User privacy in DAOs

Semaphore Protocol

Ignas Apšega

3620557

Version Control

Version	Date of change	Change description
0.1	23-02-2023	Initial Start
0.2	08-03-2023	Added Research matrix - Page 5 Updated flow diagram - Page 7
0.3	15-03-2023	Flow chart and Conclusion updated

Table of Contents

1. Introduction

1.1 Purpose of the document

The purpose of this document is to describe the integration process of the Semaphore Protocol[1] into a WEB3[2] template as part of the User Privacy in DAOs[3] project.

1.2 Context

The context of this document is within the Realisation of Zero-Knowledge[4] solutions to Byonts WEB3 template. This document will present what is Semaphore Protocol - how it works and how it could be used within the context of solving User Privacy in DAOs.

2. Research

2.1 Research Questions

This research is part of the following sub-questions, which were also researched in the previous documents:

1. **Could the solutions found be implemented in the current projects of Byont?**

To refer back to the possible solutions check:

1. Zero-Knowledge Proofs Protocols and libraries document - to get introduced to ZKPs.
2. Circom and SnarkJS implementation - to get introduced to possible libraries and implementations of ZKPs.

2.2 Research Context

Before starting with the research we have to give more context on the research questions. Kicking off with:

Could the solutions found be implemented in the current projects of Byont?

It is necessary to answer this question because if so, Byont could implement similar solutions and patterns into their other projects.

2.3 Research strategy

For this research mainly the strategy **Workshop** was chosen. It is done to explore opportunities. Prototyping, sketching, and co-creation activities are all ways to gain insights into what is possible and how things could work.

2.4 Research methods

Workshop research strategy has multiple research methods. But not all of them were used to conduct this research.

Prototyping was used to develop, evaluate, and design a solution to learn whether the libraries work and discover the technical limitations or possibilities.

Research methodology	Research question
Workshop	Could the solutions found be implemented in the current projects of Byont?

3. Research Results

3.1 Could the solutions found be implemented in the current projects of Byont?

To be able to answer this question we have to dig deeper if the found solutions are viable for Byont.

Research Matrix of Possible solutions

A couple more solutions were considered for the implementation of ZKPs. ***The main criterion was whether they explicitly had a use case for private user voting***. Other criteria were also taken into consideration, such as the programming language, as Byont's tech stack includes JavaScript/TypeScript for its front-end and the choice of smart contracts is Solidity. Additionally, it was checked whether the solutions use Circom circuits for zero-knowledge, as previous research has included it.

Solution	**Programming Language**	**Uses Circom circuits**	**Knockout criteria - has explicit use case of Private User Voting**
Semaphore Protocol	TypeScript/Solidity	Yes	Yes
SnarkyJs	TypeScript	No	No
Aztec SDK	JavaScript	No	No

In conclusion, Semaphore Protocol came in on top. Because it had an explicit use of User Voting in its documentation. It also uses pre-made adjustable Smart-Contracts for management of users, proposals and votes. To add, it also includes TypeScript library to generate, verify proofs and create Anonymous Identity.

Semaphore Protocol

Semaphore is a protocol, designed to be a simple and generic privacy layer for Ethereum[5] dApps[6]. Using Zero-Knowledge, Ethereum users can prove their membership in a group and send signals such as votes or endorsements without revealing their original identity. The core of the Semaphore protocol is in the Circuit logic[7]. However, Semaphore also provides Solidity[8] Smart Contracts[9] and JavaScript libraries to make the steps for Off-chain[10] proof creation and On-chain[11] verification easier.

Integration into Byonts WEB3 Template

Byonts WEB3 Template is a boilerplate for developing Ethereum-based projects. This means it is basically a dApp on which Semaphore Protocol can be developed.

