

Milestone Report: DAO Governance x Atala PRISM (Milestone 4)

Testing Report

August 13, 2025

Contents

1	Introduction	2
2	Testing & Demo of On-Chain DID Voting	2
2.1	Step 1: Mint DID Token via Atala PRISM / Proofspace Authentication	2
2.2	Step 2: Election / Proposal Creation	3
2.3	Step 3: Staking DID Token	3
2.4	Step 4: Casting the Vote	3
3	Conclusion	4

1 Introduction

This milestone report documents the completion of **Milestone 4**: “On-chain Voting” for the *DAO Governance x Atala PRISM* project by MuesliSwap.

The deliverables for this milestone were:

- Adjustment of existing on-chain voting solutions to the project’s requirements, both in terms of backend integration and smart contract design.
- Full integration of on-chain elections into the existing off-chain voting platform.
- Preparation of test elections and execution of an internal security audit.

This document includes:

- A detailed testing report demonstrating the functionality of the integrated on-chain voting system.
- A step-by-step demonstration of how to interact with the implemented on-chain solution, fully integrated with the backend and frontend.
- User interface screenshots illustrating the voting process.
- References to on-chain transactions showing the casting of votes via **DID tokens**.

2 Testing & Demo of On-Chain DID Voting

2.1 Step 1: Mint DID Token via Atala PRISM / Proofsphere Authentication

In this step, the user logs into our DID token minting tool by scanning a QR code with the Proofsphere app. The authentication process verifies the user’s identity via their Atala PRISM DID, ensuring that only the authenticated individual can mint a DID token with the corresponding DID specification. Once authenticated, the DID token is minted directly into the user’s wallet.

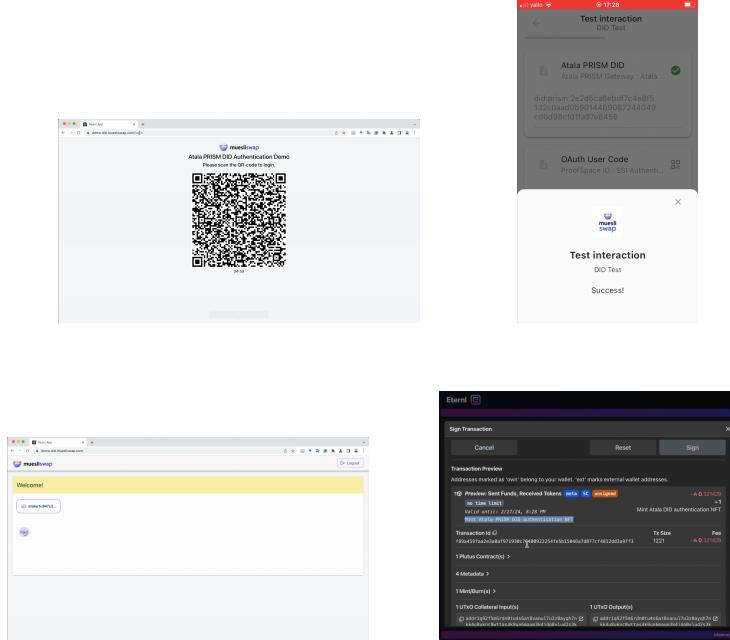


Figure 1: Step 1: DID token minting process. Top row: Login screen with QR code (left) and login confirmation in the Proofsphere mobile app (right). Bottom row: Minting interface (left) and transaction signing in the user’s wallet (right).

Transaction: d8f482fb2a1b143d62027682c74200e6504e8271c14b618d7a10fb7886e49d1 – This transaction shows the minting of the DID token, visible as a new asset in the user’s wallet.

2.2 Step 2: Election / Proposal Creation

Through the on-chain DAO interface, specifically adapted for DID-authenticated elections, users can create proposals to be voted on. The UI allows adding a proposal name, a detailed description, and multiple voting options. Before proposals can be created, a governance thread must be initialized by an administrator (see first transaction below).

