Self-Governing Public Decentralised Systems

KING'S College LONDON

Moritz Platt (moritz.platt@kcl.ac.uk), **Peter McBurney** (peter.mcburney@kcl.ac.uk)

10th International Workshop on Socio-Technical Aspects in Security (STAST2020), 17 September 2020

Agenda

1 **Background:** Modern public decentralised systems (like various ‘Blockchain’ protocols) directly build on early findings in distributed systems research.

2 **Membership Selection:** Various membership selection strategies, built on ‘Proof-of-Work’, ‘Proof-of-Stake’, and others exist in decentralised systems.

3 **Towards Achieving ‘One Person/One Vote’:** Existing membership selection protocols often aim to approximate democratic ideals. We propose a more direct approach.

Decentralised Record-Keeping Systems

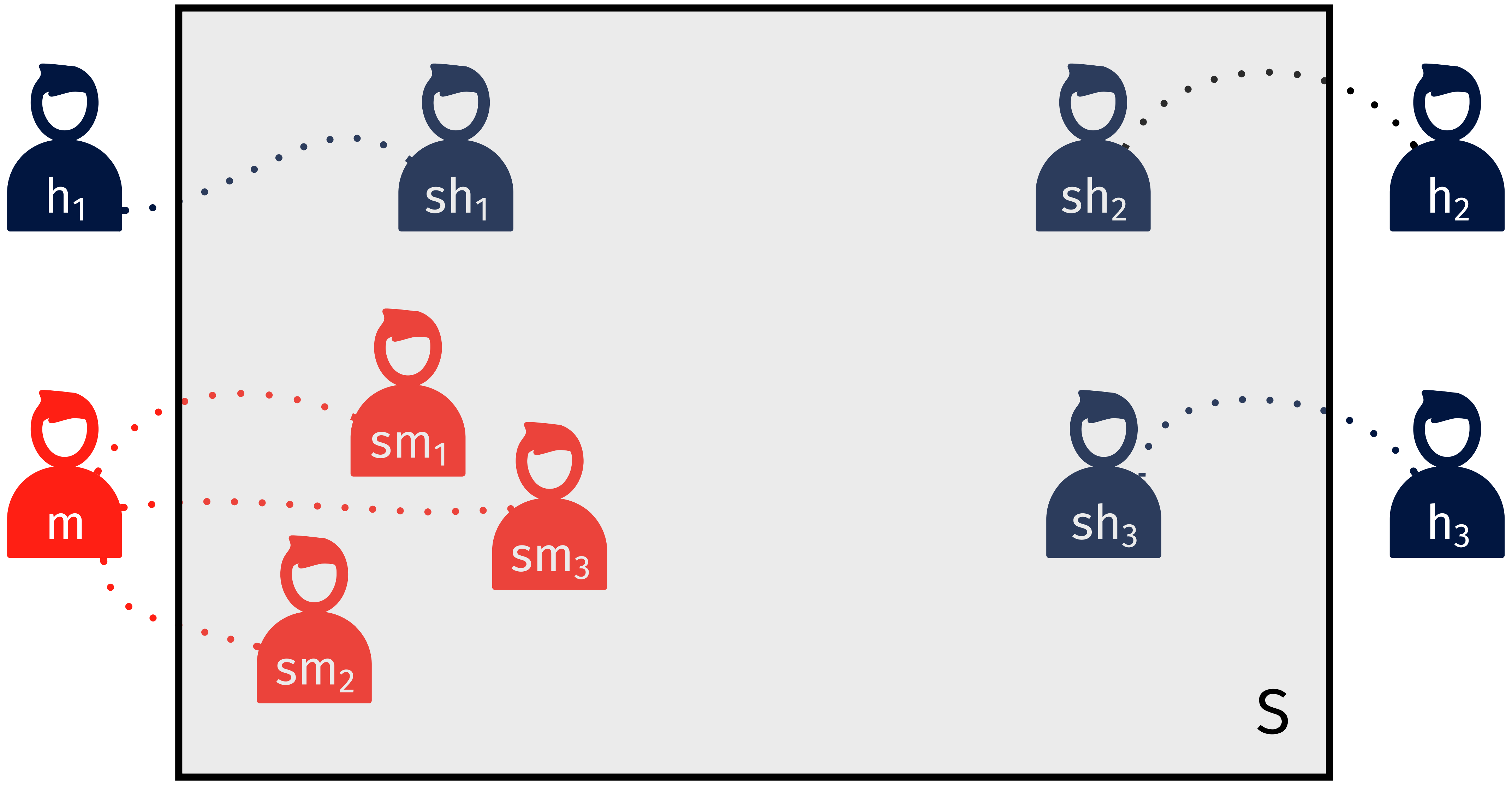
□ **Decentralised:** There are no privileged authorities, i.e. every actor on the network has the same *intrinsic* permissions.

