AN OVERVIEW OF BLOCKCHAINS' DE-ANONYMIZATION ATTACKS

Andrea Gangemi

Politecnico di Torino

Blockchains became popular in 2009, after the inception of Bitcoin. One important characteristic is their pseudoanonymity: users feel safe when they exchange cryptocurrency because their identity is protected by an address. However, a smart analysis of a blockchain allows to reveal a lot of details that were supposed to be secret. In this talk, we focus on the attacks which have been deployed in the recent years that are based on Machine Learning algorithms. We describe how these attacks can de-anonymize the main blockchains, like Bitcoin, Ethereum or Monero. We discuss how these attacks can be improved and how blockchains are reacting to overcome to the privacy issue.