MANTAPAY Protocol Specification

Shumo Chu and Brandon H. Gomes

October 29, 2021

Abstract

This article outlines a generalized transfer protocol based on the original Mantadap protocol outlined in the Manta whitepaper. In this protocol, the Manta transfer types, (Mint, PrivateTransfer, Reclaim), are replaced by one transfer type Transfer who's fundamental verification algorithm is uniform over all possible transfer shapes. In this specification, we also introduce a reusable address system to replace the one-time shielded address scheme. This specification also outlines "semantic transactions" and the algorithm for building them from the Transfer primitive.

Contents