□ **Record-keeping:** The system is stateful. State can be evolved by actors in the system, according to rules that are *system-wide* properties.

In order to be truly decentralised, systems need to be ‘permissionless’, in the sense that ‘any network participant has the ability to create a candidate record’ (Rauchs *et al.* 2018). In absense of a central authority, validating what candidate records are admissible, and replicating them throughout the system, is the task of regular participants on the network.

‘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.

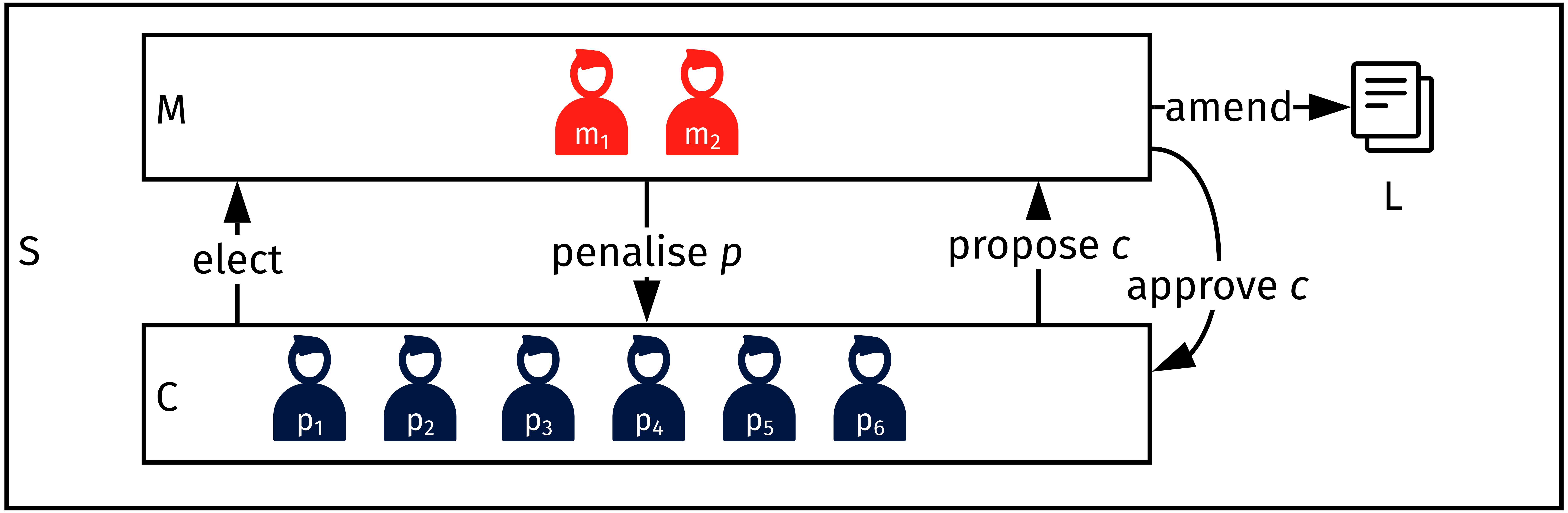
□ *Proof-of-Stake* (Conceptual Bitcoin forum post, later formalised by King *et al.*, 2012): Being able to prove ownership of currency determines the difficulty of creating a new block, thus making participants who have held larger quantities of currency for longer more influential.

