Proof-of-Social-Capital: Privacy-Preserving Consensus Protocol Replacing Stake for Social Capital

Juraj Mariani, Ivan Homoliak

BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

Security@FIT

(A) Problem

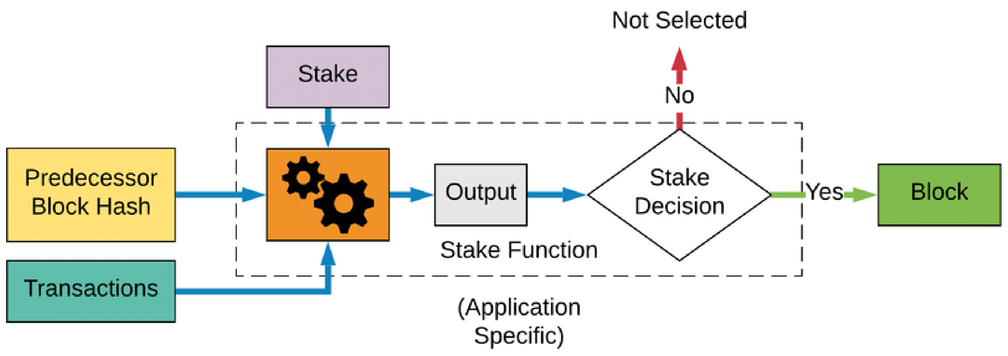
Expensive scarce resources
- e.g., HW in PoW, Tokens in PoS, ...
- current systems favor wealthy individuals
- centralized/pooled resource holders

Incentives
- regular users are “too poor” to secure the consensus
- onboarding and adoption does not rely on regular users

(B) Background - Proof-of-Stake

Proof-of-Stake consensus [1]
- replaces PoW mining with **economic commitment**
- block proposers get elected based on their **collateral stake**
- **higher** stake => **more** blocks proposed => **higher** reward

Ethereum [2]
- validators need to stake 32ETH
- incentives:
  - honest behavior is rewarded => transaction fees + reward
  - maliciousness is punished => slashing
- regular users can enter staking pools
  - includes service fees
  - stake centralization



PoS consensus mechanism [3]

