Proof-of-Personhood

How to resist Sibyl attacks

DEDIS, EPFL
Linus Gasser, Philipp Jovanovic, Eleftherios Kokoris,
Frederic Pont, Bryan Ford

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"

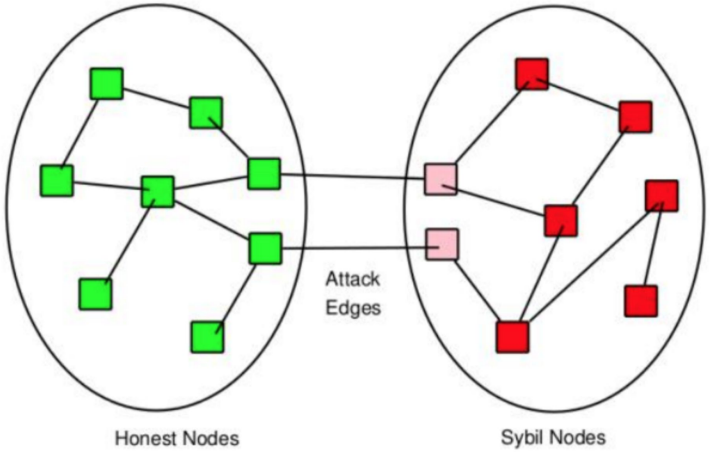
Graph analysis on trust networks

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

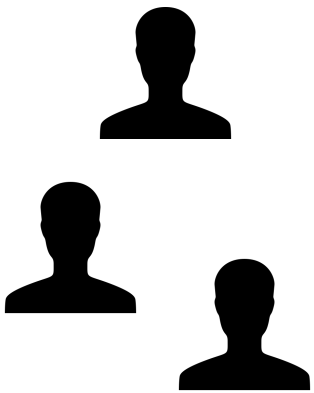
Proof of Personhood

Objective:
Number of tokens per person = 1

How: Organizing a party in which people are verified, but not identified

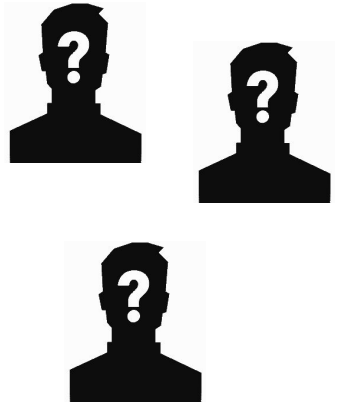
Pseudonym-party - Setup

Organizers
Anytrust



Configuration
Name, Purpose, Place, Time

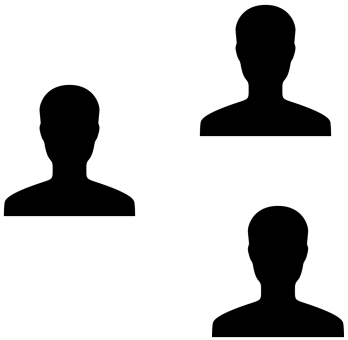