Semaphore protocol, a Zero-Knowledge Proof (ZKP) technique, will be implemented into BYONT's WEB3 Template as a proof of concept for bringing privacy to users' voting participation in DAOs. Semaphore protocol allows users to perform computations on encrypted data, without revealing any information about the data itself. This ensures that users' voting participation in DAOs can be kept private, protecting them from discriminatory practices and off-chain coercion

Proof of Concept - Flow

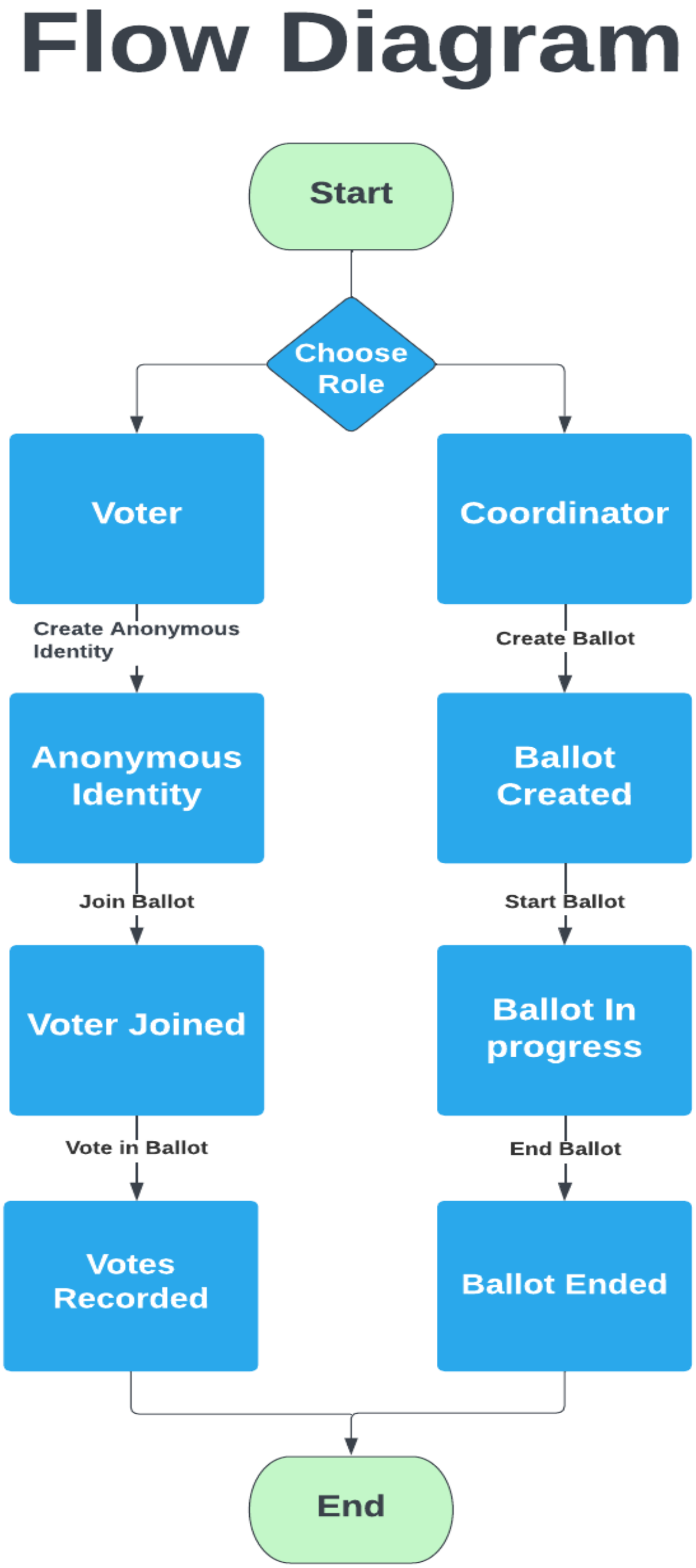
The proof of concept for bringing privacy to users' voting participation in DAOs using Semaphore protocol will consist of two components - a coordinator and a voter. The coordinator will have the ability:

- Create a ballot
- Start the ballot
- End the ballot.

On the other hand, the voter will be able to:

- Create an anonymous identity
- Join the ballot
- Cast their vote anonymously using the Semaphore protocol.

