KIER DISCUSSION PAPER SERIES

KYOTO INSTITUTE OF ECONOMIC RESEARCH

Discussion Paper No.1018

"Information Design in Blockchain: A Role of Trusted Intermediaries"

Hitoshi Matsushima

January 2020

KYOTO UNIVERSITY

KYOTO, JAPAN

Information Design in Blockchain: A Role of Trusted Intermediaries

Hitoshi Matsushima*

University of Tokyo

July 19, 2019

Abstract

This study clarifies that blockchain cannot replace the strategic value of trusted intermediaries, despite sufficient technological advancement for its implementation. Given the progress expected in the future, this study assumes that blockchain can implement various commitment devices for communication explored in the information design literature, without disclosing their details to anonymous record keepers. By considering revelation incentives explicitly, we show that substituting the verification task of players' pre-owned private signals with a trusted intermediary can reduce transaction costs in liability, which cannot be achieved non-judicially by blockchain. Hence, trusted intermediaries play a significant role in executing information design through blockchain.

Keywords: Blockchain, Information Design, Verification, Intermediary, Limited Liability.

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), University of Tokyo. I am grateful to Shunya Noda and the participants of the study sessions hosted by Auction and Market Design Forum (AMF, University of Tokyo) in January and February 2019 for their insightful comments.

Owing to recent advancements in new technologies such as blockchain, various institutional devices related to mechanism design, contract design, and information design are expected to be securely operated in a non-judicial manner. Matsushima (2019) showed that any state-contingent side-payment contract can be executed in a self-enforcing manner without the aid of trusted intermediaries, by broadcasting a simple combination of an escrow transaction and a redistribution transaction to a public blockchain. Moreover, by incorporating smart contracts with zero-knowledge proof technologies such as zk-SNARKs (Zcash On Ethereum), or, more substantially, by exploring secret contracts to address privacy concerns (Enigma), we can expect an information design device (Bergemann and Morris, 2019; Kamenica, 2019) to be enforceable by storing the corresponding program with secrecy in the blockchain. Thus, transaction costs can be drastically reduced in the future, because the legal proceedings originally conducted by trusted intermediaries can be reduced significantly.

This study clarifies that it is still difficult to replace a certain aspect of judicial procedures with blockchain in spite of sufficient technological progress. Specifically, from the viewpoint of information design, we show the importance of the role of intermediaries as follows. We regard information design as a commitment device for communication among multiple players (economic agents, business parties), which collects their pre-owned private signals and then recommends to each player the action that he/she should select as partial information about this signal collection. Importantly, the action recommendation to each player will be unknown to the other players for the time being. This secrecy has a significant effect in terms of incentivizing each player to obey the action recommendation (Bergemann and Morris, 2013, 2016).

When dealing with real data such as private signals, we need to convert such data into digital data. Correctly entering these signals into the program is an inevitable issue in many situations from the viewpoint of players' revelation incentives, because this conversion cannot be automated by knowledge-based digital technologies. However, the literature on Bayesian persuasion and information design generally assumes, as the benchmark, that players can make a pre-commitment to translate their signals into action recommendations correctly, thereby ignoring the above-mentioned incentive issue in revelation.

This study explicitly considers this incentive issue as follows. Suppose that private signals are verifiable and that each player is forced to verify his/her private signal to the other players when converting it into digital data. In this case, the entire body of private signals becomes common knowledge among the players before they make action selections. Thus, the secrecy is lost, which makes the information design device meaningless.

Therefore, to take advantage of information design, players should not carry out this verification task until they complete their action selections. However, when players only carry out this task ex-post, we should have an additional penalty scheme to incentivize each player to make a truthful revelation ex-ante. This penalty would increase the transaction (opportunity) costs through liability limitation.

This study points out that trusted intermediaries play an important role in avoiding the above-mentioned difficulty in taking advantage of information design. Suppose that players hire an intermediary and substitute him/her for the verification task; the intermediary is trusted so that according to their request, he/she will force each player to verify his/her private signal as unknown to the other players. In this case, each player can receive the action recommendation without knowing the details of the other players' private signals. With such secrecy, the players obey their action recommendations more easily than without it.

