Identity Based Consensus for Self-Governing Systems

Defence and Security Doctoral Symposium 2020

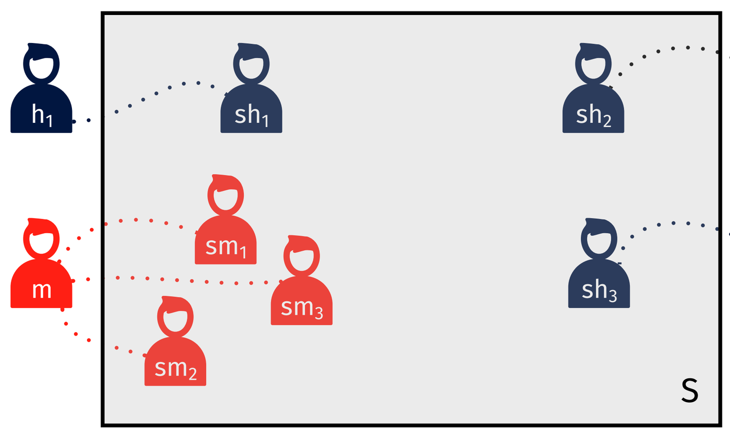
Data on a Blockchain is grouped in *blocks*, each of which contains multiple *transactions*. Blocks have to be resistant to replication over a 'byzantine' network. On those networks, writers can act maliciously in different ways:

- ☐ Attempt to store incorrect/invalid transactions on the Blockchain
- ☐ Use one input multiple times ('double spend')
- ☐ Censor the Blockchain by systematically withholding particular transactions

The selection of members responsible for data replication is a challenge in decentralised record-keeping systems.

'Byzantine' and 'Sybil' Actors

Lamport *et al.* (1982) show how a decentralised system (*S*) behaves when actors (*h, m*) spread incorrect or conflicting information, or withhold information. They describe how a system tolerates a limited fraction of these actors, often referred to as 'byzantine' actors. Douceur (2002) describes how a 'single faulty entity' (*m*), often referred to as a 'sybil' actor, can gain control of a redundant network by 'presenting multiple identities' ($sm_{1..3}$).

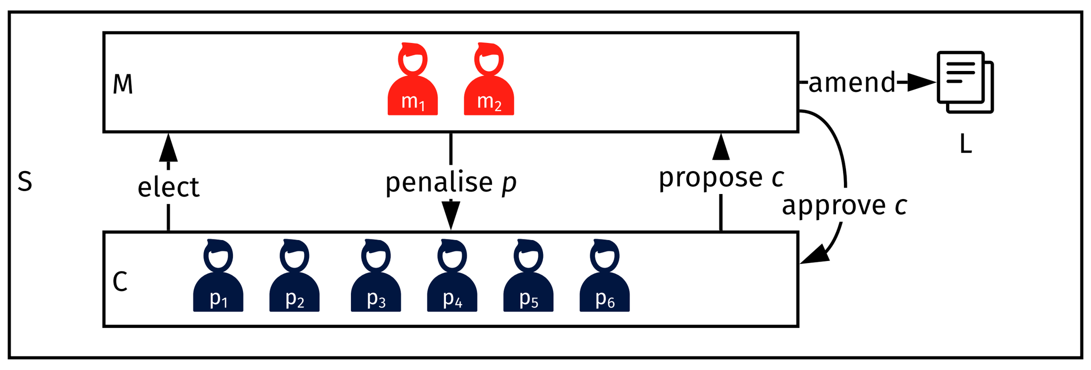


Membership Selection Strategies

- ☐ Proof-of-Work (Bitcoin; Nakamoto, 2008): Select a 'miner' to validate transactional data and to act as an ordering authority of transactions. Participants qualify as miners by expending computing resources.
- ☐ Proof-of-Stake (Conceptual Bitcoin forum post, later formalised by King et al., 2012): Being able to prove ownership of currency determines the difficulty of creating a new block, thus making participants who have held larger quantities of currency for longer more influential.
- ☐ Delegated Proof-of-Stake (Larimer, 2014): A variation to proof-of-stake, introducing a delegation scheme, in which 'shareholders may delegate their voting power to a representative'.
- ☐ Proof-of-Authority: Membership seclection 'by policy', i.e. through a pre-defined list of privileged actors (i.e. Schwartz et al., 2014, Hearn and Brown, 2019, Libra Association, 2020).

