Introduction

ScopeLift was commissioned as part of a governance improvementproposal put forward by Tally to research private voting and partial delegation solutions for the Arbitrum DAO.

Private Voting Solutions Assessments

The current onchain governance architecture provides complete transparency to the voting process. While this has many benefits, it can also pose challenges in running a fair election such as electing security council members.

Some of the solutions discussed below will require a direct integration into the governor while others can be supported through an integration with Flexible Voting. Both of these paths would require a governor upgrade, however an upgrade to the Core and Treasury Governors which includes Flexible Voting has already been planned for later this month.

In no particular order, we evaluated five existing private voting solutions and explored three avenues of creating a new private voting solutions using relevant privacy tools. We assessed each solution by analyzing their potential tradeoffs, implementation feasibility, and effort needed to incorporate them into a DAO governance structure.

Assessment Factors

To prevent major delegates from influencing election and voting results, we considered hiding the identity of the voter as the most important factor in our assessment. Several other key factors were also considered in assessing each privacy solution:

1. Ballot privacy: Whether the vote preference of a voter is revealed.

2. Tallying transparency and correctness: Whether the vote is tallied in a decentralized and transparent manner

3. Optionality and verifiability: If the voter has the choice of voting privately or in public, including the option to reveal their vote if desired. And the ability to verify the final results.

MACI

MACI offers voter privacy along with vote privacy and bribery protection. MACI 1.0 was released in 2021 and version 2 is coming out in 2024. They have revamped the documentation and are looking to integrate it into existing projects. Currently, the clr.fund is using MACI.

MACI can stand alone as a voting system. New users must deposit their tokens when signing and will create a new key pair to vote. There will need to be some customization in order to integrate MACI into the Security council governor. One other complication is that MACI relies on a trusted coordinator to gather and report the vote tally. This coordinator can decrypt votes and can choose to never conclude a round.

Voter

Ballot

Tallying

Optionality

Private

Private, but votes can be read by the trusted coordinator.

Needs a trusted coordinator

The voter cannot reveal their vote

The project is under active development and is a promising solution despite its complexity.

Semaphore

Semaphore offers anonymous group-based signaling and can be used as a foundation to build a private voting system. It has censorship resistance and is well documented with examples and guides on integrating it into existing smart contracts.

It does require users to register an identity to be part of a voting group. The voting groups may need frequent updates to reflect token transfers, potentially increasing complexity and gas costs. While Semaphore provides voter anonymity, it doesn’t encrypt the votes themselves, requiring additional steps for complete vote secrecy.

Voter

Ballot

Tallying

Optionality

Private

Public

Public

N/A

A deeper look into the identity registration process, group update mechanisms, and additional vote privacy measures will be necessary to adapt it to a comprehensive private voting solution.

Cicada

Cicada uses a time-lock puzzle scheme to delay revealing voter preferences until voting period has ended. It needs a membership proving system like Semaphore in order to protect voter identity and hence shares similar trade-offs.

Voter

Ballot

Tallying

Optionality

Public

Private until voting ends

Public once voting ends

Votes will be public once voting ends

It provides a novel method for implementing private voting but will most likely need some layer for voter anonymity.

Plume/Nouns Aztec Private Voting

We didn’t consider these ready because they are either explicitly a work in progress or they lacked enough documentation in relation to a private voting solution. That is not to say these are not worth considering if a new approach is taken.

New Approaches

Shielded pool

This allows an address to deposit their tokens into a contract and vote using another address. As the number of depositors increase the anonymity of the votes increase, and deposits should be represented in fixed numbers. An account that has multiple deposits will have to vote multiple times using multiple transactions. An account will also have to face the trade-off of privately voting and losing their liquidity

Implementation

In this construction, a user would deposit their ARB tokens along with a commitment hash of two secrets.

Voter

Ballot

Tallying

Optionality

Private

Public

Public

N/A

Depositors of the token pool, through a relayer, can cast their vote fractionally using Flexible Voting. A valid proof of a deposit, and a proposal id is required to prevent double voting. Using a zero knowledge proof, depositors can generate a merkle proof without revealing their secrets. Snapshots of merkle tree roots should be stored in order to prevent late depositors to vote for a proposal that has already started.

To withdraw their deposits, the users will provide their secrets and will be able to withdraw back to the original depositor address that corresponds to the deposit commitment hash. Although all the technological pieces for this solution exist, and have been proven to work in other contexts, a non-trivial amount of work would be required to put them together to construct production-ready privacy preserving voting. Nonetheless, this approach seems promising, as the work needed is primarily engineering work, rather than fundamental research…

Stealth voting

Another possible bespoke solution is a voting system that utilizes stealth addresses via ERC-5564 and ERC-6538. This implementation will require a trusted coordinator that is responsible for holding private keys corresponding stealth meta-addresses and tallying votes correctly.

