Blockchain Disables Real-World Governance

By

Hitoshi Matsushima (University of Tokyo)

May 2019

CREPE DISCUSSION PAPER NO. 55

CENTER FOR RESEARCH AND EDUCATION FOR POLICY EVALUATION (CREPE)
THE UNIVERSITY OF TOKYO
http://www.crepe.e.u-tokyo.ac.jp/

Blockchain Disables Real-World Governance

Hitoshi Matsushima*
University of Tokyo

May 31, 2019

Abstract

This study indicates that the improper uses of a public blockchain disable real-world governance in organizations and marketplaces. By using any basic application of smart contracts, such as escrow transactions, along with a revelation mechanism outside the blockchain, individuals can execute illegal cartel acts in a self-enforcing and non-judicial manner. Cartel members can then implement collective deviations without help from trusted intermediaries or any requirements on reputation or word-of-honor. We show that a first price auction is vulnerable to cartel threats even if the seller can hide bidders' prices because bidders take a countermeasure to hidden prices by using blockchain.

Keywords: Blockchain, Smart Contract, Cartelization, Economic Governance, Non-Judicial Mechanism, Implementation
JEL Classification: D44, D82, D86, G20, L86

* Department of Economics, University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo 113-0033, Japan. E-mail: hitoshi@e.u-tokyo.ac.jp
This study was financially supported by a grant-in-aid for scientific research (KAKENHI 25285059) from the Japan Society for the Promotion of Science (JSPS) and the Ministry of Education, Culture, Sports, Science, and Technology (MEXT), Japan, as well as by the Center of Advanced Research in Finance (CARF) at the University of Tokyo. I am grateful to Shunya Noda and the participants to the study sessions hosted by Auction and Market Design Forum (AMF, University of Tokyo) in January and February 2019 for their useful comments. All remaining errors are mine.

This study indicates that improper uses of blockchain disables real-world governance. By using smart contracts such as escrow transactions, anyone can execute an inherently illegal cartel act without making others aware of its illegality because recordkeepers can add a transaction to the ledger without considering its purpose.

This contrasts with the case without blockchain. To create a cartel without using a blockchain, economic agents will delegate the execution of their agreements to an outside intermediary. Then, the intermediary opens an escrow account in their names and each agent makes deposits to this account. The agents subsequently design a revelation mechanism to reach consensus on how to redistribute the escrow deposits in a state-contingent and self-enforcing manner. Accordingly, the intermediary finally executes the redistribution. Here, it is essential that the intermediary is a trusted person, because there exists the risk of appropriating the escrow deposits. However, a trusted person might refuse to be involved in illegal activities, declining the request of delegation whenever the purpose is determined to be illegal, because he/she dislikes reputation loss.

Once a blockchain becomes available, agents can execute agreements regardless of their legality and without help from trusted intermediaries. The blockchain plays the role of a platform in executing the escrow and redistributing the escrow deposits, keeping the purpose secret from the public. As such, when a blockchain can be used without restrictions, any real-world scheme must be robust against cartel deviations, as well as unilateral deviations. This dramatically narrows the availability of contract and market design.

A blockchain is a new ledger technology that records safely various transactions and data, has low transaction costs, and no risk of double-spending or tampering. Blockchains have become known as a foundation supporting cryptocurrencies such as Bitcoin (Böhme et al., 2015; Nakamoto, 2008). Currently, blockchains are expected to serve as platforms for individuals to freely create and execute a wide variety of smart contracts (Cong and He, 2017; Narayanan et al., 2016).

A blockchain is expected to remain *public*, so that it is not exclusively or privately ruled by anyone. A public blockchain should be maintained by an unspecified number of distributed recordkeepers, who are untrusted and do not thus pay attention to own reputations. As such, game-theoretic considerations as to how distributed recordkeepers

are motivated to reach consensus on the validity of transactions have drawn significant attention. Therefore, various incentive schemes for recordkeepers to maintain public blockchains, such as proof-of-work (Abadi and Brunnermeier, 2018; Biais et al., 2019; Budish, 2018; Huberman et al., 2017), proof-of-stake (Saleh, 2018), proof-of-importance, among others, are being developed and considered.

Conversely, this study focuses on blockchain *user* incentives instead of recordkeeper incentives and clarifies the impact of smart contracts on real-world governance from a game-theoretic viewpoint. In this respect, the study of Cong and He (2017) is related to this one, in that they argued that, to execute a smart contract as precisely as possible, economic agents need to disclose a lot of information to the public that should be kept secret. They pointed out that this disclosure can be a serious factor in disrupting industrial organizations.

Contrary to their claim, this study demonstrates that individuals can execute various smart contracts in a self-enforcing manner even if they do not disclose information about the content of their businesses. Specifically, instead of creating a smart contract that details a state-contingent transaction, economic agents can design an incentive-compatible revelation mechanism outside the blockchain, through which they reach a consensus on how to make side-payments. More importantly, without help from trusted intermediaries, they can enforce this consensus by using basic smart contract applications such as *escrow transactions* in a complementary manner to real-world revelation mechanisms. This simple implementation is a serious threat to governance.

