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

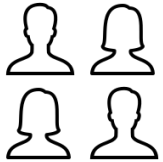
A. Russo[1], A. Fernández Anta[1],
M. I. González Vasco[2], S. P. Romano[3]

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

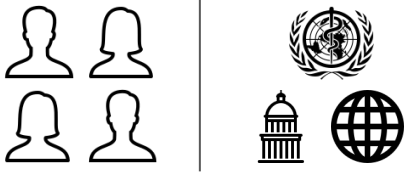
Communication of the ACM - Regional Special Issue 26/8

Context

Voters



Organizer



Third parties

Stakeholders

Independent certifiers

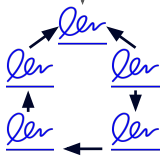
Service providers

Solution

Identification

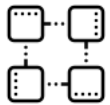
Identification Manager

Privacy



Linkable ring signature

Untamperable

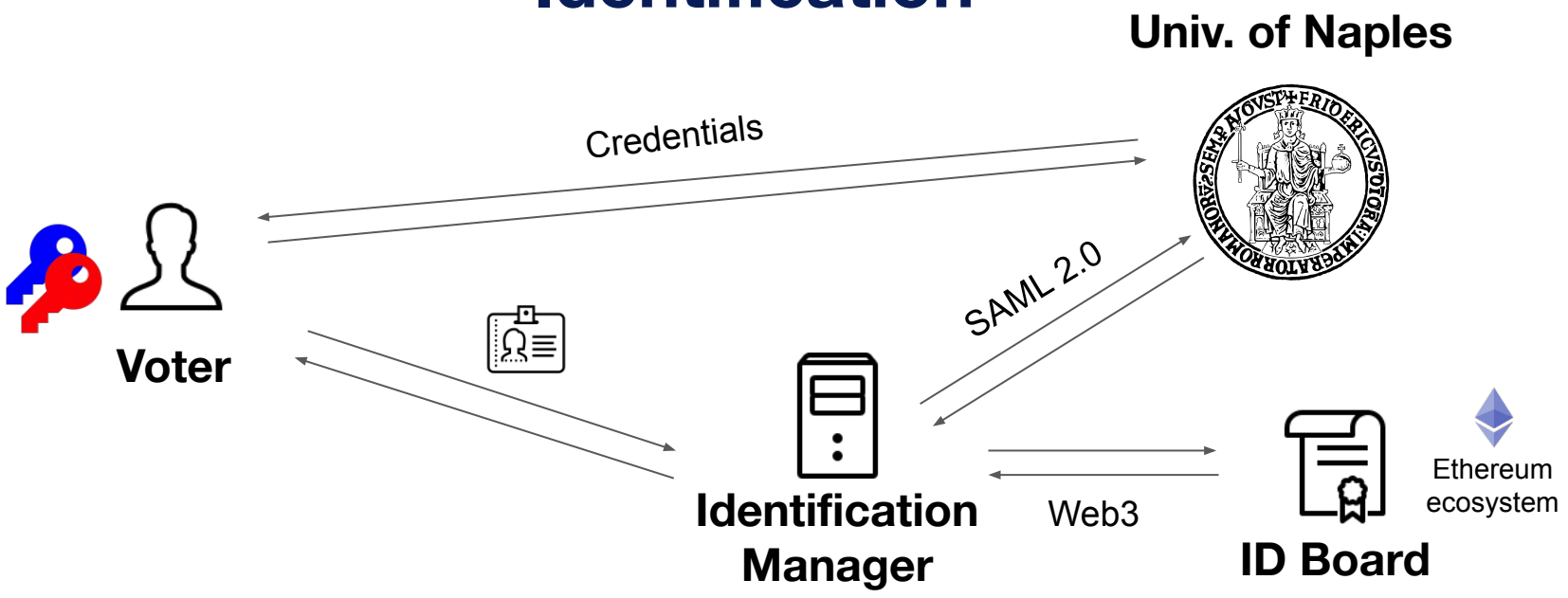


Blockchain

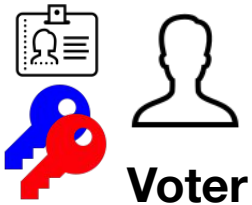
ID Board

Ballot Box

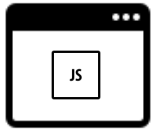
Identification



Vote

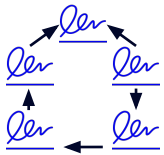


Voter

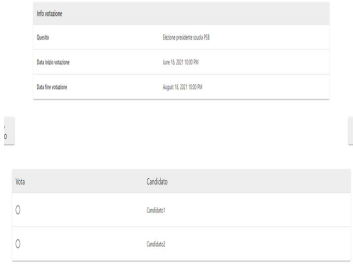


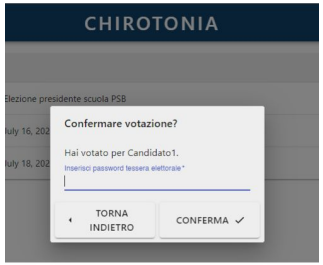
- WebCrypto API
- elliptic*

Ethereum



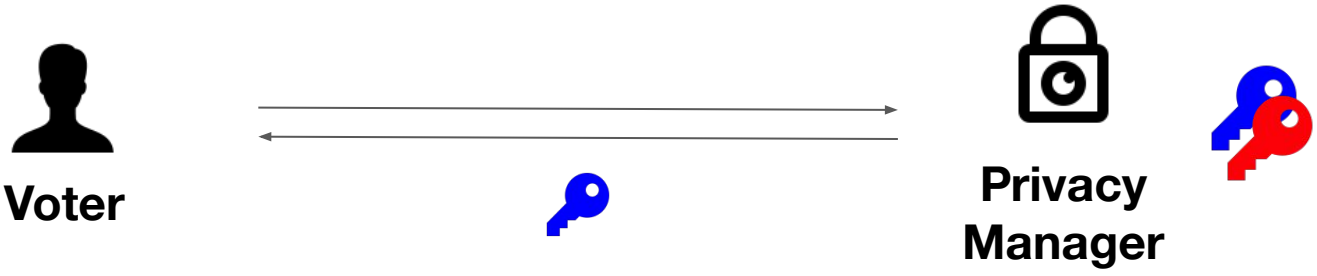
Ballot Box





*https://github.com/indutny/elliptic

Privacy (Secrecy)



