Proof-of-Personhood: Redemocratizing Permissionless Cryptocurrencies

**Maria Borge**, Eleftherios Kokoris-Kogias, Philipp Jovanovic, Linus Gasser, Nicolas Gailly and Bryan Ford

EPFL
Talk overview

● Problem
● Proof of personhood (PoP)
● PoPCoin
● Conclusions
Problem

Control in current permissionless blockchain-based cryptocurrencies systems lies in hands of a small number of entities

Re-centralization
Permissionless cryptocurrencies

- Enable open participation
- Provide pseudonymity
- Avoid double spending attacks
- Extend the blockchain in a secure manner
Proof-of-Work

- Special purpose hardware
- Massive consumption of electricity
- Only entities with the resources are able to mine
- Re-centralization!
Proof-of-Stake

- Participants use *their* assets to create new assets
- Rich participants have an advantage, more assets implies faster creation of new assets
- Shareholder corporation that favors the rich
Goal

Create a **sybil attack resistant** cryptocurrency that ensures **fair** and **accessible** wealth creation process
Talk overview

- Problem
- Proof of personhood (PoP)
- PoPCoin
- Conclusions
Proof-of-Personhood (PoP)

**Objective:** Verify people, rather than identify them

**How:** Organizing a party and generate tokens
Proof-of-Personhood (PoP)

**CoSi** - Scalable collective signing

**Cothority** - Collective Authority

**Linkable ring signatures** - Anonymity and accountability in the same context
Pseudonym party - Setup

Configuration-file:
- Start, End
- Location, Use
- Expiration
- Organizers’ public keys
Pseudonym party - Setup

Configuration-file:
- Start, End
- Location, Use
- Expiration
- Organizers’ public keys
Pseudonym party

Registration-room

Party-room
Pseudonym party - Barrier Point
Pseudonym party

Registration-room

Party-room
Pseudonym party - Termination / Finalization

Party Transcript:
- Configuration file
- Public keys of attendees
- Hash-file of videos
- Collective signature

Private key + Signed transcript = PoP-Token
Usage of PoP-Tokens

Attendee

Attendees public keys

Linkable Ring Signature

Context, M

Service

Aggregate public key of trustworthy cothorities

Attendees public keys

Table with tags
Talk overview

- Problem
- Proof of personhood (PoP)
- PoPCoin
- Conclusions
PoPCoin

- **Open membership**: Proof-of-Personhood
- **Fairness**: Randhound
- **Consensus**: Byzcoin
Set of organizers throw a pseudonym party to create PoP-tokens

Attendees authenticate their PoP-tokens

If successfully authenticated attendee deposits a public key, to identify as a minter

The set of public keys form a minting-pool
PoPCoin - Implementation - Minting

1. Minters part of the minting-pool are eligible to create new blocks

2. Last N miners run RandHound, to select the next minter allowed to create next block

3. The process repeats every M minutes, if minter fails a new one is selected
PoPCoin - Overview
PoPCoin - Deployment

Local cryptocurrency
Challenges

We propose a cryptocurrency that builds on:

- Proof-of-Personhood
- Randhound
- Byzcoin
Related Work

We propose a cryptocurrency that builds on:

- Proof-of-Personhood
- Randhound
- Byzcoin
Thank you!
Questions?