Blockchain is a new ledger technology for recording transactions and data securely in a tamper-proof manner. Beyond the role of supporting cryptocurrencies such as Bitcoin (Nakamoto, 2008; Bohme et al., 2015), blockchain is expected to play the role of a platform on which various smart contracts are programed, stored, and executed to create new businesses in a non-judicial manner (Narayanan et al., 2016; Tapscott and Tapscott, 2016). Moreover, blockchain can be applied to a wide range of network and market designs such as supply chains (Mao et al., 2018; Vyas et al., 2019) and energy markets (Mengelkamp et al., 2018). However, blockchains are under development and they still need to overcome various shortcomings such as low scalability, high electricity consumption, and lack of privacy. Above all, ensuring privacy should be regarded as the most important requirement for a blockchain to become a powerful platform for implementing various devices of institutional design (Cong and He, 2017).

With the steady evolution of cryptographic technologies for ensuring privacy, it has become possible for blockchain record keepers to validate the correctness of transactions, data, and programs without knowing the details of these contents in many situations. Hence, we expect that such technological progress will enable information design to inform each player only about partial information exclusively. As these technological advancements will be incorporated in the future, this study assumes full secrecy so that various information design devices can be implemented through blockchains.

Matsushima (2019) investigated the impact of blockchain technology on real-world economic governance and showed that blockchain facilitates harmful cartelization because it is a non-judicial mechanism without reputation considerations, whereby the blockchain record keepers tend to validate the correctness of a transaction without checking whether its purpose is legal. By contrast, an intermediary is trusted and he/she is likely to decline any request of delegation whenever the purpose is determined to be illegal, because he/she is averse to reputation loss. This study demonstrates another aspect of the importance of trusted intermediaries that cannot be delegated to blockchain from the viewpoint of information design.

Mathevet et al. (2019) investigated the possibility that the commitment device in information design is replaced by enforcement through players' reputation in their long-term relationship. By contrast, this study assumes that each player does not know about the other players' concerns regarding their own reputations and hence ignores the reputation effect on business parties. Meanwhile, players know that the intermediary is extremely concerned about his/her reputation and he/she is thus motivated to work in accordance with the players' requests of delegation once accepted.

Hence, without the aid of such intermediaries, each player has to deposit a monetary amount as escrow by converting it into cryptocurrency in the same manner as Matsushima (2019), and this deposit is considered as a penalty to prevent himself/herself from cheating. This escrow deposit acts as the player's barometer that indicates the degree to which it is difficult for him/her to cooperate with the other players from the viewpoint of limited liability. This study shows that the aid of an intermediary reduces the need for such escrow deposits.

The seminal study by Kamenica and Gentzkow (2011) introduced the basic concept of information design in the Bayesian persuasion problem, where an informed sender

makes a commitment device for communication with a single, uninformed receiver by using randomization. Bergemann and Morris (2013, 2016, 2019) generalized this framework to multiple receivers who have pre-owned private signals and are forced to make truthful revelations. They presented the Bayes correlated equilibrium and the associated revelation principle, guaranteeing the sufficiency of action recommendation devices. To focus on the role of secrecy in information design, this study considers a subclass of this multi-receiver (multi-player) case where the intermediary (sender) has no pre-owned private signal and does not use randomization. However, such restrictions are not essential to this study's argument.

Further, we examine the case in which private signals are not verifiable and each player can provide a false information. The incentive issue in cheap talk such as that discussed by Crawford and Sobel (1982) is also considered in our problem.

Matsushima (2019, Proposition 5) presented an argument with regard to a sealed-bid auction, where the auctioneer executes a program for a first-price auction on the blockchain that hides even the winner's bid. This study extends this secrecy device to environments with more general information design. In some interdisciplinary studies, cryptographic technology has been used to implement equilibrium correlation devices (see Dodis et al., 2000, for instance).

The remainder of this paper is organized as follows. Section I presents the basic model. Section II introduces and analyzes three scenarios for the decision procedure depending on the differences in the settings for the verification and the intermediary. Section III presents a numerical example in which it is impossible for each player to obey the action recommendation in a self-enforcing manner if the players' private signals are not verifiable, while it is possible even without escrow devices if their private signals are verifiable and a trusted intermediary is available. Finally, Section IV concludes the paper.

I. Blockchain and Information Design

Consider a situation in which n players make action selections. Each player $i \in N \equiv \{1,...,n\}$ receives a private signal $\omega_i \in \Omega_i$, where Ω_i denotes the finite set of private signals for player i. We define the state space as $\Omega \equiv \underset{i \in N}{\times} \Omega_i$. A prior distribution

is given by $p:\Omega\to(0,1)$, where we assume full support. Each player $i\in N$ selects an action a_i from a finite set A_i. His/her payoff is given by $u_i(a,\omega)$. Further, quasi-linearity is assumed.

