Abstract

If we allow groups of people to signal with complete anonymity we can reduce the signaling components in human interactions. This will considerably reduce the cost of expressing contention opinions. However these systems can be abused. So its important to have the ability to revoke users from these groups if they break the rules.

Previously we build Semaphore allows static anonymous reputation system. Here we propose an expansion of Semaphore where we can destroy a users reputation without knowing their Identity. We use this to build a binary reputation system which can trivially be expanded to a non binary reputation system.

Background

With semaphore we create a merkle tree of user identities. Where each user knows some secret information (the hash seed of the leaf) about their leaf in the merkle tree.

We then use snarks to prove that users know the secret information of a leaf in the tree. They can also signal their support of statements (32 bytes string currently), like a vote or a tweet. We call this a signature. Finally we expanded this with a malleable nullfier so that users can only signal once about a given statement. So a user can signal about the same string twice but everyone will know that they did. If a user signals about different strings it will be impossible to link them together.

This is quite powerful construction and can be used for voting, social media, anonymous credentials…

Reputation system

In order to build a reputation system we need to be able to burn users reputation if they break some rules.

Roles in the system

The system has two roles

1. The users who signal about things
2. The admin who is able to remove users from the system if they break some rules, this could be a smart contract.

Reputation system

We can use the nullifier to prevent a user from signalling but because it is malliable we cannot tell when they are signalling about something different. So its trivial for an attacker to avoid some nullifier based bans.

To prevent this we have an epoch system, during the epoch the users can signal. The admin can select various signals that broke the rules. They collect these illegal signals into a smart contract.

At the end of the epoch each user is required to move to a new merkle tree, to move to this new tree they must prove via snark that they did not make any of the illegal signals

. If they cannot prove this they cannot move and their reputation is burned.

This way we can burn users reputations if they break the rules.

Conclusions

Forcing users to move merkle trees once an epoch is a limitation choosing the epoch length is difficult If its too short users will need to be online to perform this action. If its too long the admin will be unable to stop malicious activity until the end of an epoch. There are a few ways to limit this be allowing users to jump from epoch 1 to epoch 12 skipping the intermediate stages, however this limits the anonymity set.

We can use this to build non binary reputation systems in a few ways. We could add an int reputation

to the leaves and limit how much people are able to transfer to the new tree if they made an “illegal” signal we could just give multiple users multiple leaves each being 1 unit of reputation