SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

Conclave: A Collective Stake Pool Protocol

Dimitris Karakostas * Aggelos Kiayias * Mario Larangeira †

Keywords: Proof-of-Stake, Blockchain, Consensus, Delegation, Threshold ECDSA.

Abstract

Proof-of-Stake (PoS) distributed ledgers are the most common alternative to Bitcoin's Proof-of-Work (PoW) paradigm, replacing hardware dependency with stake, i.e., assets that a party controls. Similar to PoW's mining pools, PoS's stake pools, i.e., collaborative entities comprising of multiple stakeholders, allow a party to earn rewards more regularly, compared to participating on an individual basis. However, stake pools tend to increase centralization, since they are typically managed by a single party that acts on behalf of the pool's members. In this work we propose *Conclave*, a formal design of a *Collective Stake Pool*, i.e., a decentralized pool with no single point of authority. Among Conclave's building blocks is a weighted threshold signature scheme (WTSS); we define the WTSS ideal functionality — which is of independent interest — and propose two threshold ECDSA based constructions which enable (1) fast trustless setup and (2) identifiable aborts.

The Delegated PoS. Bitcoin combined PoW, to prevent sybil attacks, with financial rewards, to incentivize participation. However, PoW's deficiencies, particularly its egregious environmental cost,[1] have driven research on alternative designs, most prominently PoS, which removes hardware and energy requirements altogether and internalizes sybil resilience by relying on parties' *stake*, i.e., the assets that they own. Interestingly, both PoW and PoS are economies of scale, who favor parties with large amounts of participating power. One reason is poorly-designed incentives, resulting in disproportionate power accumulation [2, 4]. Another is temporal discounting, i.e., the tendency to disfavor rare or delayed rewards [5]. In contrast, accumulating the power of multiple small parties in "pools" yields a steadier reward. As a result, PoS usually favors delegation to stake pools [1, 3] over "pure" PoS, i.e., not delegated. Finally, the ledger's performance and security are often better under fewer participants. Namely, PoS requires constant online participants since abstaining is a security hazard, which is more easily guaranteed within a small set of dedicated delegates.

The Collective Stake Pool. A major drawback of existing stake pools is that they are typically managed by a single party, the *operator*. This party participates in consensus, claims the rewards offered by the system, and then distributes them among the pool's members (after subtracting a fee). However, the operator is a single point of failure. In this work, we explore a more desirable design, which allows players to jointly form a *collective pool*, i.e., the *Conclave*. This design assumes no single operator, minimizing excess fees, trust and security concerns, altogether. Collective stake pools also promote a more fair and decentralized environment.

* University of Edinburgh and IOHK, {dimitris.karakostas@,akiayias@inf.}ed.ac.uk and {dimitris.karakostas,aggelos.kiayias}@iohk.io.
† Tokyo Institute of Technology and IOHK, mario@c.titech.ac.jp / mario.larangeira@iohk.io.
This work is supported by JSPS KAKENHI No. JP21K11882.
[1] The carbon footprint of: i) a single Bitcoin transaction is equivalent to 1,202,422 VISA transactions; ii) the total Bitcoin network is comparable to Sweden. (https://digiconomist.net/bitcoin-energy-consumption; May 2021)

References

[1] E. Community. Eos.io technical white paper v2, 2018. https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md.

[2] G. C. Fanti, L. Kogan, S. Oh, K. Ruan, P. Viswanath, and G. Wang. Compounding of wealth in proof-of-stake cryptocurrencies. In I. Goldberg and T. Moore, editors, *FC 2019*, volume 11598 of *LNCS*, pages 42–61. Springer, Heidelberg, Feb. 2019.

[3] D. Karakostas, A. Kiayias, and M. Larangeira. Account management in proof of stake ledgers. In C. Galdi and V. Kolesnikov, editors, *SCN 20*, volume 12238 of *LNCS*, pages 3–23. Springer, Heidelberg, Sept. 2020.

[4] D. Karakostas, A. Kiayias, C. Nasikas, and D. Zindros. Cryptocurrency egalitarianism: A quantitative approach. In V. Danos, M. Herlihy, M. Potop-Butucaru, J. Prat, and S. T. Piergiovanni, editors, *International Conference on Blockchain Economics, Security and Protocols, Tokenomics 2019, May 6-7, 2019, Paris, France*, volume 71 of *OASIcs*, pages 7:1–7:21. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019.

[5] D. D. Reed and J. K. Luiselli. *Temporal Discounting*, pages 1474–1474. Springer US, Boston, MA, 2011.