction
- Smart contract interactions and fee management
- Refinement and expansion of the existing UI
- Implementation of new features and interactions
- Integration with Aztec's PXE
- Implementation of privacy features and account abstraction
- Smart contract interactions and fee management
- Refinement and expansion of the existing UI
- Implementation of new features and interactions
- UX/UI Design and Improvement: $16,000
- Continuous improvement of user flows and interactions
- Creation of educational materials and onboarding processes
- Design of new features and privacy controls
- Ensuring responsive and intuitive user experience across browsers
- Continuous improvement of user flows and interactions

- Creation of educational materials and onboarding processes
- Design of new features and privacy controls
- Ensuring responsive and intuitive user experience across browsers
- Security and Testing: $11,000
- Third-party security review
- Penetration testing and vulnerability assessment
- Comprehensive testing across various browsers and devices
- Third-party security review
- Penetration testing and vulnerability assessment
- Comprehensive testing across various browsers and devices
- Operational Expenses: $5,000
- Development tools and infrastructure
- Project management and communication tools
- Marketing and community engagement
- Development tools and infrastructure
- Project management and communication tools
- Marketing and community engagement

This budget allows us to build upon our successful Alpha build 1 version, creating a robust, user-friendly wallet while ensuring long-term commitment to the Aztec ecosystem. Our team is dedicated to delivering high-quality work, leveraging our existing codebase and experience with the Aztec network.

Questions

1. What is the expected timeline for Devnet being available to developers ?