Attendees
Anonymity-group



Room

Step 1: Pseudonym-party - Configuration

Organizers



Each organizer signs

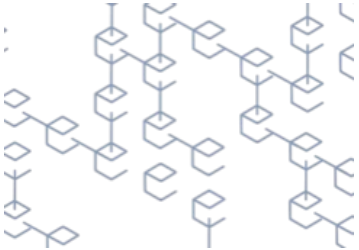
the configuration

Collective Signature

Configuration and

Signature stored on

Blockchain



Step 2: Attendee Configuration

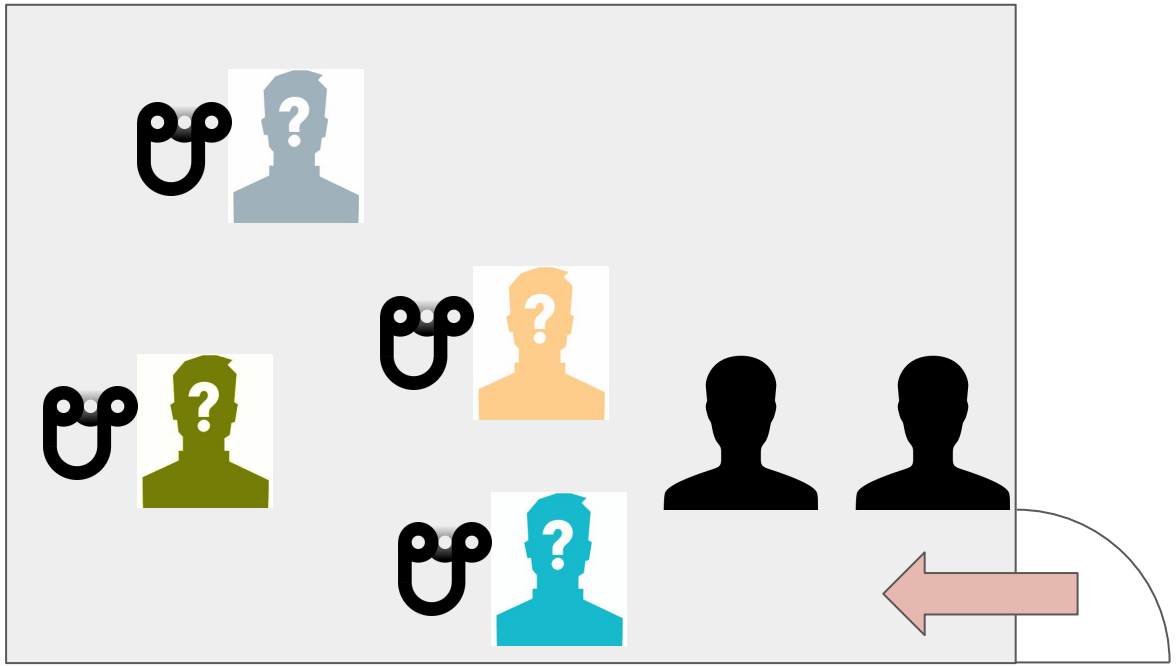
https://applivery.com/popcoin

Pop-party #11
4th of September 2018
BC410

Step 3: Start of Party

Be sure to:

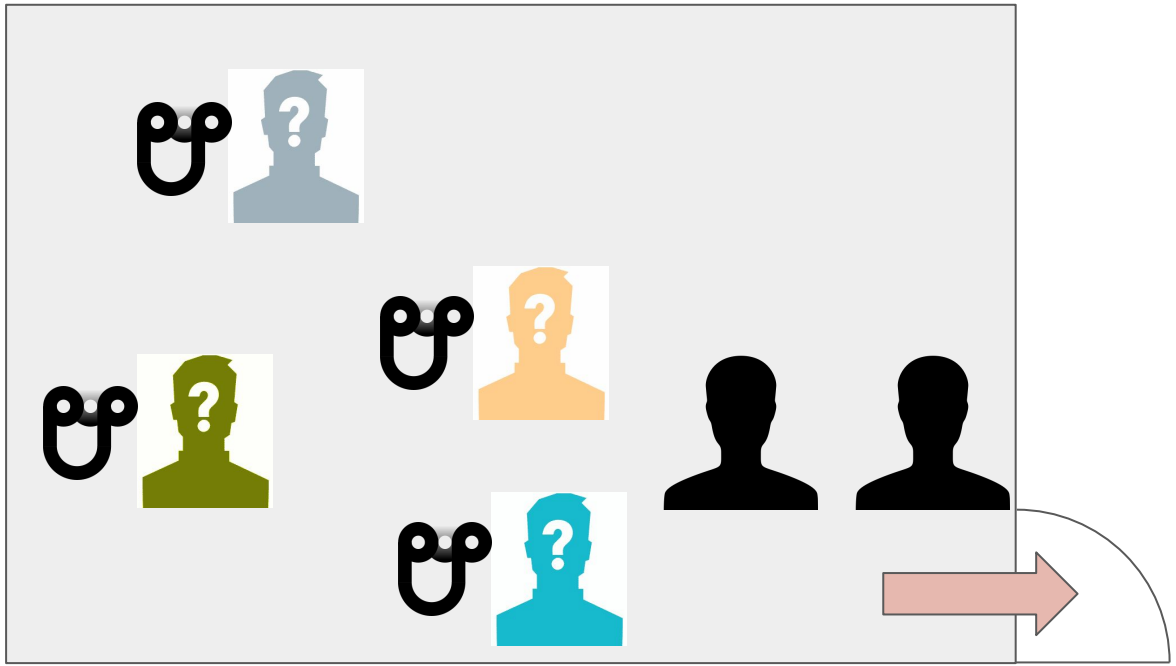
- Install the latest version from https://applivery.com/popcoin
- Scan the QRCode of the party



Step 4: Barrier Point - Exit and Scan

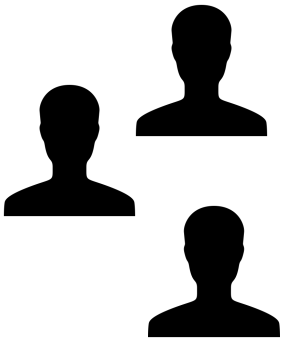
You’re allowed to exit the party.

