Chirotonia: a scalable and secure e-voting framework based on blockchain and linkable ring signatures

A. Russo¹, A. Fernández Anta¹, M. I. González Vasco², S. P. Romano³

¹IMDEA Networks Institute
²Universidad Rey Juan Carlos
³Università degli Studi di Napoli, Federico II
Solution

Identification
- Identification Manager
- ID Board

Privacy
- Linkable ring signature

Untamperable
- Blockchain

Ballot Box
Vote

Voter → WebCrypto API
- elliptic*

Ethereum

Ballot Box

*https://github.com/indutny/elliptic
Privacy (Secrecy)

The key pair should be generated in a distributed manner in order to avoid a Single point of failure and trust.

**Distributed Key Generation**

Each member holds a secret key share generated through a centralized portal.

**ETHDKG**

Schindler et al.

Fully decentralized and Byzantine Fault Tolerant distributed key generation

https://github.com/PhilippSchindler/EthDKG
Deployment (AWS)

To blockchain nodes and validators at UNINA (Naples), UC3M (Madrid), IMDEA Networks (Madrid)

- Blockchain explorer
- Node A (HL Besu)
- Node B (HL Besu)
- Anonymous proxy
- WebAPP and Identity manager
- Committee portal
- Public subnet
- Private subnet
- Validator (HL Besu)
- CouchDB

1 validator out of a total of 4
Usages and feedbacks

Election of the Head of Engineering, Design and Chemistry division
- 127 voters
- 119 ballots
- Online during one week for voters’ registration
- 8 hours voting session
- Electoral committee made of 3 members

Election of the Head of the Information Technology and Electrical Engineering department - 170 voters (September 2021)

Scale on all University votes ~ 50000 voters (end 2022)

“Nice interface, easy to use and secured by the blockchain, congrats !”
Prof. Rippa, coordinator of the Management Engineering classes at the University of Napoli Federico II

“Linear and effective workflow”
Comments from voters

“Everything went fine. Nice Job !”
Comments from electoral committee members
Thanks for the attention

Antonio Russo - antonio.russo@imdea.org
Antonio Fernández Anta - antonio.fernandez@imdea.org
Maria Isabel Gonzalez Vasco - mariaisabel.vasco@urjc.es
Simon Pietro Romano - spromano@imdea.org

credits for icons: icons8 https://icons8.com/
The Identification manager:

- defines the group of voters’ digital identities
- integrates with existing systems
- can be a set of cooperating entities with a K on N threshold mechanism
Requirements

- Verifiability
- Transparency
- Legitimacy
- Completeness
- Neutrality
- Consistency
- Anonymity
- Confidentiality
- Coercion resistance

- Remote voting
- Immediate result
- Auditability
- Security
- Scalability
Blockchain anonymous interaction

**Anonymous Proxy**
A third entity packs ballots in blockchain transactions
- Web API
- Small voter overhead

**Vote token**
Vote coins are physically distributed to voters
- Blockchain specific API
- Physical interaction needed

**Application specific blockchain**
The blockchain execution layer embeds the voting logic
- Transactions are signed with ring signature
- Only private/consortiated deployments

**Implemented**
For very large deployments

WIP