PoP-Party #8 - 180814

DEDIS, EPFL

The Sybil Identity Problem

Internet has no protection from malicious users cheaply creating a few (or many) fake accounts

- Online ballot stuffing, fake upvotes/reviews
- Sock puppetry, bot armies pushing fake news
- Whack-a-mole: “banned” trolls just resurface

Fundamental unsolved decentralization problem

- John Douceur, “The Sybil Attack” [IPTPS ‘01]”
- Bitcoin PoW is another disastrous failed attempt

Mapping the Known Solution Space

Major approaches proposed so far:

- “Real names” based on verified identities
- Biometric collection in central database
- Proof-of-Investment: CAPTCHA, PoW, PoS, …
- Graph analysis on trust networks
- Pseudonym parties

“Real names” and verified identities

Trusted third-party verifies government-issued ID

- Blue checkmarks, banking KYC checks, ...

Downsides:

- Privacy-invasive, excludes poor/undocumented
- Cumbersome, expensive verification process
- Fake IDs relatively easy, cheap to acquire
- Vulnerable to 1 compromised/coerced verifier

Biometric collection & verification

Collect fingerprints, iris, etc., record in database

- Appeals: efficiency, automation, security(?)
- Large-scale trials by India, United Nations

Downsides:

- Even more privacy-invasive, surveillance risks
- False positives & negatives create big problems
- One hacked scanner could still register many fake “people” with unique biometric fingerprints

Proof-of-Investment

Rate-limit Sybil attacks via artificial barrier-to-entry

- CAPTCHAs: waste time proving you're human
- PoWork: prove you wasted compute energy
- PoStake: prove you have money to invest

Downsides:

- Undemocratic: not "one-person-one-vote"
- More money, more voice: "rich get richer"

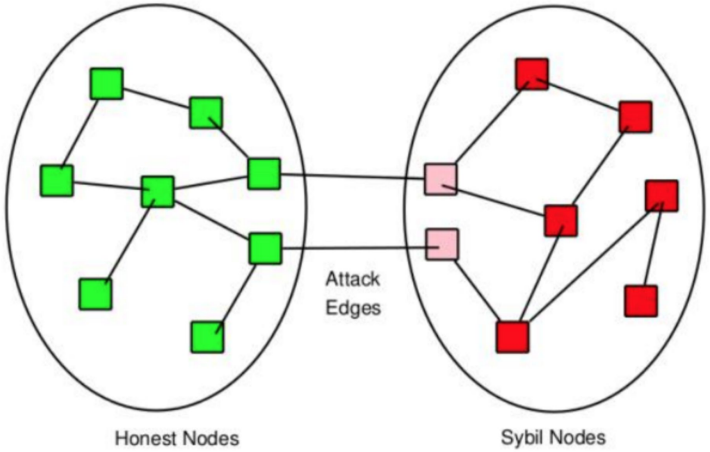
Graph analysis on trust networks

Classic P2P idea in SybilLimit, SumUp, etc.

Assumes nodes are cheap but edges are expensive to a Sybil attacker.

Downsides:

- Secure & usable “trust networks” don’t exist
  - Facebook/LinkedIn/etc: many friend promiscuously
- Only weak defense against massive cheating
  - Easy for many people, or everyone, to cheat a little



Pseudonym Parties

Build anonymous one-per-person tokens

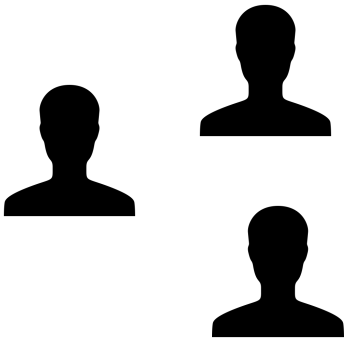
- Physical security: real person has one body, can be in only one place at a time
- Synchronized events similar to, but simpler than, in-person voter registration or PGP key signing
- No ID checking, no biometrics, no trust network

Downsides:

- Requires some organization in the physical world
- Those who want one must show up, periodically

