Cross-Platform Mobile Application for the Cothority

Cedric Maire & Vincent Petri

Semester Project

Fall 2017

Supervisor

Linus Gasser

EPFL/DeDiS

Responsible

Prof. Bryan Ford

EPFL/DeDiS

Decentralized and Distributed Systems Lab

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

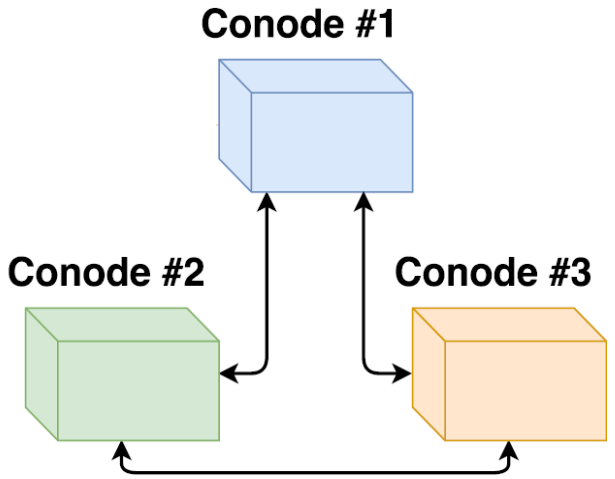
Summary

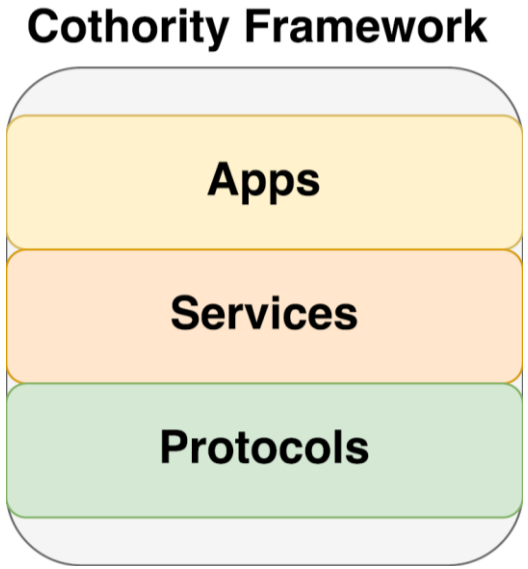
- Introduction
- Problem Statement
- Solutions and Implementation
- Future Work
- Demo

- Introduction
  - Context
  - Cisc
  - PoP
- Problem Statement
- Solutions and Implementation
- Future Work
- Demo

Context

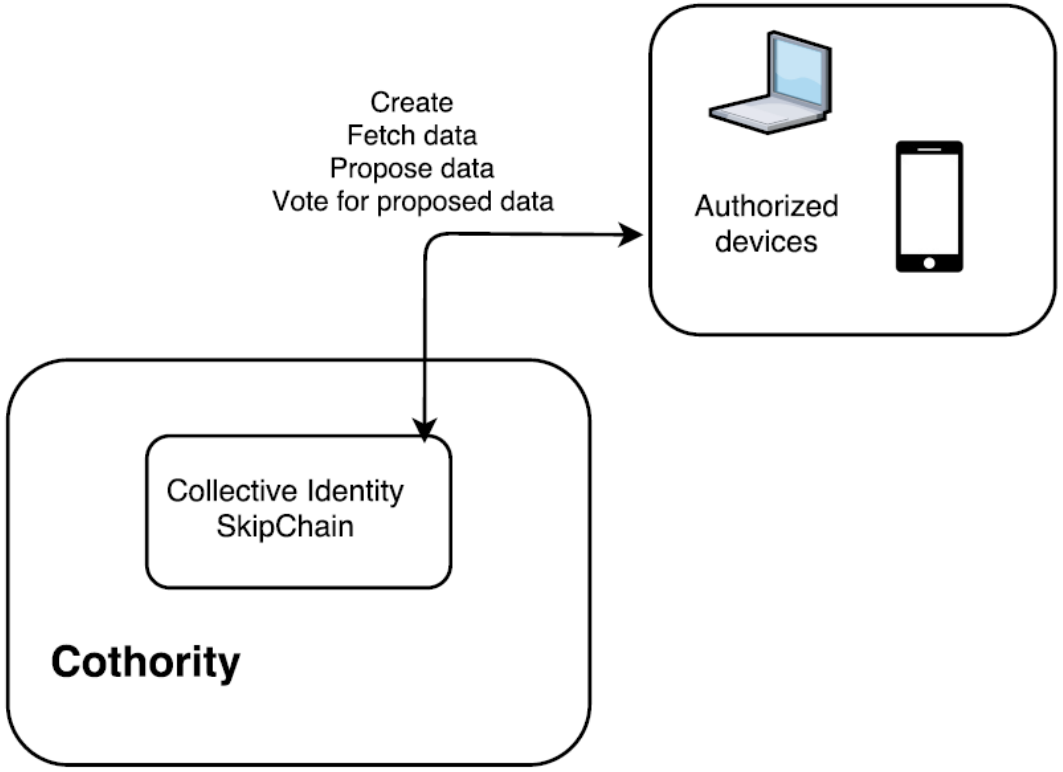
- Cothority framework
  - Protocols between conodes
  - Services (CoSi, Status…)
  - Apps (Cisc, PoP)





