Foteini Baldimtsi

foteini@baldimtsi.com
www.baldimtsi.com
@FBaldimtsi

Anonymity in Bitcoin

Tuesday, May 31 2016, 11:30-12:30

Although Bitcoin was initially perceived to be anonymous, research has shown that a user's Bitcoin transactions can be linked to compromise his anonymity. To address this problem, the community has reacted by proposing two key approaches to improve the anonymity of Bitcoin: (1) new anonymity mechanisms that are compatible with Bitcoin, so-called mixing or tumbler services, and (2) new anonymous cryptocurrencies that are independent of Bitcoin. In this talk I will review these approaches along with the required cryptographic primitives and discuss the trade-offs between efficiency and anonymity.

Reading:

- Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, Madars Virza, Zerocash: Decentralized Anonymous Payments from Bitcoin, Proceedings of the IEEE Symposium on Security & Privacy (“Oakland”) 2014.
- Ethan Heilman, Foteini Baldimtsi, Sharon Goldberg, Blindly Signed Contracts: Anonymous On-Blockchain and Off-Blockchain Bitcoin Transactions, BITCOIN Workshop, 2016