Abstract

In this paper, we revisit the fundamental question of Bitcoins security against selfish-mine attack introduced by I. Eyal and E. G. Sirer in [5]. We study the state machine of Bitcoin’s network under the influence of one pool miner adopting the selfish mine strategy while the rest of the community following the standard protocol. We prove that the process following by the states of Bitcoin’s system is a irreducible, positive-recurrent, aperiodic, and discrete Markov chain. We give an invariant (stationary) distribution for this Markov chain and deduce easily the rate of convergence towards the stationary equilibrium situation.

References


Index Terms

Computer Science | Security

Keywords

Blockchain, Bitcoin, Security, Miners, Attack, Markov chain