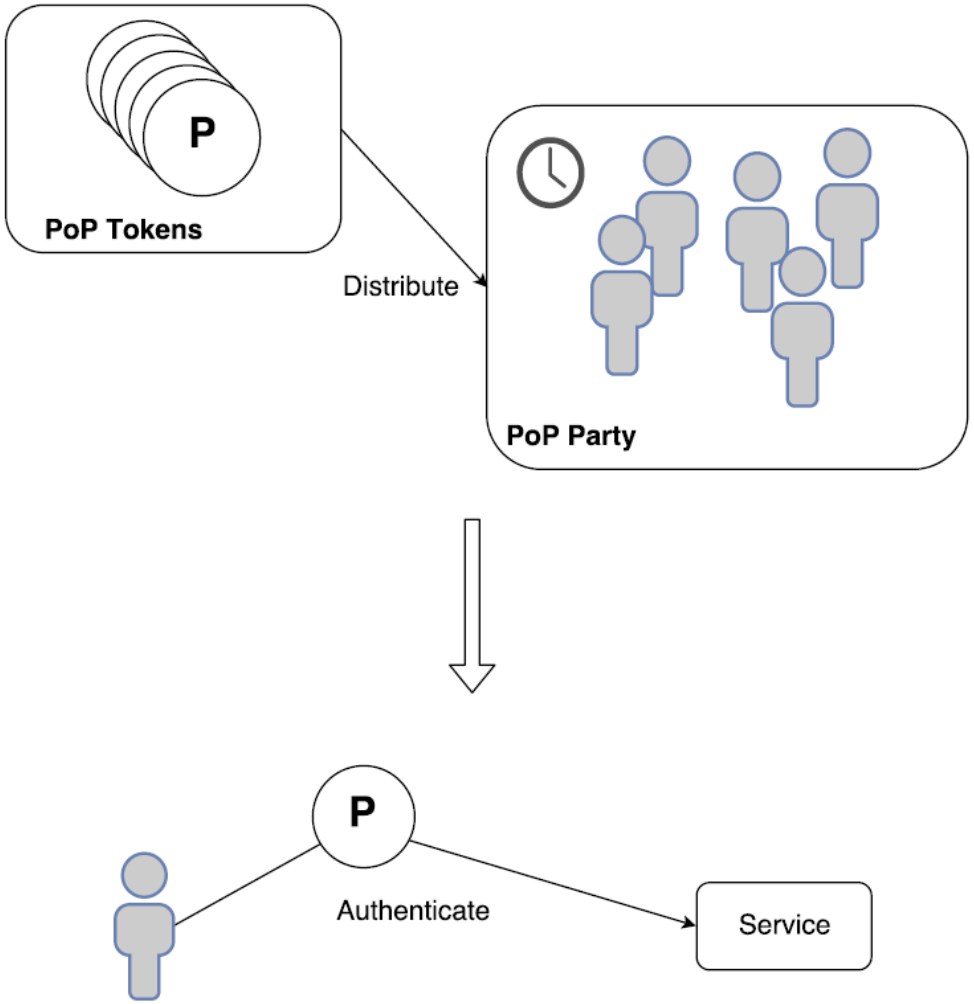
Collective Identity SkipChain (CISC)

- Data storage
  - Key/value pairs
  - SSH public keys
  - Webpages
- Provisioned skipchain
  - Only registered devices can modify data
  - New data need to be accepted by a threshold of devices



Proof-of-Personhood (PoP)

