Zerocash

Lars Erik Wik

April 19, 2022

Summary

In Bitcoin, all transactions are broadcasted into a public ledger which can be used in order to prove that the conditions of a transaction are valid. This prevents malicious nodes from executing double spending attacks. But this is at the expense of privacy. Even though transactions are conducted through pseudonyms, transactions can easily be traced, which can reveal the true identity of the users. What if we could instead prove that the conditions of a transaction is valid, but without revealing any information about what addresses or values where involved? Well, this can be done using zero-knowledge proofs.

A zero-knowledge proof is a statement that proves that an entity has some knowledge, without revealing what that knowledge is. For a statement to be a zero knowledge proof, it must have the three following properties:

1. **Completeness**: if the statement is true, a validator will be convinced that the statement is true.

2. **Soundness**: if the statement is false, a validator will be convinced that the statement is false.

3. **Zero-knowledge**: if the statement is true, the verifier does not learn anything other than that the statement is true.

Ben-Sasson et. al. proposes Zerocash, a system that can be deployed as a fork of bitcoin that uses a flavor of zero knowledge proofs called zk-SNARK, in order to anonymize transactions. zk-SNARKS are a special type if zero-knowledge proof in that they allow the verification to happen non-interactively.