Cardano Catalyst Fund 10 Report:
DAO Governance × Atala PRISM

MuesliSwapTeam

December 15, 2023

Contents

1 Introduction

Governance in decentralized systems is a multifaceted challenge, encompassing a spectrum of structures from community votings to intricate decentralized treasury management and protocol parameter control. The landscape is characterized by diverse implementations, each entailing trade-offs in decentralization, transaction costs, and user-friendliness. Current governance solutions often necessitate utility tokens to balance voting power, preventing double voting. However, the proposed project seeks to revolutionize this paradigm by integrating Atala PRISM Decentralized Identifiers (DID), eliminating the dependency on utility tokens and enabling advanced voting power weighting.

The purpose of this document is to articulate the research objectives and proposed solutions for the initial milestone of the unified governance platform project. This milestone focuses on comprehensive exploration and conceptualization, with key areas of investigation including the integration of Atala PRISM DID into existing off-chain voting systems, the design and functionality outline for treasury contracts and protocol parameter update interfaces, as well as an extensive review of existing on-chain governance solutions. The document aims to provide a clear roadmap for the research phase, delineating the tasks and considerations essential to achieving the overarching goal of a robust and flexible governance platform.

Scope and Structure. The scope of this milestone centers on the research aspect of the project. The remainder of this document is structured as follows:

- **Integration of Atala PRISM DID into Off-chain Voting Systems:** This involves a conceptual sketch outlining how Atala PRISM DID can seamlessly integrate with existing governance systems. The objective is to enhance security, eliminate transaction fees, and introduce advanced voting power weighting without relying on utility tokens.

- **Design and Interplay of Governance Solution with Treasury Smart Contract & Parameter Update Mechanism:** Delving into the intricacies of treasury management, the document will outline the basic functionality required for smart-contract governed treasuries. Additionally, it will explore the interface needed for protocol parameter updates, fostering decentralization in critical decision-making processes.

- **Comparison of Existing Governance Solutions on Cardano:** Evaluating existing governance solutions will involve a meticulous examination of their features, strengths, and weaknesses. A comprehensive comparison will guide the selection of components that align with the project's objectives.

- **Integration Plan for New Governance Components:** The document will detail the strategic plan for integrating the new governance components into the off-chain voting platform developed in Fund9. This integration aims to create a seamless and comprehensive governance ecosystem that combines the strengths of both on-chain and off-chain mechanisms.

By addressing these aspects, the document sets the foundation for subsequent stages of development, ensuring a well-informed and strategic approach towards achieving the ultimate goal of a unified and decentralized governance platform on Cardano.

2 Integration of DID Solutions into Governance Systems

In this section, we conceptually sketch the integration of the Atala PRISM digital identity solution into a governance/voting system. We proceed by exploring and comparing two possible approaches in order to justify our planned route for further development. The two approaches are analyzed in terms of ease of integration for both off-chain and on-chain governance solutions.

2.1 Approach 1: Direct integration via parsing of PRISM protocol transactions

Design idea. In Atala PRISM, DIDs issued by cloud agents are written onto the (Cardano) blockchain by a PRISM node. Therefore, one way of implementing user authentication on a governance platform is to directly read and parse such PRISM protocol transactions from the blockchain in order to check whether the respective user has presented a valid DID.

Off-chain governance integration. For off-chain governance, this requires off-chain parsing of PRISM protocol transaction which is already implemented in the PRISM node and cloud agent components. However, in order for users to hold any issued DIDs, one needs to provide some sort of DID wallet. To the best of our knowledge, such a wallet implantation is currently not available yet and would need to be created from scratch.

On-chain governance integration. For truly decentralized on-chain governance, elections need to be tallied on-chain. Therefore, voter authentication also need to happen on-chain. This however requires parsing of PRISM protocol transactions which seems highly non-trivial to implement on-chain as a Plutus smart contract. Additionally, as for off-chain governance, a DID wallet would need to be implemented.