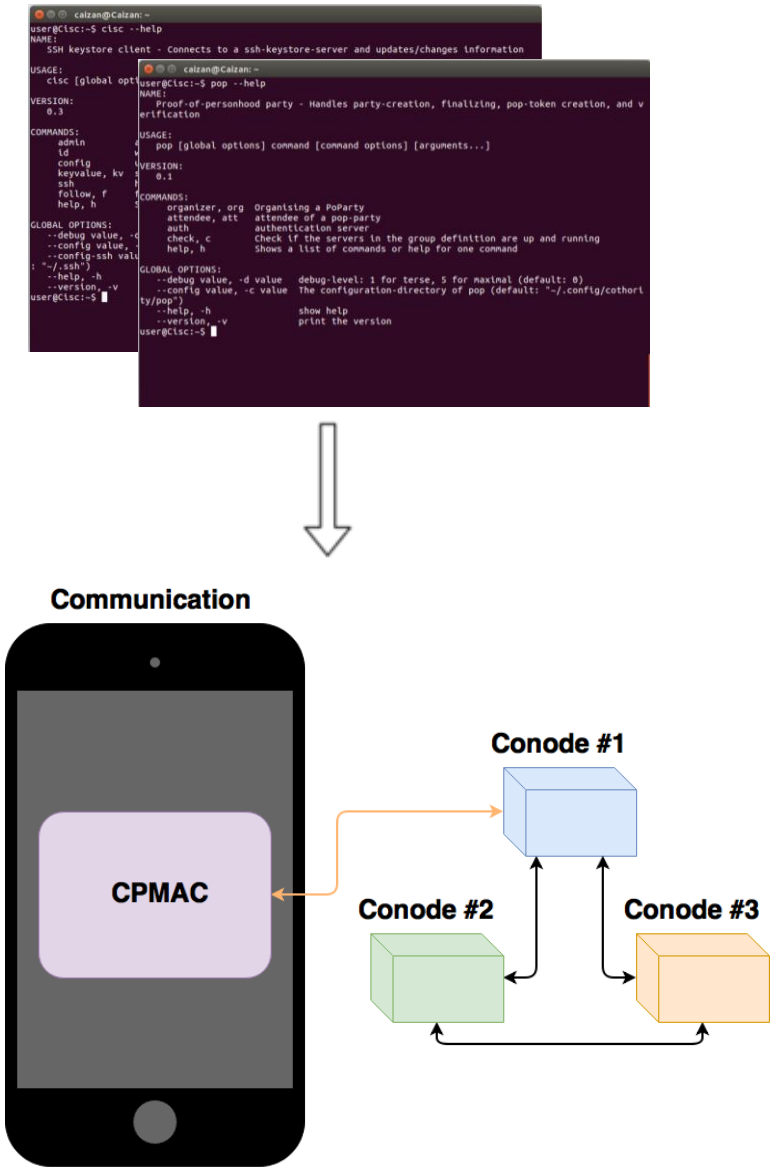
- Anonymous authentication method
- People get tokens
- Use it to authenticate without giving away your identity:
  - We only know that the user is part of a group of person, but not his identity



- Introduction
- Problem Statement
- Solutions and Implementation
- Future Work
- Demo

Problem Statement

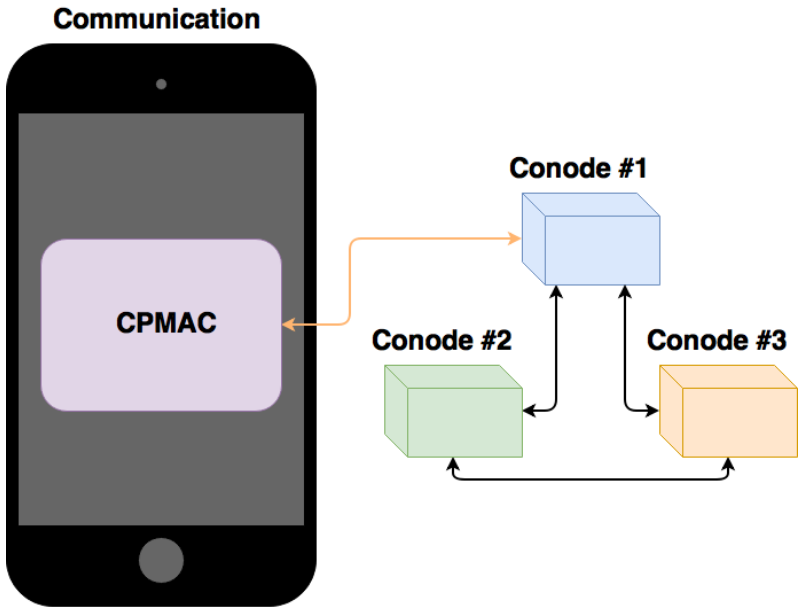
- Current solution
  - User have to use a Command Line Interface (CLI) to access these services
  - Cumbersome
  - Not adapted to the non technical user
- Our project
  - Replace the CLI by a Cross-Platform Mobile Application (CPMAC)