In this context, this study provides a new perspective to the theory of organizations. Specifically, the enforcement of a cartel agreement generally relies on *non-judicial* mechanisms. Tirole (1992) listed reputation (long-term relationship) and word-of-honor (one-shot relationship) as representatives. This study presents blockchain as the third non-judicial mechanism, being considered a more serious threat to real-world governance than reputation or word-of-honor.

In auction theory, a first price auction has been considered robust against cartelization (bidding ring), because, unlike second price auction, a cartel agreement in the former is generally not self-enforcing (Krishna, 2009; McAfee and McMillan, 1992). However, this study shows that, once a blockchain becomes available, even first price auctions are exposed to cartel threats. We further consider a seller's measure to prevent

cartels by hiding bids even after the end of auction and the bidders' countermeasure to defeat the seller's measure by using blockchain; we show that the first price auction is still vulnerable to cartel threats.

The rest of this paper is organized as follows. The following section presents the basic model according to which, using blockchain, any state-contingent side-payment (target function) becomes implementable in the non-judicial manner. The subsequent section considers incentives in organizations as an application. Subsection A shows an example in that the *rank-order tournament* is vulnerable to cartel deviations. Subsection B shows that the prevention of cartel deviations is generally a substantial constraint. We then discuss the methods of designing incentive schemes robust against cartel deviations as well as unilateral deviations by introducing *direct monitoring*. The following section considers auction as another application. We focus on the first price auction, because it has been considered robust against bidding ring. We show that even a first price auction is vulnerable to bidding ring once a blockchain becomes available. Subsection C provides a new perspective on strategic aspects, where, making use of cryptography, the seller hides bidders' prices to prevent cartels even after the end of auction, while the bidders seek countermeasures to share information about their prices. We show that the first price auction is still vulnerable to cartelization even if the seller can hide bidders' prices. The final section concludes the paper.

I. Basic Model

We consider the situation in which $n \geq 2$ players make side payments $t = (t_i)_{i \in N} \in R^n$ in the following state-contingent manner. Each player $i \in N = \{1, ..., n\}$ observes his/her private signal $\omega_i \in \Omega_i$, where Ω_i denotes the set of possible private signals for player i. A profile of private signals $\omega = (\omega_i)_{i \in N} \in \underset{i \in n}{\times} \Omega_i$ is determined stochastically according to a probability distribution $p : \underset{i \in n}{\times} \Omega_i \to R_+$. We define *state space* $\Omega \subset \underset{i \in N}{\times} \Omega_i$ as its support, where for each $\omega \in \underset{i \in n}{\times} \Omega_i$,

$$[\omega \in \Omega] \Leftrightarrow [p(\omega) > 0].$$

The payoff of player $i \in N$ is quasi-linear, given by $u_i(\omega) + t_i$.

A *target function* is defined as $f = (f_i)_{i \in N} : \Omega \to R^n$, according to which each player i receives monetary amount $t_i = f_i(\omega) \in R$ at each state $\omega \in \Omega$. We assume *budget balancing* so that

$$\sum_{i \in N} f_i(\omega) = 0 \quad \text{for all} \quad \omega \in \Omega.$$

To realize a target function f, players make a self-enforcing agreement by designing a *direct mechanism* $x = (x_i)_{i \in N}$, where $x_i : \underset{j \in N}{\times} \Omega_j \to R$. According to x, each player i announces message $m_i \in \Omega_i$ and receives monetary amount $x_i(m) \in R$, where $m = (m_i)_{i \in N} \in \underset{i \in N}{\times} \Omega_i$.

A direct mechanism x is said to *implement a target function* f if

$$x(\omega) = f(\omega) \quad \text{for all} \quad \omega \in \Omega,$$

and it is incentive compatible in that truth-telling is a Bayesian Nash equilibrium, that is, for every $i \in N$, $\omega_i \in \Omega_i$, and $m_i \in \Omega_i$,

$$E[u_i(\omega) + x_i(\omega) \mid \omega_i] \geq E[u_i(\omega) + x_i(m_i, \omega_{-i}) \mid \omega_i],$$

or equivalently,

$$E[x_i(\omega) \mid \omega_i] \geq E[x_i(m_i, \omega_{-i}) \mid \omega_i],$$

where $E[\cdot \mid \omega_i]$ denotes the expectation operator conditional on ω_i. Fix an arbitrary non-negative vector $k = (k_i)_{i \in N} \in R^n$, which is set sufficiently large so that

$$k_i \geq \max[-\min_{\omega \in \Omega} f_i(\omega), 0] \quad \text{for all} \quad i \in N.$$

We specify a direct mechanism $x = x^k$ so that

$$x(m) = f(m) \qquad \text{if players reach } \textit{consensus}, \text{ that is, } m \in \Omega,$$

and

$$x(m) = -k \qquad \text{if players fail to reach consensus, that is, } m \notin \Omega.$$

