# Design of Trusted B2B Market Platforms using Permissioned Blockchains and Game Theory

Shivika Narang
*Indian Institute of Science*
shivika@iisc.ac.in

Megha Byali
*Indian Institute of Science*
megha@iisc.ac.in

Pankaj Dayama
*IBM India Research Lab*
pankajdayama@in.ibm.com

Vinayaka Pandit
*IBM India Research Lab*
pvinyaka@in.ibm.com

Y Narahari
*Indian Institute of Science*
narahari@iisc.ac.in

***Abstract*—Trusted collaboration satisfying the requirements of (a) adequate transparency and (b) preservation of privacy of business sensitive information is a key factor to ensure the success and adoption of online business-to-business (B2B) collaboration platforms. Our work proposes novel ways of stringing together game theoretic modeling, blockchain technology, and cryptographic techniques to build such a platform for B2B collaboration involving enterprise buyers and sellers who may be strategic. The B2B platform builds upon three ideas. The first is to use a permissioned blockchain with smart contracts as the technical infrastructure for building the platform. Second, the above smart contracts implement deep business logic which is derived using a rigorous analysis of a repeated game model of the strategic interactions between buyers and sellers to devise strategies to induce honest behavior from buyers and sellers. Third, we present a formal framework that captures the essential requirements for secure and private B2B collaboration, and, in this direction, we develop cryptographic regulation protocols that, in conjunction with the blockchain, help implement such a framework. We believe our work is an important first step in the direction of building a platform that enables B2B collaboration among strategic and competitive agents while maximizing social welfare and addressing the privacy concerns of the agents.**

***Index Terms*—component, formatting, style, styling, insert**

## I. Introduction

Recent progress in distributed ledgering technology, collectively referred to as *blockchain technology*, has gained much attention from the industry [1]. In the last few years, it has transitioned from an exciting technology having a cult user-base for Bitcoin [2], to becoming a powerful tool for transformation of business ecosystems. The initial research focus on blockchain has been on various aspects of distributed consensus mechanisms for cryptocurrency applications. The focus of our work is on using blockchains to build a powerful, trusted B2B platform for transparent, yet privacy-assuring, collaboration among strategic enterprise buyers and sellers. To this end, we use game theoretic and cryptographic techniques in conjunction with a permissioned blockchain.

One specific motivation for our work is as follows. In an industrial setting, it is vital for a business to ensure that collaborators do not learn any sensitive information through its transactions. Standard reputation systems, such as in [3], [4], involve revealing information about collaborators and cannot be used to ensure the robustness of the market platform. We use a permissioned blockchain and multi-party computation to provide a simple decentralized reputation system, which is convenient to use and robust to attacks such as unfair ratings.

There has been a stream of research that has discussed game theoretic aspects of incentivization of the computation required for achieving consensus in blockchain networks [5]–[9]. However, most of the business applications on blockchain networks have addressed only distributed orchestration of cross-organization business workflows. Till date, there is no work that offers a framework to achieve trusted, distributed, and privacy preserving collaboration among network participants with provable social welfare properties. Consequently, the initial promise of blockchain giving rise to collaborative business networks with guarantees on the social welfare of the overall ecosystem, has not been realized. In this paper, we fill this critical gap in the realization of collaborative business works. For the purpose of concreteness, we address this problem in the context of privacy preserving rating of sellers in a B2B market platform.

### A. The Problem: Enabling Trusted, Honest Collaboration among Strategic Buyers and Sellers on a B2B Platform

A reputation system on a typical online marketplace, such as Amazon or eBay, is built by encouraging buyers to provide feedback about the products they receive. Customers on these platforms accordingly make their decisions based on the price quoted and the reputation of the seller. Enterprise agents would also like to have such information at hand to be able to choose the right supply chain partners [3]. However, providing such feedback is a strategic issue for enterprise buyers and sellers, who cannot have their identity and buying history leaked by way of such feedback. Further, anonymous feedback in itself is neither reliable nor effective. As a result, while there is a pressing need for a B2B collaboration platform, the sensitive nature of the information that must be exchanged on such a platform restricts its deployment. Our work attempts to

978-1-7281-1328-9/19/$31.00 ©2019 IEEE

develop a B2B platform that overcomes these challenges with a judicious mix of permissioned blockchains, game theoretic modeling, and multi-party computation.

We consider an online decentralized B2B platform for repeated procurement transactions of enterprise agents. Each seller, offering a product or service (henceforth referred to as product), will deliver either a high or a low quality product. The cost of producing high quality goods is (naturally) higher than that of low quality goods. The goods may be sold at a price fixed by the platform or more sophisticated pricing strategies may be followed. Goods are purchased in multiple rounds: in each round, a buyer chooses a seller to buy from and having received the product, the buyer gives a binary feedback or rating (high/low) on the quality received.

We aim to develop a decentralized market protocol (which we call a mechanism) that provides a network-wide transparent rating of the suppliers that is reflective of their aggregate performance. The protocol must ensure that:
(i) Information exchange is such that, each entity knows only its own buyer-seller relationship,
(ii) In any given round, sellers cannot decipher the exact rating given by their buyers in that round,
(iii) The mechanism induces the buyers to provide honest feedback and the sellers to supply high quality products.

