Bitcoin's Security Revisited

Aviv Zohar

Hebrew University, Jerusalem

Abstract

The talk will revisit the fundamental question of Bitcoin's security against double spending attacks which was first analyzed by Satoshi in his original work. We will explore different notions of security in this context and the problems that arise with some of them, correct some previous errors in the analysis, and derive tighter results for each notion. If time permits I will also discuss attacks against non-relaying nodes (SPV clients) and show that these can be attacked more easily than their full node counterparts.

Based on joint work with Yonatan Sompolinsky.