A *decision rule* is defined as $g=(g_i)_{i\in N}$, where $g_i:\Omega\to A_i$ for all $i\in N$. A *side-payment rule* is defined as $x=(x_i)_{i\in N}$, where $x_i:\Omega^2\times A\to R$ for all $i\in N$. Each player i announces a message $m_i\in\Omega_i$ about his/her private signal. According to g and $m=(m_i)_{i\in N}\in\Omega$, each player i is recommended the selection of $g_i(m)\in A_i$. He/she selects $a_i\in A_i$, which is not necessarily the same as the action recommendation $g_i(m)$, depending on his/her incentive. After the players complete their action selections, both the message profile $m\in\Omega$ and the action profile $a\in A$ become observable to all the players and contractible. Whether the state ω is contractible ex-post depends on how the details of the decision procedure are specified. For this specification, refer to Section II.

According to x and $(\omega,m,a)\in\Omega^2\times A$, each player i receives the monetary amount $x_i(\omega,m,a)\in R$. Note that $x_i(\omega,m,a)$ cannot depend on the state ω whenever it is not verified; we simply write $x_i(m,a)$ instead of $x_i(\omega,m,a)$ in this case.

We confine our attention to *budget-balancing* side-payment rules x, where no side-payment is made if all the players obey their respective recommendations:

$$\sum_{i\in N}x_i(\omega,m,a)=0 \quad \text{for all} \quad (\omega,m,a)\in\Omega^2\times A,$$

and

$$x_i(\omega,\omega,g(\omega))=0 \quad \text{for all} \quad i\in N \quad \text{and} \quad \omega\in\Omega.$$

This study examines the possibility that the players obey their action recommendations in a self-enforcing manner under the assumption that no side-payment is made on the path.

As $x_i(\omega,m,a)$ can be negative, we need to adopt measures to prevent payment defaults. One approach is to hire a trusted legal intermediary to act on behalf of this payment. Another approach is to use blockchain non-judicially, without hiring any intermediary, as follows. The players collectively create and broadcast an *escrow transaction*, with their added signatures, to a blockchain, which is described by

$e=(e_i)_{i\in N}\in R^n$; each player i deposits a non-negative monetary amount $e_i\geq 0$ as escrow. This escrow transaction is validated by the blockchain record keepers in a tamper-proof manner.

The players also collectively create a computer program that executes the action recommendations by the decision rule g, which is stored on the blockchain in a tamper-proof manner. Each player i announces his/her message $m_i\in\Omega_i$. This message is entered into the program. He/she privately receives the action recommendation $g_i(m)\in A_i$ from this program and then makes an action selection $a_i\in A_i$ offline.

Owing to the cryptographic secrecy, each player i cannot observe either the other players' messages $m_{-i}\in M_{-i}$ or the action recommendations given to the other players, $g_{-i}(m)=(g_j(m))_{j\in N\setminus\{i\}}\in A_{-i}$, until he/she completes the action selection. However, after all the players complete their action selections, this program automatically sends the message profile $m\in M$, and therefore, the recommendation profile $g(m)$, to all the players. We assume perfect monitoring in that after their action selections, all the players observe the action selections $a\in A$ offline.

After observing $(m,a)\in M\times A$, the players collectively create and broadcast a *redistribution transaction*, with their added signatures, to the blockchain. If the state ω is verified and becomes contractible ex-post, they can make the redistribution transaction dependent on it, which is described by $x(\omega,m,a)=(x_i(\omega,m,a))_{i\in N}\in R^n$. Otherwise, the redistribution must be independent of ω, which is described by $x(m,a)=(x_i(m,a))_{i\in N}\in R^n$. This transaction is also validated by the blockchain record keepers in a tamper-proof manner.

Each player i finally receives the monetary amount given by

$$e_i+x_i(\omega,m,a)$$

from this escrow. As no player can have a negative receipt for side-payments to be carried out, the side-payment rule x must satisfy a liability constraint in that for every $i\in N$ and $(\omega,m,a)\in\Omega^2\times A$,

$$e_i+x_i(\omega,m,a)\geq 0\,.$$

According to Matsushima (2019), we can achieve the redistribution $x(\omega, m, a) \in R^n$ in a self-enforcing manner. To implement the side-payment rule x, we do not need to broadcast the corresponding program to execute the contingent claim implied by x. This aspect is in contrast to the implementation of the decision rule (information design) g on the blockchain.

