Cross-Platform Mobile Application for the Cothority

Sacha Kozma

June 12, 2018

Decentralized and Distributed Systems lab, EPFL

Responsible Prof. Bryan Ford
Supervisor Linus Gasser

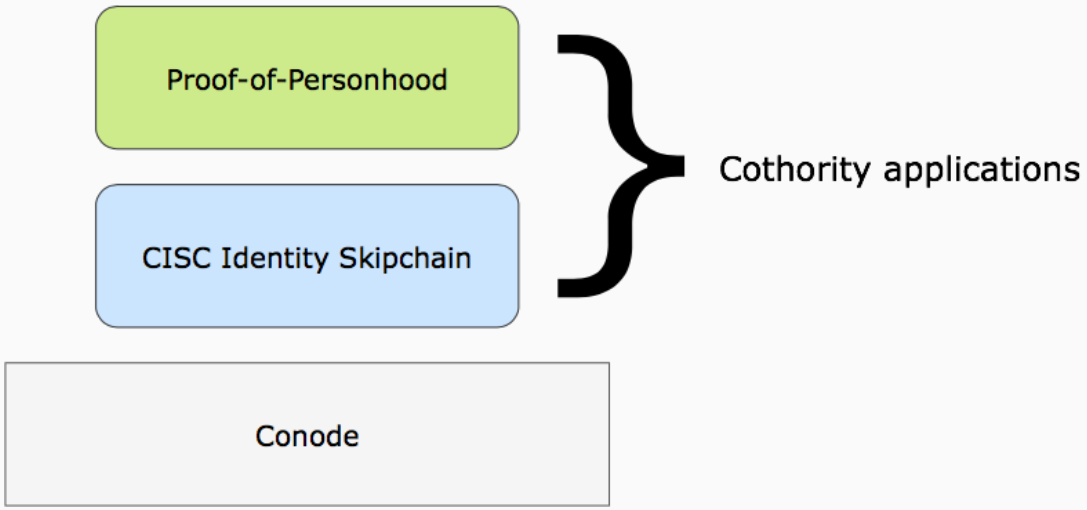
1. CPMAC Presentation
2. Improvements
3. Proof-of-Personhood
    - Presentation
    - PoP in CPMAC
4. Linkable Ring Signatures
5. BeerCoin
    - Presentation
    - Drawback
6. Demo
7. Conclusion

What is CPMAC ?

iOS and Android application used for Cothority.

What is CPMAC ?

iOS and Android application used for Cothority.



What is CPMAC ?

iOS and Android application used for Cothority.

Currently supported applications:

- Status
- Proof-of-Personhood
- Cisc Identity SkipChain

Built on top of NativeScript.

Improvements

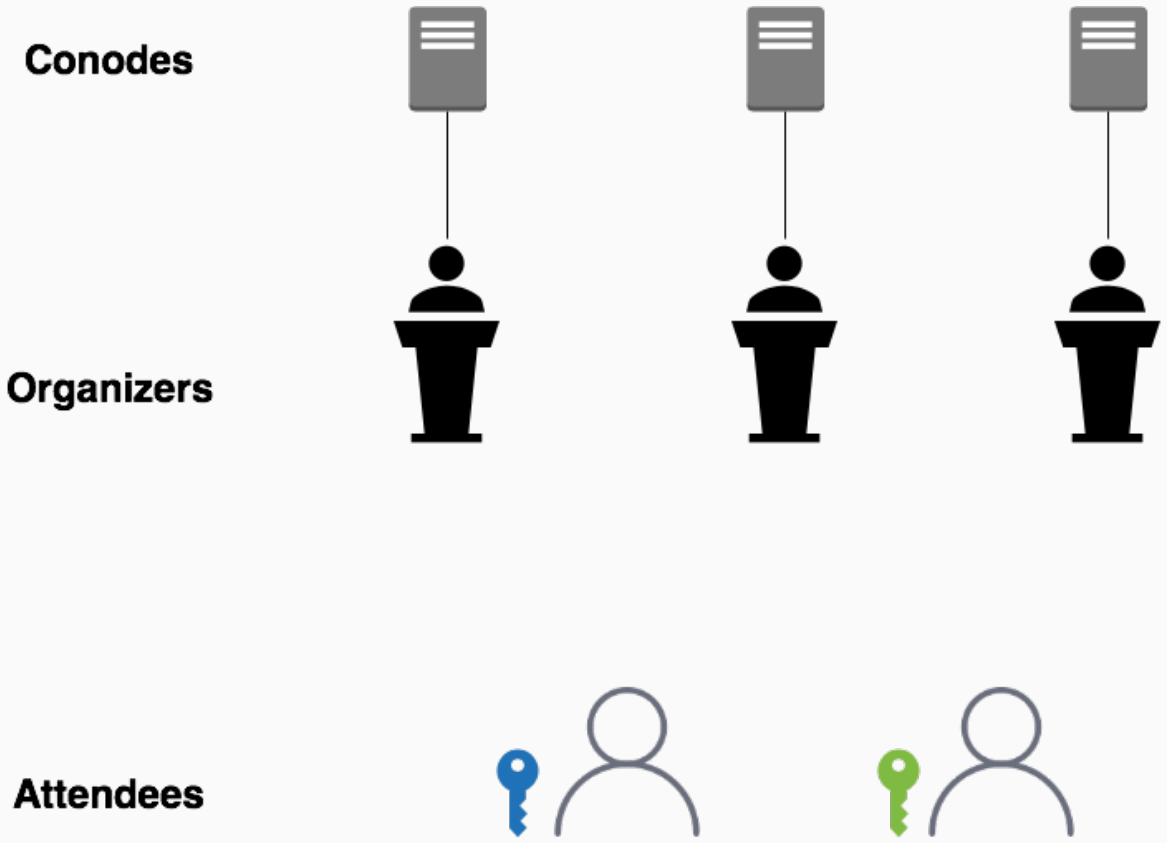
Work has been done on several points :