Distributed Key Generation

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

Electoral Committee

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

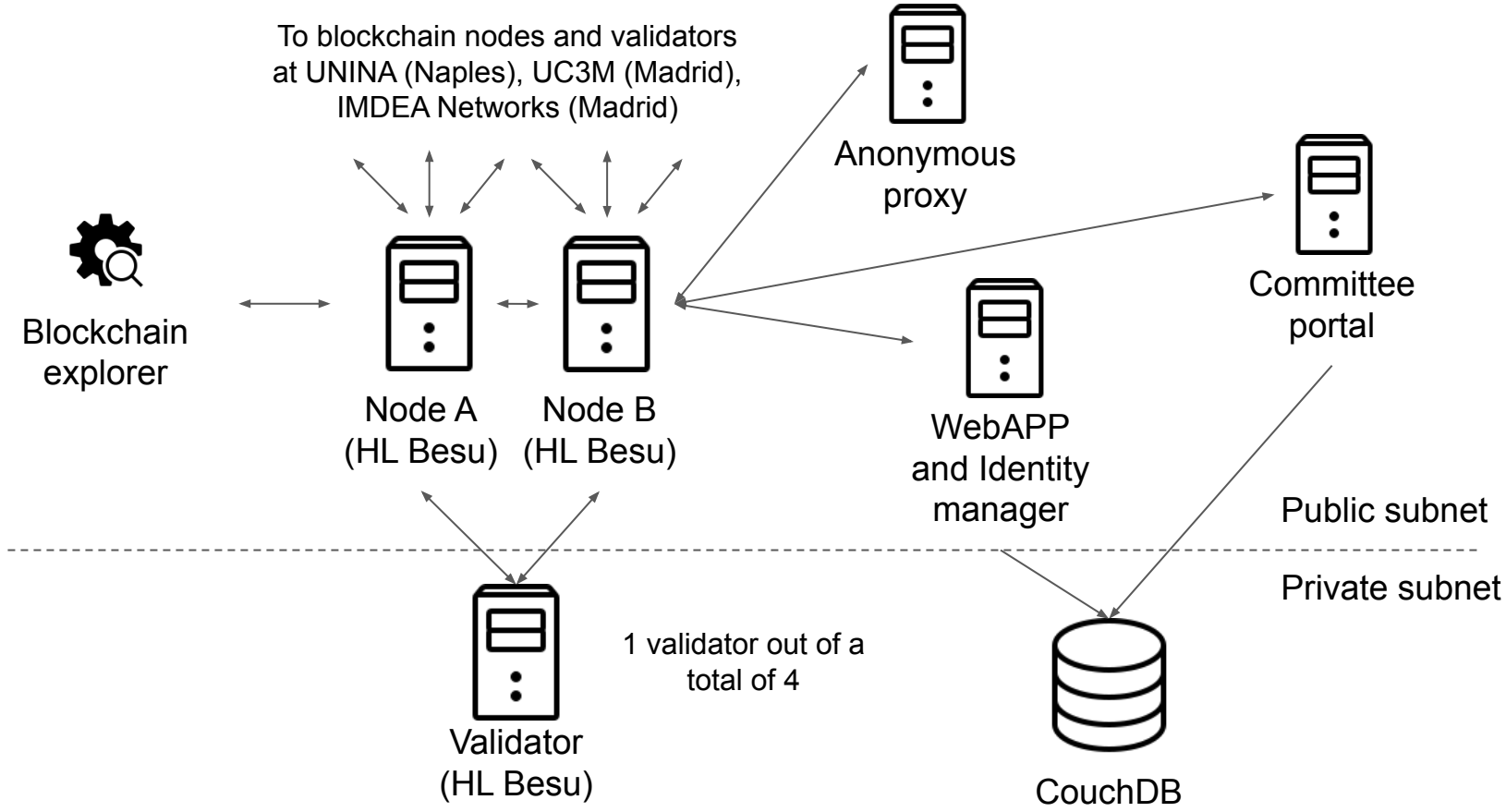
Implemented in Committee portal

ETHDKG Schindler et al.

Fully decentralized and Byzantine Fault Tolerant distributed key generation

https://github.com/PhilippSchindler/EthDKG

Deployment (AWS)



Usages and feedbacks

University of Naples - Federico II

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

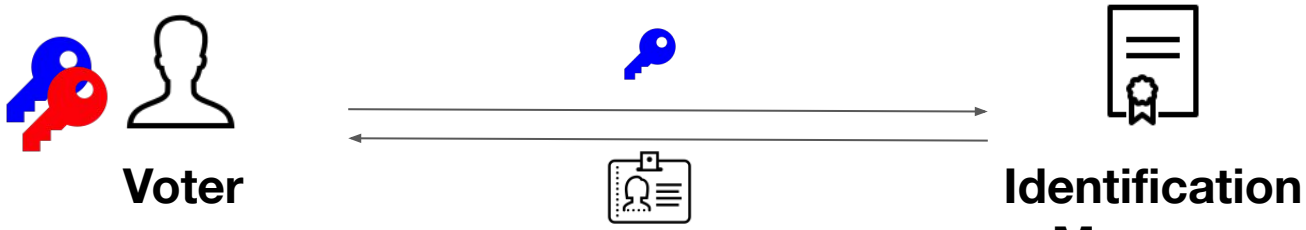
"Everything went fine. Nice Job !"
Comments from electoral committee members

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/

Identification



The Identification manager:

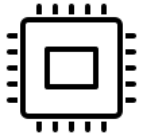
defines the group of voters' digital identities

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

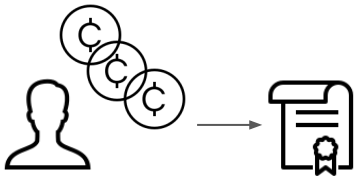
- Web API
- Small voter overhead

Implemented

Vote token

Vote coins are physically distributed to voters

- Blockchain specific API
- Physical interaction needed

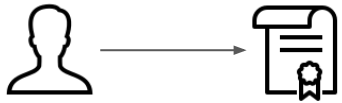


WIP

Application specific blockchain

The blockchain execution layer embeds the voting logic

- Transactions are signed with ring signature
- Only private/consortiated deployments



For very large deployments