Z: On Integrating ZCsh on Ethereum

An Abstract

This paper presents Z as a viable and secure protocol for private transactions on Ethereum blockchain.

Zcash, which was created to solve the privacy issue for Bitcoin and other systems like it, had no workable solution for Ethereum, which displays transactions publicly.

A smart contract-based privacy payment which could have resolved this is expensive and does not give total protection.

Z cloaks the transactions and relationships between senders and recipients. Also, funds are uniquely linked to an owner and cannot be double-spent.

As Z is based on Zcash's protocol, it underwent adaptions to resolve the lack of privacy in Ethereum transactions. Users of the Z protocol need not interrogate the blockchain directly to know the state of their contract, which prevents data leakages.

Although Z is still a work in progress with the current version of Ethereum, it promises transaction privacy, has clear guidelines for users of the protocol and works well in consortium, and permissioned chains.