A Treasury System for Cryptocurrencies: Enabling Better Collaborative Intelligence*

Bingsheng Zhang[1], Roman Oliynykov[2], Hamed Balogun[3], and Tamara Finogina[4]

[1] Lancaster University, UK
b.zhang2@lancaster.ac.uk
[2] IOHK
and V.N.Karazin Kharkov National University, Ukraine
roman.oliynykov@iohk.io
[3] Lancaster University, UK
h.balogun@lancaster.ac.uk
[4] Scytl R & D, Spain
tamara.finogina@skolkovotech.ru

Abstract. A treasury system is a community controlled and decentralized collaborative decision-making mechanism for sustainable funding of the underlying blockchain development and maintenance. During each treasury period, project proposals are submitted, discussed, and voted for; top-ranked projects are funded from the treasury. The Dash governance system is a real-world example of such kind of systems. In this work, we, for the first time, provide a rigorous study of the security of the treasury system. We modelled, designed, and implemented a provably secure treasury system that is compatible with most existing blockchain infrastructures, such as Bitcoin, Ethereum, etc. More specifically, the proposed treasury system supports liquid democracy/delegative voting for better collaborative intelligence. Namely, the voters can either vote directly on the proposed projects or delegate their votes to experts. Its core component is a distributed universally composable secure end-to-end verifiable online voting protocol. The integrity of the treasury voting decisions is guaranteed even when all the voting committee members are corrupted. To further improve efficiency, we proposed the world's first honest verifier zero-knowledge proof for unit vector encryption with logarithmic size communication. This partial result may be of independent interest to other cryptographic protocols. A pilot system is implemented under Java/Scala, and its benchmark results indicate that the proposed system can support tens of thousands of treasury participants with high efficiency.

* This work is supported by IOHK Ltd.

Table of Contents

The rest of the paper is will be updated ASAP. Stay tuned.