We call such a platform a *trusted market platform*. These conditions are prerequisites for sustained participation of strategic enterprise buyers and sellers. They mandate that a centrally deployed platform is not feasible. A decentralized rating mechanism, enabled by blockchain, would be able to aggregate the rating data while satisfying the above constraints. To do so, the mechanism should exactly mimic, distributively, a centralized oracle that has access to all the feedback and publishes ratings for the sellers. These ratings may simply be the average of the feedback that a seller gets from the buyers across all the rounds, with higher weight for recent rounds. Further, a blockchain setting can also enforce the pricing rules analyzed. To do so, several key challenges arise, which we systematically address in this paper.

### B. Our Contributions

**Formal Framework for Secure B2B Collaboration**: A key aspect of B2B collaboration is that, often, the cooperating entities are also competitors and the information required for cooperation is highly business sensitive. Designing a platform that correctly enables a healthy, privacy-preserving B2B collaboration is therefore an important requirement and requires a technical solution. For this, we develop a framework that formalizes the needs of secure and private B2B collaboration. This is described in Section II. To the best of our knowledge, this is the first attempt towards evolving a such a framework for B2B collaboration.

**Game Theoretic Modeling and Analysis of Smart Contracts**: A key ingredient for building successful sustainable collaborative platforms is to ensure honest participation by the strategic agents. To this end, we deploy a repeated game model to analyze the strategic interactions between the buyers and sellers in the context of procurement of goods. Sellers offer high or low quality products while buyers provide binary feedback on the goods received. Repeated games are a natural model for such studying market interactions [10]–[12]. Under various pricing strategies, we analyze the equilibrium behavior of the underlying repeated games and study different punishment strategies for encouraging cooperation. We find insights on inducing honest behavior from the agents. This analysis is useful in designing smart contracts to be implemented using a permissioned blockchain. This constitutes the subject of Section III. To the best of our knowledge, there is no prior work on using game theoretic analysis of B2B collaboration to set up smart contracts in the blockchain context.

**Privacy-Preserving Regulation Protocol on Blockchain**: We show how to employ a permissioned blockchain network to securely and privately mimic a centralized oracle's solution to the B2B collaboration problem. We deploy smart contracts that implement the business logic with the help of two regulation protocols: (a) a public perception protocol and (b) a monitoring protocol. The public perception protocol is a cryptographic protocol that aggregates buyer feedback about sellers into a rating, known as the public perception vector, while preserving privacy. The purpose of the monitoring protocol is to disincentivize dishonest feedback by the buyers. We show that our implementation is a secure and private simulation of a centralized oracle's supplier rating. This is covered in Section IV. We believe this paper presents the first framework for building trusted and decentralized collaborative business networks leveraging blockchain technology. The specific case of the seller rating problem and its game theoretic analysis is of independent interest in itself.

### C. Relevant Work

The motivation of our work is to achieve sustained cooperation amongst enterprise buyers and sellers. Collaboration amongst businesses has been shown to be helpful in reducing supply chain costs both theoretically and empirically [13]–[15]. Studies also show that to sustain high quality in the products purchased from a strategic agent, it is necessary for all other buyers to know when a particular seller fails to do so [10], [16]. We achieve this by means of a ratings mechanism.

Game theoretic investigations of blockchains have largely been focused on the study of the non-cooperative and cooperative games induced by the incentive schemes for mining on bitcoin type of permissionless blockchains [5]–[9]. Since we use permissioned blockchains that do not require Proof-of-Work for achieving consensus, the above body of work is only marginally relevant for our work. Some work has been done on validation and analysis of smart contracts using game theory [17], [18], however to the best of our knowledge, this is the first endeavour to use game theory to design smart contracts.

## II. Framework for Secure B2B Collaboration

In order to be capable of performing any sort of analysis, a formal framework is required. This section provides such a framework for capturing events on the blockchain to enable

the analysis of the pricing schemes and protocols discussed in the subsequent section. An event on the blockchain may be a consequence of any subset of prior events. The framework assumes that the blockchain is a permissioned one.

Let $\mathcal{N}$ be the set of participants or nodes (in this case, buyers and sellers) in the permissioned blockchain network. Let $\mathcal{E}$ be the set of all transactions (aka events) that occur as a part of interaction among nodes in $\mathcal{N}$. For each event $e \in \mathcal{E}$, there is an associated set of participants represented by $\mathcal{N}_e \subseteq \mathcal{N}$; it represents the set of participants involved with the event $e$. Further, for each event $e \in \mathcal{E}$, there is an associated record denoted by $\mathcal{R}_e$; this captures the outcome of the event $e$. Participants in the network may have selective access to the information about an event. Let $D_{h,\mathcal{R}_e}$ denote the subset of data fields of $R_e$ that can be accessed by the node $h \in N_e$. Thus, $D_h = \cup_{e \in \mathcal{E}} D_{h,\mathcal{R}_e}$ is the overall data that is accessible to participant $h$. We denote the union of all accessible information in the blockchain network by $D_U$: that is, $D_U = \cup_{h \in \mathcal{N}} D_h$. Let us consider a function $\Gamma(\mathcal{N}, \mathcal{E}, D_U)$ that can be computed by an oracle with access to the information $D_U$.