Pseudonym-party - Configuration

Organizers



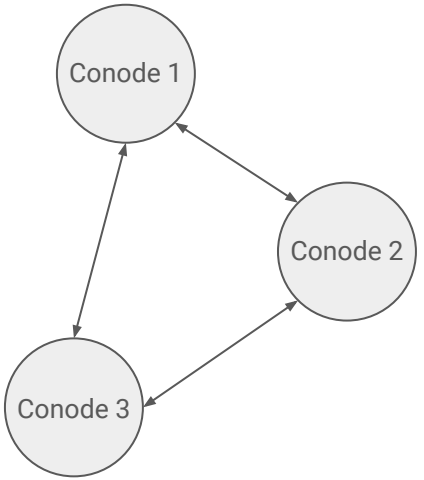
Each organizer sends the

configuration to HIS conode

The conodes collectively

sign the configuration

Cothority



Configuration File

https://applivery.com/popcoin

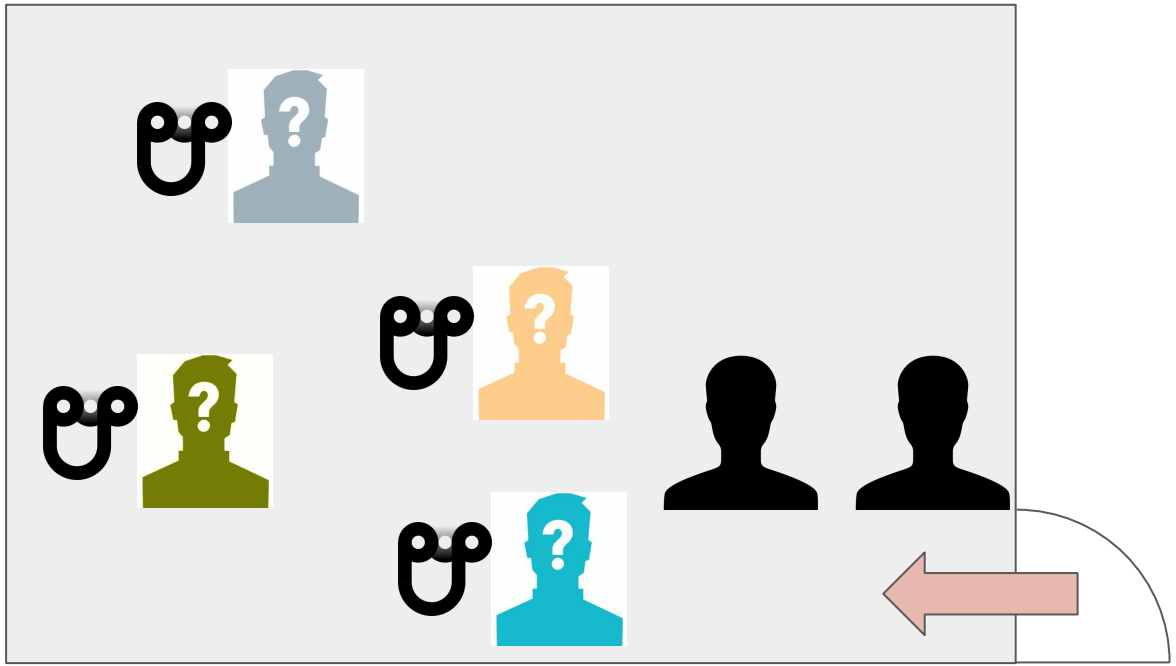
Pop-party #8
14th of August 2018
BC129

```
{
    "id":
"256130ed9fc25612baf1d126902
c91b208bb511dbaa4ba94369f13e
fba5e4f72",
    "address":
"tls://Gasser.blue:7770"
}
```

Start of Party

Be sure to:

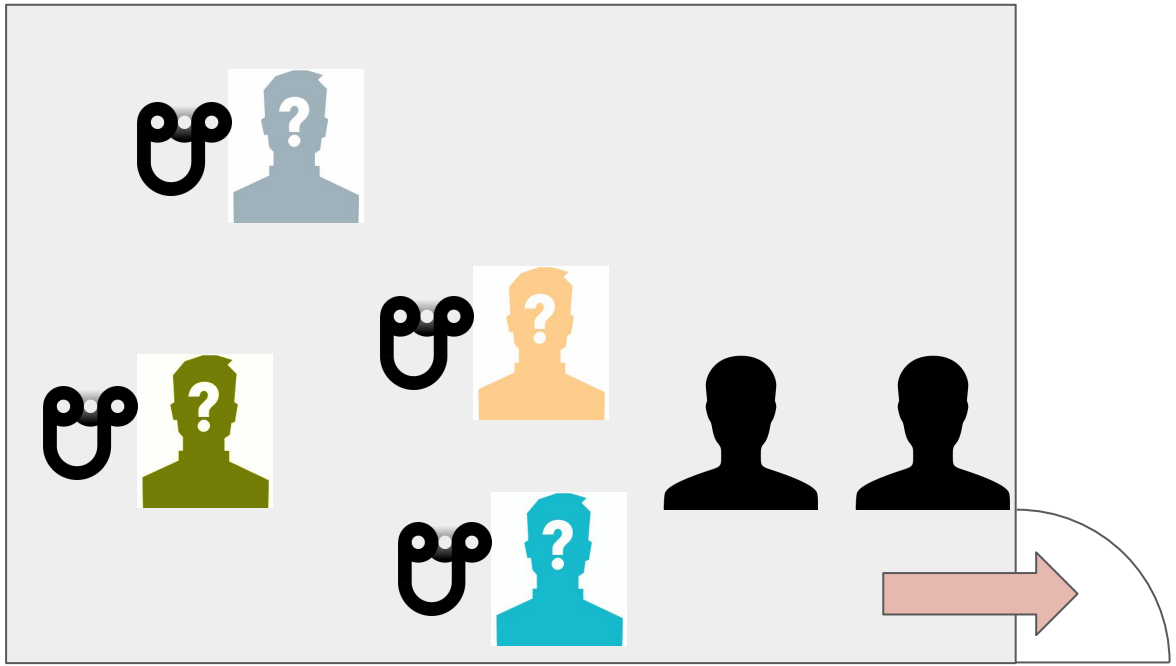
- Installed the latest version from https://applivery.com/popcoin
- Scanned the QRCode from an organizer



