FROSTDAO: Collective Ownership of wealth using FROST

Rahim Klabér

March 26, 2023

1 Introduction

The introduction of Bitcoin allowed anyone to send and receive money anonymously and without government oversight[CITE]. Subsequent Blockchains introduced the concept of "smart-contract", code that is stored on a Blockchain and runs depending on certain conditions. Smart-contracts led to the concept of Decentralized Autonomous Organizations (DAOs). These are leaderless organizations where the members can collectively determine what to do. These DAOs use Blockchain smart-contracts to allow for the collective ownership of wealth.

The behavior of certain smart-contracts can be emulated with cryptography instead of code. Most importantly, a smart-contract for collective decision-making can be replaced with threshold cryptography[CITE]. In this case the members of a DAO would jointly control a Blockchain account that serves the account of the organization.

In this paper, we introduce a DAO framework based on cryptography, instead of Blockchain smart-contracts. We substitute smart contracts with threshold signatures to create a DAO framework that is Blockchain agnostic and does not require the underlying Blockchain to support smart-contracts.

2 Problem

The goal is to create a DAO framework that can scale to hundreds or even thousands of members for Blockchains where DAOs cannot be created using smart-contracts. In particular, Bitcoin. Our framework should work in a fully decentralized and peer-2-peer setting where the only participants are smartphones and there are no servers. This is especially challenging given the unreliability of smartphone networking.

3 Background

3.1 DAO

3.2 FROST

3.3 IPV8

4 Implementation

4.1 Bitcoin specifics

5 Evaluation

6 Conclusion