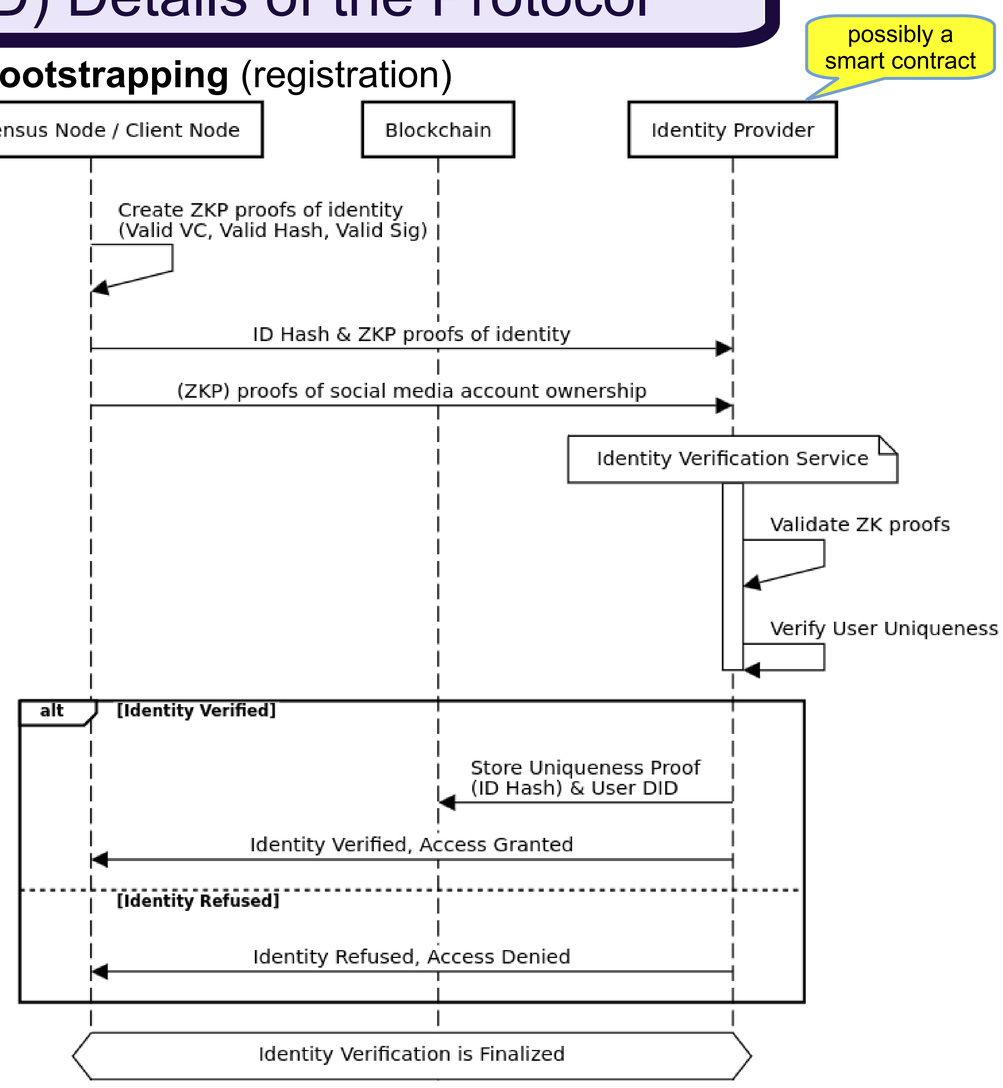
(C) Proposed Solution

Proof-of-Social-Capital (PoSC)
- users can “stake” **social capital** (e.g., fame**,** recognition, ...)
  - inspired by PoS protocol
- consensus nodes are content creators (w. social capital)
- followers can **endorse content creators**
  - we need **unique** verified identities to prevent sybils

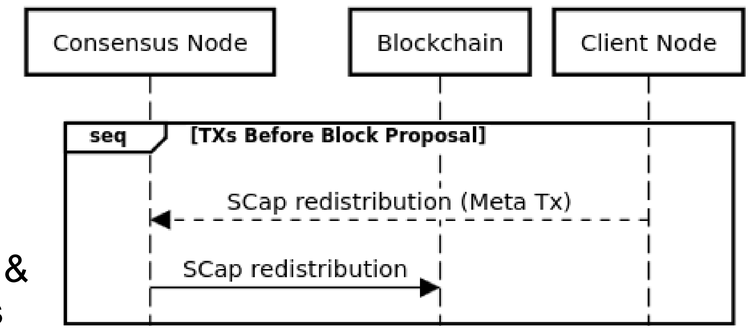
Incentives for regular users
- content creators could issue follower-rewarded content
  - claiming the reward => viewing/engagement with the content (provable)

(D) Details of the Protocol

- **(1) Bootstrapping** (registration)



- **(2) Endorsement**
  - MetaTXs
    - Off-chain assignment of social capital
  - Endorsement Txs
    - Relays on-chain & refunds MetaTxs



- **(3) Operation** (leader election)
  - same as in PoS
  - probabilistic
    - scaling function of social capital
  - Whisk-like DoS protection

(E) Implementation

- Custom PoC implementation in Python
- ZoKrates for ZKPs
- 2/3 consistency-based consensus (PoC)
  - Future work => availability-based

- **Testing environment**
  - 20 nodes
  - consistancy is a limiting factor
  - ID ZKP verification times ~0.1 sec

- **Real implementation**: TBD

References

[1] Kiayias, A., Russell, A., David, B., & Oliynykov, R. (2017, August). Ouroboros: A provably secure proof-of-stake blockchain protocol. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (pp. 263–279). ACM. [Online]. Available: https://doi.org/10.1145/3133956.3134037.
[2] Buterin, V., & Griffith, V. (2020, March). Combining GHOST and Casper. arXiv preprint arXiv:2003.03052. [Online]. Available: https://arxiv.org/abs/2003.03052.
[3] Natoli, Christopher & Yu, Jiangshan & Gramoli, Vincent & Veríssimo, Paulo. (2019). Deconstructing Blockchains: A Comprehensive Survey on Consensus, Membership and Structure. 10.48550/arXiv.1908.08316.