Proposition 1: *A target function f is implementable if and only if for every $i \in N$, $\omega_i \in \Omega_i$, and $m_i \in \Omega_i$,*

$$[[\omega \in \Omega] \Rightarrow [(m_i, \omega_{-i}) \in \Omega] \text{ for all } \omega_{-i} \in \underset{j \in N \setminus \{i\}}{\times} \Omega_j]$$

$$\Rightarrow [E[f_i(\omega) \mid \omega_i] \geq E[f_i(m_i, \omega_{-i}) \mid \omega_i]].$$

If f is implementable, there exists $\hat{k} \in R^n$ such that for every $k \geq \hat{k}$, associated direct mechanism $x = x^k$ implements f.

Proof: Consider arbitrary $i \in N$ and $\omega_i \in \Omega_i$. Suppose that, for every $\omega_{-i} \in \underset{j \in N \setminus \{i\}}{\times} \Omega_j$,

$$[\omega \in \Omega] \Rightarrow [(m_i, \omega_{-i}) \in \Omega].$$

Then, for every $\omega_{-i} \in \underset{j \in N \setminus \{i\}}{\times} \Omega_j$, whenever $\omega \in \Omega$, then

$$x_i(\omega) = f_i(\omega) \quad \text{and} \quad x_i(m_i, \omega_{-i}) = f_i(m_i, \omega_{-i}).$$

Hence,

$$E[x_i(\omega) \mid \omega_i] = E[f_i(\omega) \mid \omega_i]$$

$$\geq E[f_i(m_i, \omega_{-i}) \mid \omega_i] = E[x_i(m_i, \omega_{-i}) \mid \omega_i],$$

where $x = x^k$.

Suppose that there exists $\omega_{-i} \in \underset{j \in N \setminus \{i\}}{\times} \Omega_j$ such that

$$\omega \in \Omega, \text{ but } (m_i, \omega_{-i}) \notin \Omega.$$

The probability that such ω_{-i} occurs conditional on ω_i, denoted by q, is positive. Hence, by selecting a sufficiently large k_i,

$$E[x_i(m_i, \omega_{-i}) \mid \omega_i] \leq (1-q) \max f(\omega) - qk_i$$

$$\leq E[f_i(\omega) \mid \omega_i] = E[x_i(\omega) \mid \omega_i].$$

Q.E.D.

Remark: Our concern is different from previous works in mechanism design such as Vickrey (1961), Groves (1973), d'Aspremont and Gerard-Varet (1979), Myerson (1981), and Myerson and Satterthwaite (1983), which investigated implementation of allocations by adding side-payments. This study investigates implementation of side-payments without adding side-payments on the equilibrium path.

As a special case, we consider *complete information regarding the state*, where

$$\Omega_i = \Omega_1 \quad \text{for all} \quad i \in N,$$

and

$$[\omega \in \Omega] \Leftrightarrow [\omega_i = \omega_1 \quad \text{for all} \quad i \in N].$$

We denote $\Omega_i = \Omega$ and $\omega_i = \omega$. Note that a direct mechanism x is incentive compatible if and only if truth-telling is a Nash equilibrium, that is, for every $\omega \in \Omega$, $i \in N$, and $m_i \in \Omega_i$,

$$u_i(\omega) + x_i(\omega) \geq u_i(\omega) + x_i(m_i, \omega_{-i}),$$

or equivalently,

$$x_i(\omega) \geq x_i(m_i, \omega_{-i}).$$

Since this property is independent of state, we have *multiplicity* under complete information regarding the state, in that whenever a message profile is a Nash equilibrium at a state, then it is also a Nash equilibrium at every state. The following proposition states that under complete information regarding the state, we need no additional liability.

Proposition 2: *Assume minimal liability in that for every* $i \in N$,

$$k_i = \max[-\min_{\omega \in \Omega} f_i(\omega), 0].$$

Under complete information regarding the state, the specified direct mechanism $x = x^k$ *is incentive compatible and implements* f.

Proof: From complete information regarding the state, for every $\omega \in \Omega$, $i \in N$, and $m_i \neq \omega$,

$$x_i(\omega) = f_i(\omega) \geq \min_{\tilde{\omega} \in \Omega} f_i(\tilde{\omega})$$

$$\geq -\max[-\min_{\tilde{\omega} \in \Omega} f_i(\tilde{\omega}), 0] = -k_i = x_i(m_i, \omega_{-i}),$$

implying Nash equilibrium.

Q.E.D.

Importantly, by using a blockchain and even without legal procedures, players can carry out a direct mechanism $x = x^k$ that implements the target function f. Players

broadcast an escrow transaction to the blockchain and get recordkeepers to validate this transaction and add it to the blockchain ledger, where each player i deposits a monetary amount $e_i \geq 0$ to escrow by converting it to cryptocurrencies. Due to cryptography, nobody can tamper with this transaction or intercept the escrow deposits. Further, no one else knows the purpose of this escrow.