This study assumes that through blockchain, players can carry out (g, x) in a non-judicial manner without the aid of trusted intermediaries. Under this assumption, we focus on players' incentives to enter the correct information about the state and to obey their action recommendations by the decision rule g. We then clarify that trusted intermediaries play the significant role in fostering players' revelation incentives.

II. Verification and Intermediary

Owing to technological limitations, players cannot substitute a blockchain for the verification task, whereas they can substitute a trusted intermediary for this task. Accordingly, we introduce three scenarios for the decision procedure depending on the difference in the settings for the *verification* and the *intermediary*. Scenario 1 corresponds to the case in which private signals are not verifiable. Scenario 2 corresponds to the case in which private signals are verifiable and a trusted intermediary is available. Scenario 3 corresponds to the case in which private signals are verifiable, but no trusted intermediary is available. We show the relative ease of enforcing a decision rule g for each scenario, ordered from easiest to most difficult as Scenario 2, Scenario 3, and Scenario 1.

Fix an arbitrary vector of escrow deposits $e = (e_i)_{i \in N} \geq 0$, which describes the degree of each player's *limited liability*. The work of Legros and Matsushima (1991) is related to this study; they introduced the concept of limited liability index in a similar manner for the partnership problem with imperfect monitoring.

Scenario 1 (No Verification): Assume that private signals are not verifiable; the side-payment rule must be independent of ω, and it is thus denoted by $x(m, a)$. In this scenario, we need to incentivize each player i to make a truthful revelation as well as

select his/her action as recommended. A side-payment rule x is said to *enforce* a decision rule g *without verification* if x does not depend on ω, and for every $i \in N$, $\omega_i \in \Omega_i$, $\omega_i' \in \Omega_i$, and $k_i : A_i \to A_i$,

(1) $$\begin{aligned} & E[u_i(g(\omega),\omega) + x_i(\omega, g(\omega)) \mid \omega_i] \\ & \geq E[u_i((k_i(g_i(\omega_i',\omega_{-i})), g_{-i}(\omega_i',\omega_{-i})),\omega) \\ & + x_i((\omega_i',\omega_{-i}),(k_i(g_i(\omega_i',\omega_{-i})), g_{-i}(\omega_i',\omega_{-i}))) \mid \omega_i], \end{aligned}$$

where $E[\cdot \mid \omega_i]$ denotes the expectation operator in terms of ω_{-i} conditional on ω_i. The inequality (1) implies that player i has no incentive to announce $m_i = \omega_i'$ instead of his/her correct private signal ω_i and select the action $k_i(g_i(\omega_i',\omega_{-i}))$ instead of $g_i(\omega_i',\omega_{-i})$. A decision rule g is said to be *enforceable without verification* if there exists a side-payment rule x that enforces g without verification. Note that whenever a player can gain from deviation without disobeying his/her action recommendation, it is impossible to enforce g without verification.

Let $p(\omega_i, \omega_i', k_i)$ denote the probability that player i does not obey his/her action recommendation, i.e., $k_i(g_i(\omega_i',\omega_{-i})) \neq g_i(\omega_i',\omega_{-i})$, provided that player i observes ω_i and announces ω_i':

$$p(\omega_i, \omega_i', k_i) \equiv \sum_{\substack{\omega_{-i} \in \Omega_{-i}: \\ k_i(g_i(\omega_i',\omega_{-i})) \neq g_i(\omega_i',\omega_{-i})}} p(\omega_{-i} \mid \omega_i),$$

where $p(\omega_{-i} \mid \omega_i)$ denotes the probability of ω_{-i} conditional on ω_i. We define $e_i^* = e_i^*(g) \geq 0$ by

$$e_i^* \equiv \infty \qquad \text{if } E[u_i(g(\omega),\omega) \mid \omega_i] > E[u_i(g(\omega_i',\omega_{-i}),\omega) \mid \omega_i]$$
$$\text{for some } (\omega_i, \omega_i') \in \Omega_i^2,$$

and

$$e_i^* \equiv \max_{\substack{(\omega_i,\omega_i',k_i): \\ p(\omega_i,\omega_i',k_i)>0}} \frac{E[u_i(k_i(g_i(\omega_i',\omega_{-i})), g_{-i}(\omega_i',\omega_{-i}),\omega) \mid \omega_i] - E[u_i(g(\omega),\omega) \mid \omega_i]}{p(\omega_i,\omega_i',k_i)}$$
$$\text{otherwise.}$$

The following proposition shows that e_i^* measures player $i's$ minimal liability that is sufficient for enforceability without verification.

