BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

Excel@FIT 2025
http://excel.fit.vutbr.cz

Privacy-Preserving Consensus Protocol based on Social Capital

Bc. Juraj Mariani*

Abstract

Consensus protocols used today in blockchains often rely on computational power or financial stakes – scarce resources. We propose a novel protocol using social capital – trust and influence from social interactions – as a non-transferable staking mechanism to ensure fairness and decentralization. The methodology integrates zero-knowledge proofs, verifiable credentials, a Whisk-like leader election, and an incentive scheme to prevent Sybil attacks and encourage engagement. The theoretical framework would enhance privacy and equity, though unresolved issues like off-chain bribery require further research. This work offers a new model aligned with modern social media behavior and lifestyle, with applications in finance, providing a practical insight for decentralized system development.

*xmaria03@vutbr.cz, *Faculty of Information Technology, Brno University of Technology*

1. Introduction

The 2008 Global Financial Crisis exposed the fragility of opaque financial systems, sparking interest in transparent, decentralized alternatives like blockchain. This thesis provides a new angle on a blockchain consensus protocol that does not rely on the computational power or the amount of money an individual possesses. As powerful hardware or monetary stake is expensive (32ETH needed for staking is *50,148.55€*[1]), we look into alternative mechanisms for consensus power. The idea behind this thesis is utilizing social capital – a measure of influence and trust derived from social interactions – as a novel staking mechanism to ensure fairness and decentralization. Instead of money, people can stake their influence, which could perhaps be easier to gain with considerably fewer resources.

The core challenge is designing a consensus protocol that balances transparency with privacy, prevents Sybil attacks, and ensures equitable participation without relying on traditional financial stakes or centralized authorities. A successful protocol should be privacy-preserving, decentralized, and, most importantly, resistant to Sybil accounts.

[1]Value noted as of April 27th, 3:30pm

2. Motivation

Current consensus mechanisms like Proof-of-Work [1, 2] (PoW) and Proof-of-Stake [3, 4, 5] (PoS) prioritize security but often compromise on privacy or energy efficiency. PoW, used in Bitcoin, is energy-intensive, while PoS, as in Ethereum, favors wealthier participants, risking centralization and disadvantaging people with little funds. Privacy-focused solutions like Monero's ring signatures [6] or Zcash's zkSNARKs [7] protect transaction details but struggle with scalability, require trusted setups, or are considered unsafe from a legal perspective.

3. Related works

There are attempts to utilize socia capital, both in the Web2 and Web3 worlds with differing success. Web2 services, like YouTube, TikTok, Instagram or OnlyFans show a highly successful model of social capital utilization. On the other hand, Web3 services utilizing social capital (Farcaster, SteemIt, Friend.Tech) are less-known and have limited success.

We propose a privacy-preserving consensus protocol using social capital as a non-transferable staking asset. Social capital is assigned to users and can be awarded to content creators, influencing their likelihood of being elected as block proposers. Zero-knowledge proofs [7] (ZKPs) and verifiable credentials [8] (VCs)

ensure unique, privacy-preserving identity verification.

4. Contributions

This work introduces:

1. a novel use of social capital as a means to secure consensus, reducing financial barriers;
2. a privacy-preserving identity management system using ZKPs and VCs;
3. a reward system incentivizing user adoption and engagement through exclusive content.

5. Protocol design

The protocol integrates social capital [9, 10, 11] into a blockchain consensus framework, replacing traditional financial stakes. Verified users assign their social capital to content creators, who stake it to participate in block proposal. To prevent centralization, we apply logarithmic/square root scaling to social capital, ensuring diminishing returns for large stakes. Leader election employs a Whisk-like mechanism (secret single-leader election) where validators shuffle a candidate pool to create a secret list of future leaders.

5.1 Identity Management

Identity management, often implemented by *Proof-of-Uniqueness* (PoU) solutions [12, 13, 14], is critical to prevent Sybil attacks. We propose on-chain commitment storage, where users submit a cryptographic hash of their identity attributes from their Verifiable Credential (VC) (e.g., name, date of birth) alongside ZKPs proving VC legitimacy, to prove user uniqueness. These are verified by consensus nodes, ensuring privacy and preventing identity recycling and Sybil attacks.

Alternatively, a decentralized identity provider (IDP) blockchain using BFT-PoA consensus can validate identities, requiring a two-thirds majority for approval. This alternative would not require ZKP on-chain storage, creating a safer space (if cryptographic primitives ZKPs require are broken) at the cost of greater overhead (Id hashes would still need to be stored on-chain for uniqueness guarantees).