After the escrow transaction is validated, each player i announces message $m_i \in \Omega_i$ to the others outside the blockchain. If players reach consensus, that is, $m \in \Omega$, they create a *redistribution transaction* outside the blockchain, according to which each player i can receive $e_i + f_i(m)$ from escrow. They sign this transaction and then broadcast it to the blockchain. Importantly, the redistribution transaction can be validated and added to the blockchain *only if* players all sign it. Otherwise, the escrow deposits $e = (e_i)_{i \in N}$ remain frozen; each player receives no payment. Nobody can tamper with this redistribution. Nobody else knows its purpose. Players need no trusted intermediary. However, to incentivize them to sign the redistribution transaction, the escrow deposits must satisfy that for every $i \in N$,

$$e_i + f_i(m) \geq 0 \quad \text{for all} \quad m \in \Omega,$$

that is,

$$e_i \geq \max[-\min_{\omega \in \Omega} f_i(\omega), 0]. \tag{1}$$

If players fail to reach consensus, that is, $m \notin \Omega$, they can make no agreement on how to redistribute the escrow deposits. In this case, the escrow deposits remain frozen, and each player thus receives no payment.

Consider a direct mechanism $x = x^k$ that is incentive compatible and implements f. Importantly, the broadcasts of escrow and redistribution transactions carry out the side-payments implied by $x = x^k$. Each player i deposits to the escrow the monetary amount $e_i = k_i$, implying constraint (1). If players reach consensus, they broadcast the redistribution transaction; each player i therefore receives

$$e_i + f_i(m) = e_i + x_i(m).$$

If players fail to reach consensus, they broadcast no redistribution transaction; each player i receives no payment, that is,

$$0 = e_i - k_i = e_i + x_i(m).$$

Hence, we can conclude that *the blockchain carries out any implementable target function without legal procedures.*

Remark: We assumed that, whenever players fail to reach consensus, the escrow deposits remain frozen. However, without any substantial change, we can permit players to use the same direct mechanism $x = x^k$ to reach consensus again. They keep using it without returning to the steps of primordial bargaining such as the demand game (Nash, 1953) or sequential bargaining (Rubinstein, 1982), until they succeed in reaching consensus. This repetition, along with the budget-balancing nature of f, guarantees the renegotiation-proofness of implementation.

Because of the openness of blockchains, the public can freely observe broadcasted escrow and redistribution transactions. However, the public cannot confirm the purpose of these transactions because players do not contain any information to support their purpose. Hence, recordkeepers cannot confirm whether transactions are for buying used cars, buying illegal drugs, or another purpose. Moreover, recordkeepers are untrusted persons and pay no attention to the purpose of broadcasted transactions even if they can get information from outside the blockchain. Therefore, in circumvention of the law, individuals can utilize the blockchain not only for purchasing goods, but also for forming illegal cartels that destroy various incentive devices in the real world.

II. Collusion in Organizations

This section and the next one present two applications of blockchain, that is, collusion in organization and bidding ring in auction, respectively, showing that improper uses of blockchain disable real-world governance. We assume complete information regarding the state, although the specification of the state space depends on the context.

A. Rank-Order Tournament

Consider a situation in which an employer makes wage contracts with n employees (players) according to a *rank-order tournament*. The employer pays monetary amount $w_h \geq 0$ to the employee whose achievement is the h-th highest, where $w_1 > w_2 > \cdots > w_n$. The state space is specified as equivalent to the set of all permutations on N. We denote by $\omega(i) \in \{1,...,n\}$ the rank of employee $i's$ achievement at state $\omega \in \Omega$. The payoff of employee i at state ω is given by $w_{\omega(i)} + t_i$.

We specify f as

$$f_i(\omega) = \frac{\sum_{j \in N} w_j}{n} - w_{\omega(i)} \quad \text{for all} \quad i \in N.$$

This specification makes each employee $i's$ payoff $w_{\omega(i)} + f_i(\omega)$ equal to constant value $\frac{\sum_{j \in N} w_j}{n}$, irrespective of his/her achievement's rank. This equalization completely negates the incentive effect of rank-order tournament.

B. Direct Monitoring

We generalize Subsection A and demonstrate a method of designing reward schemes to overcome cartel threats. Each employee $i \in N$ simultaneously selects an action (effort) $a_i \in A_i$ ex-ante, where A_i is a finite set of actions of employee i. Let $A = \underset{i \in N}{\times} A_i$. Let $a = (a_i)_{i \in N} \in A$ denote an action profile. After an action profile $a \in A$ is selected, state $\omega \in \Omega$ is stochastically determined according to conditional probability distribution $p(\cdot \mid a) : \Omega \to R_+$. Each employee $i's$ payoff is given by $U_i(a) + t_i$. We express $U_i(a)$ as

$$U_i(a) = E[u_i(\omega) \mid a] - c_i(a_i),$$

where $c_i(a_i)$ denotes the cost of making action choice a_i, $u_i(\omega)$ the state-contingent monetary reward from the employer to employee i, and $E[\cdot \mid a]$ the expectation operator conditional on $a \in A$. An action profile $a \in A$ is said to be a *Nash equilibrium in the game with target function* f if for every $i \in N$ and $a_i' \in A_i$,

$$U_i(a) + E[f_i(\omega) \mid a] \geq U_i(a_i', a_{-i}) + E[f_i(\omega) \mid a_i', a_{-i}].$$