Proposition 1: *A decision rule* g *is enforceable without verification if and only if* $e_i \geq e_i^*$ *for all* $i \in N$.

Proof: It is sufficient to consider a side-payment rule that imposes the severest punishment e_i on any player i who does not obey his/her action recommendation. Let

$$N(m,a) \equiv \{i \in N \mid a_i \neq g_i(m)\}$$

denote the set of players who disobey their action recommendations. We specify $x = \tilde{x}$ by

$$\tilde{x}_i(m,a) = e_i + \frac{1}{n-1} \sum_{j \in N(m,a) \setminus \{i\}} e_j \qquad \text{if } i \notin N(m,a),$$

and

$$\tilde{x}_i(m,a) = \frac{1}{n-1} \sum_{j \in N(m,a) \setminus \{i\}} e_j \qquad \text{if } i \in N(m,a).$$

According to $\tilde{x}$, any player i who disobeys his/her action recommendation will be fined e_i. Hence, we can replace the incentive constraint (1) with the incentive constraint associated with $\tilde{x}$, i.e., for every $i \in N$, $\omega_i \in \Omega_i$, $\omega_i' \in \Omega_i$, and $k_i : A_i \to A_i$,

$$E[u_i(g(\omega),\omega) \mid \omega_i] \geq E[u_i((k_i(g_i(\omega_i',\omega_{-i})), g_{-i}(\omega_i',\omega_{-i})),\omega) \mid \omega_i]$$
$$-e_i p(\omega_i,\omega_i',k_i),$$

which, along with the definition of e_i^*, implies that $e_i \geq e_i^*$.

Q.E.D.

Note that $e_i^* = \infty$ implies that g is not enforceable without verification regardless of the value of e.

Scenario 2 (Verification with Intermediary): Assume that private signals are verifiable and the side-payment rule depends on ω, denoted by $x(\omega,m,a)$. In addition, assume

that the players substitute an intermediary for the verification task in the ex-ante term. In the process of this ex-ante delegated verification task, the intermediary forces each player i to make his/her message m_i equal to ω_i, while each player i cannot see the other players' messages m_{-i} until he/she completes his/her action selection. As each player i obeys the action recommendation $g_i(\omega)$ and then makes an action selection without knowing the details of ω_{-i}, we require only a relatively weak incentive constraint for each player i with regard to the action selection as follows. A side-payment rule x is said to *enforce* a decision rule g *with verification and with intermediary* if for every $i \in N$, $\omega_i \in \Omega_i$, $a_i \in A_i$, and $a_i' \neq a_i$, whenever $g_i(\omega) = a$ for some $\omega_{-i} \in \Omega_{-i}$, then

$$(2) \qquad E[u_i(g(\omega),\omega) + x_i(\omega,\omega,g(\omega)) \mid \omega_i, g_i(\omega) = a_i]$$
$$\geq E[u_i((a_i', g_{-i}(\omega)),\omega) + x_i(\omega,\omega,(a_i', g_{-i}(\omega))) \mid \omega_i, g_i(\omega) = a_i],$$

where $E[\cdot \mid \omega_i, g_i(\omega) = a_i]$ denotes the expectation operator in terms of ω_{-i} conditional on ω_i and $g(\omega) = a_i$. A decision rule g is said to be *enforceable with verification and with intermediary* if there exists a side-payment rule x that enforces g with verification and with intermediary. We define $e_i^{**} = e_i^{**}(g) \geq 0$ by

$$e_i^{**} \equiv \max_{\substack{(\omega_i, a_i, a_i') \\ \exists \omega_{-i}: g_i(\omega) = a_i}} \{E[u_i((a_i', g_{-i}(\omega)),\omega) \mid \omega_i, g_i(\omega) = a_i]$$
$$- E[u_i(g(\omega),\omega) \mid \omega_i, g_i(\omega) = a_i]\}.$$

The following proposition shows that e_i^{**} measures player $i's$ minimal liability that is sufficient for enforceability with verification and with intermediary.