- Introduction
- Problem Statement
- Solutions and Implementation
  - Design choices
  - User friendliness
- Future Work
- Demo

NativeScript

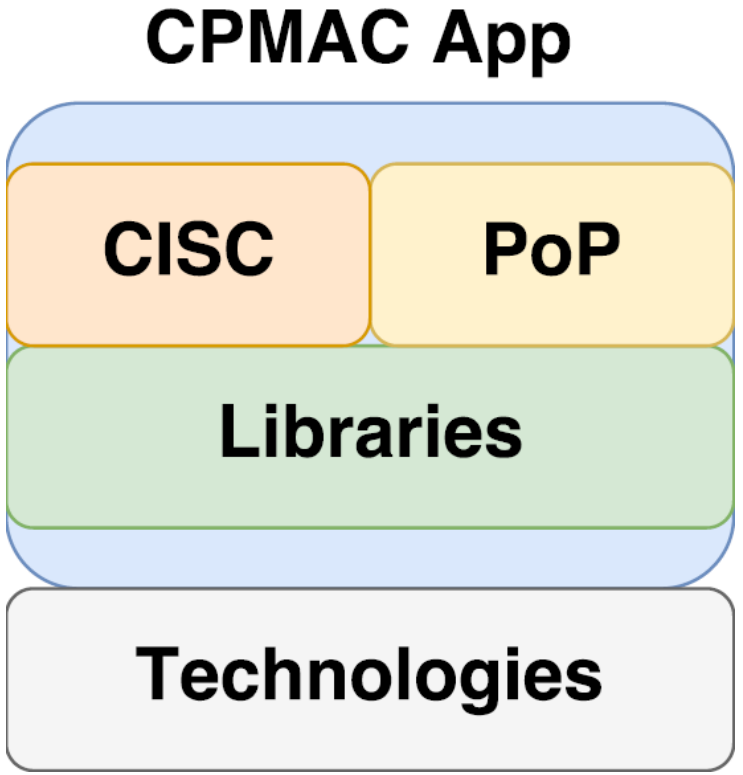
- Real native application
- Using XML => same code for both platforms
- Highly extensible
  - NPM
  - Gradle
  - CocoaPods



Application Design

- Extensible
  - New features
  - New apps

- Could be adapted to browser



User Friendliness

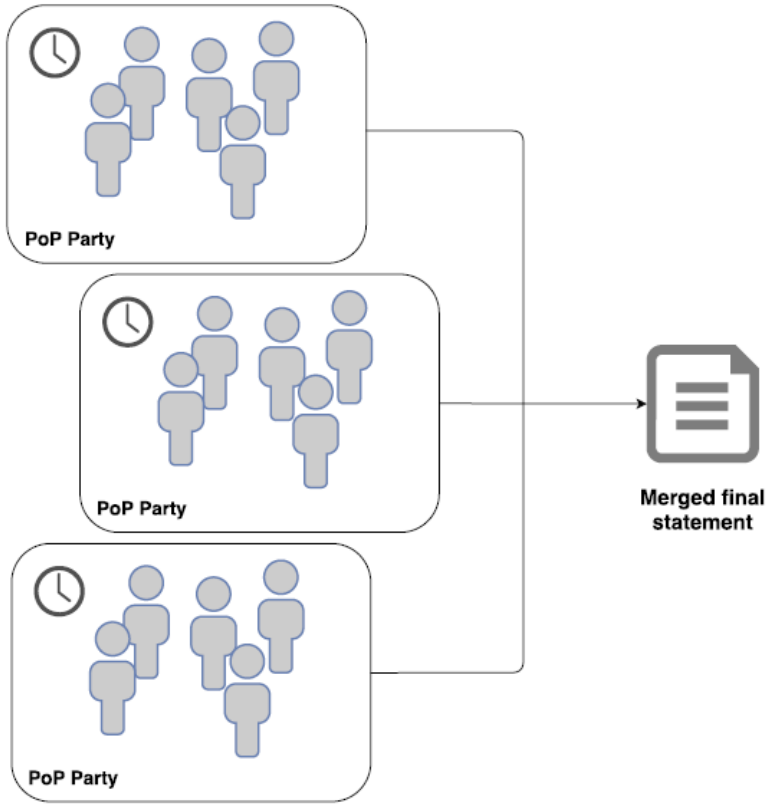
- QR codes:
  - Share configurations
  - Add conodes
  - Register to a PoP party

