



ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

DEDIS laboratory

Proof of Personhood tokens on the Ethereum blockchain

Bachelor project
Hugo Roussel

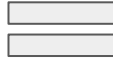
Responsible Bryan Ford
Supervisor Linus Gasser 1

What are Proof of Personhood (pop) tokens?

“Accountable anonymous credentials”

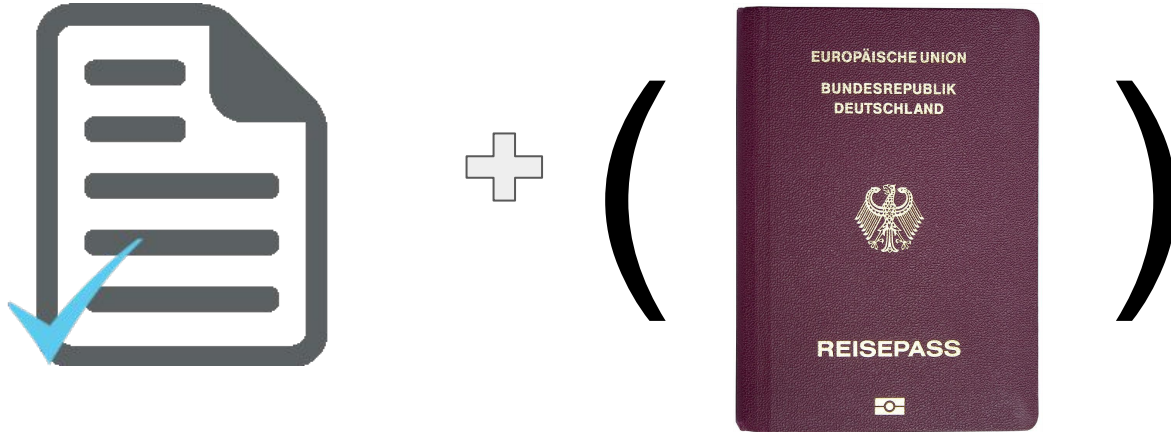
What are PoP tokens?

“Accountable anonymous credentials”

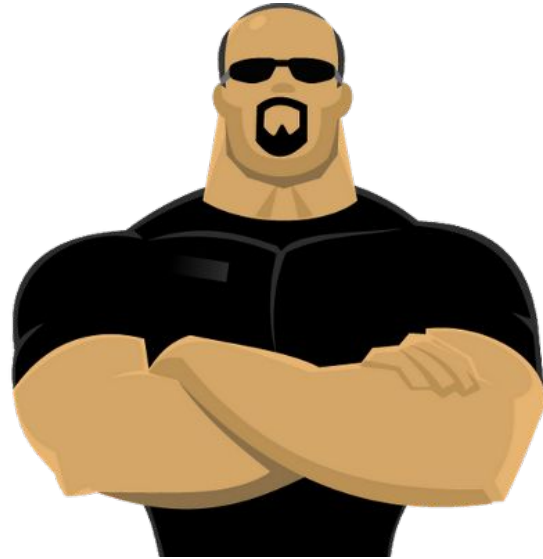


A turnstile

Accessing a website. Instead of :



Accessing a website. Use :



Applications in :

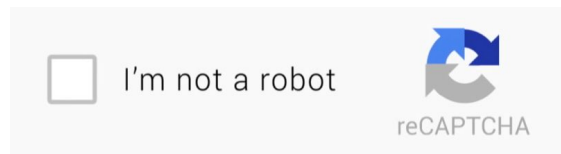
- Forums



- Wikipedia article editing



- Anti-Sybil attacks mechanisms



Problematic :

Reconciling anonymity and accountability on internet



How to start?



A party!

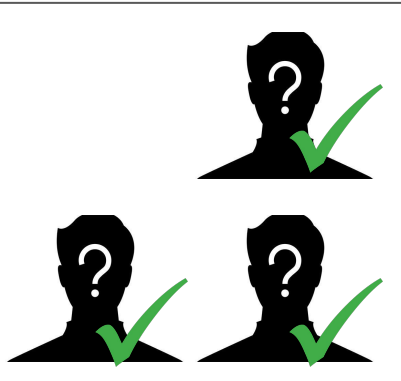
A pseudonym party



Party transcript is then
pushed to the blockchain

Lausanne
23.01.18
Pk1
Pk2
Pk3

Already registered users are separated
and marked



Organizers



Public Key



Attendees



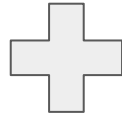
Keeps
private key



PoP token

Party transcript

Lausanne
19.01.2018
Pk1
Pk2
Pk3
...