- PoP-Parties
  - Attendees support
  - Configuration sharing
- Usability
  - User Interface
  - Process simplifications
- New feature : BeerCoin

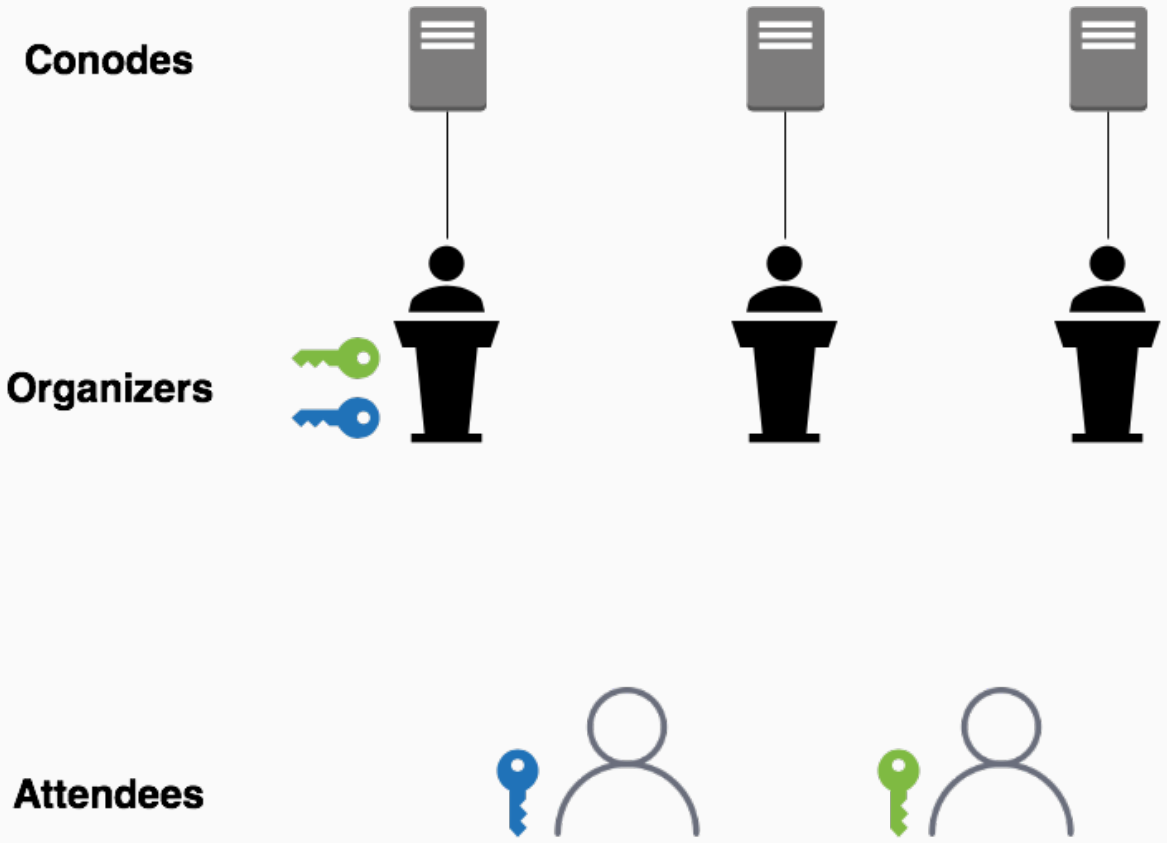
Proof-of-Personhood

Organizers agree on the party details

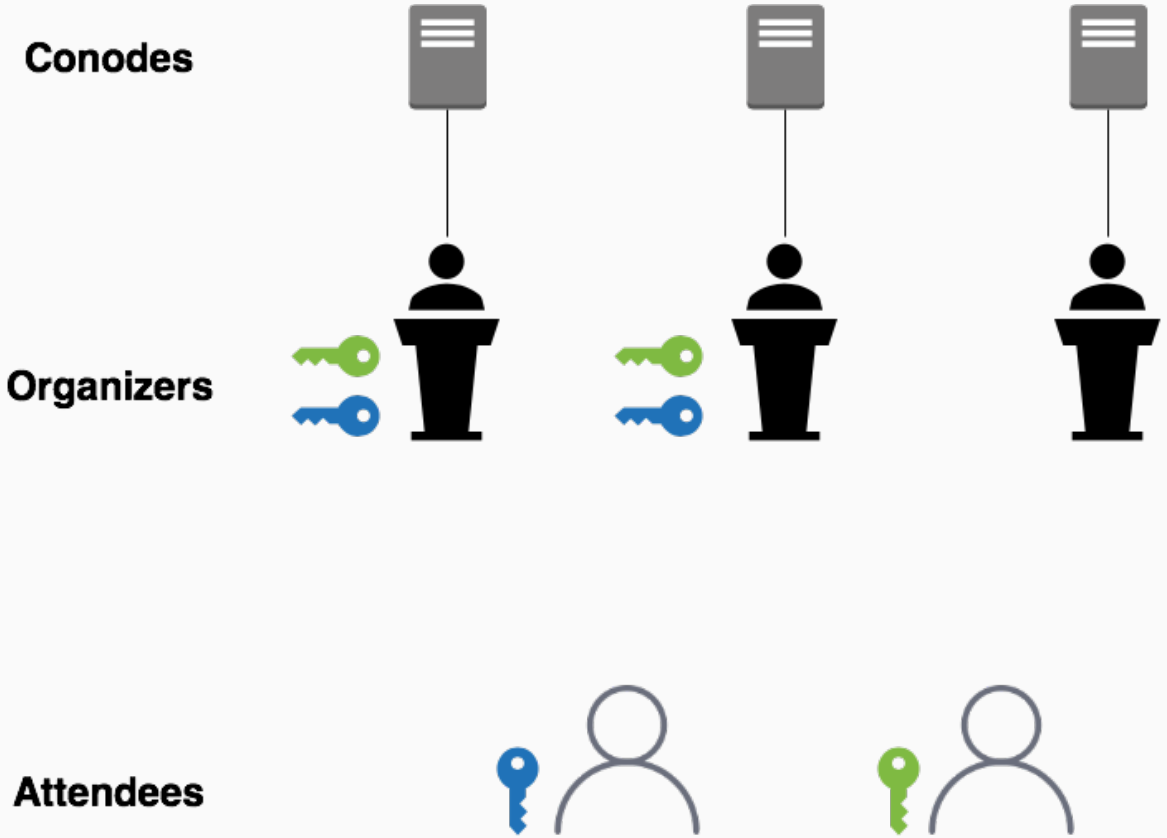
Proof-of-Personhood



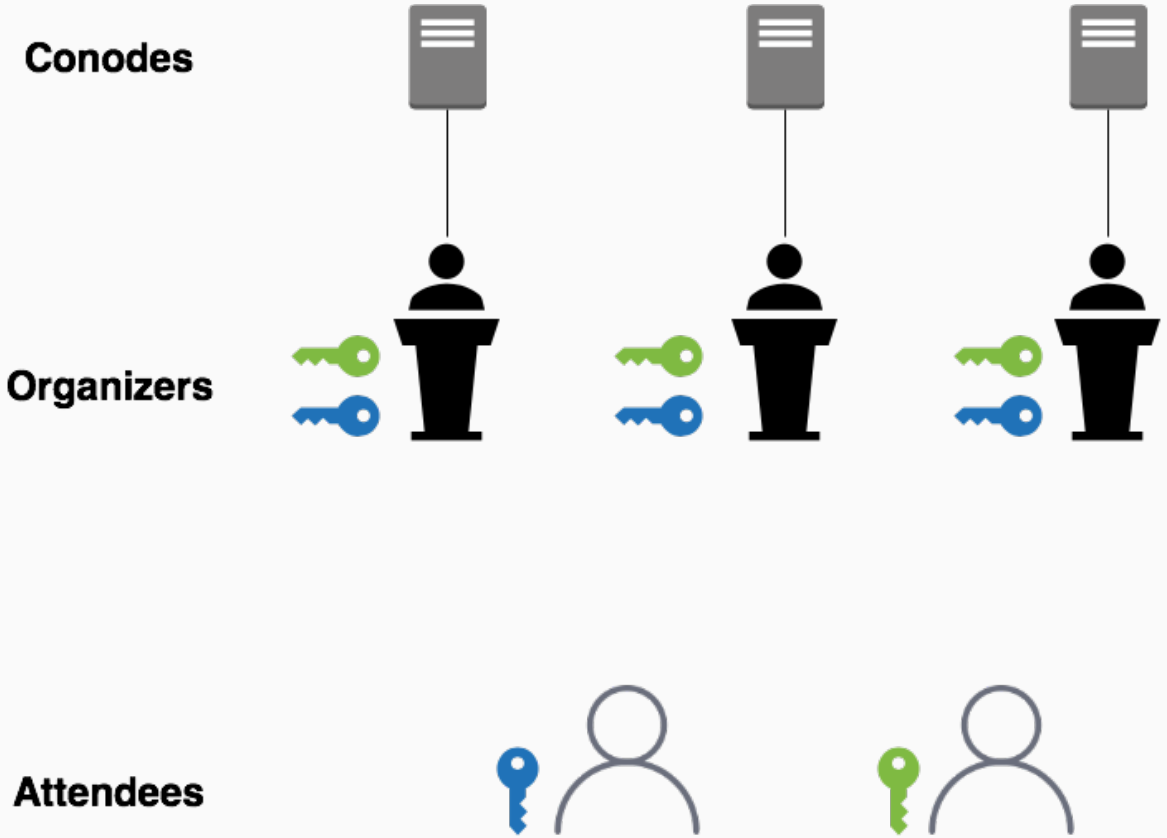
Proof-of-Personhood



Proof-of-Personhood



Proof-of-Personhood



Proof-of-Personhood

At the end of the party, the conodes generate :

 + collective signature = Final statement

And each attendee can generate :

Final statement + attendee's key pair = PoP-Token

Party description sharing

Until now, CPMAC used PasteBin to share the party description to the other organizers.

Party description sharing

Until now, CPMAC used PasteBin to share the party description to the other organizers.

This approch has drawbacks !

- Depends on third-party services
- Party description is publicly available

Party description sharing

Until now, CPMAC used PasteBin to share the party description to the other organizers.