Conclusion. Due to the described difficulties in particular for on-chain solutions, this design approach is difficult to implement in practice. Moreover, the design lacks modularity (this will become more apparent in Approach 2), since voter authentication would be directly tied to PRISM transaction via a smart contract. We therefore decide against further pursuing this approach and propose the following alternative.

2.2 Approach 2: Modular design via authentication NFT

Design idea. We propose a modular two-step voter authentication process:

1. Users authenticate themselves via their DID (this happens off-chain) in order to be able to mint an authentication NFT that uniquely represents their DID via its token name on-chain.

2. Users present their authentication NFT during the voting process in order to protect the system against double-counting of votes.

Importantly, we point out that for step 1, existing identity solutions built on top of Atala PRISM such as e.g. ProofSpace can be leveraged. This also enables the reuse of existing and well-tested DID wallet implementations which ProofSpace provides.

While step 1 from above is done equivalently for both off-chain and on-chain governance, we outline below how to implement step 2 in either case.

Off-chain governance integration. Here, the tallying process can happen similarly as in MuesliSwap's current off-chain governance solution. For each election, a snapshot of on-chain information is taken at a previously specified time. Each vote cast by a user is signed via its Cardano stake key hash (SKH). Then, when the election is tallied, only those votes are counted, for which an address associated with the signers SKH has held an valid authentication NFT at snapshot time.

On-chain governance integration. Here, the voter locks its DID authentication NFT in a staking smart contract during the election. Then, a governance smart contract needs to check the validity of the this NFT during the on-chain tallying process.

Conclusion. We conclude that the described approach is well-suited for our use case, as its modular design enables applicability in both the off-chain as well as on-chain setting. Moreover, the ability ot leverage existing DID solutions including wallet implementations makes this design significantly more robust and will allow us to provide high quality implementations of the remaining parts. In the following, we therefore focus on further developing this Approach 2.

3 Design and Interplay of Governance Solution with Treasury Smart Contract & Parameter Update Mechanism

In the following, we describe the intended design of the MuesliSwap On-Chain governance platform by outlining the interplay of the involved governance and treasury smart contracts, as well as protocol parameter update mechanisms.

Modular Smart Contract Design. The platform is designed with a set of modular smart contracts that facilitate control over funds and on-chain parameters for the MuesliSwap development treasury and decentralized exchange.

Governance Contract. The *Governance* contract is the central component responsible for managing the overall governance process. It tracks proposals, tallies voting results, and ensures that the voting power of locked funds is maintained throughout the voting period.

Protocol Parameter Update Interface. The *Governance* contract serves as an immutable tally result, providing a reference UTxO for protocol components to update their internal state based on the outcomes of the voting process.

Treasury Distribution Interface. The *Treasury* contract manages the funds of the MuesliSwap development treasury. It consumes the result of the voting process and distributes funds accordingly. The UTxO flow for treasury distribution is similar in nature to the parameter update process.

Functional Requirements. The platform must allow every token holder to participate in the governance process through proposal submission or voting. It should provide both accessible user interfaces and manual interaction with contracts. The platform's operability must remain decentralized, preventing any single entity from controlling the outcome or blocking the voting process.

User Interface Design The user interface will mirror the existing off-chain governance platform, prioritizing an intuitive design that displays on-chain proposals and votes clearly and concisely.

Security Considerations. To prevent spam, the platform requires a minimum token lock for proposal submission. If a proposal passes, locked tokens are returned; otherwise, they are distributed to voters or the treasury. Voting results are made effectual once, avoiding multiple fund withdrawals or outdated parameter changes. Monotonously increasing proposal IDs ensure proper consumption. The staking contract prevents unauthorized creation of staking positions on behalf of users, avoiding undesired vote retractions.

4 Comparison of Existing Governance Solutions on Cardano

In this section, we present a comparative analysis of various governance models on Cardano, focusing on both on-chain and off-chain solutions. Our methodology involves assessing each model based on predefined evaluation metrics, including efficiency, security, decentralization, and user incentivization. Data is collected from diverse sources, and the analysis encompasses both qualitative and quantitative aspects.