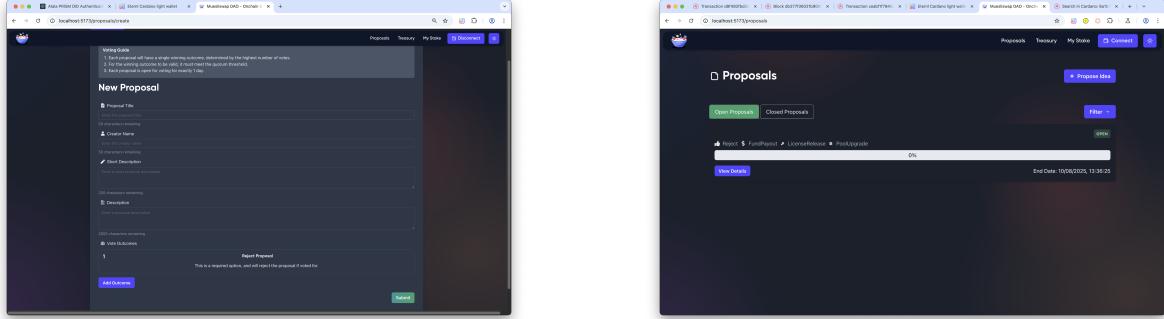


Figure 2: Proposal creation form (left) and proposal appearing in UI after having been submitted on-chain (right).

Transactions:

- bce826c7e739c3115432c6e9ecd14e517f2ecb8ea37ca8af1465c8fc8153ce87 – Governance thread creation transaction.
- ceabf1f7940cf5e79f1e5dc2b90b8c39f250790f1a109ccd73fe8fd7e36f82f2 – Proposal/tally creation transaction, containing metadata with proposal details.

2.3 Step 3: Staking DID Token

To participate in voting, users must stake their DID token into the governance smart contract. Once staked, the smart contract authenticates the user for the duration of the staking period, enabling them to vote on multiple proposals without restaking.

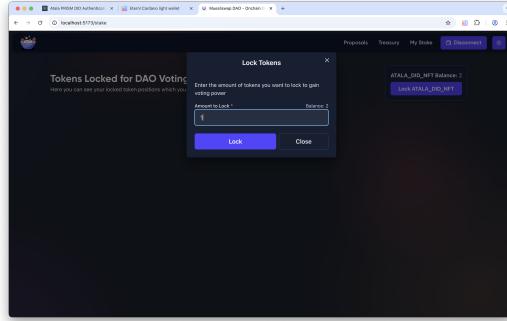


Figure 3: Locking interface for staking DID token.

Transaction: 2450d065c3aaaf3cf577638c59e417a51e8cca0616280f9d0f75e2d8b9fdaca7a – DID token staking transaction, showing the asset moving from the user's wallet into the governance contract address.

2.4 Step 4: Casting the Vote

Once authenticated via a staked DID token, the user can cast their vote on any active proposal through the voting UI. Each DID token corresponds to at most one vote, ensuring that no user can vote more than once per proposal.

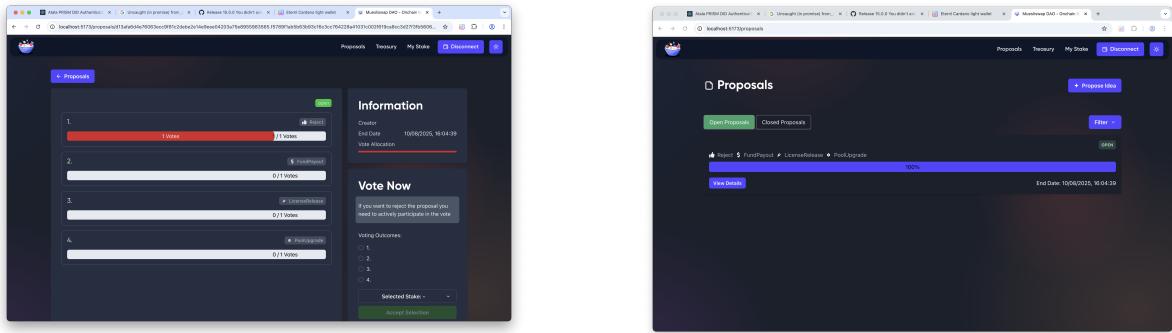


Figure 4: Voting process (left) and proposal results display (right).

Transaction: 8e97052cfcfefa684cf35765516458826d25fbd564972a475ea52dca373c46ea – Voting transaction, recording the user’s choice in the smart contract and updating the on-chain tally.

3 Conclusion

In this milestone, we successfully implemented and tested a fully integrated on-chain DID voting system. We demonstrated the process from DID token minting and proposal creation to staking and casting votes, supported by UI screenshots and on-chain transaction evidence. The internal security audit confirmed no critical issues.

Looking ahead, the next and final milestone will focus on **protocol parameter update mechanisms**. This will involve integrating parameter update functionality into one or more widely used open-source DeFi protocols, adapting smart contracts accordingly, and developing the required off-chain tooling. We will conduct test elections that trigger example parameter updates on the testnet, complete a full internal audit, and prepare public-facing documentation, tutorials, and community engagement materials to facilitate adoption. The milestone will conclude with open-sourcing the code and publishing a close-out report video as required by Fund 10.