By having these features, users can ensure their privacy and vote without fear of repercussions or discrimination. The integration of these components into the BYONT WEB3 Template could promote a fair, transparent, and inclusive environment in DAOs.



Conclusion

In conclusion, the research results show that Semaphore Protocol is the most suitable solution for implementing Zero-Knowledge Proofs (ZKPs) into Byont's current projects. The Semaphore Protocol meets the criteria set for this research, including having an explicit use case for private user voting, compatibility with Byont's tech stack (JavaScript/TypeScript and Solidity), and using Circom circuits for zero-knowledge. Furthermore, the Semaphore Protocol's simplicity and generic nature make it ideal for integration into Byont's WEB3 Template, a boilerplate for Ethereum-based projects.

The proof of concept demonstrates how the Semaphore Protocol can bring privacy to users' voting participation in DAOs. By separating the roles of a coordinator and a voter, it allows for a secure, anonymous, and efficient voting process. The coordinator manages the ballot creation, start, and end, while the voter can create an anonymous identity, join the ballot, and vote without revealing their true identity.

The integration of the Semaphore Protocol into Byont's WEB3 Template has the potential to significantly improve the privacy and security of voting participation in DAOs. It protects users from discriminatory practices and off-chain coercion while promoting a fair, transparent, and inclusive environment within these decentralized organizations. As a result, the Semaphore Protocol stands out as a promising solution for Byont's ongoing projects and the broader Ethereum ecosystem.

Citation and References

1. “AnonyVote: A DAO Tooling Platform for Anonymous Voting With ZK.” *Harmony forum*, 11 March 2022, https://talk.harmony.one/t/anonyvote-a-dao-tooling-platform-for-anonymous-voting-with-zk/13810. Accessed 28 October 2022.
2. “Blockchain Facts: What Is It, How It Works, and How It Can Be Used.” *Investopedia*, https://www.investopedia.com/terms/b/blockchain.asp. Accessed 26 October 2022.
3. Book, Adrien. “Everything Wrong With DAOs |.” *cult by Honeypot*, 5 July 2022, https://cult.honeypot.io/reads/everything-wrong-with-daos/. Accessed 27 October 2022.
4. “Collab.Land.” *Welcome to Collab.Land*, https://collab.land/. Accessed 26 October 2022.
5. “DAO Nation — Clay.” *Clay*, 16 August 2021, https://clay.mirror.xyz/DwJ60O0R1IyRiPAZFBw4L05L3fd8PPxWnzDNedKtOas. Accessed 27 October 2022.
6. “Ethereum.” *Wikipedia*, https://en.wikipedia.org/wiki/Ethereum. Accessed 26 October 2022.
7. Frankenfield, Jake. “What Are Crypto Tokens, and How Do They Work?” *Investopedia*, 20 May 2022, https://www.investopedia.com/terms/c/crypto-token.asp. Accessed 26 10 2022.
8. “Introduction to dapps | ethereum.org.” *Ethereum.org*, https://ethereum.org/en/developers/docs/dapps/. Accessed 28 October 2022.

9. “On Chain Transactions (Cryptocurrency) Definition.” *Investopedia*, https://www.investopedia.com/terms/c/chain-transactions-cryptocurrency.asp. Accessed 26 October 2022.
10. Ouaddah, Aafaf. “Arithmetic Circuit.” *ScienceDirect*, 2019, https://www.sciencedirect.com/topics/engineering/arithmetic-circuit. Accessed 25 10 2022.
11. “Testnet.” *Wikipedia*, https://en.wikipedia.org/wiki/Testnet. Accessed 28 October 2022.
12. “Uniswap.” *Wikipedia*, https://en.wikipedia.org/wiki/Uniswap. Accessed 26 October 2022.
13. “Web3.” *Wikipedia*, https://en.wikipedia.org/wiki/Web3. Accessed 27 October 2022.
14. “Welcome to Snapshot!” *Home - snapshot*, https://docs.snapshot.org/. Accessed 26 October 2022.
15. “What are smart contracts on blockchain?” *IBM*, https://www.ibm.com/topics/smart-contracts. Accessed 26 October 2022.
16. “What is SushiSwap? (SUSHI).” *Kraken*, https://www.kraken.com/learn/what-is-sushiswap-sushi. Accessed 26 October 2022.
17. “Zero-knowledge proof.” *Wikipedia*, https://en.wikipedia.org/wiki/Zero-knowledge_proof. Accessed 27 October 2022.
18. “ZKU-Vote: Anonymous voting within DAO - zkDAO - Harmony Community Forum.” *Harmony forum*, 12 May 2022, https://talk.harmony.one/t/zku-vote-anonymous-voting-within-dao/18423. Accessed 28 October 2022.