Fix an arbitrary Nash equilibrium $a^* \in A$ in the game *without* target function, where

$$U_i(a^*) \geq U_i(a_i, a_{-i}^*) \quad \text{for all} \quad i \in N \quad \text{and} \quad a_i \in A_i.$$

Assume that the fixed action profile a^* does not maximize employees' total surplus. Consider an arbitrary action profile $a \in A$ that is better than a^* in total surplus, that is,

$$\sum_{i \in N} U_i(a) > \sum_{i \in N} U_i(a^*).$$

Let α_i denote a *mixed* action for employee i and let Δ_i denote the set of all mixed actions for employee i. Let $\Delta = \underset{i \in N}{\times} \Delta_i$ and $\alpha = (\alpha_i)_{i \in N} \in \Delta$. According to Legros and Matsushima (1991), with finiteness of state space, there exists target function f so that action profile a is a Nash equilibrium in the game with f and is preferred to the play without f by all employees, that is,

$$U_i(a) + \sum_{\omega \in \Omega} f_i(\omega) p(\omega \mid a) > U_i(a^*) \quad \text{for all} \quad i \in N,$$

if and only if for every $\alpha \in \Delta$,

$$[\, p(\cdot \mid \alpha_i, a_{-i}) = p(\cdot \mid \alpha_1, a_{-1}) \quad \text{for all} \quad i \in N \,] \Rightarrow [\, \sum_{i \in N} U_i(a) \geq \sum_{i \in N} U_i(\alpha_i, a_{-i}) \,].$$

This condition *generically* holds in the space of conditional probability distributions, provided the size of state space is sufficient.

Hence, to overcome cartel threats, we should consider methods of designing reward schemes that ensure that action profile a^* maximizes total surplus, that is,

$$\sum_{i \in N} U_i(a^*) = \max_{a \in A} \sum_{i \in N} U_i(a).$$

We demonstrate *direct monitoring* as an example of such a method. For each $i \in N$, we introduce a partition on the state space, denoted by Ξ_i. A generic element of Ξ_i is denoted by $\theta_i \subset \Omega$. We assume that $p(\theta_i \mid a) \equiv \sum_{\omega \in \theta_i} p_i(\omega \mid a)$ depends *only* on a_i. We thus write $p(\theta_i \mid a_i)$ instead of $p(\theta_i \mid a)$. An interpretation is that each employee $i's$ action choice a_i is directly, but imperfectly, monitored by the employer through the observation of θ_i. Further assume that the monetary reward from the employer to each

employee i is contingent *only* on θ_i. We thus write $u_i(\theta_i)$ instead of $u_i(\omega)$.

Proposition 3: *With direct monitoring, action profile* a^* *maximizes the employees' total surplus.*

Proof: From the Nash equilibrium property of a^*, we have

$$\max_{a' \in A} \sum_{i \in N} U_i(a') = \max_{a' \in A} \sum_{i \in N} \{E[u_i(\omega) \mid a'] - c_i(a_i')\}$$

$$= \max_{a' \in A} \sum_{i \in N} \{E[u_i(\theta_i) \mid a_i'] - c_i(a_i')\}$$

$$= \sum_{i \in N} \max_{a_i' \in A_i} \{E[u_i(\theta_i) \mid a_i'] - c_i(a_i')\} = \sum_{i \in N} U_i(a^*).$$

Q.E.D.

From Proposition 3, Nash equilibrium a^* without target function is robust against cartel deviations. Hence, with direct monitoring, the incentive constraints on unilateral deviations automatically guarantee the incentive constraints on cartel deviations.

III. Bidding Ring

This section investigates a *first price auction*, which is known to be robust against bidding rings because of its sealed-bid and pay-as-bid nature. We, however, show that once a blockchain becomes available, even the first price auction turns out to be vulnerable to bidding ring; bidders can carry out their cartel agreement without being disturbed by the law.

A. Example: Common Value

Consider a situation in which a single commodity is sold to some of n bidders (players) by using a first price auction with reserve price $\underline{v} \geq 0$. Each bidder $i \in N$ submits price $b_i \geq 0$. The bidder whose price is highest and not less than reserve price

$\underline{v}$ wins the commodity and pays the winning bid (the first price). If all bids are below $\underline{v}$, the commodity remains unsold. We assume complete information regarding their valuations. We also assume they have a *common value* $v > \underline{v}$. Without bidding ring, the only Nash equilibrium is for every bidder i to submit $b_i = v$ equally; the seller can extract the full surplus. This example does not assume that bidders' prices are observable to each other. In this scenario, we permit the seller to hide bidders' prices by using cryptography.

