Title: Note Viewing Library

Contact Details:

- Email: porcorossoj89@gmail.com
- Telegram: porco_rosso_j

Summary:

Note Viewing Library is a typescript library that offers fast and sophisticated note querying and decryption with viewing keys for businesses on Aztec, such as explorers, wallets, and apps. Additionally, it can be useful for individuals and businesses that want to disclose their historical transaction data to their accountants and auditors. The primary goal of this grant work is developing a typescript library for other services to use, not a note-viewing website itself.

Estimated Start and End Date:

- Start Date: August 15th, 2024
- End Date: November 15th, 2024

Project Details:

Team:

- Porco : Full-Stack Developer with experience in smart contract development in Ethereum and Aztec
- Tech Stack: NodeJs, Typescript, React, Solidity, Noir
- Projects / Past Commitments
- AztecSnap Wallet: A MetaMask Snap that works on Aztec. It's a smart contract wallet that supports ECDSA signature and enables private calls to any Aztec contract.
- Batcher Contract: It allows users to obfuscate their swap amounts when they trade on AMMs on Aztec. It leverages an additive homomorphic encryption scheme to encrypt and aggregate users' input amounts without revealing individual amounts.
- *More: portfolio page

- AztecSnap Wallet: A MetaMask Snap that works on Aztec. It's a smart contract wallet that supports ECDSA signature and enables private calls to any Aztec contract.
- Batcher Contract: It allows users to obfuscate their swap amounts when they trade on AMMs on Aztec. It leverages an additive homomorphic encryption scheme to encrypt and aggregate users' input amounts without revealing individual amounts.
- *More: portfolio page
- Tech Stack: NodeJs, Typescript, React, Solidity, Noir
- Projects / Past Commitments
- AztecSnap Wallet: A MetaMask Snap that works on Aztec. It's a smart contract wallet that supports ECDSA signature and enables private calls to any Aztec contract.
- Batcher Contract: It allows users to obfuscate their swap amounts when they trade on AMMs on Aztec. It leverages an additive homomorphic encryption scheme to encrypt and aggregate users' input amounts without revealing individual amounts.
- *More: portfolio page
- AztecSnap Wallet: A MetaMask Snap that works on Aztec. It's a smart contract wallet that supports ECDSA signature and enables private calls to any Aztec contract.

- Batcher Contract: It allows users to obfuscate their swap amounts when they trade on AMMs on Aztec. It leverages an additive homomorphic encryption scheme to encrypt and aggregate users' input amounts without revealing individual amounts.
- *More: portfolio page

Technical Description:

This typescript library exposes methods that filter and query notes with various parameters only with provided incoming and outgoing viewing keys. The reason why this type of solution is needed is that while the PXE service provides methods such as getIncomingNotes

and getOutgoingNotes

for such a purpose, it doesn't work unless accounts have already been registered in the PXE. There should be a way for third parties, such as auditors and accountants, to obtain and monitor the client's transaction history using the client's viewing keys but not secret keys.

Also, this library offers a high-quality and inclusive query experience with more customizable parameters, including block numbers, tagging keys, app viewing keys, and a toggle enabling one to fetch only specific types of tokens. Token-dedicated methods that exclusively track and output the history of token balances and movements might be very crucial and beneficial for apps such as wallets, portfolio apps, and explorers. Directly querying notes is verifiable and possibly faster than calling unconstrained methods for fetching balances.

Long-term View:

I'm currently developing AztecSnap, a MetaMask Snap designed to work on the Aztec network. Additionally, I have plans to create a standalone browser extension wallet, equipped with extensive Account Abstraction features. Although my primary aim for this product is to support explorers developed by other grantees, I believe integrating it into our own wallets could be beneficial, enhancing the user experience and expanding its functionalities. Hence, committing to its continued development and maintenance would make sense beyond the grant period.

Grant Milestones and Roadmap:

Milestone 1: Basic Library Methods (by 15th Sep)

- Research on Aztec protocol's workings: Keys, Notes, and PXE
- Design and implement basic methods for querying with viewing keys and a few advanced filter params
- Design and implement methods for token-dedicated querying

Milestone 2: Testing & Frontend Example (by 15th Oct)

- Implement testing for methods developed in the Milestone 1
- Implement an example frontend that showcases how to show the queried data through the library
- Start talking to other grantees about potential integrations for the Milestone 3

Milestone 3: Integrations (by 15th Nov)

- Working on the integration with one of the grantees *If none of them is interested, consider developing a note-viewing website as MVP
- AztecSnap Wallet's portfolio and transaction history page
- e.g. Debank, Zerion, and Safe
- e.g. Debank, Zerion, and Safe

Grant Amount Requested:

- Total Requested:

$10,000 for compensating developer salaries over 3 months (~3k / month) and other minor/potential expenses, e.g. server cost, hiring a designer.