5.2 Incentive & Reward Scheme

The system uses a native token with a capped supply, similar to Bitcoin, and periodic reward reductions to control inflation. Unlike traditional financial stakes, social capital is non-transferable (beyond the endorsement process) to prevent centralization and maintain fairness, with each node starting with an equal amount. To encourage user participation without financial sacrifice, the system incentivizes engagement through exclusive creator-paid content, including personalized material, advertisement campaigns, and sponsored content. Users must prove engagement (e.g., via ZKPs of content interaction) to claim rewards, ensuring active participation and preventing abuse. Creators pay transaction fees associated with users' social capital assignments, mitigating DoS attacks by allowing them to reject spam transactions.

5.3 Security Considerations

1. **Sybil attacks [15]:** The biggest problem is Sybil attacks, as it would shift the paradigm of social capital being a scarce resource to an abundant and creatable resource, making it worthless.
2. **Attacks towards IDP (if present):** As IDPs would be the arbiters of user uniqueness, they could be attacked to create fraudulent accounts. We propose various mechanisms to tackle this problem, the most promising of which are *IDP consensus mechanism* or *ZKP*[2] *on-chain storage* (i.e., not requiring an IDP in the first place).
3. **Leader election attack [16]:** In Ethereum, block producers are known in advance, introducing DoS attack possibilities. While not directly solving the issue, Whisk introduces an anonymity set, lowering the probability of a successful execution.
4. **Off-chain bribery attack:** Users can be paid or otherwise coerced to endorse creators that they would not otherwise endorse. As the bribes could be done off-chain, there would be no trace, and thus no action could be taken. This attack vector will remain unresolved and should be subject to future proposals.

6. Conclusions

This thesis presents a privacy-preserving consensus protocol that leverages social capital to shift consensus power from money to merit. By integrating ZKPs, VCs, and a Whisk-based leader election, we achieve robust privacy, security, and fairness. Future work could explore post-quantum cryptography to enhance long-term security and hybrid PoS-social capital models (including monetary stakes) to balance economic and social incentives. The protocol offers a scalable, inclusive framework for decentralized systems, with potential applications beyond finance, such as social media and governance.

[2] ZKP proving the legitimacy of Id-hahses

Acknowledgements

I would like to express my deepest gratitude to my supervisor, doc. Ing. Ivan Homoliak, Ph.D. His constant support, expert guidance, and patient encouragement have been invaluable at every stage of this work. His friendly approach and unwavering belief in my abilities gave me the confidence and motivation to tackle every aspect of this work.

References

[1] Satoshi Nakamoto et al. Bitcoin. *A peer-to-peer electronic cash system*, 21260, 2008.

[2] Juan Garay, Aggelos Kiayias, and Nikos Leonardos. The bitcoin backbone protocol: Analysis and applications. *J. ACM*, 71(4), August 2024.

[3] Vitalik Buterin and Virgil Griffith. Casper the friendly finality gadget, 2019.

[4] Vitalik Buterin et al. A next-generation smart contract and decentralized application platform. *white paper*, 3(37):2–1, 2014.

[5] Aggelos Kiayias, Alexander Russell, Bernardo David, and Roman Oliynykov. Ouroboros: A provably secure proof-of-stake blockchain protocol. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology – CRYPTO 2017*, pages 357–388, Cham, 2017. Springer International Publishing.

[6] Ronald L. Rivest, Adi Shamir, and Yael Tauman. *How to Leak a Secret: Theory and Applications of Ring Signatures*, pages 164–186. Springer Berlin Heidelberg, Berlin, Heidelberg, 2006.

[7] Lance Fortnow. The knowledge complexity of interactive proof systems. *The Journal of Symbolic Logic*, 56(3):1092–1094, 1991.

[8] World Wide Web Consortium. Verifiable Credentials Data Model 1.0: Expressing verifiable information on the Web. https://www.w3.org/TR/vc-data-model/, November 2019. W3C Recommendation, 19 November 2019.

[9] Gary S Becker. *Human capital: A theoretical and empirical analysis, with special reference to education*. University of Chicago press, 2009.

[10] Michael H Goldhaber. The attention economy and the net. *First Monday*, 1997.

[11] Lawrence Ang Susie Khamis and Raymond Welling. Self-branding, 'micro-celebrity' and the rise of social media influencers. *Celebrity Studies*, 8(2):191–208, 2017.

[12] BrightID. Brightid whitepaper. 2022.

[13] Dr. A. Shaji George, A. S. Hovan George, and Dr. T. Baskar. Worldcoin: A decentralized currency for a unified global economy. *Partners Universal International Research Journal*, 2(2):136–155, Jun. 2023.

[14] Omer Dogan. Developing digital identity applications using hyperledger indy, ursa and aries frameworks — concepts, 2012.

[15] John R Douceur. The sybil attack. In *International workshop on peer-to-peer systems*, pages 251–260. Springer, 2002.

[16] Least Authority. Ethereum 2.0 specifications audit report. Technical report, Least Authority, November 2018. See "Technical Details" on RANDAO-based proposer DDoS attack.