- Current functionalities
  - User
    - Manage conodes
    - Fetch statuses
  - PoP
    - Create/Manage PoP Party
    - Attend PoP Party
    - Create PoP Token
  - Cisc
    - Connect to an Identity Skipchain
    - Browse the data on the chain
    - Vote for proposed data

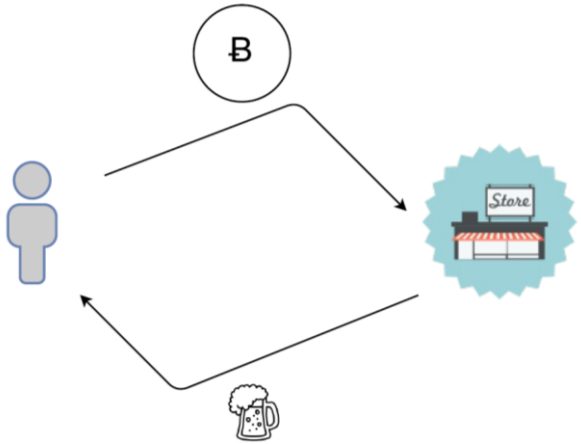
- Introduction
- Problem Statement
- Solutions and Implementation
- Future Work
- Demo

Future Work - PoP

- PoP party merging



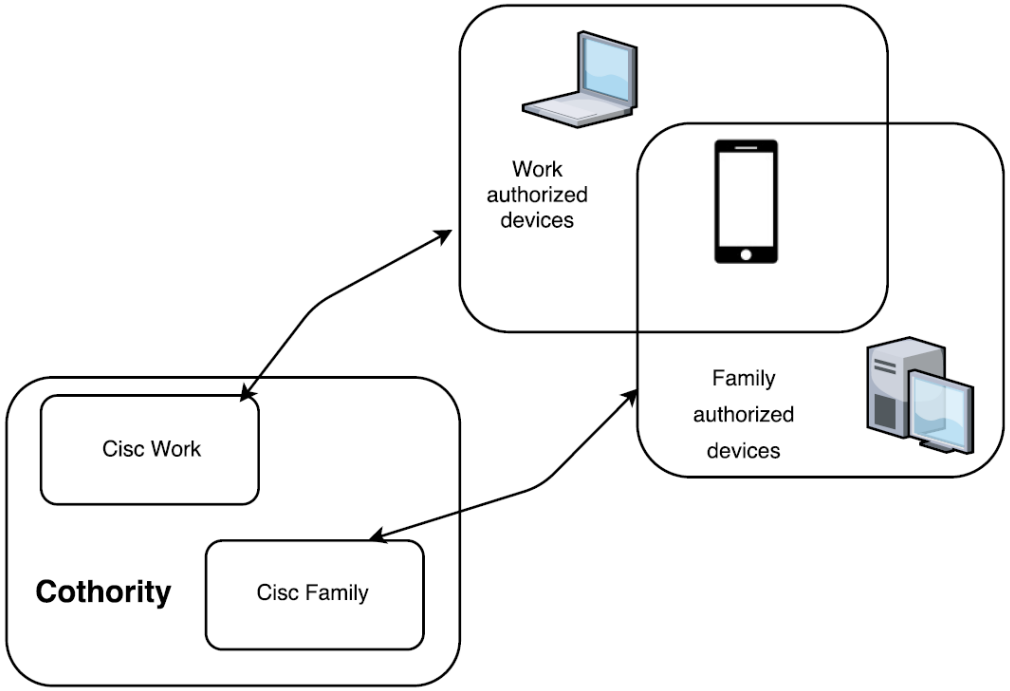
- Sign and Verify Services
  - Ex: BeerCoin



Future Work – Cisc

- Managing multiple Identity SkipChains

- Creating an Identity Skipchain
  - Using Public key Authentication
  - Using a PoP Token



Future Work – General

- Remove the use of PasteBin

- Known bugs
  - Random number generation

- Introduction
- Problem Statement
- Solutions and Implementation
- Future Work
- Demo

Conclusion

- Created a mobile app to replace the current necessity to use the CLI
- Strong focus on extensibility
- Currently supports the basic functionalities for PoP and Cisc