Our analysis employs a comprehensive methodology to evaluate existing governance solutions. We consider a set of predefined metrics, including efficiency, security, decentralization, and user incentivization, to provide a thorough assessment. Data is collected from academic journals, press releases, reports, and whitepapers to ensure a well-rounded understanding. It is important to note certain limitations and assumptions regarding data availability and the general applicability of each model in different blockchain ecosystems.

MuesliSwap Off-Chain Governance. The MuesliSwap Off-Chain Governance platform utilizes a decentralized voting system based on the Helios protocol[1]. Users can securely, privately, and scalably vote on proposals related to the MuesliSwap protocol. While offering transparency and verifiability, it does not support enforceable on-chain effects. Advantages include high efficiency and security, but drawbacks include centralized control and a lack of direct user incentivization.

SundaeSwap On-Chain Governance. SundaeSwap, a decentralized exchange on Cardano, implements an ”on-chain governance” model similar to MuesliSwap Off-Chain Governance. It provides transparency through on-chain commitments but lacks enforceable on-chain effects. The efficiency is high, but security details are unclear, and decentralization is limited due to server reliance. User incentivization remains moderate.

Wingriders On-Chain Governance. Wingriders, a decentralized exchange on Cardano, introduced its on-chain governance platform in October 2022. It exhibits high efficiency and security, leveraging the Cardano blockchain. However, it lacks decentralization as protocol operators control the voting process. User incentivization is low, and enforceable on-chain effects are absent.

Agora. LiqwidDAO’s Agora implements an on-chain governance system using LQ tokens for staking. The protocol achieves high security and decentralization by allowing on-chain enforceability. However, efficiency is limited by the sequential submission of votes. User incentivization is low, as participation incurs a cost.

[1] see `https://vote.heliosvoting.org`

Clarity DAO. Clarity DAO builds on LiqwidDAO's Agora, focusing on providing DAO infrastructure to projects on Cardano. While maintaining high security and decentralization, efficiency is compromised due to the sequential nature of vote submission. Similar to Agora, user incentivization is low.

To conclude, our analysis reveals that on-chain governance enhances transparency and immutability but introduces challenges, such as the lack of enforceable on-chain effects. Best practices include a modular approach, separating governance tallying from protocol component effects. Self-upgrade mechanisms are common, and careful consideration of parameters and security is crucial. In conclusion, MuesliSwap On-Chain Governance stands as a valuable addition to Cardano's ecosystem, contributing to the evolution of blockchain governance practices.

5 Integration Plan for New Governance Components

The current governance platform on MuesliSwap allows users to submit and vote on proposals tracked in an efficient and secure off-chain voting platform. The platform can be accessed through the internet[2] and users can connect their Web3 wallets to the platform to participate in the voting process. Votes are tallied off-chain and cryptographically signed by the participants, then weighted by the amount of tokens that the participants hold. The governance platform is built on top of a modified helios server. This introduces additional complexity when trying to integrate a conceptually different on-chain governance platform.

Integration Strategy. We propose to introduce a new "DID component" into the platform that allows users to authenticate themselves via their Atala PRISM DID in order to mint the described authentication NFT. Since the current off-chain governance platform is conceptually very different and re-using the existing off-chain platform is difficult, we propose to integrate the new on-chain governance platform in a separate process. This involves designing a new user interface for the on-chain governance platform, as well as a new backend that interacts with the Cardano blockchain. The existing governance platform will be adapted to support vote weighting via authentication NFTs, but otherwise operate as usual and will be used to discuss proposals and to vote on proposals that do not require on-chain effects. Since the new user interface will be built from scratch, it will be possible to integrate the old off-chain governance platform into the existing governance platform natively in the future.

[2] The governance platform can be accessed at `https://vote.muesliswap.com`