□ *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.



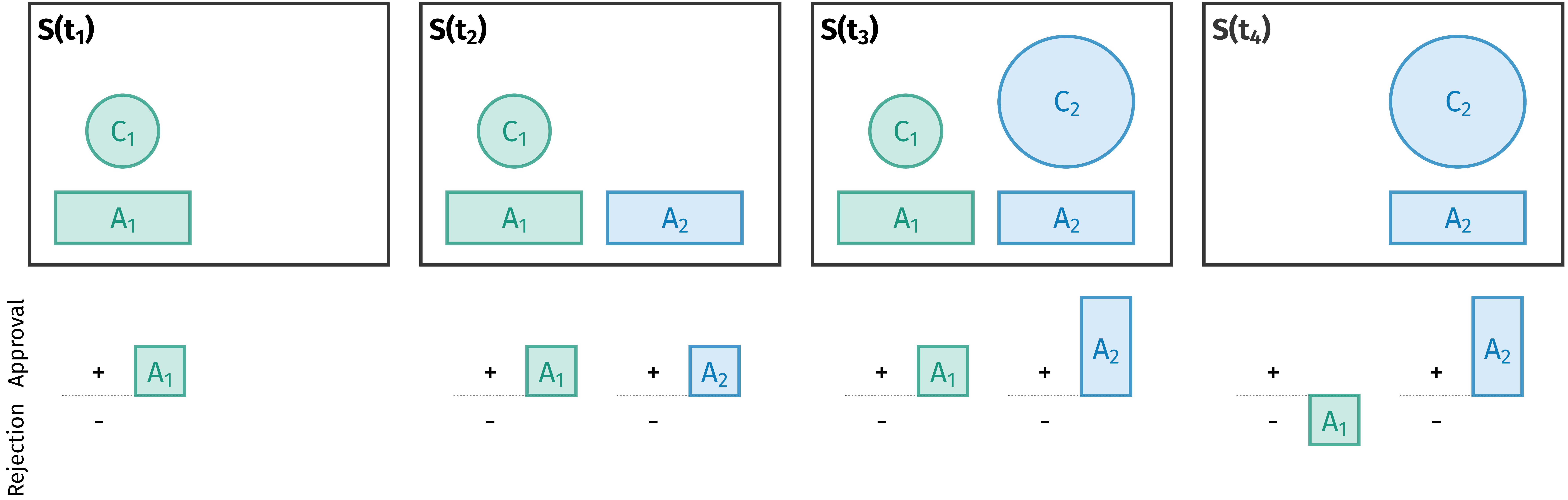
‘One Person/One Vote’ in Delegated Proof-of-Stake

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:

1. Delegated proof-of-stake is performed using personhood tokens as stake.
2. Every person with voting rights on the network receives a fixed number of personhood tokens once they enter the network.
3. There is no other source of personhood tokens.
4. 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.

Bibliography

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.

Baird, Leemon, Mance Harmon, and Paul Madsen. 2019. ‘Hedera: A Public Hashgraph Network & Governing Council.’ Whitepaper 2.0. Hedera Hashgraph. https://www.hedera.com/hh-whitepaper-v2.0-17Sep19.pdf.

Barone, Raffaella, and Donato Masciandaro. 2019. ‘Cryptocurrency or usury? Crime and alternative money laundering techniques.’ *European Journal of Law and Economics* 47 (2): 233–54. https://doi.org/10.1007/s10657-019-09609-6.

block.one. 2018. ‘EOS.IO Technical White Paper.’ Whitepaper v2. https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md.

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.

Cannarsa, Michel. 2018. ‘Interpretation of Contracts and Smart Contracts: Smart Interpretation or Interpretation of Smart Contracts?’ *European Review of Private Law*, 773–85.

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.

Conti, M., E. Sandeep Kumar, C. Lal, and S. Ruj. 2018. ‘A Survey on Security and Privacy Issues of Bitcoin.’ *IEEE Communications Surveys Tutorials* 20 (4): 3416–52. https://doi.org/10.1109/COMST.2018.2842460.