Voter

Ballot

Tallying

Optionality

Public

Private

Needs a trusted coordinator

Can be optional with an additional governance extension contract

Implementation

The basic idea is that a trusted coordinator will generate stealth meta-addresses corresponding to each option in a proposal. And anyone can announce their vote preference for a given proposal by including a stealth address generated using one of the stealth meta-addresses. Once the voting period ends, the trusted coordinator can tally the announcements each stealth meta-address owner has received, and output the winning option.

This implementation would have the usual benefits that comes with stealth addresses. Voters can vote without an extra step and with their full voting weight, but their vote preference is linked to the stealth address' hidden owner. There's no liquidity concern as long as your voting weight can be queried from the token. The trusted coordinator portion could potentially be improved by incorporating a zero knowledge proof step to prove that tallying was done correctly. The governor will need to be upgraded to accept tallying results and an extension could be added to overwrite the behaviors of the default castVote

function.

Railgun

Railgun as it is now offers transaction anonymity, meaning the identity of the sender, recipient, token, and amount remain private once onboarded onto the system with new private key pairs. Critically, Railgun allows those who have deposited into the privacy pool to interact with external contracts by submitting zero knowledge proofs. Wallet software must be developed to construct the proofs for specific external calls and forward them to Railguns relayer network. The Railgun protcol charges a fee for each transaction sent in this manner.

Voter

Ballot

Tallying

Optionality

Private

N/A

N/A

N/A

Customizing or creating a solution based on Railgun might prove challenging while introducing new reliance on the existing Railgun infrastructure. It still is a great privacy framework to keep in mind and Railgun SDK could help with this process. Bridging the gap between its current implementation and unique requirements of an onchain governance system will require significant research and effort.

Conclusion

Our assessment of existing private voting solutions concludes that although there are several projects and tools that enable private voting, none of them are plug and play with Arbitrum DAO’s existing governance system. Any effort to add private voting would require additional effort to integrate a privacy solution with a new customized governor.

We provided different trade-offs and it’s crucial to seek DAO members’ input on implementing an onchain private voting solution, their priorities and preferences, including voter anonymity, result verifiability, and potential trade-offs.

We recommend the DAO to further explore the proposed new approaches when considering how to bring private voting to the security council election processes. In particular, the Shielded Pool solution seems the most promising in terms of a system that could be producitionized with a reasonable amount of effort, yet has minimal tradeoffs as it relates to privacy properties. Nonetheless, such an effort would require significant resource to be dedicated to developing proof of concepts, further research, audits and bug bounties.

Partial Delegation Solutions Assessments

The current delegation structure limits token holders to delegating their voting power to a single address. To enhance flexibility and empower token holders, we explored various solutions that enable delegation to multiple addresses. In this document, we aim to highlight the key trade-offs associated with each solution, providing a comprehensive analysis to guide decision-making

Assessment Factors

1. Separate vote flow: Whether the solution allows a token holder to submit the paritial delegation vote using one of the Governor’s cast vote methods.
2. Loss of liquidity: Whether the solution requires the delegator to deposit the ERC20Votes token into a contract in order to partially delegate their votes.

Franchiser

Franchiser was developed by the Noah Zinmeister to allow token holders to delegate their voting power across multiple addresses. It works by having a user deposit the funds into a Franchiser contract that delegates them to the desired delegate. This system allows for the tokens to also be redelegated to another franchiser address.

Separate Vote flow

Loss of liquidity

No

Yes

Paritial Delegation ERC20Votes

This solution was developed by Agora with help from ScopeLift. It overrides the ERC20Votes token contract to allow a token holder to delegate to multiple addresses. It maintains the voting flow and does not cause the token holder to lose liquidity. Some drawbacks: it increases gas costs for token transfers, would require a token upgrade for Arbitrum, and does not support subdelegation.

Separate Vote flow

Loss of liquidity

No

No

Conclusion

Among the solutions explored, the Partial Delegation ERC20Votes contract offers a balanced set of trade-offs for the Arbitrum DAO. It enables token holders to delegate voting power to multiple addresses without losing liquidity and maintains the existing voting flow. Although, it requires a token upgrade and introduces higher gas costs for token transfers, these issues are not a deal breaker because Arbitrum's token is upgradeable and the token existing on Arbitrum makes gas costs less of a concern. Additionally, the absence of sub-delegation support is not a critical limitation for the current needs of the DAO. Therefore, this solution aligns well with the DAO's objectives for improved governance flexibility.

References

Semaphore Demo

Semaphore Demo

A zero-knowledge protocol for anonymous signaling on Ethereum.

https://projects.ethberlin.org/submissions/334

github.com

GitHub - plume-sig/zk-nullifier-sig: Implementation of PLUME: nullifier friendly...

Implementation of PLUME: nullifier friendly signature scheme on ECDSA

research.aragon.org

Nouns Private Voting Research Sprint - General Report - Aragon ZK Research -...

Nouns sprint report

blog.rs – 12 Dec 23

The State of Private Voting in Ethereum

The State of Private Voting in Ethereum and beyond. A report supported by MolochDao | Reading Time: 28 minutes