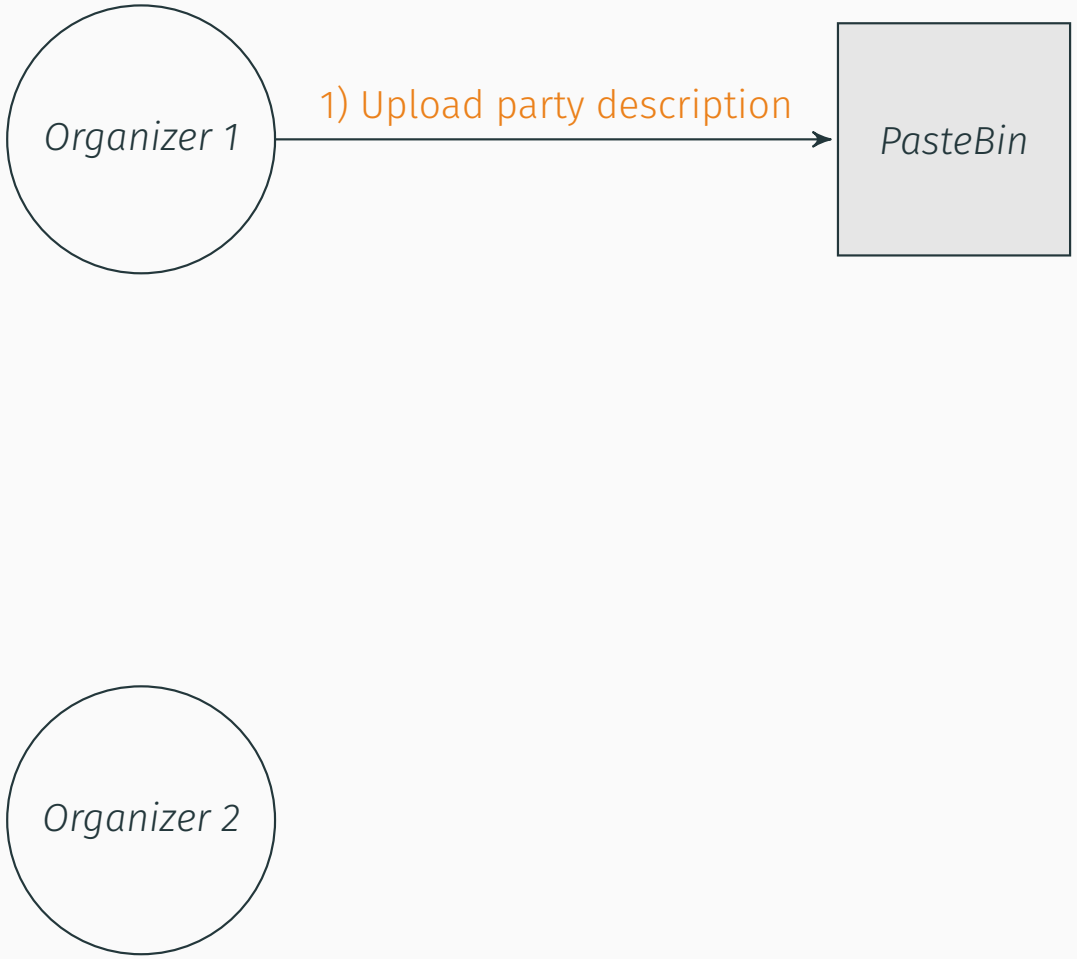
This approch has drawbacks !

- Depends on third-party services
- Party description is publicly available

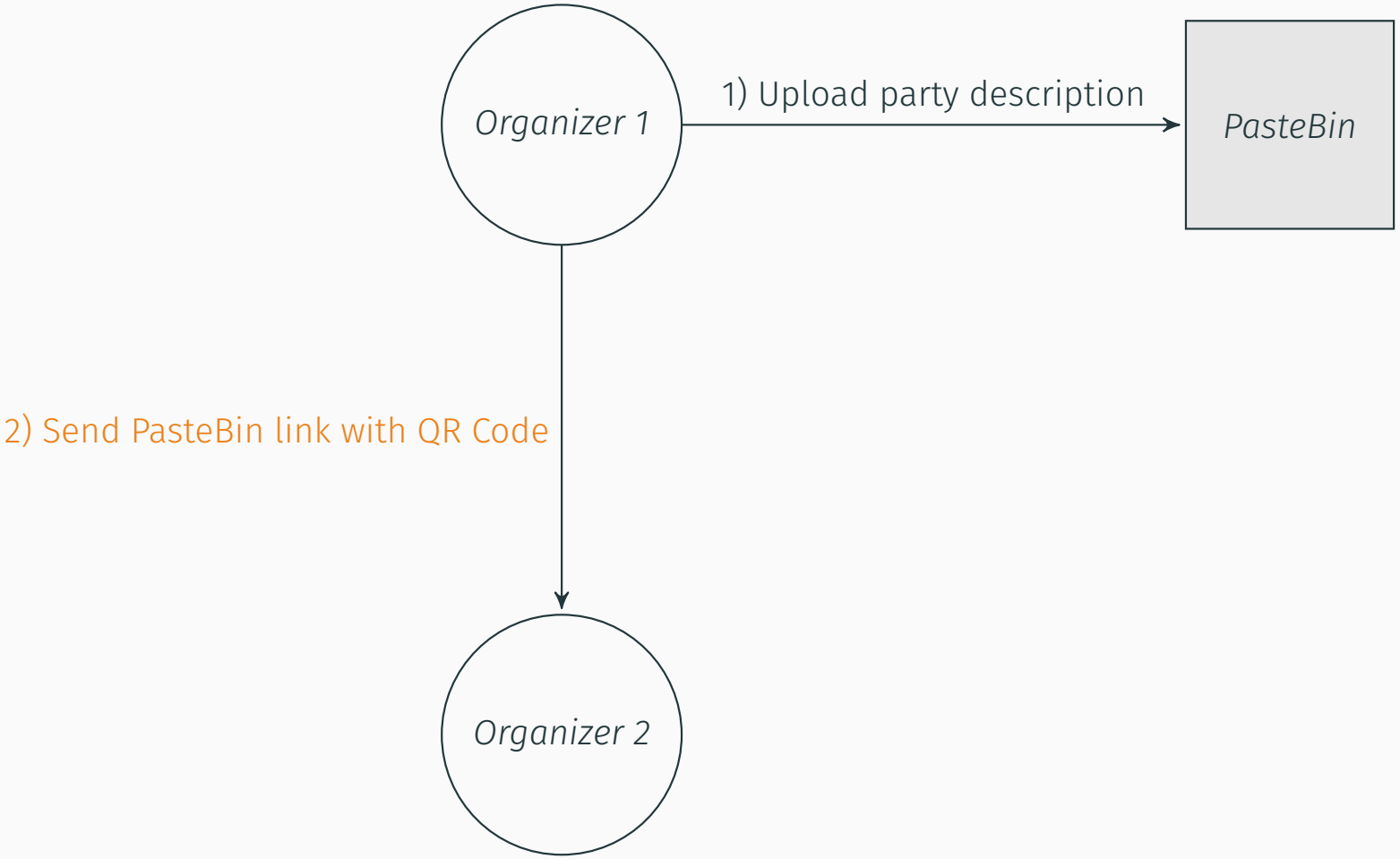
Instead, adapt Cothority to use conodes !

