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

1. Andes. Bitcoin’s cryptonite: the 51% attak, 2011.
2. Gavin Andressen. Back-of-the-envelope calculations for marginal cost of transactions, 2014, 03.
3. Christian Decker and Roger Wattenhofer. Information Propagation in the Bitcoin Network. September 2013.
4. Pardoux Etienne. Markov Processes and Applications: Algorithms, Networks, Genome and Finance. Willey series of Probability and Statistic, 2008.
5. Ittay Eyal and Emin G’un Sirer. Majority is not enough: Bitcoin mining is vulnerable. pages 436–454, 2014.
6. Johannes G"obel, Holger Paul Keeler, Anthony E. Krzesinski, and Peter G. Taylor. Bitcoin blockchain dynamics: The selfish-mine strategy in the presence of propagation delay. Perform. Eval., 104:23–41, 2016.
7. Jens Hougaard, Juan Moreno-Ternero, Mich Tvede, and Lars Peter sterdal. Sharing the proceeds from a hierarchical venture. Games and Economic Behavior, 104:23–41, 2016.
8. Nicolas Houy. It will cost you nothing to 'kill' a proof-ofstake crypto-currency, 2014,01.
9. Nicolas Houy. The bitcoin mining game. Ledger, vol. 1:pp. 53–68, 2016.
10. Joshua A. Kroll, Ian C. Davey, and Edward W. Felten. The economics of bitcoin mining, or bitcoin in the presence of adversaries, 2013.
11. Yoad Lewenberg, Yoram Bachrach, Yonatan Sompolinsky, Aviv Zohar, and Jeffrey S. Rosenschein. Bitcoin mining pools: A cooperative game theoretic analysis. In Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems, AAMAS 2015, Istanbul, Turkey, May 4-8, 2015, pages 919–927, 2015.
12. Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Bitcoin.org, 2008.
13. John Von Neumann and Oskar Morgenstern. Theory of Games and Economic Behavior. Princeton University Press, 1944.
14. Meni Rosenfeld. Analysis of bitcoin pooled mining reward systems, 2011.
15. Yonatan Sompolinsky and Aviv Zohar. Bitcoin’s security model revisited. CoRR, abs/1605.09193, 2016.
16. E. Swanson. Bitcoin’s mining calculator, 2013.

**Index Terms**

Computer Science Security

**Keywords**

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