The state space is specified as $\Omega = N \bigcup \{0\}$, where $\omega = i \in N$ implies that bidder i is the winner and $\omega_i = 0$ that the commodity remains unsold. We specify f so that

$$f_i(\omega) = 0 \quad \text{for all} \quad i \in N \qquad \text{if} \quad \omega = 0,$$

and for every $i \in N$,

$$f_i(\omega) = -\frac{n-1}{n}(v - \underline{v}) \quad \text{and} \quad f_j(\omega) = \frac{v - \underline{v}}{n} \quad \text{for all} \quad j \in N \setminus \{i\}$$

$$\text{if} \quad \omega = i.$$

According to f, a loser's payoff is equal to $\frac{v - \underline{v}}{n}$, while the winner's payoff is equal to $v - b - \frac{n-1}{n}(v - \underline{v})$, the winner's bid being denoted by $b \geq \underline{v}$. Hence, with establishment of bidding ring associated with f, the only Nash equilibrium is for every bidder to make his/her price equal to reserve price $\underline{v}$; the seller fails to extract full surplus because of $v > \underline{v}$. If the seller sets reserve price $\underline{v}$ equal to zero, he/she gains nothing from the auction. Hence, with blockchain, the first price auction with reserve price $\underline{v}$ becomes practically the same as posted price $\underline{v}$.

B. Incomplete Information Regarding Valuations

This subsection considers the first price auction under *incomplete information regarding bidders' valuations*. Each bidder $i's$ valuation v_i is randomly and independently drawn according to the *uniform* distribution on interval $[0,1]$. We assume no reserve price, that is, $\underline{v} = 0$. We make these assumptions for simplicity.

A strategy for each bidder $i \in N$ is defined as $\tilde{b}_i : [0,1] \to [0,1]$; the bidder submits price $b_i = \tilde{b}_i(v_i) \in [0,1]$ when his/her valuation is given by $v_i \in [0,1]$. With no blockchain, it is a Nash equilibrium for each bidder i to make a price bid according to

$$\tilde{b}_i(v_i) = \frac{n-1}{n} v_i \quad \text{for all} \quad v_i \in [0,1].$$

Because of the presence of information rents, the seller cannot extract the full surplus. However, the seller can receive a sufficiently large gain. In fact, he/she can almost obtain the full surplus provided the number of bidders n is sufficient.

However, by broadcasting escrow and redistribution transactions on the blockchain, bidders can collectively extract the almost full surplus irrespective of n, even under incomplete information regarding valuations; in this scenario, the seller receives almost no gain from the auction.

Fix an arbitrary $l \in (0, \frac{n-1}{n}]$. We specify strategy $\tilde{b}_i$ for each bidder i by

$$\tilde{b}_i(v_i) = l v_i \quad \text{for all} \quad v_i \in [0,1].$$

We specify a state as a profile of bidders' prices, that is, $\omega = b = (b_i)_{i \in N} \in \Omega$, where $\Omega \equiv [0,1]^n$. We assume complete information regarding the state, but incomplete information regarding valuations.

We fix an arbitrary $k > 0$ and specify f by

$$f_i(b) = -(n-1)k b_i \quad \text{if bidder } i \text{ is the winner}$$

and

$$f_i(b) = k \max_{j \in N} b_j \quad \text{if bidder } i \text{ is a loser.}$$

According to specified f, each bidder $i's$ payoff is given by

$$v_i - b_i - (n-1)k b_i \quad \text{if he/she is the winner}$$

and

$$k \max_{j \in N} b_j \quad \text{if he/she is a loser.}$$

Proposition 4: *Assume*

$$k = \frac{n(1-l)-1}{l(n^2-1)}.$$

Then, specified strategy profile $\tilde{b}$ *is a Bayesian Nash equilibrium in the first price auction associated with specified target function* f.

Proof: By submitting $l\hat{v}_i$ instead of $\tilde{b}_i(v_i) = lv_i$, bidder i with valuation v_i receives expected payoff

$$\int_{\hat{v}_i}^{1} klwdw^{n-1} + \hat{v}_i^{n-1}\{v_i - l\hat{v}_i - (n-1)kl\hat{v}_i\}.$$

We derive the first-order condition in terms of $\hat{v}_i$ at $\hat{v}_i = v_i$ as

$$-(n-1)kl + (n-1)[1 - l\{1 + (n-1)k\}] - l\{1 + (n-1)k\} = 0,$$

or equivalently,

$$k = \frac{n(1-l)-1}{l(n^2-1)}.$$

The second-order condition holds in this case.

Q.E.D.