Party description sharing with PasteBin

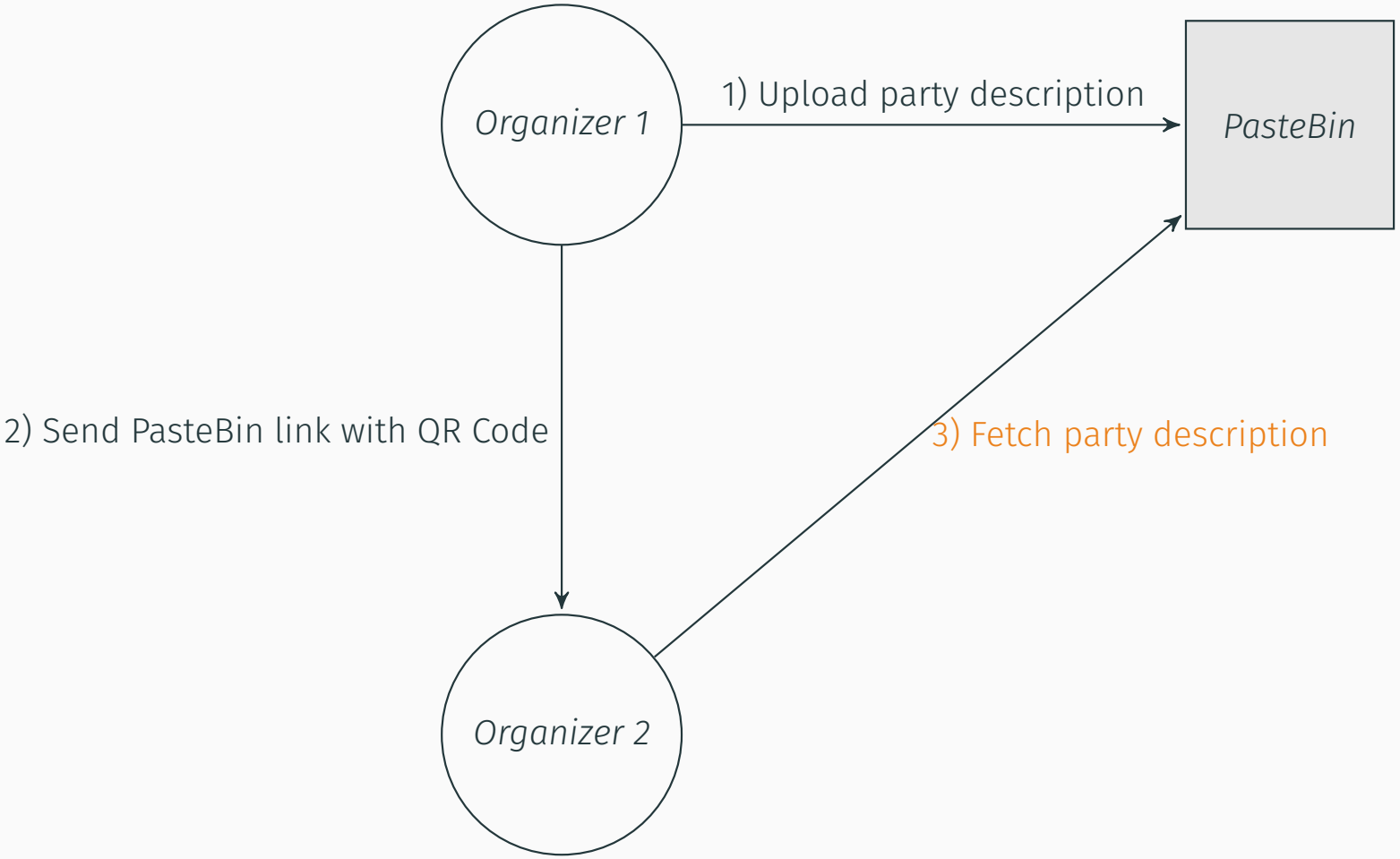
Party description sharing with PasteBin



Party description sharing with PasteBin

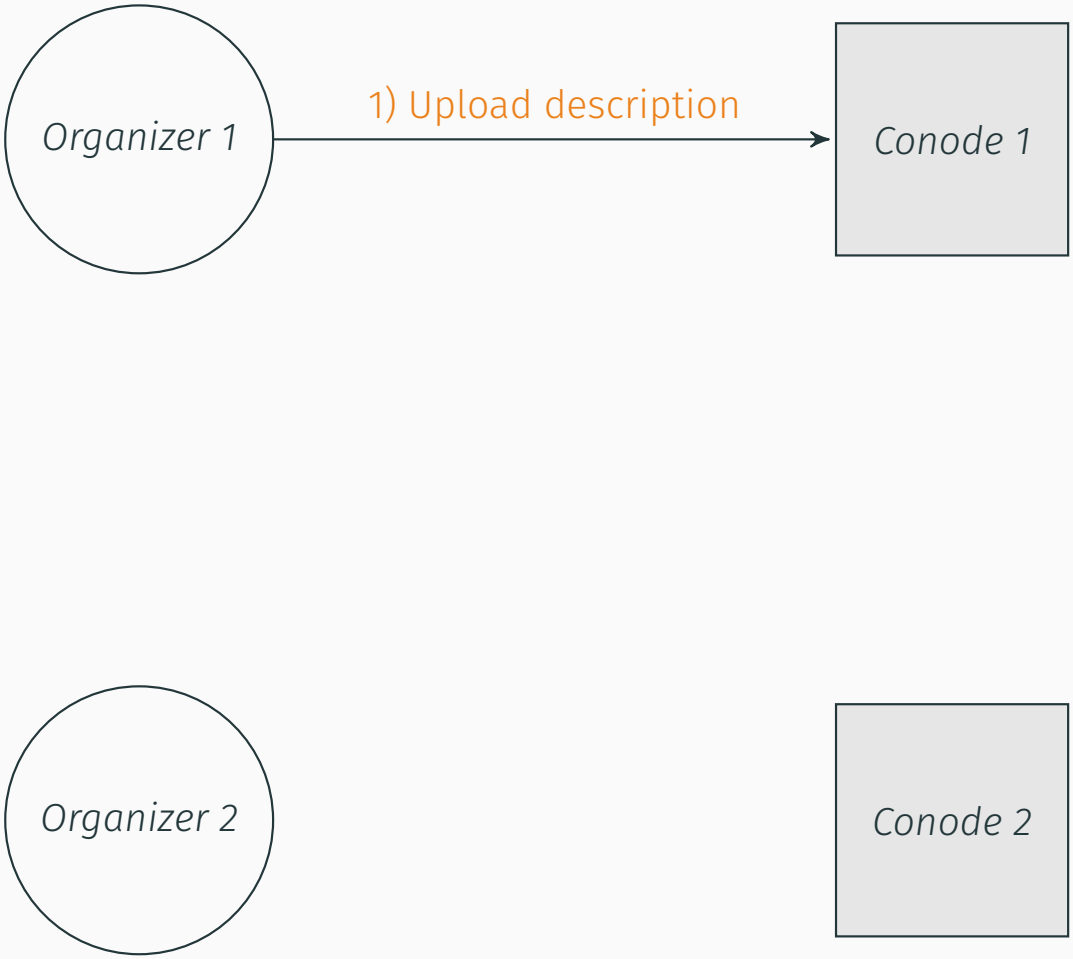


Party description sharing with PasteBin

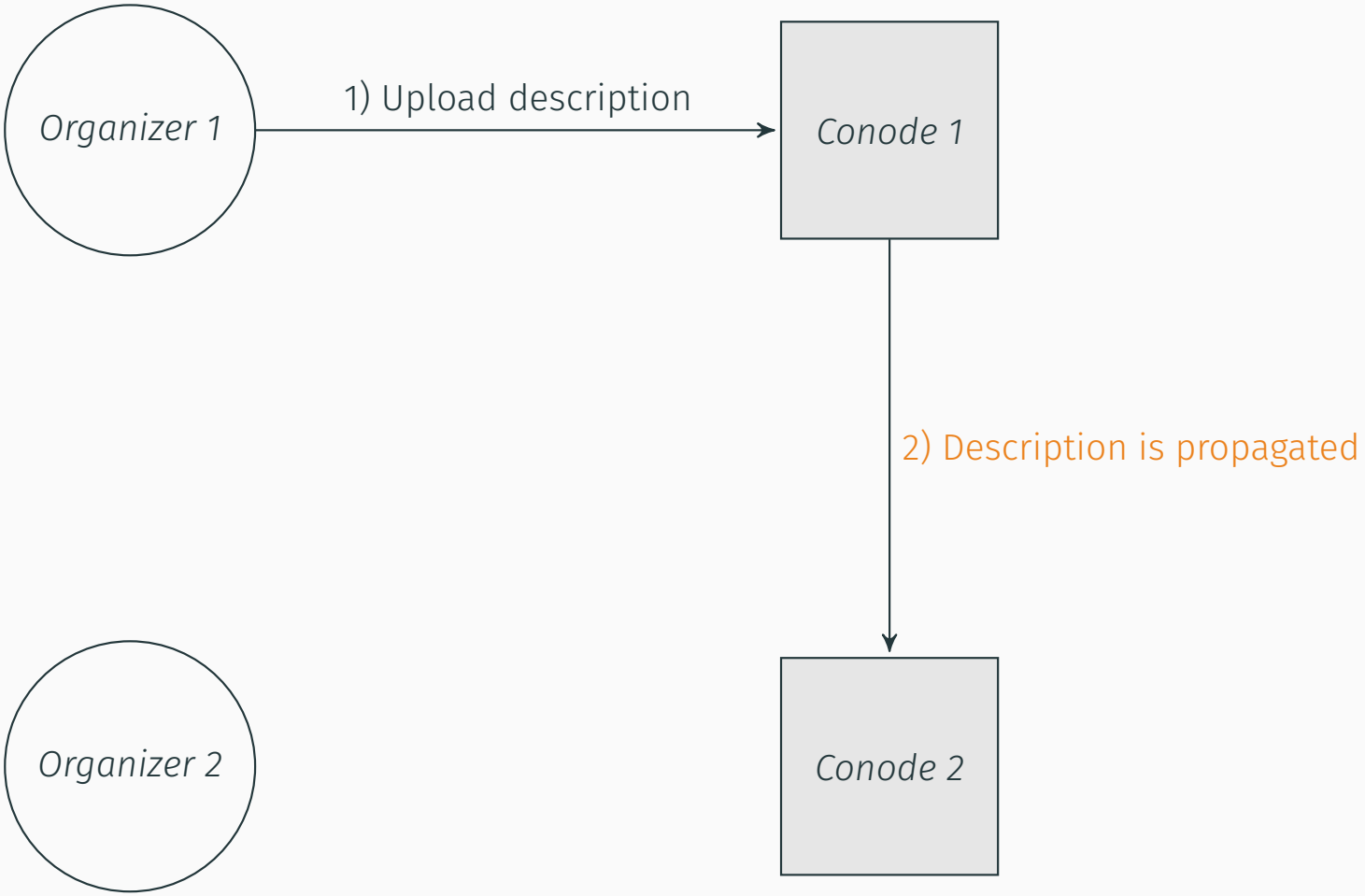


Party description sharing with conodes

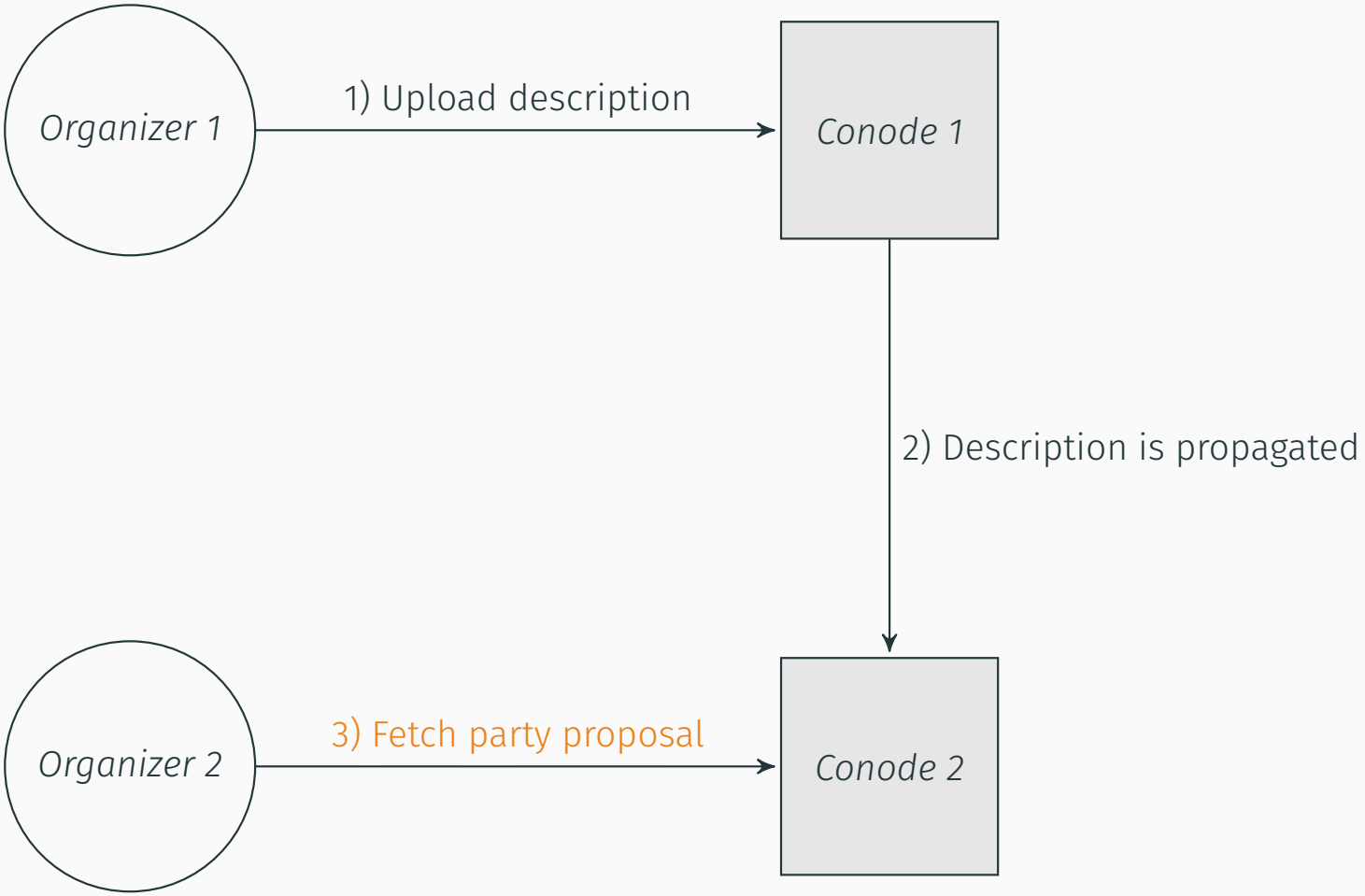
Party description sharing with conodes



Party description sharing with conodes



Party description sharing with conodes



Linkable Ring Signatures

Ring Signatures:

- Allow a user to sign on behalf of a group
- One can verify that someone from this group effectively signed the data
- But he cannot know *which* member precisely

Linkable Ring Signatures

Ring Signatures:

- Allow a user to sign on behalf of a group
- One can verify that someone from this group effectively signed the data
- But he cannot know *which* member precisely

Linkable Ring Signatures:

- Same as ring signatures
- But a linkage scope can be defined, and the verification process will then yield a tag, which is unique to the signer under that scope

BeerCoin

A long-running joke at DEDIS !

BeerCoins are distributed in a group and each day/month/week they can have a beer. In CPMAC, it's called a Bar

It allows showing a simple example of what could be done with the current primitives implemented in CPMAC.

BeerCoin

A long-running joke at DEDIS !

BeerCoins are distributed in a group and each day/month/week they can have a beer. In CPMAC, it's called a Bar

It allows showing a simple example of what could be done with the current primitives implemented in CPMAC.

