Title

: Pegasus

Contact Details

: aztecscan7@gmail[.]com

Summary

:

We’re interested in building a state-of-the-art, privacy-centric block explorer for Aztec. User experience and longevity (and subsequently self reliance) would be our priority.

our ask - USD 22k

Timeline

:

Mid July’24 to Mid Jan’25

Team:

Currently it’s one full stack developer with a designer on standby, we’ll aim to onboard more developers on an hourly basis as we progress according to our need. This would be our first Aztec project. Having studied the docs in the last few weeks, we feel confident in delivering a state of the art block explorer for the aztec network. Previously we have worked with the Stacks Foundation, Protocol labs, won in hackathon pool prize and further some personal long tail MEV projects. More on previous work would be shared with Rahul (on email).

Additionally, we’re open to keeping milestone payments after each milestone is submitted such that it’s paid if the milestone is completed.

Design Philosophy

:

Familiarity with etherscan would be kept in mind. Responsiveness. Light and dark mode. A chatbot bubble (trained on Aztec architecture and common questions) for normie users so they don’t feel lost.

Unique points

:

- we envision it to cater to normie, non tech, relatively new web3 userbase - not assuming that they understand etherscan either.
- Chatbot that tells what a contract might be doing, answers common questions and more based on aztec docs, blogs.
- Cowswap style aztec theme horn audio on every new block (reconsidering, may not do)
- A whiteboard walkthrough of aztec protocol down on the home page for normie users in non tech, ELI5 fashion
- Dark and light mode
- Design the explorer to handle increasing amounts of data and user interactions as the Aztec network grows.

Tech Stack:

- Frontend - typescript, tailwind CSS
- Backend - node.js
- Database - PostgreSQL
- Additional - Docker, AWS for hosting, mistral or llama3 for chatbot

Grant Milestones and roadmap:

If there’s a small tweak or changes in this, it’ll be communicated weeks in advance, rest assured ordering could change but all milestones would be completed compulsorily. Taking inspiration from the points mentioned in the RFGP. (have directly pasted your appendix 1 points)

Milestone 1. (Basic MVP plus Block page info)

- Etherscan like homepage with recent blocks and txns.
- Block page covering (as specified in RFP Appendix 1 Block section)
- block hash
- timestamp
- number of transactions and their transaction hashes
- stats on logs
- block header data
- transaction state effects
- gas related information
- block hash
- timestamp
- number of transactions and their transaction hashes
- stats on logs
- block header data
- transaction state effects
- gas related information

Milestone 2. (txn related) (divided in 2 sub halves for the milestone payment - specification would be communicated in advance)

- Txn page (as specified in RFP Appendix 1 txn section)
- Transaction hash (identifier)
- status (mining/preconf/proving/success/dropped)
- block number
- L1 batch transaction
- timestamp
- transaction fee
- Transaction effects
- num notes + note hashes and note encrypted logs
- num nullifiers + hashes
- l1->l2 message hash
- l2->l1 message hash
- encrypted logs
- unencrypted logs
- public state reads/writes
- public function call(s)
- num notes + note hashes and note encrypted logs
- num nullifiers + hashes
- l1->l2 message hash

- l2->l1 message hash
- encrypted logs
- unencrypted logs
- public state reads/writes
- public function call(s)
- Fee related information
- FPA used
- gas price
- gas
- fee divided per dimensions (DA, L1, L2)
- coinbase (recipient of block reward)
- fee recipient (Address to receive fees)
- any public teardown call
- any public fee information
- FPA used
- gas price
- gas
- fee divided per dimensions (DA, L1, L2)
- coinbase (recipient of block reward)
- fee recipient (Address to receive fees)
- any public teardown call
- any public fee information
- Transaction hash (identifier)
- status (mining/preconf/proving/success/dropped)
- block number
- L1 batch transaction
- timestamp
- transaction fee
- Transaction effects
- num notes + note hashes and note encrypted logs
- num nullifiers + hashes
- l1->l2 message hash
- l2->l1 message hash
- encrypted logs
- unencrypted logs
- public state reads/writes
- public function call(s)

- num notes + note hashes and note encrypted logs
- num nullifiers + hashes
- l1->l2 message hash
- l2->l1 message hash
- encrypted logs
- unencrypted logs
- public state reads/writes
- public function call(s)
- Fee related information
- FPA used
- gas price
- gas
- fee divided per dimensions (DA, L1, L2)
- coinbase (recipient of block reward)
- fee recipient (Address to receive fees)
- any public teardown call
- any public fee information
- FPA used
- gas price
- gas
- fee divided per dimensions (DA, L1, L2)
- coinbase (recipient of block reward)
- fee recipient (Address to receive fees)
- any public teardown call
- any public fee information

Milestone 3. (contract related)

- contract public code (or bytecode)
- contract private code (or bytecode)
- contract class ID
- version
- hash of the initialization function that ran
- deployer address
- salt
- note tagging scheme registered
- public keys associated to the address (e.g nullifier, viewing etc)
- hash of public keys deployed with the contract
- Any public transactions where this address was either a from or a to

Milestone 4.

- Search and filtering functionality
- More work on design
- Chatbot to understand a contract and to ask general questions
- Testnet deployment (Nov-Dec 2024)

Milestone 5. (divided in 2 halves, one is mainnet deployment in q2'25 as per Aztec's roadmap)

- Homepage to have a 1-2 ELI5 (explain me like I'm 5) type whiteboard vids and FAQs
- Aztec ecosystem section/page
- Feedback page
- Mainnet deployment [note : since the mainnet is planned for '25 Q2, this milestone can be deemed completed half, other half stipend for this milestone can be reserved for when the explorer is deployed on the mainnet].

Grant amount requested:

USD 22,000

Grant budget rationale:

Idea is to divide the cost at USD 3.5k/mo for 1 part-time full stack dev and additionally hires on hourly basis when required (including a designer). USD 2.5k to be reserved for infra cost. If this cost grows due to demand, we can apply for small retroactive funding later (only for infra).

We'll try to get a chatbot funded initially with free credits from Gemini or other llm token grants by providers, or directly a self hosted version of llama3 trained on aztec docs and noir lang. Etherscan too has this feature, using gpt4.

We believe if we get enough people using the feature, we may be eligible for retroactive grants later. We'd try to use a self-hosted open source version of llama3/mistral that permits commercial use. Until then we can depend on free gpu/token credits.

Monetization/sustainability:

Haven't thought too deeply on this yet but I'm sure as aztec ecosystem grows we'll be able to figure things out. Paid API is an obvious suggestion.

Questions:

all necessary questions have been answered, if there's any more doubt, we'd reach out in discord/email and get it clarified.