

An Economic Analysis of Difficulty Adjustment Algorithms in Proof-of-Work Blockchain Systems*

Shunya Noda[†] Kyohei Okumura[‡] Yoshinori Hashimoto[§]

First Draft: June 26, 2019; Current Draft: January 30, 2020

Abstract

The design of the *difficulty adjustment algorithm* (DAA) of the Bitcoin system is vulnerable as it dismisses miners' response to the difficulty adjustment. We develop an economic model of the Proof-of-Work based blockchain system. Our model allows miners to pause operation when the expected reward is below the shutdown point. Hence, the supply of aggregate hash power can be elastic in the cryptocurrency price and the difficulty target of the mining puzzle. We prove that, when the hash supply is elastic, the Bitcoin DAA fails to adjust the block arrival rate to the targeted level. In contrast, the DAA of another blockchain system, Bitcoin Cash, is shown to be stable even when the cryptocurrency price is volatile and the supply of hash power is highly elastic. We also provide empirical evidence and simulation results supporting the model's prediction. Our results indicate that the current Bitcoin system might collapse if a sharp price reduction lowers the reward for mining denominated in fiat money. However, this crisis can be prevented through the upgrading of DAA.

JEL Codes: C61, D47, G20, L86

Keywords: Blockchain, Proof-of-Work, Difficulty Adjustment, Mining, Market Design

*This paper was previously titled as "A Lucas Critique to the Difficulty Adjustment Algorithm of the Bitcoin System." We are grateful to Shumpei Goke, Shota Ichihashi, Fuhito Kojima, Hitoshi Matsushima, Daisuke Oyama, Takuo Sugaya, and all the seminar participants in the University of British Columbia, the University of Tokyo, Waseda University, the Scaling Bitcoin Workshop 2019 at Tel Aviv, and Otaru University of Commerce for helpful comments. All remaining errors are our own.

[†]Contact Author. Vancouver School of Economics, University of British Columbia, 6000 Iona Dr, Vancouver, BC V6T 1L4 Canada. E-mail: shunya.noda@gmail.com Noda has been supported by the Funai Overseas Scholarship and the E. K. Potter fellowship.

[‡]Graduate School of Economics, University of Tokyo, 7-3-1, Hongo, Bunkyo-ku, Tokyo 113-0033, Japan. E-mail: kyohei.okumura@gmail.com

[§]BUIDL, Ltd., Neutrino, 12-10, Sakuragaoka, Shibuya-ku, Tokyo-to, 150-0031, Japan. E-mail: yoshi.h@buidl.jp The opinions expressed in this article are Hashimoto's own and do not reflect the view of BUIDL, Ltd.