zkVote

Anonymous Voting with Polygon ID and Semaphore

Polygon @The Pit Singapore

Problem

DAOs are groups that exist online in the world of blockchains.

At its current state, blockchain isn’t great for privacy.

How do we vote anonymously in a DAO?

Solution

zkVote = Polygon ID + Semaphore

Polygon ID for DID

Polygon ID is self-sovereign, private and decentralized identity system

It allow us to:

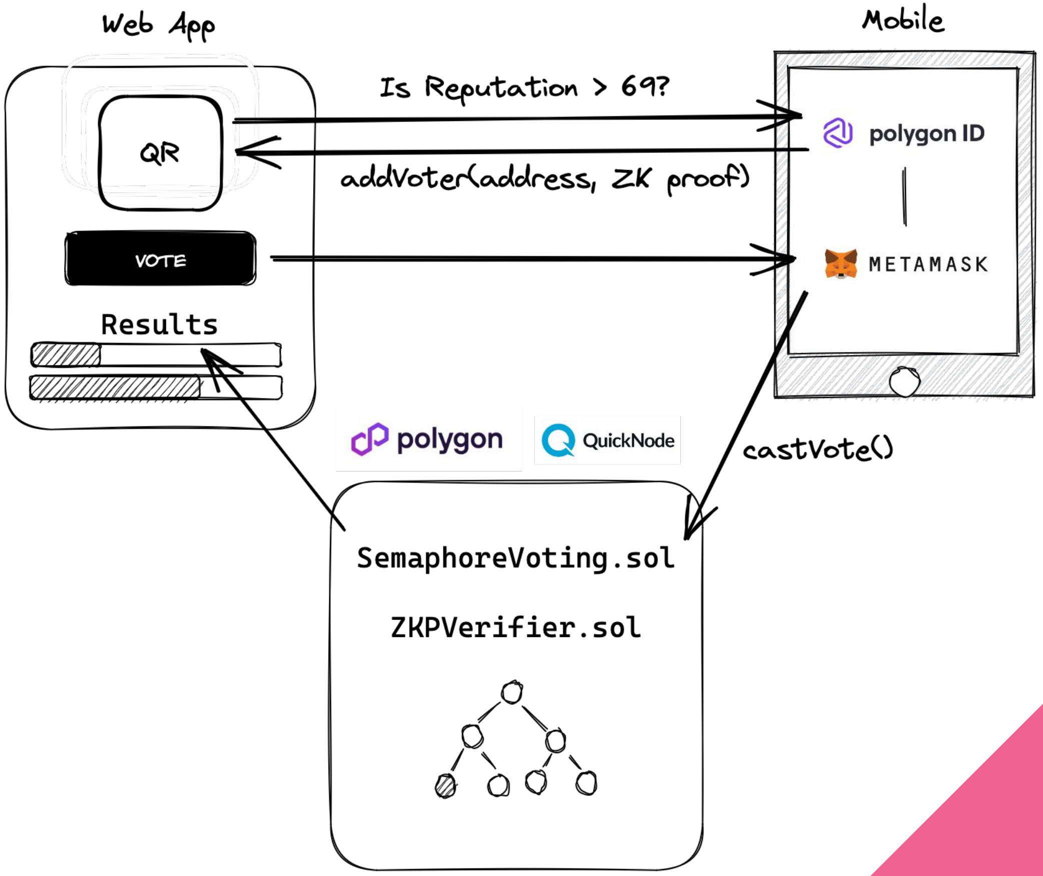
1. Prove that one is a member of a group
   - e.g. DAO
2. Only let members who fit arbitrary criteria to vote
   - e.g. one has to be in the group for a certain period of time

Anonymous Voting with Semaphore

Semaphore:

- ZKP created by Ethereum Foundation
- Allows users to signal anonymously within a predefined group
- Prevents double-signaling
- Creates an off-chain proof that can be verified on-chain
- Proves:
  1. User is a member of a group
  2. User who cast the vote is the same user who created the proof

System Architecture



Demo

Thank you!

Appendix

Current Limitations

- Polygon ID currently does not allow us to associate a claim ID with a semaphore ID

Future Ideas

- Polygon ID will release a major version update in ~1 week
- Technically anonymous voting can also be done in Polygon ID right now but that involves a lot of fiddling as the Polygon ID app is closed source and also lacks customization (e.g. no custom payload)