Kasper Borgbjerg
kasperib@uio.no

Zerocash

Bitcoin has for long been thought of as being a secure and anonymous form of online payment on the blockchain. However, the anonymity of the protocol is not 100% as there have been developed a lot of analysis tools that are capable of associating identities to different public key addresses. Regardless, the protocol is public, which entails that everyone can download the full ledger and look through the transactions and reveal the sender and recipient addresses, as well as the amount that was transferred. Zerocash is a protocol that uses a consensus known as zero-knowledge proof, which is aimed at making the transactions between the parties secure while keeping the information of the sender, recipient, and amount opaque (zCash 2018).

More specifically, zerocash uses a form of cryptography known as zk-SNARKs, which can assure zero-knowledge privacy. The quirk here is that the consensus must prove the validity of a transaction, without revealing the information of the parameters at which the function was applied – this is done in a non-interactive fashion, where there is a prover and a validator of a transaction, that share a common string that's secure the confidentiality of the parameters of the transactions. This public string essentially secures the privacy of the parameters exchanged in the transaction. To solve this puzzle without revealing any information about the parameters, or the identity of the prover or verifier, the consensus constructs the equivalent of the solution that is to be proven, into an arithmetic circuit that holds this solution; as sort of alias or pseudo computation that can yield the validity of the origin proof.

References:

zCash.com, Research and development(2018), What are zk-SNARKs, accessed 20.4.2022. link

Kasper Borgbjerg
kasperib@uio.no