Private Key

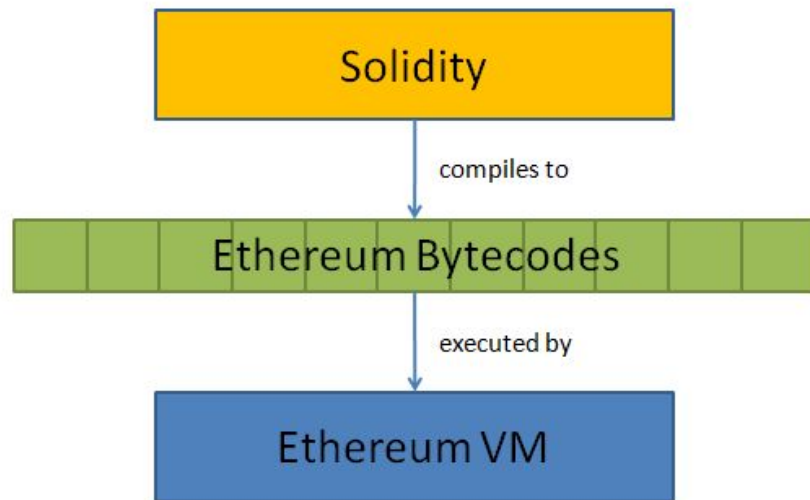


Personhood token

What is Ethereum? Why use it?



