



# Anonymous Proof-of-Presence Groups for Messaging and Voting

## PoP Team

*Students: Céline Camacho, Gabriel Fleischer, Sébastien Fulpius, Raoul Gerber, Jean-Baptiste Michel, Romain Pugin, Nicolas Raulin, Ouriel Sebbagh, Alexis Tabin, Maxime Würsch*

*Pr. Bryan Ford, Advisor  
Pierluca Borsò, Advisor  
Louis-Henri Merino, Supervisor  
Haoqian Zhang, Supervisor*



# Outline

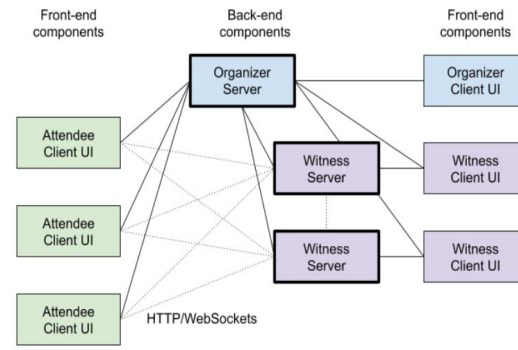
1. Problem



2. Concept

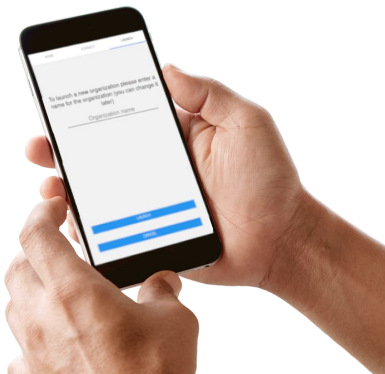


3. Communication



4. Application

5. Demo



6. Conclusion



# Big Picture

Problem

Concept

Communication

Application

Demo

Conclusion

*How to guarantee online accountability while preserving anonymity?*

# Proof of Personhood

Problem

**Concept**

Communication

Application

Demo

Conclusion

- Bind physical to virtual identities
- Verify rather than identify
- One person one vote
- Pseudonym parties

# Proof of Personhood

Problem

## Concept

Communication

Application

Demo

Conclusion

- Bind physical and virtual identities
- Verify rather than identify
- One person one vote
- Pseudonym parties



# The Concept

Problem

**Concept**

Communication

- Applied Proof of Personhood

Application

Demo

Conclusion



# The Application

Problem

**Concept**

Communication

Application

Demo

Conclusion

- Web and Android front-end, Go and Scala back-end
- QR Code
  - Organizer
  - Identity
- Local Autonomous Organization (LAO) creation and modification
- Schedule events (meetings, roll-call, poll, vote)

Problem

Concept

**Communication**

Application

Demo

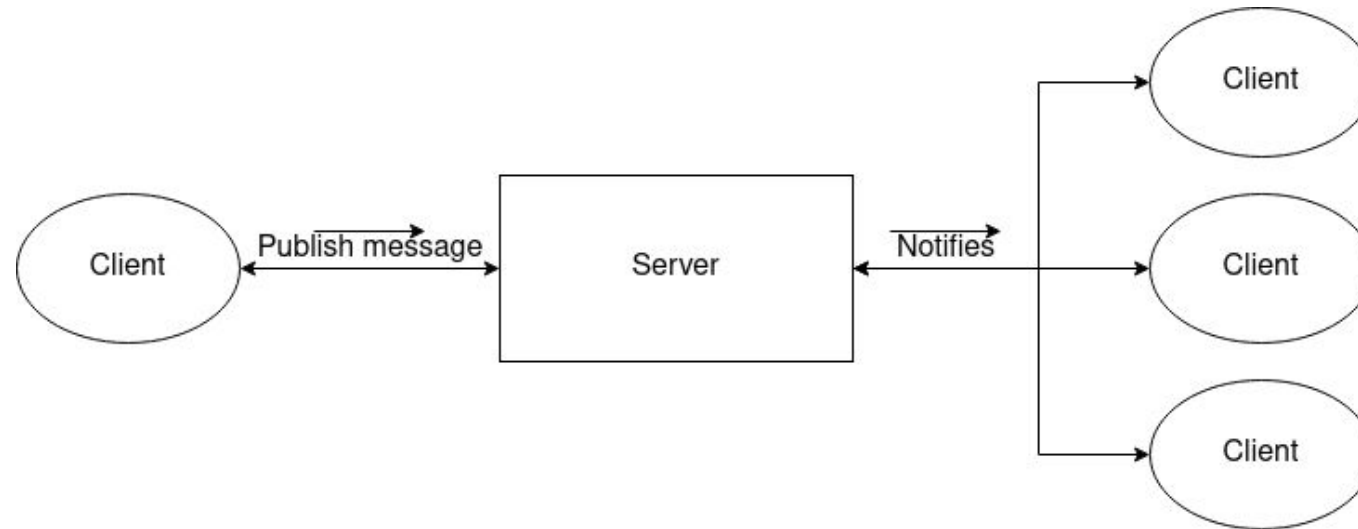
Conclusion

## Publish Subscribe pattern

- Channels, Publishers and Subscribers
- Easily scalable

## Web Sockets

- Persistent, full duplex, connections
- Easy to use





# Communication

Problem

Concept

**Communication**

Application

Demo

Conclusion

```
{
  json_rpc: "2.0",
  id: 0,
  method: "publish",
  params: {
    channel: "/root",
    message: {
      data: base64({ object:"lao", action:"create", id:"YmFp", ...})
      sender: "b3Vp",
      signature: "eWVz",
      message_id: "c2k=",
      witness_signatures: [base64({witness: "amE=", signature:"dGFr"}),
                           base64({...}),
                           base64({...})]
    }
  }
}
```