Appendix

Term	Explanation
1. Semaphore Protocol	Using zero knowledge, Semaphore allows Ethereum users to prove their membership of a group and send signals such as votes or endorsements without revealing their original identity. (“Semaphore Protocol”)
2. WEB3	**Web3** is an idea for a new iteration of the World Wide Web which incorporates concepts such as decentralization, blockchain technologies, and token-based economics (“Web3”)
3. Decentralized Autonomous Organization (DAO)	A decentralized autonomous organization (DAO) is an emerging form of legal structure that has no central governing body and whose members share a common goal to act in the best interest of the entity. Popularized through cryptocurrency enthusiasts and blockchain technology, DAOs are used to make decisions in a bottom-up management approach. (Reiff)
4. Zero-Knowledge Proofs (ZKP)	Zero-Knowledge Proofs (ZKPs) — a method for one party to cryptographically prove to another that they possess knowledge about a piece of information without revealing the actual underlying information. In the context of blockchain networks, the only information revealed on-chain by a ZKP is that some piece of hidden information is valid and known by the prover with a high degree of certainty.
5. Ethereum	Ethereum is a decentralized, open-source blockchain with smart contract functionality. Ether is the native

	cryptocurrency of the platform. Among cryptocurrencies, ether is second only to bitcoin in market capitalization. Ethereum was conceived in 2013 by programmer Vitalik Buterin (“Ethereum”)
6. dApps (Decentralized Applications)	A decentralized application (dApp) is an application built on a decentralized network that combines a smart contract and a front-end user interface. On Ethereum, smart contracts are accessible and transparent – like open APIs – so your dApp can even include a smart contract that someone else has written. (“Introduction to dapps | ethereum.org”
7. Circuit Logic	An arithmetic circuit is a set of gates with a separate set of inputs for each number that has to be processed. The gates are connected so as to carry out an arithmetic action, and the outputs of the gate circuit are the digits of the result (addition, subtraction, multiplication, or division). Arithmetic circuits are used to define problems in the arithmetic way(Ouaddah)
8. Solidity	It is an object-oriented programming language for implementing smart contracts on various blockchain platforms, most notably, Ethereum. It was developed by Christian Reitwiessner, Alex Beregszaszi, and several former Ethereum core contributors. Programs in Solidity run on Ethereum Virtual Machine. (“Solidity”)
9. Smart Contract	Smart contracts are simply programs stored on a blockchain that run when predetermined conditions are met. They are typically used to automate the execution of an agreement so that all participants can be immediately certain of the outcome without any intermediary’s involvement or time loss. They can also automate a workflow, triggering the next

	action when conditions are met. (“What are smart contracts on blockchain?”)
10. Off-Chain	Off-chain transactions are conducted outside of the blockchain network. Off-chain transactions can be done by the participants in which they have an agreement that a third-party guarantees the transaction or verifies that it's valid or complete. The two participants could also exchange their private keys so that the crypto assets are exchanged without moving any money out of their digital wallets. (“On Chain Transactions (Cryptocurrency) Definition”)
11. On-chain	On-chain transactions refer to transactions that are recorded and verified on the blockchain. Off-chain transactions don't occur on the blockchain network but instead are transacted on another electronic system such as PayPal. (“On Chain Transactions (Cryptocurrency) Definition”)