From Proposition 4, the winner's payoff is given by

$$\{1 - l - (n-1)kl\} \max_{i \in N} v_i = \frac{2-l}{n+1} \max_{i \in N} v_i,$$

while the loser's payoff is given by

$$kl \max_{i \in N} v_i = \frac{n(1-l)-1}{n^2-1} \max_{i \in N} v_i,$$

which is less than the winner's payoff. By selecting $l > 0$ as positive but close to zero, the winner's and loser's payoffs are approximated by

$$\frac{2}{n+1} \max_{i \in N} v_i \quad \text{and} \quad \frac{1}{n+1} \max_{i \in N} v_i,$$

respectively. The bidders' total surplus is approximated by

$$\frac{2}{n+1} \max_{i \in N} v_i + (n-1)\frac{1}{n+1} \max_{i \in N} v_i = \max_{i \in N} v_i.$$

Hence, even under incomplete information regarding valuations, by using blockchain, bidders can almost extract the full surplus, while the seller receives almost nothing, from

the first price auction.

C. Hidden Prices

Apart from informational incompleteness regarding valuations, there exists a difference between Subsections A and B. Subsection A did not assume that each bidder is informed of submitted prices, while Subsection B assumed each bidder is informed of them.

To prevent a bidding ring, the seller designs a sophisticated smart contract so that any bidder's submitted price (even the winner's) is not disclosed to the other bidders even after the end of auction. Issues that are related to this, but just outside the blockchain, have been identified by Ashenfelter (1989) and Akbarpour and Li (2018). In contrast, this subsection considers the possibility that bidders seek a countermeasure to share information about their submitted prices by designing a smart contract.

We modify Subsection B by assuming that each bidder cannot observe the other bidders' submitted prices even after the end of auction. We modify the specifications of the target function, mechanism, and strategy profile, as follows. Each bidder $i \in N$ selects two prices at the same time, that is, $b_i \in [0,1]$ and $d_i \in [0,1]$. His/her strategy is defined as $(\tilde{b}_i, \tilde{d}_i)$, where $\tilde{b}_i : [0,1] \to [0,1]$ and $\tilde{d}_i : [0,1] \to [0,1]$. According to $(\tilde{b}_i, \tilde{d}_i)$, bidder i with valuation v_i submits price $b_i = \tilde{b}_i(v_i)$ to the auction. Bidder i also determines $d_i = \tilde{d}_i(v_i)$, but, by using cryptography, he/she will keep it secret until the end of auction. The other bidders can observe $d_i = \tilde{d}_i(v_i)$ after the end of auction.

In this scenario, a state is specified as $\omega = (d, i) \in [0,1]^n \times N$, where $d = (d_j)_{j \in N}$ and bidder i wins the commodity. We assume complete information regarding the state, but incomplete information regarding valuations.

We specify f as follows:

$$f_i(\omega) = -(n-1)kd_i \qquad \text{if bidder } i \text{ is the winner and } d_i = \max_{j \in N} d_j,$$

$$f_i(\omega) = -(n-1)kl \qquad \text{if bidder } i \text{ is the winner but } d_i < \max_{j \in N} d_j,$$

$f_i(\omega) = kd_h$ if bidder $h \neq i$ is the winner and $d_h = \max_{j \in N} d_j$,

$f_i(\omega) = \frac{n-1}{n-2} kl$ if bidder $h \neq i$ is the winner but $\max[d_i, d_h] < \max_{j \in N} d_j$,

and

$f_i(\omega) = 0$ if bidder $h \neq i$ is the winner but $d_h < d_i = \max_{j \in N} d_j$.

Each bidder i must pay a large monetary amount $(n-1)kl$ if he/she is the winner but d_i is not the greatest. This motivates bidder i to make d_i not less than b_i. Moreover, bidder i receives no payment if he/she is not the winner but d_i is the greatest. This motivates bidder i to make d_i not greater than b_i. Hence, the submitted prices can be exposed to all bidders even if the seller hides them.

We specify a strategy $(\tilde{b}_i, \tilde{d}_i)$ for each bidder i by

$$\tilde{b}_i(v_i) = \tilde{d}_i(v_i) = lv_i \quad \text{for all} \quad v_i \in [0,1].$$

By playing this strategy profile, each bidder can obtain the same expected payoff as in Subsection B.

Proposition 5: *In the same manner as in Proposition 4, assume*

$$k = \frac{n(1-l)-1}{l(n^2-1)}.$$

Then, specified strategy profile $(\tilde{b}, \tilde{d})$ *is a Bayesian Nash equilibrium associated with specified target function* f.

Proof: From Proposition 4, it is sufficient to show that each bidder i has incentive to make d_i equivalent to b_i, provided the others play according to $(\tilde{b}, \tilde{d})$. Bidder i has no incentive to submit a price b_i that is greater than $l = \max_{v_1 \in [0,1]} \tilde{b}_1(v_1) = \tilde{b}_1(1)$.

Suppose that bidder i makes d_i less than b_i. Then, whenever bidder i wins the commodity, he/she pays the total of the expected monetary amount given by

$$(n-1)k\{lb_i^{n-1}+(1-l)d_i^{n-1}\}.$$

By selecting b_i instead of d_i, he/she pays the total of expected monetary amount given by

$$(n-1)kb_i^n,$$

which is less than $(n-1)k\{lb_i^{n-1}+(1-l)d_i^{n-1}\}$ because $b_i \le l < 1$. Since the expected payment to receive when he/she is a loser is unchanged, he/she better replaces d_i with b_i.

