

Zerocash: Decentralized Anonymous Payments from Bitcoin

Eli Ben-Sasson
Technion University

11/12/2014 at 09:30 am
CoRE A (Room 301)

Abstract

Bitcoin is the first digital currency to see widespread adoption. While payments are conducted between pseudonyms, Bitcoin cannot offer strong privacy guarantees: payment transactions are recorded in a public decentralized ledger, from which much information can be deduced. Zerocoin (Miers et al., IEEE S&P 2013) tackles some of these privacy issues by unlinking transactions from the payment's origin. Yet, it still reveals payments' destinations and amounts, and is limited in functionality.

Zerocash – the focus of this talk – is a full-fledged ledger-based digital currency with strong privacy guarantees. It leverages recent advances in zero-knowledge Succinct Non-interactive Arguments of Knowledge (zk-SNARKs).

First, we formulate and construct decentralized anonymous payment schemes (DAP schemes). A DAP scheme enables users to directly pay each other privately: the corresponding transaction hides the payment's origin, destination, and transferred amount. We provide formal definitions and proofs of the construction's security.

Second, we build Zerocash, a practical instantiation of our DAP scheme construction. In Zerocash, transactions are less than 1 kB and take under 6 ms to verify — orders of magnitude more efficient than the less-anonymous Zerocoin and competitive with plain Bitcoin.

Joint work with Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza,

Details at www.zerocash-project.org