CS291D Final Report: a Basic Zcash Implementation

Gwyneth Allwright, Karl Wang, Dewei Zeng

December 5, 2020

Abstract

In this project, we attempt a basic implementation of Zerocash [1] in Python. Zerocash is a ledger-based digital currency that makes use of zero-knowledge Succinct Non-Interactive Arguments of Knowledge (zk-SNARKs) to provide stronger privacy guarantees than currencies such as Bitcoin [2] and Zerocoin [3]. This functionality is provided through a decentralized anonymous payment (DAP) scheme that hides a transaction's origin, destination and amount. We follow [1] to implement the following core functions: `Setup`, `CreateAddress`, `Receive`, `Mint`, `VerifyTransaction` and `Pour`, which form the foundations of Zerocash.

Contents

1 Introduction

2 Problem Definition

3 Solution

4 Related Work

5 Evaluation

References

[1] Eli Ben-Sasson et al. "Zerocash: Decentralized Anonymous Payments from Bitcoin". In: *IEEE Symposium on Security and Privacy* (2014), pp. 459–474.

[2] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System.* URL: `https://bitcoin.org/bitcoin.pdf`.

[3] Ian Miers et al. "Zerocoin: Anonymous Distributed E-Cash from Bitcoin". In: *IEEE Symposium on Security and Privacy* (2013), pp. 397–411.