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



Step 5a: Creation of Party Transcript

Organizers



Organizers reach consensus

Collective Signature

+

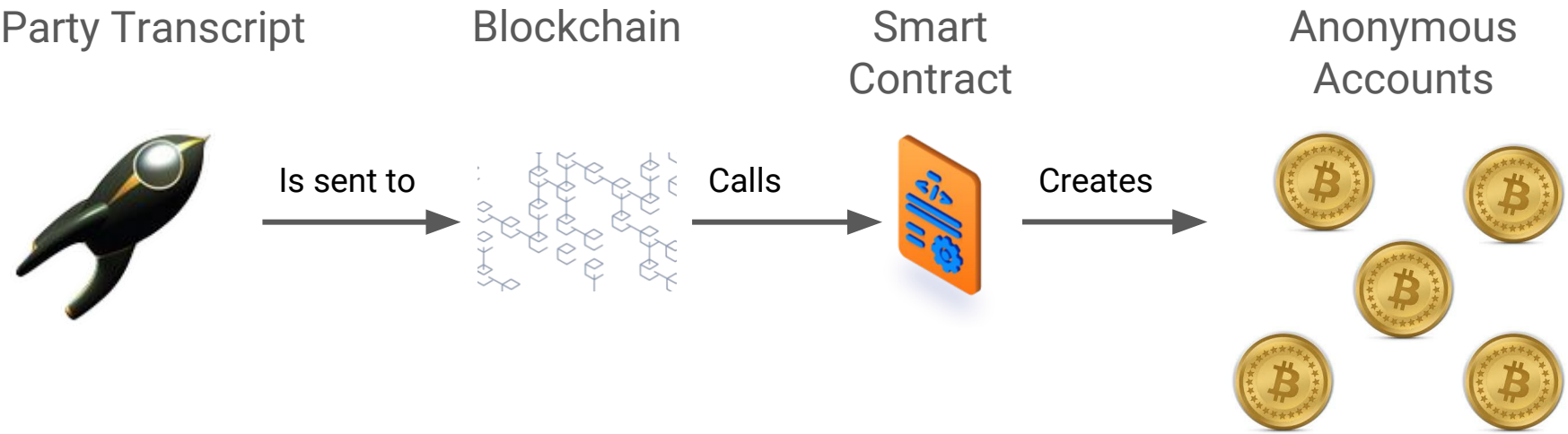
Configuration

Public Keys

=

Party Transcript

Step 5b: Storage of Party Transcript



Step 5c: Tokenization of Attendee’s Keypair

Keypair

Party transcript

PoP-token

Usage of PoP-Coins and PoP-Tokens

Attendee

Transfers

Coins

Economic

Other Attendees

Services

Social

Sybil-resistant Twitter

Spam-protected Communication

Signs

Anonymously

Democratic

Voting

Deliberation

Details of Anonymous Signatures

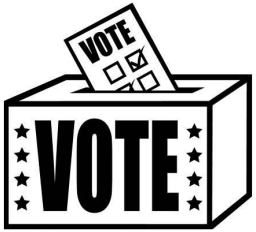
Attendee

Request

Message + Context

Signature + Tag

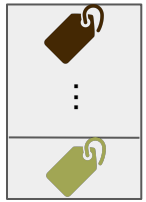
Services



WIKIPEDIA
The Free Encyclopedia

Each service trusts the Party Transcript

Each service holds a list of tags:



Log

- Date: 4th of September 2018, 1:30pm - Place: BC410 in EPFL, Lausanne, CH
- Organizers: Linus, Kelong, and Sacha
- Total Attendees (including organizers):
- Observer:
- Nodes: conode.dedis.ch:7770, conode.dedis.ch:7772, conode.gasser.blue:7770
- Chocolate/fruits for everybody!

Next steps

- Don’t lose tokens!
- Have a minimal mock-up of the following functionality:
  - Creating and answering Questionnaires
  - PoP-twitter where sending costs money and reading gets you money
  - Get coins from a token to get a certain amount of coins and being able to exchange coins
- Having organizer functionality in iOS version