Simulating Propagation of Cryptocurrency Transactions

Vladimír Veselý, Marek Marcel, Vladimír Jeřábek

Cryptocurrencies are built on decentralized, trustless, peer-to-peer networks maintaining blockchain as the only synchronization point providing ground truth about accounted transactions. Since every peer is broadcasting information about transactions (i.e., relaying it to all its peers apart from the peer from which it receives it), it is hard to tell, which peer is the originator of the transaction. We thoroughly monitor Bitcoin network and collect information about peers and the propagation of blockchain artefacts (e.g., transactions, blocks). We want to create a small framework in OMNeT++, which would be able to generate ad hoc cryptocurrency peer-to-peer networks and simulate transaction propagation with various parameters. We want to compare real-life data from our monitoring infrastructure with the simulation results. The goal would be to answer whether network intelligence is enough to conduct successful correlation attacks on transaction originators.