Mechanism Design with Blockchain Enforcement*

Hitoshi Matsushima† Shunya Noda‡

A Preliminary Draft. Still Updating.

Abstract

We study the design of self-enforcing mechanisms that rely on neither the trusted third parties (e.g., the court) nor the long-term relationship between participants. Instead, we use a smart contract written on blockchains as a commitment device. We design a *judgment mechanism* that identifies and punishes agents who did not take actions specified by the agreement. The judgment mechanism substitutes the role of the court in traditional mechanisms. We show that any social choice function that is implementable with court enforcement can also be implemented with enforcement by the judgment mechanism. As our judgment mechanism can be used for implementing general social choice functions, it does not leak the detailed information about the agreement even if it is written on a public blockchain (e.g., Ethereum) as a smart contract.

JEL Codes: D47, D82, L86

Keywords: Implementation, Decentralized Mechanism, Privacy, Oracle Problem, Self-Judgment

*We are grateful to Shumpei Goke, Yoshinori Hashimoto, and Kyohei Okumura for helpful comments. All remaining errors are our own.

†Department of Economics, University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo 113-0033, Japan. E-mail: hitoshi@e.u-tokyo.ac.jp.

‡Vancouver School of Economics, University of British Columbia, 6000 Iona Dr, Vancouver, BC V6T 1L4, Canada. E-mail: shunya.noda@gmail.com