UNIVERSITÀ
DI TRENTO

Politecnico
di Torino

Towards a Privacy-Preserving Dispute Resolution Protocol on Ethereum

Andrea Gangemi

DLT 2023, 25 Maggio

Department of Mathematics, University of Trento
Department of Mathematical Sciences, Politecnico di Torino

Overview

We present a new dispute resolution protocol that can be built on the Ethereum blockchain.

The idea uses the following protocols and tools:

1. *Semaphore* and *MACI*;
2. *quadratic voting*;
3. *soulbound tokens*.

State-of-the-art

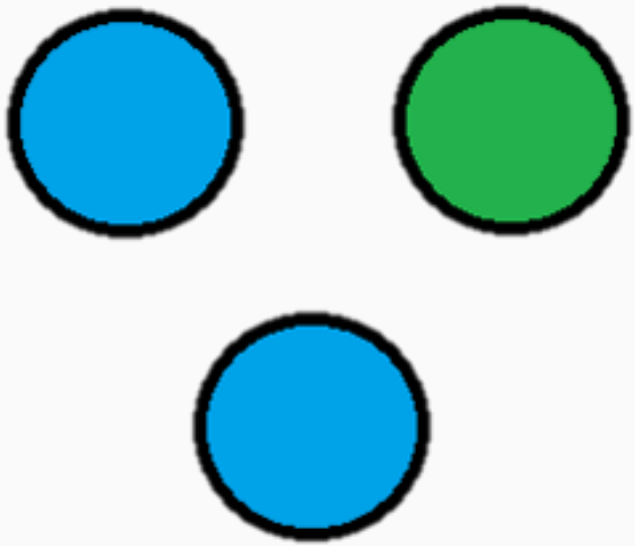
The most active dispute resolution platform on the Ethereum blockchain is *Kleros* [2].

- It is a is a crowdsourced arbitration protocol;
- Arbitrators are chosen according to a Proof-of-Stake mechanism, and their aim is to find a fair solution to the conflict, using a game-theory model known as *Schelling game* [4];
- They will vote the option they repute to be the correct one, and at the end the option that has been chosen by the majority of arbiters will be enforced;
- Judges that chose that option receive a economical (ERC20 token) reward, while the stake of the other judges will be slashed.

Schelling game

A *Schelling point* is a solution that people tend to choose by default during absence of communication.

Assume that three people win a prize only if they select the same circle: which one will they choose?



Kleros: pro and cons

Pros:

1. Everyone can vote;
2. The dispute is resolved quickly;
3. The protocol can be implemented in any blockchain that allows smart contracts.

Cons:

1. Parties are forced to accept the judge's decision;
2. There is not a real resistance to collusion attacks.

Examples of disputes include the following areas: *curated lists, token listings, social networks, Gitcoin grants*.

Semaphore

Semaphore [5] is a zero-knowledge protocol which allows Ethereum users to prove their membership in a group and send signals such as votes, without revealing their identity.

- Semaphore can be regarded as a Sybil-resistance mechanism;
- Each signal sent contains a zero-knowledge proof, generated off-chain and validated on-chain, about the sender's membership of a certain group as well as the validity of the signal itself.

MACI

MACI (Minimal Anti-Collusion Infrastructure) [3] is a protocol that allows users to vote on-chain with a greatly increased collusion resistance.

The issue: all transactions are public, so a voter can easily show to a briber which option they voted for.

- MACI uses zero-knowledge proofs to hide how each user voted, while still allowing to know the final vote result;
- There are two different actors: *users*, the people that send a encrypted vote through a smart contract, and a single *trusted coordinator*, which makes the tally of the votes and releases the final result.

The idea

Suppose that a conflict happens. The new dispute resolution process can be divided into two phases:

- **Phase 1**: judges, that is member of a certain Sempahore group, will send a signal containing a vote and a solution to the issue. At the end of this process, the MACI coordinator does the tally of the votes and gives a proportional score to each user;
- **Phase 2**: the users involved in the conflict will now be able to vote on their favourite solutions to the dispute. At the end, the proposal that have received the biggest preference will be enforced.

Both votes can be done using the *quadratic voting* [1] mechanism.

Quadratic voting

Quadratic voting is an alternative to more traditional voting mechanisms.

- In this model, every person can vote all the time he wants, but the n-th vote will cost n.
- Quadratic voting has already been used in practice, for example to allocate *Gitcoin grants*.

Social incentive

Judges that contribute to the resolution of the conflict have a social incentive, thanks to the use of *soulbound tokens* [6].

- A soulbound token is a non-transferable, non fungible and publicly visible token that encodes some kind of subjective quality.
- The idea is to reward with a soulbound token the judges that acted correctly or that misbehaved towards the platform.
- The goal is to have the governance of the DAO in the hands of those judges who have spent their time on the proper functioning of the platform, instead of giving it to those who own the ERC-20 tokens, as is usually the case.

References i

S. P. Lalley and E. G. Weyl.
Quadratic voting: How mechanism design can radicalize democracy.
In *AEA Papers and Proceedings*, volume 108, pages 33–37, 2018.

C. Lesaege, F. Ast, and W. George.
Kleros.
Whitepaper available at https://kleros. io/assets/whitepaper. pdf, 2018.

Maci github page, 2023.
`https://github.com/privacy-scaling-explorations/maci`,
Last accessed on 2023-05-23.

References ii

- T. C. Schelling.
  The Strategy of Conflict: with a new Preface by the Author.
  Harvard university press, 1980.
- Semaphore website, 2023.
  https://semaphore.appliedzkp.org/, Last accessed on 2023-05-23.
- E. G. Weyl, P. Ohlhaver, and V. Buterin.
  Decentralized society: Finding web3's soul.
  Available at SSRN 4105763, 2022.