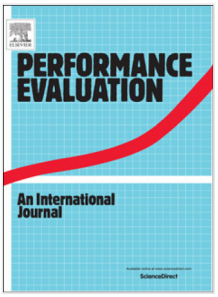
Accepted Manuscript



Bitcoin Blockchain dynamics: The selfish-mine strategy in the presence of propagation delay

J. Göbel, A.E. Krzesinski, H.P. Keeler, P.G. Taylor

PII: S0166-5316(16)30089-X
DOI: http://dx.doi.org/10.1016/j.peva.2016.07.001
Reference: PEVA 1873

To appear in: *Performance Evaluation*

Received date: 8 June 2015
Revised date: 12 July 2016
Accepted date: 13 July 2016

Please cite this article as: J. Göbel, A.E. Krzesinski, H.P. Keeler, P.G. Taylor, Bitcoin Blockchain dynamics: The selfish-mine strategy in the presence of propagation delay, *Performance Evaluation* (2016), http://dx.doi.org/10.1016/j.peva.2016.07.001

Bitcoin Blockchain Dynamics: the Selfish-Mine Strategy in the Presence of Propagation Delay

J. Göbel[a], A.E. Krzesinski[b,*], H.P. Keeler[c], P.G. Taylor[c]

[a] *Department of Informatics, University of Hamburg, 22527 Hamburg, Germany*
[b] *Department of Mathematical Sciences, Stellenbosch University, 7600 Stellenbosch, South Africa*
[c] *Department of Mathematics and Statistics, University of Melbourne, Vic 3010, Australia*

Abstract

In the context of the 'selfish-mine' strategy proposed by Eyal and Sirer, we study the effect of communication delay on the evolution of the Bitcoin blockchain. First, we use a simplified Markov model that tracks the contrasting states of belief about the blockchain of a small pool of dishonest miners and the 'rest of the community' to establish that the use of block-hiding strategies, such as selfish-mine, causes the rate of production of orphan blocks to increase. Then we use a spatial Poisson process model to study values of Eyal and Sirer's parameter γ, which denotes the proportion of the honest community that mines on a previously-secret block released by the pool in response to the mining of a block by the honest community. Finally, we use discrete-event simulation to study the behaviour of a network of Bitcoin miners, a proportion of which is colluding in using the selfish-mine strategy, under the assumption that there is a delay in the communication of information between miners. The models indicate that both the dishonest and the honest miners were worse off than they would have been if no dishonest mining was present, and that it is possible for the mining community to detect block-hiding behaviour, such as that used in selfish-mine, by monitoring the rate of production of orphan blocks.

Keywords:
Bitcoin, blockchain, block hiding strategies, honest mining, selfish-mine.

1. Introduction

Bitcoin is a peer to peer electronic payment system in which transactions are performed without the need for a central clearing agency to authorize transactions. Bitcoin users conduct transactions by transmitting electronic messages which identify who is to be debited, who is to be credited, and where the change (if any) is to be deposited.

*Corresponding author
Email addresses: goebel@informatik.uni-hamburg.de (J. Göbel), aek1@cs.sun.ac.za (A.E. Krzesinski), keeler@unimelb.edu.au (H.P. Keeler), taylorpg@unimelb.edu.au (P.G. Taylor)