Suppose that bidder i makes d_i greater than b_i. Then, whenever bidder i wins the commodity, he/she must pay large monetary amount $b_i+(n-1)kd_i$ instead of lower monetary amount $b_i+(n-1)kb_i$, which he/she pays when he/she replaces d_i with b_i. Whenever bidder i loses the commodity, he/she receives either $k\max_{j\in N} d_j$ or zero instead of a lower monetary amount $k\max_{j\in N} d_j$, which he/she pays when he/she replaces d_i with b_i. From these observations, bidder i better replaces d_i with b_i.

Q.E.D.

IV. Conclusions

A public blockchain is expected to be a valuable ledger technology for securely recording transactions that do not involve fraudulent payments. Currently, there is the risk that public blockchains can be abused because there is no agreement on how recordkeepers should confirm the purpose of a broadcasted transaction. Therefore, the blockchain technology can adversely affect real-world governance.

If players can use revelation mechanisms without worrying about legal legitimacy, they should be able to freely make self-enforcing agreements that threaten others. Section II showed that blockchains will dramatically increase the potential of this threat.

Subsection II.B demonstrated direct monitoring, which is a rather limited incentive

method that can counter such blockchain threats in organization. Direct monitoring requires an employer to measure each employee's effort in a manner that distinguishes it from other employees' efforts. However, such an approach may not be desirable because it would violate the employee's independent living environment.

Subsection III.C provided the new perspective on auction theory. Both the seller and buyers are free to create smart contracts for further countermeasures. Hence, strategic issues may become unprecedentedly complex in appearance. It is worthwhile further deepening game-theoretical considerations in this direction, but this topic is beyond the purpose of this study.

References

Abadi, J., and M. Brunnermeier. 2018. "Blockchain Economics." Mimeo, Princeton University.

Akbarpour, M., and S. Li. 2018. "Credible Mechanisms." Mimeo, Stanford University.

Ashenfelter, O. 1989. "How Auction Works for Wine and Art." *Journal of Economic Perspectives* 3 (3), 23-36.

Biais, B., C. Bosière, M. Bouvard, and C. Casamatta. 2019. "The Blockchain Folk Theorem." *The Review of Financial Studies* 32 (5), 1662-715.

Böhme, R., N. Christin, B. Edelman, and T. Moore. 2015. "Bitcoin: Economics, Technology, and Governance." *Journal of Economic Perspectives* 29 (2), 213-38.

Budish, E. 2018. "The Economic Limits of Bitcoin and the Blockchain." NBER Working Paper 24717.

Cong, L. W., and Z. He. 2017. "Blockchain Disruption and Smart Contracts." *Review of Financial Studies* 32 (5), 1754-97.

d'Aspremont, C., and L. Gerard-Varet. 1979. "Incentive and Incomplete Information." *Journal of Public Economics* 11, 25-45.

Groves, T. 1973. "Incentives in Teams." *Econometrica* 41 (4), 617-31.

Huberman, G., J. Leshno, and C. Moallemi. 2017. "Monopoly without a Monopolist: An Economic Analysis of the Bitcoin Payment System." Bank of Finland Research Discussion Paper No. 27/2017.

Krishna, V. 2009. *Auction Theory*. Academic Press.

Legros, P., and H. Matsushima. 1991. "Efficiency in Partnerships." *Journal of Economic Theory* 55 (2), 296-322.

McAfee, P., and J. McMillan. 1992. "Bidding Rings." *American Economic Review* 82 (3), 579-99.

Myerson, R. (1981) "Optimal Auction Design." *Mathematics of Operations Research* 6 (1), 58-73.

Myerson, R., and M. Satterthwaite. 1983. "Efficient Mechanisms for Bilateral Trade." *Journal of Economic Theory* 29 (2), 265-81.

Nakamoto, S. 2008. "Bitcoin: A Peer-to-Peer Electric Cash System." Mimeo.

Narayanan, A. J. Bonneau, E. Felten, A. Miller, and S. Goldfeder. 2016. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton: Princeton University Press.

Nash, J. 1953. "Two-Person Cooperative Games." *Econometrica* 21 (1), 128-40.

Rubinstein, A. 1982. "Perfect Equilibrium in a Bargaining Model." *Econometrica* 50 (1), 97-109.

Saleh, F. 2018. "Blockchain without Waste: Proof-of-Stake." Mimeo, New York University.

Tirole, J. 1992. "Collusion and the Theory of Organizations." In *Advances in Economic Theory: Sixth World Congress, Vol. II*, edited by J.-J. Laffont. Cambridge: Cambridge University Press, 151-206.

Vickrey, W. 1961. "Counterspeculation, Auction, and Competitive Sealed Tenders" *Journal of Finance* 16 (1), 8-37.