Anonymity in the Bitcoin Peer-to-Peer Network

Giulia Fanti, ECE, Carnegie Mellon University

Abstract:

Bitcoin enjoys a public perception of being a privacy-preserving financial system. In reality, Bitcoin has a number of privacy vulnerabilities, including the well-studied fact that transactions can be linked through the public blockchain. More recently, researchers have demonstrated deanonymization attacks that exploit a lower-layer weakness: the Bitcoin peer-to-peer (P2P) networking stack. In particular, the P2P network currently forwards content in a structured way that allows observers to deanonymize users by linking their transactions to the originating IP addresses. In this work, we first demonstrate that current protocols exhibit poor anonymity guarantees, both theoretically and in practice. Then, we consider a first-principles redesign of the P2P network, with the goal of providing strong, provable anonymity guarantees. We propose a simple networking policy called Dandelion, which achieves nearly-optimal anonymity guarantees at minimal cost to the network's utility.

Bio:

Giulia Fanti is an assistant professor of ECE at Carnegie Mellon University, with a focus on privacy-preserving technologies. She obtained her Ph.D. in EECS from U.C. Berkeley, and her B.S. in ECE from Olin College of Engineering in 2010. She is a recipient of the National Science Foundation Graduate Research Fellowship, as well as a Best Paper Award at ACM Sigmetrics 2015 for her work on anonymous rumor spreading, in collaboration with Peter Kairouz, Sewoong Oh and Pramod Viswanath.