Open-source, public, blockchain-based distributed computing platform

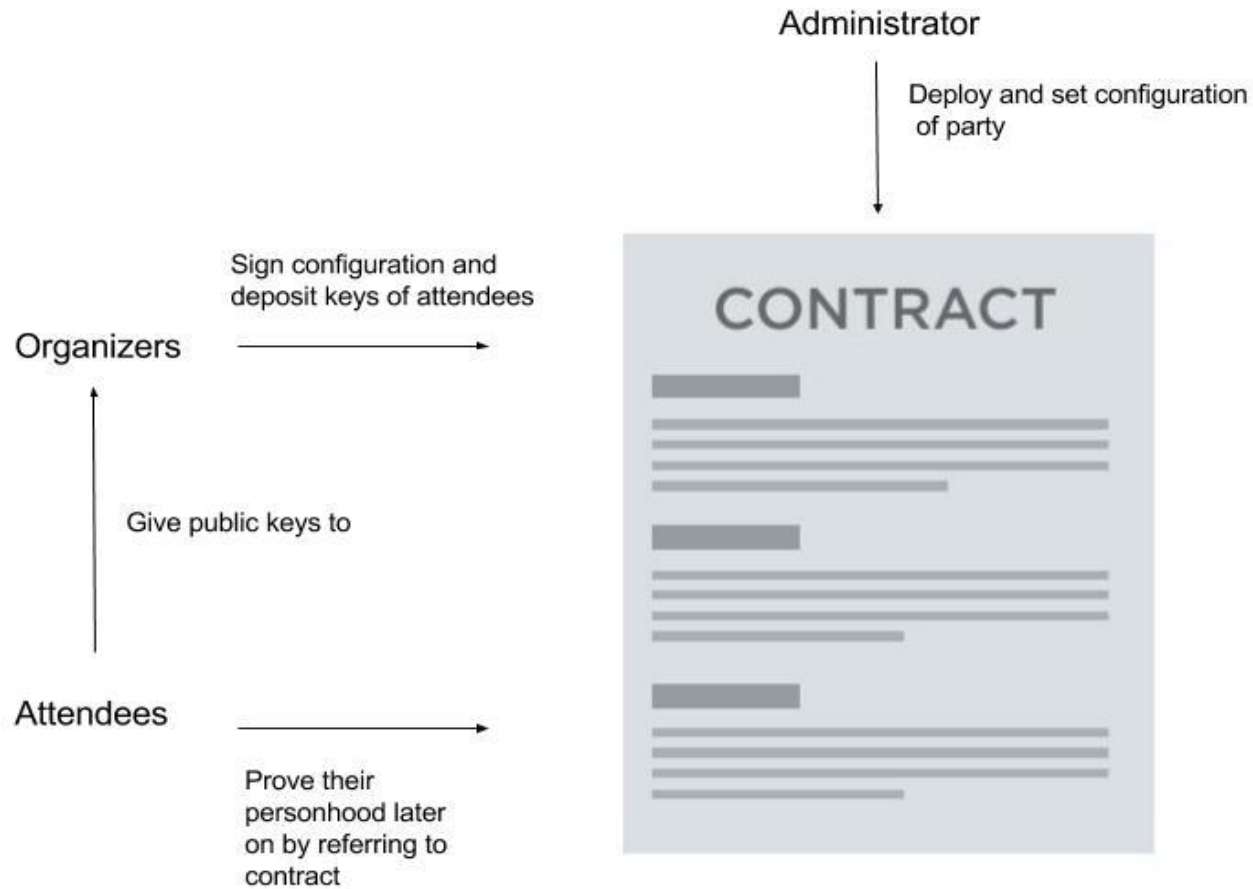


Random stats :

- 30000+ nodes
- Started in 2015
- 16 sec average block time (vs 10 min block time for Bitcoin)

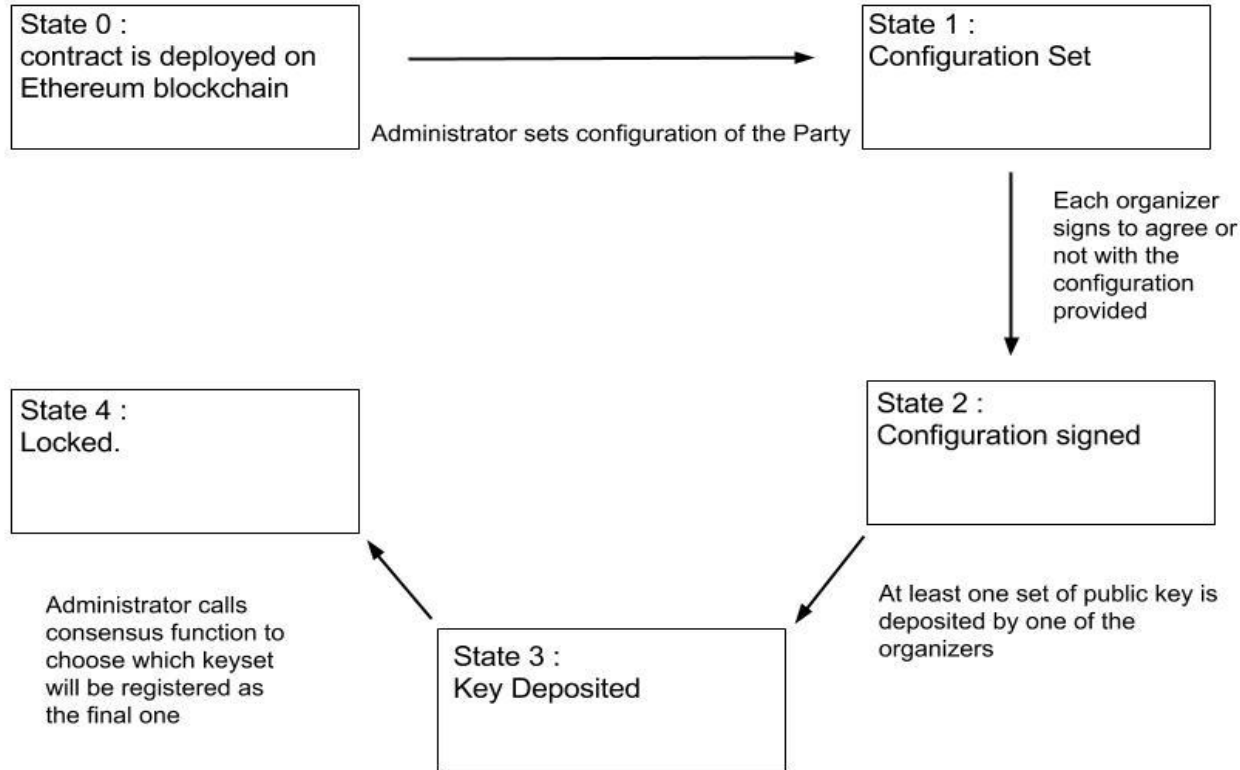
Proof of personhood smart-contract :

Use a smart-contract to organize and store information of a pseudonym party



How to ensure security?

Model the smart-contract as a finite state machine



Demo

Conclusion

Goal : let people ***trust*** each other on internet while also ***staying anonymous***

Realisation : physical party + cryptographic tools + a immutable decentralized ledger (ethereum blockchain)

Further improvements :

- price is high (100\$+) but can be run on testnet
- add new functionalities
- not very user-friendly