Membership Selection and Political Representation

A decentralised system *S*, comprised of regular participants ($p_{1..n}$) and participants with additional duties ('miners' $m_{1..n}$) who are appointed or elected to fulfil these duties. Participants propose candidate records, *c*, to be included in the entirety of public records. Miners decide, based on a legislative framework, *L*, whether a candidate record is permissible.



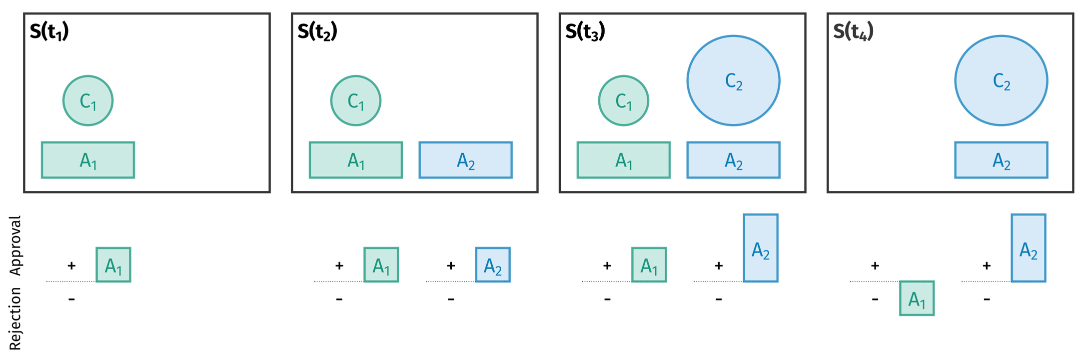
'One Person/One Vote' in Delegated Proof-of-Stake

Given that delegated 'Proof-of-Stake' effectively already implements a 'One Share/One Vote' paradigm, it can be easily restructured to support a 'One Person/One Vote' paradigm by introducing additional constraints to limit the number of shares and how they can circulate:

- ☐ Delegated proof-of-stake is performed using personhood tokens as stake.
- ☐ Every person with voting rights on the network receives a fixed number of personhood tokens once they enter the network.
- ☐ There is no other source of personhood tokens.
- ☐ Personhood tokens cannot be traded and are not given out as a reward.

Constituencies Evolve Over Time

Through messages of approval and rejection, authorities ($A_{1..2}$) are voted onto the system and removed from it. Authorities issue personhood tokens to their constituents ($C_{1..2}$).



Arithmetic Properties of Personhood Tokens

Members can endorse or discourage gatekeeping authorities via a broadcast message. These actions directly impact the reputation of the authority and thus the personhood score the authority can grant. Per authority $A_{1..n}$ a vector of endorsement scores $\vec{e}_{A_{1..n}}$ and a vector of discouragement scores $\vec{d}_{A_{1..n}}$ are kept publicly. Participants add to either of the vectors via a message they broadcast. This means that the influence a participant can exert on the reputation of another authority is proportional to their reputation.

Counteracting Sybil Attacks

A single malevolent authority can flood the network with sybil actors, who can disrupt any record-keeping and record-evolving activity on the network, permanently. We therefore need to implement countermeasures:

- ☐ *Temporal normalisation* can mitigate sybil attacks that go along with a sudden influx of bogus identities.
- ☐ An overall *constituency size ceiling* that limits the total number of identities, created by one authority, is introduced.
- ☐ A *quantitative safeguard enforcing diversity* is introduced. This gives reputational signals from diverse sources more weight.
- ☐ A *lower bound for personhood scores* is introduced.

Future Work

The protocol proposed lacks formalisation, intuition suggests that the concept of evolving constituencies, backed by identity authorities, that can be added to and removed from a network dynamically, has merit.

Future work must focus on formalising the protocol to evaluate its robustness.
A formal approach will ultimately prove or disprove its advantages over existing membership selection protocols, in the context of attacks.

Bach, L. M., B. Mihaljevic, and M. Zagar. 2018. 'Comparative analysis of blockchain consensus algorithms.' In *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (Mipro)*, 1545–50. https://doi.org/10.23919/MIPRO.2018.8400278.

Boldyreva, Alexandra, Adriana Palacio, and Bogdan Warinschi. 2010. 'Secure Proxy Signature Schemes for Delegation of Signing Rights.' *Journal of Cryptology* 25 (1): 57–115. https://doi.org/10.1007/s00145-010-9082-x.