Croman, Kyle, Christian Decker, Ittay Eyal, Adem Efe Gencer, Ari Juels, Ahmed Kosba, Andrew Miller, et al. 2016. 'On Scaling Decentralized Blockchains.' In *Financial Cryptography and Data Security*, edited by Jeremy Clark, Sarah Meiklejohn, Peter Y. A. Ryan, Dan Wallach, Michael Brenner, and Kurt Rohloff, 106–25. Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-53357-4_8.

Daian, Phil, Rafael Pass, and Elaine Shi. 2019. 'Snow White: Robustly Reconfigurable Consensus and Applications to Provably Secure Proof of Stake.' In *Financial Cryptography and Data Security*, edited by Ian Goldberg and Tyler Moore, 23–41. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-32101-7_2.

Dhillon, Amrita, Grammateia Kotsialou, Peter McBurney, and Luke Riley. 2019. 'Introduction to Voting and the Blockchain: some open questions for economists.' CAGE Online Working Paper Series 416. Competitive Advantage in the Global Economy (CAGE). https://ideas.repec.org/p/cge/wacage/416.html.

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.

Duxbury, Scott W., and Dana L. Haynie. 2017. 'The Network Structure of Opioid Distribution on a Darknet Cryptomarket.' *Journal of Quantitative Criminology*, June. https://doi.org/10.1007/s10940-017-9359-4.

Foster, Charles, and Jonathan Herring. 2017. 'Theories of Personhood.' In *Identity, Personhood and the Law*, 21–34. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-53459-6_2.

Gilad, Yossi, Rotem Hemo, Silvio Micali, Georgios Vlachos, and Nickolai Zeldovich. 2017. 'Algorand.' In *Proceedings of the 26th Symposium on Operating Systems Principles*. ACM. https://doi.org/10.1145/3132747.3132757.

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.

Gui, George, Ali Hortacsu, and Jose Tudon. 2018. 'A Memo on the Proof-of-Stake Mechanism.' http://arxiv.org/abs/1807.09626v1.

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.

Hellwig, Daniel, Goran Karlic, and Arnd Huchzermeier. 2020. ‘Privacy and Anonymity.’ In *Build Your Own Blockchain: A Practical Guide to Distributed Ledger Technology*, 99–121. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-40142-9_5.

Heusser, Jonathan. 2013. ‘SAT solving–An alternative to brute force bitcoin mining.’ February 2013. https://jheusser.github.io/2013/02/03/satcoin.html.

Karame, Ghassan O., Elli Androulaki, and Srdjan Capkun. 2012. ‘Double-Spending Fast Payments in Bitcoin.’ In *Proceedings of the 2012 Acm Conference on Computer and Communications Security*, 906–17. CCS ’12. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/2382196.2382292.

Kethineni, Sesha, and Ying Cao. 2019. ‘The Rise in Popularity of Cryptocurrency and Associated Criminal Activity.’ *International Criminal Justice Review*, February, 105756771982705. https://doi.org/10.1177/1057567719827051.

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

Kroll, Joshua A, Ian C Davey, and Edward W Felten. 2013. ‘The economics of Bitcoin mining, or Bitcoin in the presence of adversaries.’ In *Proceedings of Weis*, 2013:11.

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.

Lee, Charles. 2011. ‘Litecoin.’

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.

McBurney, Peter, and Simon Parsons. 2004. ‘Engineering Democracy in Open Agent Systems.’ In *Engineering Societies in the Agents World IV*, 66–80. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-25946-6_4.

McCorry, Patrick, Siamak F. Shahandashti, and Feng Hao. 2017. ‘A Smart Contract for Boardroom Voting with Maximum Voter Privacy.’ In *Financial Cryptography and Data Security*, edited by Aggelos Kiayias, 357–75.

Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-70972-7_20.