Proposition 2: *A decision rule g is enforceable with verification and with intermediary if and only if*

$$e_i \geq e_i^{**} \text{ for all } i \in N.$$

Proof: As $\omega = m$ is assumed, it is sufficient to consider the specified side-payment rule $\tilde{x}$. As with the proof of Proposition 1, we can replace the incentive constraint (2) with

the one associated with $\tilde{x}$; for every $i \in N$, $\omega_i \in \Omega_i$, $a_i \in A_i$, and $a_i' \neq a_i$ such that $g(\omega) = a_i$ for some $\omega_{-i} \in \Omega_{-i}$,

$$E[u_i(g(\omega),\omega) \mid \omega_i, g_i(\omega) = a_i]$$
$$\geq E[u_i((a_i', g_{-i}(\omega)),\omega) \mid \omega_i, g_i(\omega) = a_i] - e_i,$$

which, along with the definition of e_i^{**}, implies that $e_i \geq e_i^{**}$.

Q.E.D.

Note that $e_i^{**} < 0$ for all $i \in N$, that is, g is enforceable with verification and with intermediary if e is sufficiently large.

Scenario 3 (Verification without Intermediary): Assume that private signals are verifiable. In addition, assume that the players cannot substitute an intermediary for the verification task. To implement the action recommendation scheme (the decision rule g), the players should perform the verification task ex-post, i.e., after they complete their action selections. In this case, we need to consider the incentive constraint with regard to both revelation and action selection as follows. A side-payment rule x is said to *enforce* a decision rule g *with verification and without intermediary* if for every $i \in N$, $\omega_i \in \Omega_i$, $\omega_i' \in \Omega_i$, and $k_i : A_i \to A_i$,

(3)
$$E[u_i(g(\omega),\omega) + x_i(\omega,\omega,g(\omega)) \mid \omega_i]$$
$$\geq E[u_i((k_i(g_i(\omega_i',\omega_{-i})), g_{-i}(\omega_i',\omega_{-i})),\omega)$$
$$+x_i(\omega,(\omega_i',\omega_{-i}),(k_i(g_i(\omega_i',\omega_{-i})), g_{-i}(\omega_i',\omega_{-i}))) \mid \omega_i].$$

The inequality (3) implies that player i has no incentive to announce $m_i = \omega_i'$ instead of his/her correct private signal ω_i and select the action $k_i(g_i(\omega_i',\omega_{-i}))$ instead of $g_i(\omega_i',\omega_{-i})$. A decision rule g is said to be *enforceable with verification and without intermediary* if there exists a side-payment rule x that enforces g with verification and without intermediary. We define $e_i^{***} = e_i^{***}(g) \geq 0$ by

$$e_i^{***} \equiv \max[e_i^{**},$$

$$\max_{\substack{(\omega_i,\omega_i',k_i):\\ \omega_i\neq\omega_i'}} \{E[u_i((k_i(g_i(\omega_i',\omega_{-i})),g_{-i}(\omega_i',\omega_{-i})),\omega)\,|\,\omega_i]-E[u_i(g(\omega),\omega)\,|\,\omega_i]\}].$$

The following proposition shows that e_i^{***} measures player $i's$ minimal liability that is sufficient for enforceability with verification and without intermediary.

Proposition 3: *A decision rule* g *is enforceable with verification and without intermediary if and only if*

$$e_i \geq e_i^{***} \text{ for all } i \in N.$$

Proof: It is sufficient to consider a side-payment rule that imposes the severest punishment e_i on any player i who either disobeys his/her action recommendation or makes a dishonest revelation. Let

$$N(\omega,m,a) \equiv \{i \in N \,|\, \textit{either } a_i \neq g_i(m) \textit{ or } m_i = \omega_i\}.$$

We specify $x = \hat{x}$ by

$$\hat{x}_i(\omega,m,a) = e_i + \frac{1}{n-1}\sum_{j\in N(\omega,m,a)\setminus\{i\}} e_j \qquad \text{if } i \notin N(\omega,m,a),$$

and

$$\hat{x}_i(\omega,m,a) = \frac{1}{n-1}\sum_{j\in N(\omega,m,a)\setminus\{i\}} e_j \qquad \text{if } i \in N(\omega,m,a).$$