Messages are signed with an Elliptic Curve Digital Signing Algorithm (EdDSA)

# Trusting the Application

Problem

Concept

Communication

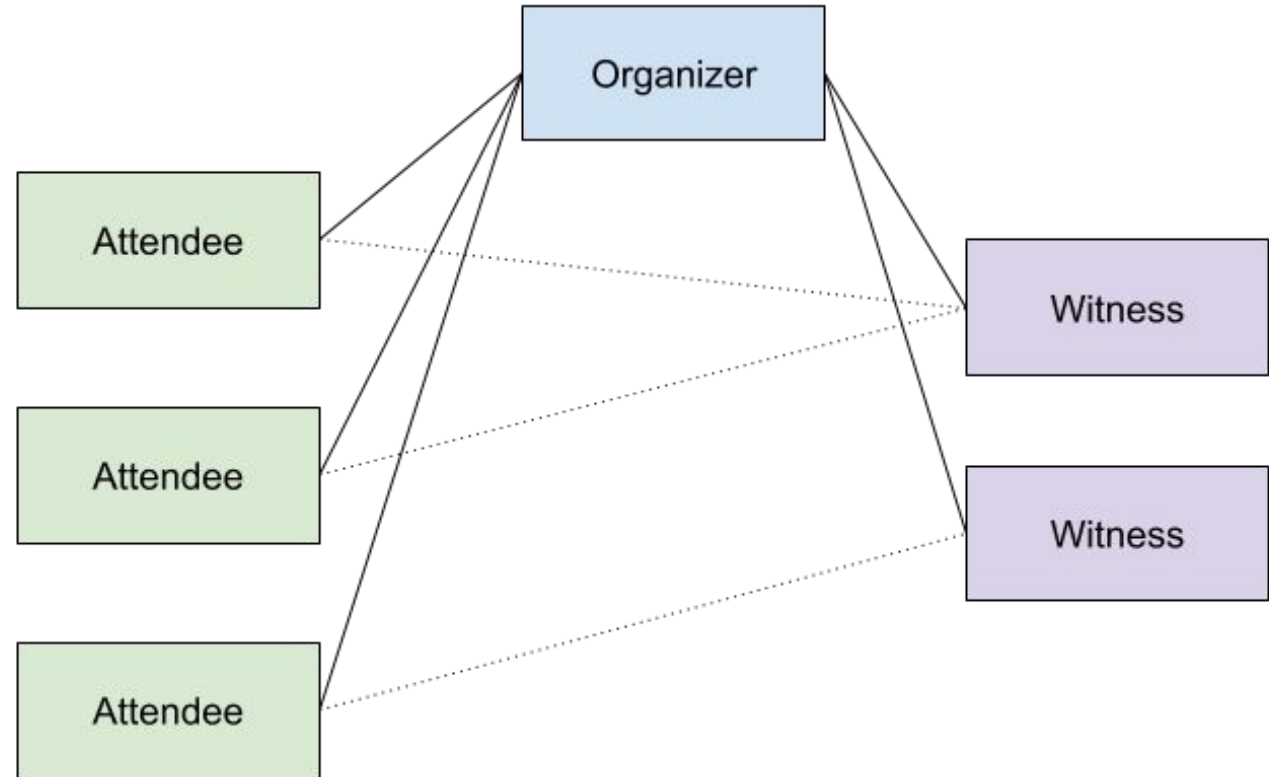
**Application**

Demo

Conclusion

The witness ecosystem:

- Make the system easier to trust
- Human validation on important data and events
- Compensate for an organizer failure or for a dishonest organizer



# State of the Application

Problem

Concept

Communication

**Application**

Demo

Conclusion

## Core features

- Create and update LAO
- Create and close events
- Join a LAO
- Witness signing
- QR code generation & scanning

## Extensions

- Vote event
- Witness routing messages
- Multi-organizer LAO

Problem

Concept

Communication

Application

**Demo**

Conclusion

Anonymous Proof-of-Presence  
Groups for Messaging and Voting

HOME CONNECT LAUNCH

To launch a new organization please enter a name for the organization (you can change it later)

Organization name

---

LAUNCH

CANCEL

HOME ATTENDEE MY IDENTITY LAO 1

Past

Events 1  
Start at 10-12-2020 17:08:3  
End at 10-12-2020 17:41:30  
A location, test.com

Events 2  
Start at 10-12-2020 17:08:3  
End at 10-12-2020 17:41:30  
A location, test.com

Events 3  
Start at 10-12-2020 17:08:3  
End at 10-12-2020 17:41:30  
A location, test.com

Status: Open  
Participants #  
QR code

Events 5	
Question 1	4
Discussion 1	1
Question 2	

If discussion open

Your question SEND

Events 6  
Status (Future, Open or Closed)  
Participants: N of M

- param1
- param2
- param3
- param4

# Conclusion

Problem

Concept

Communication

Application

Demo

**Conclusion**

- Core functionalities implemented
  - User Interfaces for front-end
  - Organizer back-end
- Base for future work
  - Interaction with back-end
  - Witness back-end server



# Q & A

Problem

Concept

Communication

Application

Demo

**Conclusion**

