Intuitive Interpretation of Non-Interactive Zero-Knowledge Cryptography

A jargon-free approach to understanding zk-SNARKs and zk-STARKs

Avneet Singh
Interplanetary Company UG
sshmatrix@proton.me

ABSTRACT

zk-SNARKs and zk-STARKs are relatively new concepts in cryptography, yet they are being touted as the next forefront in modern cryptotech. In blockchain space specifically, there is large interest in these subfields in context of zk-Rollups to Layer 1 blockchains such as Ethereum, or as standalone decentralised ledgers with high rates of transactions per second (TPS), e.g. Aztec Network (zk-STARK), zkSync, Loopring, ZCash (zk-SNARKs) etc. Despite their great importance in cryptography, it is unfortunately difficult to understand zk-SNARKs and zk-STARKs due to limited and jargon-ridden literature. This paper is an attempt to introduce zero-knowledge (zk) cryptography to garden-variety mathematicians, physicists and/or curious developers in an intuitive manner.

INTRODUCTION

REFERENCES

METADATA

Github:
Contracts:
Source:
SHA-1 Checksum:
Date: July 2, 2023