According to $\hat{x}$, any player i who either disobeys his/her action recommendation or makes a dishonest revelation will be fined e_i. As with the proofs of Propositions 1 and 2, we can replace the incentive constraint (3) with the one associated with $\hat{x}$; for every $i \in N$, $\omega_i \in \Omega_i$, $a_i \in A_i$, and $a_i' \neq a_i$ such that $g(\omega) = a_i$ for some $\omega_{-i} \in \Omega_{-i}$,

$$E[u_i(g(\omega),\omega)\,|\,\omega_i, g_i(\omega) = a_i] \geq E[u_i((a_i', g_{-i}(\omega)),\omega)\,|\,\omega_i, g_i(\omega) = a_i] - e_i,$$

and for every $i \in N$, $\omega_i \in \Omega_i$, $\omega_i' \neq \omega_i$, and $k_i : A_i \to A_i$,

$$E[u_i(g(\omega),\omega)\,|\,\omega_i] \geq E[u_i((k_i(g_i(\omega_i',\omega_{-i})), g_{-i}(\omega_i',\omega_{-i})),\omega)\,|\,\omega_i] - e_i,$$

which, along with the definition of e_i^{**} and e_i^{***}, implies that $e_i \geq e_i^{***}$.

Q.E.D.

Note that $e_i^{***} < 0$ for all $i \in N$, that is, g is enforceable with verification and without intermediary if e is sufficiently large.

By definition, it holds straightforwardly that the incentive constraint (2) for Scenario 2 (Verification with Intermediary) is less restrictive than the incentive constraint (3) for Scenario 3 (Verification without Intermediary), and that the incentive constraint (3) is less restrictive than the incentive constraint (1) for Scenario 1 (No Verification). Hence, a decision rule is more easily enforced with verification than without it, and is more easily enforced with trusted intermediation than without it.

Theorem 4: *If a side-payment rule x enforces a decision rule g without verification (Scenario 1), x also enforces g with verification and without intermediary (Scenario 3). If x enforces g with verification and without intermediary (Scenario 3), x also enforces g with verification and with intermediary (Scenario 2). We have*

$$e_i^* \geq e_i^{***} \geq e_i^{**}.$$

III. Example

We present a numerical example, where (i) it is impossible for a decision rule g to be enforceable without verification ($e_i^* = \infty$), (ii) it is impossible for g to be enforceable with verification and without intermediary if the players do not use the escrow device ($0 < e_i^{***} < \infty$), and (iii) it is possible for g to be enforceable with verification and with intermediary even if the players do not use the escrow device ($e_i^{**} = 0$). Let $\Omega_i = \{0,1,2,3\}$, $A_i = \{0,1\}$, and

$$p(\omega) = 1/4^n \quad \text{for all} \quad \omega \in \Omega.$$

We define $k_i(\omega_{-i}) \in \{0,1,2,3\}$ such that for every $b \in \{0,1,2,3\}$,

$$k_i(\omega_{-i}) = b \quad \text{if} \quad n(\omega_{-i}, b) \geq n(\omega_{-i}, b') \quad \text{for all} \quad b' \quad \text{and}$$
$$n(\omega_{-i}, b) > n(\omega_{-i}, b') \quad \text{for all} \quad b' < b,$$

where we denote $n(\omega_{-i}, b) \equiv \left| \{ j \in N \mid j \neq i, \omega_j = b \} \right|$. We specify u_i by

$$u_i(a, \omega) = \frac{2.5}{n-1} \sum_{j \neq i} a_j - k_i(\omega_{-i}) a_i .$$

By selecting $a_i = 1$, player i enhances the other players' welfare by 2.5, while he/she pays the cost $k_i(\omega_{-i})$, which corresponds to the majority value of the other players' private signals.

Consider the decision rule g that maximizes the total surplus, i.e.,

$$g_i(\omega) = 0 \qquad \text{if and only if } k_i(\omega_{-i}) = 3 .$$

Note that $g_i(\omega)$ does not depend on ω_i, but it depends on the details of ω_{-i}. In Scenario 1 (Non-Verification), we can see that it is impossible for g to be enforceable, i.e., $e_i^* = \infty$, because each player i has no incentive to announce $m_i = 3$. He/she always wants to let the other players select action 1 as far as possible, even with a lie.

In Scenario 2 (Verification with Intermediary), each player i is informed as to whether $g_i(\omega) = 0$ or $g_i(\omega) = 1$, but is not provided with the entire body of ω_{-i}. Equivalently, he/she is only informed as to whether $k_i(\omega_{-i}) = 3$ or $k_i(\omega_{-i}) = 1$ in expectation. When $k_i(\omega_{-i}) = 1$ in expectation, regardless of his/her action selection, the expected payoff of player i is given by

$$E\left[\frac{2.5}{n-1} \sum_{j \neq i} g_j(\omega) \mid \omega_i, k_i(\omega_{-i}) \neq 3 \right],$$

where $E[\cdot \mid \omega_i, k_i(\omega_{-i}) \neq 3]$ denotes the expectation operator conditional on ω_i and $k_i(\omega_{-i}) \neq 3$. As each player $i's$ action selection does not influence his/her expected payoff, he/she has an incentive to select $a_i = 1$ even without the aid of the escrow device; $e_i^{**} = 0$.

