Zero-Knowledge Credentials for Smart Contracts

Lucas Switzer, Tjaden Hess

May 11, 2018

Abstract

Public blockchains present unique opportunities for the implementation of autonomous and trustless systems, but suffer from trade-offs between privacy and expressivity. In this paper we present an implementation of a zkSNARK-based anonymous credential scheme for the Ethereum blockchain and give benchmarks for usage costs. We present as well an example application.

1 Introduction

While blockchains have found use cases in publicly accessible distributed systems, they pose a challenge in that due to their public nature it is currently impossible to attest to aspects of one's identity without some trusted credential issuer.

1.1 Prior Work

A generalized scheme was proposed by Garman et al. [1]

2 Properties and Features

3 Implementation

4 Benchmarks

5 Example Application

6 Future Work

7 Conclusion

References

[1] Christina Garman, Matthew Green, and Ian Miers. Decentralized Anonymous Credentials. URL http://eprint.iacr.org/2013/622.