Barrier Point - Exit

You’re allowed to exit the party.

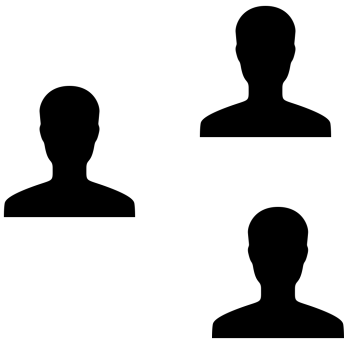
Be sure to have your public key scanned by all the organizers!



Pseudonym-party - Finalization

Organizers

Cothority

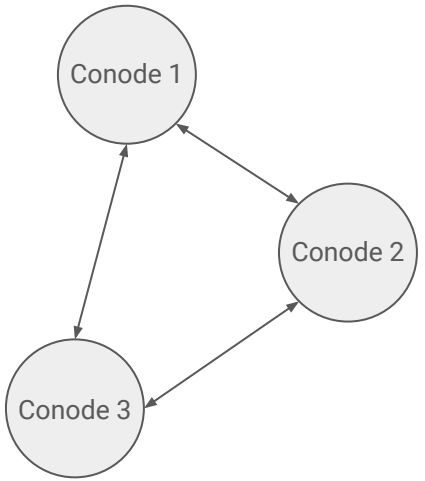


Each organizer sends his

scanned keys to his conode

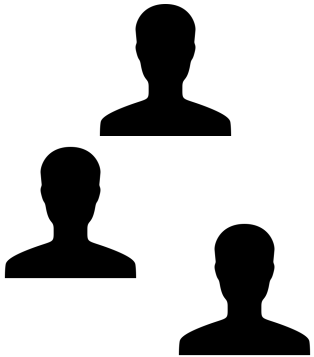
The conodes verify and

collectively sign the keys

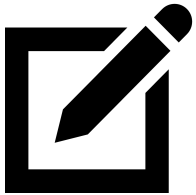


Pseudonym-party - Party Transcript

Organizers



Configuration



+

Public keys

+

Collective Signature

=

Party Transcript

Pseudonym-party - Tokenization

Each Attendee

Party transcript

Keypair

PoP-token

Usage of PoP-tokens

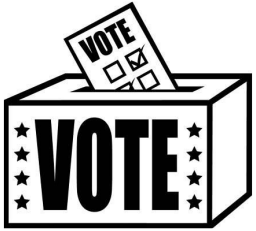
Attendee

Request

Message + Context

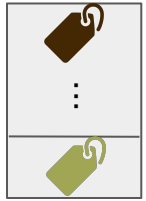
Signature + Tag

Services



Each service trusts the Party Transcript

Each service holds a list of tags:



Log

- Date: 14th of August 2018, 2pm - Place: BC129 in EPFL, Lausanne, CH
- Present: Linus Gasser, Joseph Attieh, Jeff Allen, Shaohua Li, Fred, Kelong, Lefteris, Philipp, Nicolas, Sacha
- Organizers: Linus, Jeff, and Kelong
- Observer: Linus' videocam and Rosie
- Nodes: conode.dedis.ch:7770, dedis.nella.org:6879, conode.gasser.blue:7770
- Chocolate for everybody!

Next steps

- Attendee’s feedback when being scanned by organizer - OK to go through server
  - What about using PriFi to hide who has which public key?
- Having organizer functionality in iOS version
- Coins
  - Get coins from a token to get a certain amount of coins and being able to exchange coins

Renaming / Branding

- PoP-tokens -> PoP (w/o token)
- PoP-party ->
- PoP-coin ->

Locality

Before accepting the transcript, add a test that the organizers and attendees are in the same spot.

Start the video with a view on a GPS device and the latest news of a big newspaper.

-> to ensure we can trust that other synchronous parties are legitimate.

Location-based games, like ingress.