Borge, M., E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, and B. Ford. 2017. 'Proof-of-Personhood: Redemocratizing Permissionless Cryptocurrencies.' In *2017 Ieee European Symposium on Security and Privacy Workshops (Euros Pw)*, 23–26. https://doi.org/10.1109/EuroSPW.2017.46.

Buterin, Vitalik, and Virgil Griffith. 2017. 'Casper the Friendly Finality Gadget.' http://arxiv.org/abs/1710.09437.

Chaum, David, Amos Fiat, and Moni Naor. 1990. 'Untraceable Electronic Cash.' In *Advances in Cryptology CRYPTO' 88*, 319–27. Springer New York. https://doi.org/10.1007/0-387-34799-2_25.

Douceur, John R. 2002. 'The Sybil Attack.' In *Revised Papers from the First International Workshop on Peer-to-Peer Systems*, 251–60. IPTPS '01. Berlin, Heidelberg: Springer-Verlag. https://doi.org/10.5555/646334.687813.

Durlauf, Steven N., and Lawrence E. Blume. 2010. 'Incentive Compatibility.' In *Game Theory*, edited by Steven N. Durlauf and Lawrence E. Blume, 158–68. London: Palgrave Macmillan UK. https://doi.org/10.1057/9780230280847_16.

Grossman, Sanford J, and Oliver D Hart. 1987. 'One Share/One Vote and the Market for Corporate Control.' Working Paper 2347. Working Paper Series. National Bureau of Economic Research. https://doi.org/10.3386/w2347.

Hearn, Mike, and Richard Gendal Brown. 2019. 'Corda: A Distributed Ledger.' Whitepaper Version 1.0. R3. https://www.r3.com/wp-content/uploads/2019/08/corda-technical-whitepaper-August-29-2019.pdf.

King, Sunny, and Scott Nadal. 2012. 'PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake.' Self-published. https://decred.org/research/king2012.pdf.

Lamport, Leslie, Robert Shostak, and Marshall Pease. 1982. 'The Byzantine Generals Problem.' *ACM Transactions on Programming Languages and Systems* 4 (3): 382–401. https://doi.org/10.1145/357172.357176.

Larimer, Daniel. 2014. 'Delegated Proof-of-Stake (DPOS).' April 2014. http://107.170.30.182/security/delegated-proof-of-stake.php.

Li, Wenting, Sébastien Andreina, Jens-Matthias Bohli, and Ghassan Karame. 2017. 'Securing Proof-of-Stake Blockchain Protocols.' In *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, edited by Joaquin Garcia-Alfaro, Guillermo Navarro-Arribas, Hannes Hartenstein, and Jordi Herrera-Joancomartí, 297–315. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-67816-0_17.

Libra Association Members. 2020. 'The Libra Payment System.' Whitepaper 2.0. Geneva, Switzerland: Libra Association. https://libra.org/en-US/wp-content/uploads/sites/23/2020/04/Libra_WhitePaperV2_April2020.pdf.

Nakamoto, Satoshi. 2008. 'Bitcoin: A peer-to-peer electronic cash system.'

Natoli, Christopher, Jiangshan Yu, Vincent Gramoli, and Paulo Esteves-Verissimo. 2019. 'Deconstructing Blockchains: A Comprehensive Survey on Consensus, Membership and Structure.' http://arxiv.org/abs/1908.08316.

QuantumMechanic. 2011. 'Proof of Stake Instead of Proof of Work.' Bitcoin Forum Post. https://bitcointalk.org/index.php?topic=27787.0.

Saleh, Fahad. 2018. 'Blockchain Without Waste: Proof-of-Stake.' *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3183935.

Schwartz, David, Noah Youngs, and Arthur Britto. 2014. 'The Ripple Protocol Consensus Algorithm.' Whitepaper. Ripple Labs Inc.

Szabo, Nick. 1997. 'Formalizing and Securing Relationships on Public Networks.' *First Monday* 2 (9). https://doi.org/10.5210/fm.v2i9.548.

Wood, Gavin. 2017. 'Ethereum: A Secure Decentralised Generalised Transaction Ledger.' Yellow Paper. Stiftung Ethereum. https://ethereum.github.io/yellowpaper/paper.pdf.

Moritz Platt, PhD Student, Department of Informatics, King's College London
moritz.platt@kcl.ac.uk