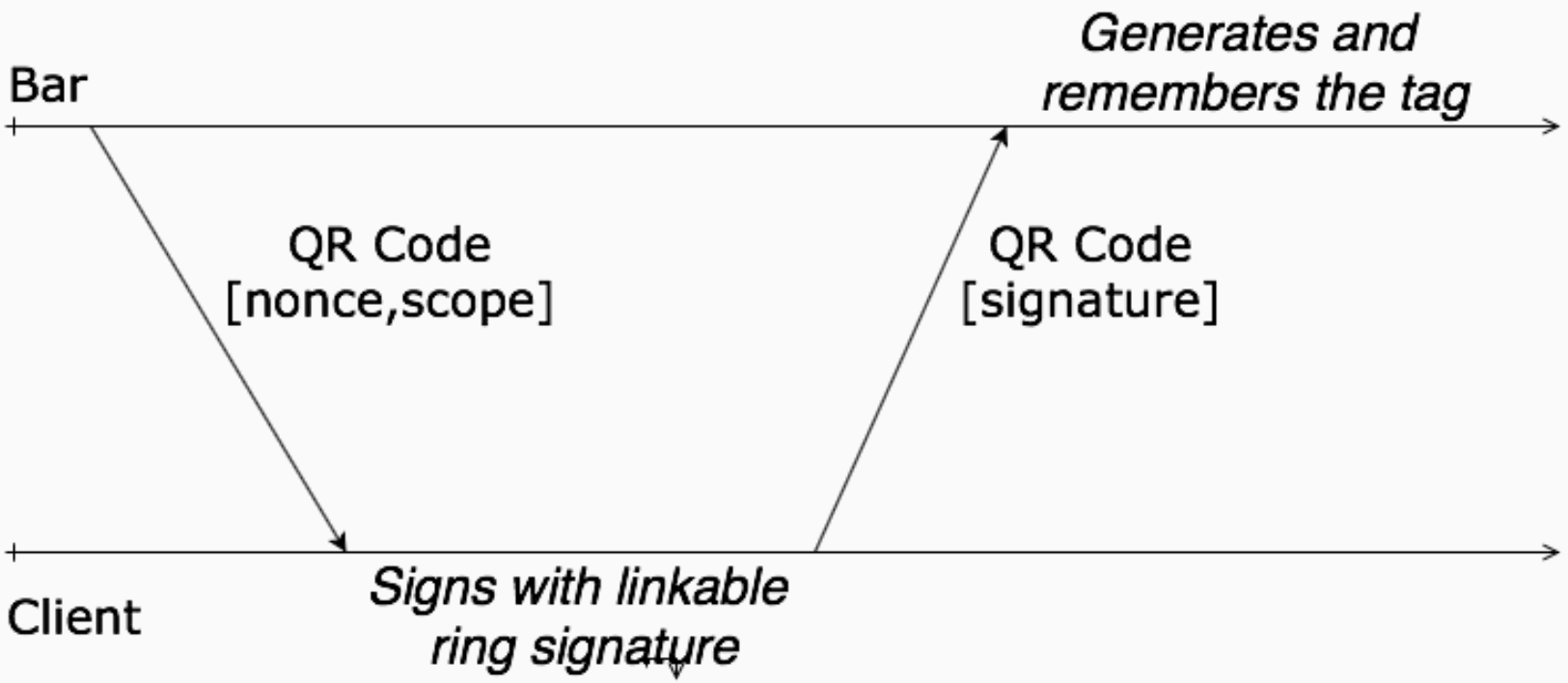
Each member of the group gets a PoP-Token and the Bar uses linkable ring signatures to verify it.

In the case of BeerCoin, the scope should be unique for each Bar **and** each period :

$$scope = bar\_name \| frequency \| year \| month \| day$$

$$frequency \in \{daily, weekly, monthly\}$$

Linkable Ring Signatures: Client verification



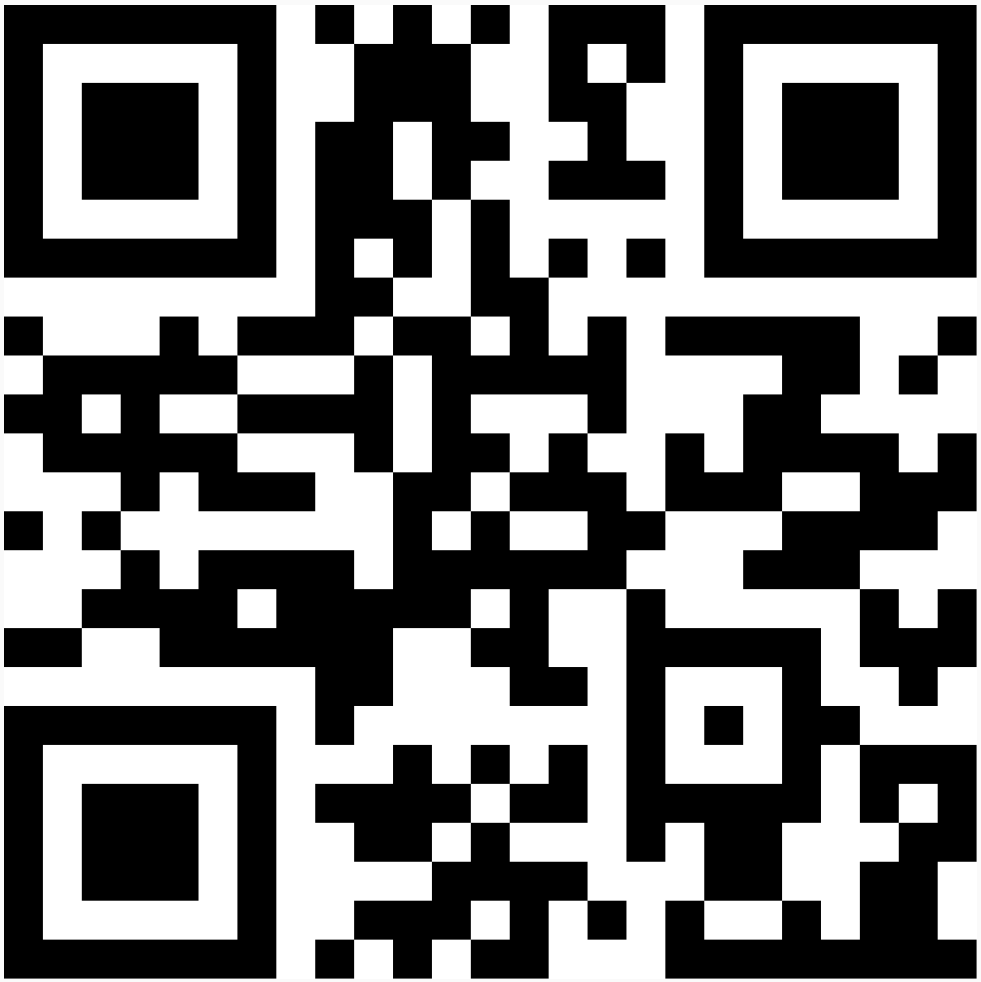
Drawbacks

One major drawback comes from the association of QR Code with linkable ring signatures :

- Length of signatures is proportional to the number of member in the group
- But QR Code has fixed capacity

Actually, CPMAC could handle a maximum of 90 members per group.

Drawbacks



Demo time !

Conclusion

CPMAC is increasingly becoming a large public app.

The primitives currently added allows some interesting applications :

- Voting system
- Online chat
- Authentication
- and many more

Questions ?