In Scenario 3 (Verification without Intermediary), in contrast to Scenario 1, we can incentivize each player to make a truthful revelation by imposing monetary penalties contingent on the ex-post verification. Hence, we have $0 < e_i^{***} < \infty$.

IV. Conclusion

This study clarified the role of third-party, trusted intermediaries in partnerships with regard to privacy protection by considering highly developed blockchain technology. When multiple players who cannot trust one another attempt to execute a joint venture by using commitment devices of information design, substituting the ex-ante verification task of the players' private signals by a trusted intermediary has a significant effect on lowering the transaction costs by saving the players' escrow deposits, because this task cannot be replaced with blockchain. Therefore, to use blockchain in establishing a business, it can be assumed that intermediaries play a significant complementary role regardless of the degree of technological progress of blockchain.

Previous studies in the information design literature have intensively considered benchmark cases under the assumption that players can commit to entering their pre-owned private signal to the program truthfully while ignoring incentives in revelation. In contrast to these studies, the present study explicitly considered this incentive issue and then showed the importance of the role of intermediaries. This result opens up the possibility of applying the concept of information design to real economies while simultaneously highlighting its limitations.

This study explicitly considered revelation incentives in information design to demonstrate that converting real data into digital ones cannot be automated by knowledge-based technologies. We then showed that trusted intermediates play a significant role in complementing the automation by blockchain. This discovery makes a significant contribution not only to relevant research fields but also to society; for a blockchain to support the creation of new business successfully, its technological progress alone is not enough, and an effort to establish appropriate institutional conditions from the strategic viewpoint, such as trusted intermediations, is essential.

Throughout this study, we only considered a weak implementation, in that obeying action recommendations can be supported by an equilibrium; there may exist another equilibrium according to which some players disobey action recommendations. Hence, the investigation of a strict (unique) implementation that eliminates such unwanted equilibria remains as important future research. This is beyond the scope of this study.

References

Bergemann, D. and S. Morris. 2013. "Robust Predictions in Games with Incomplete Information." *Econometrica* 81 (4), 1251-1308.

Bergemann, D. and S. Morris. 2016. "Bayes Correlated Equilibrium and the Comparison of Information Structure in Games." *Theoretical Economics* 11, 487-522.

Bergemann, D. and S. Morris. 2019. "Information Design: A Unified Perspective." *Journal of Economic Literature* 57 (1), 44-95.

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

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

Crawford, V., and J. Sobel. 1982. "Strategic information transmission." Econometrica 50 (6), 1431-1451.

Dodis, Y., S. Halevi, and T. Rabin. 2000. "A Cryptographic Solution to a Game Theoretic Problem." Annual International Cryptology Conference, Springer.

Kamenica, E. and M. Gentzkow. 2011. "Bayesian Persuasion." *American Economic Review* 101 (6), 2590-2615.

Kamenica, E. and M. Gentzkow. 2019. "Bayesian Persuasion and Information Design." *Annual Review of Economics* 11, 249-272.

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

Mao, D., Z. Hao, F. Wang, and H. Li. 2018. "Innovative Blockchain-Based Approach for Sustainable and Credible Environment in Food Trade: A Case Study in Shandong Province, China." *Sustainability* 10 (9), Article Number 3149.

Mathevet, L., D. Pearce, and E. Stacchetti. 2019. "*Reputation and Information Design*." New York University.

Matsushima, H. 2019. "Blockchain Disables Real-World Governance." CARF-F-459.

Mengelkamp, E., J. Gaerttner, K. Rock, S. Kessler, L. Orsini, and C. Weinhardt. 2018. "Designing Microgrid Energy Markets A Case Study: The Brooklyn Microgrid." *Applied Energy* 210, 870-880.

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.

Tapscott, D., and A. Tapscott. 2016. *Blockchain revolution: How the technology behind Bitcoin is changing money, business, and the world*. New York: Penguin.

Vyas, N., A. Beije, and B. Krishnamachari. 2019. *Blockchain and The Supply Chain*. New York: Kogan Page.