Miller, Andrew. 2013. 'Feather-Forks: Enforcing a Blacklist with Sub-50% Hash Power.' Bitcoin Forum Post. https://bitcointalk.org/index.php?topic=312668.0.

Mora, Camilo, Randi L. Rollins, Katie Taladay, Michael B. Kantar, Mason K. Chock, Mio Shimada, and Erik C. Franklin. 2018. 'Bitcoin emissions alone could push global warming above 2°C.' *Nature Climate Change* 8 (11): 931–33. https://doi.org/10.1038/s41558-018-0321-8.

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.

Orman, Hilarie. 2018. 'Blockchain: The Emperors New PKI?' *IEEE Internet Computing* 22 (2): 23–28. https://doi.org/10.1109/mic.2018.022021659.

Ostrom, E. 1999. 'Self-Governance and Forest Resources.' Occasional Paper 20. Center for International Forestry Research (CIFOR); Center for International Forestry Research.

Ostrom, Elinor, James Walker, and Roy Gardner. 1992. 'Covenants with and without a Sword: Self-Governance Is Possible.' *American Political Science Review* 86 (2): 404–17. https://doi.org/10.2307/1964229.

Patrick, Aaron, and David Marin-Guzman. 2020. '"Everyone Knew What Was Going on".' *The Australian Financial Review*, June.

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

Rauchs, Michel, Andrew Glidden, Brian Gordon, Gina Pieters, Martino Recanatini, Francois Rostand, Kathryn Vagneur, and Bryan Zhang. 2018. *Distributed Ledger Technology Systems. A Conceptual Framework*. Cambridge, UK: Cambridge Centre for Alternative Finance, Cambridge Judge Business School, University of Cambridge. https://doi.org/10.2139/ssrn.3230013.

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.

Shehar, Bano, Christian Catalini, George Danezis, Nick Doudchenko, Ben Maurer, Alberto Sonnino, and Nils Wernerfelt. 2019. 'Moving Toward Permissionless Consensus.' Geneva, Switzerland: Libra Association. https://libra.org/wp-content/uploads/2019/06/MovingTowardPermissionlessConsensus_en_US.pdf.

Stroukal, Dominik, and Barbora Nedvědová. 2016. 'Bitcoin and other cryptocurrency as an instrument of crime in cyberspace.' Proceedings of Business and Management Conferences 4407036. International Institute of Social; Economic Sciences. https://ideas.repec.org/p/sek/ibmpro/4407036.html.

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

Thin, Wai Yan Maung Maung, Naipeng Dong, Guangdong Bai, and Jin Song Dong. 2018. 'Formal Analysis of a Proof-of-Stake Blockchain.' In *2018 23rd International Conference on Engineering of Complex Computer Systems (ICECCS)*. IEEE. https://doi.org/10.1109/iceccs2018.2018.00031.

Townsend, Ralph E. 1995. 'Fisheries Self-Governance: Corporate or Cooperative Structures?' *Marine Policy* 19 (1): 39–45. https://doi.org/10.1016/0308-597x(95)92571-n.

Vasek, Marie, Micah Thornton, and Tyler Moore. 2014. 'Empirical Analysis of Denial-of-Service Attacks in the Bitcoin Ecosystem.' In *Financial Cryptography and Data Security*, edited by Rainer Böhme, Michael Brenner, Tyler Moore, and Matthew Smith, 57–71. Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-44774-1_5.

Waidner, M., and B. Pfitzmann. 1990. 'Loss-Tolerance for Electronic Wallets.' In *[1990] Digest of Papers. Fault-Tolerant Computing: 20th International Symposium*, 140–47. https://doi.org/10.1109/FTCS.1990.89349.

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

Wuille, Pieter. 2014. 'Dealing with Malleability.' Bitcoin Improvement Proposal. https://github.com/bitcoin/bips/blob/master/bip-0062.mediawiki.

Zheng, Z., S. Xie, H. Dai, X. Chen, and H. Wang. 2017. 'An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends.' In *2017 Ieee International Congress on Big Data (Bigdata Congress)*, 557–64. https://doi.org/10.1109/BigDataCongress.2017.85.