Consider a protocol $\mathcal{P}$ which consists of (a) an ordered set of encrypted messages $\mathcal{S}$ generated by the nodes in $\mathcal{N}$, and, (b) executes a sequence of computation steps, denoted by $\mathcal{C}$, with each step being carried out by a subset of nodes, where, each step may consume any subsequence of previously generated messages. Suppose the protocol computes a function $\Gamma^{'}(\mathcal{S}, \mathcal{C})$. Conceptually, one may regard the last step as a step carried out by a set of special *monitor* nodes. The protocol $\mathcal{P}$ is said to be a secure and private simulation of $\Gamma(\mathcal{N}, \mathcal{E}, D_U)$ if it satisfies the following conditions:

(i) $\Gamma^{'}(\mathcal{S}, \mathcal{C}) \approx \Gamma(\mathcal{N}, \mathcal{E}, D_U)$

(ii) If $h \notin \mathcal{N}_e$, then, even with access to $\mathcal{S}$ and $\mathcal{C}$, $h$ cannot infer the exact set $N_e$

(iii) No node $h \in \mathcal{N}$ can infer any data belonging to $D_U \setminus D_h$

We regard $\mathcal{S}$, the set of messages generated by all the nodes, as constituting the blockchain ledger. A B2B collaboration is essentially a sequence of computation steps $\Gamma_i, \forall i = 1, 2, \ldots$. We say that the collaboration can be securely and privately simulated on the blockchain if each of the steps has a secure and private simulation protocol. This framework is general enough to capture a host of B2B collaboration scenarios.

*Framework for the Current Instance*

For our current problem, $\mathcal{N}$ is the set of all buyers and sellers. Each transaction between a buyer seller pair represents an event $e \in \mathcal{E}$. Associated with each event $e$ is the record <price, cost, quality, rating>; the buyer knows <price, quality, rating> while the seller knows <price, cost, quality>. Our goal is to compute the supplier rating that closely approximates the rating an oracle with complete access to all required information would compute, while satisfying trust and privacy issues captured in Section I-A. A typical blockchain fabric like Hyperledger Fabric [19] can be used to implement the proposed system. Hyperledger Fabric allows channels where the data and the ledger are shared across participants in the channel. A particular supplier and buyer will be part of one private channel (a B2B network) and a buyer or seller can be part of multiple such channels. Transactional privacy is maintained across blockchain channels (different B2B networks). All data related to a channel (channel information, member, transaction, etc.) is not accessible by any network participant not explicitly granted access to that channel. Having set up the formal framework, we now discuss the game theoretic analysis which can be used to construct effective smart contracts.

## III. Game Theoretic Analysis and Design of Smart Contracts

This section sets up a game theoretic model to analyze various pricing rules and punishment strategies, in order to induce honest behavior from the agents. While this analysis is of independent interest, a *blockchain platform provides a convenient way to enforce these rules* by means of smart contracts *without the need for a centralized social planner*. Due to space constraints, several proofs have been deferred to a more detailed version of this work.

We consider a market platform where buyers and sellers interact repeatedly. Each seller delivers either high or low quality products. Each seller incurs a cost $c$ to produce a high quality product; the cost to produce a low quality product is assumed to be 0. Our analysis holds good with non-zero costs for low quality products as well; we assume zero cost for ease of presentation. In fact, $c$ could be thought of as the difference between the costs of producing high and low quality. After each round, each buyer reports whether the product received was of high or low quality in an encrypted way.

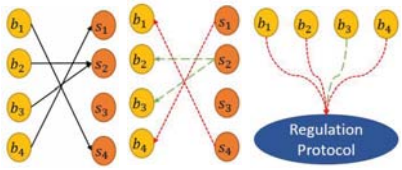
Let $B$ be the set of buyers and $S$, the set of sellers. Let $n_B$ be the number of buyers and $n_S$ the number of sellers. We assume that $n_S > 2$ and $n_B > 2$; else, it isn't possible to meet the anonymity constraints. If $n_S < 3$, then each seller knows that the buyer who did not buy from him, chose to buy from the other seller, if any. If $n_B < 3$, the sellers who have made a sale know which buyer has bought from whom. We assume that the list of sellers who have made at least one sale in a given round is made public at the end of that round. Thus, it is imperative to assume that $n_B > 2$ and $n_S > 2$.

The interactions between the agents are modeled as a repeated game, in which each round involves the following:

1. Each buyer selects a seller and places an order
2. Each seller decides what quality to offer to which buyer
3. Based on the quality received, the buyer submits (an encrypted) binary feedback

We defer the details of the cryptographic protocol required for the implementation and analysis of the mechanism to Section IV. In this section, we assume that all quantities used in the mechanism can be obtained in a privacy preserving manner, and that the list of sellers who made at least one sale is shared at the end of each round. The regulation protocols are then deployed for computing the ratings of the sellers.

*Notations and Assumptions:* We now present some important notations used in this section. The value of a high quality item and low quality item are denoted by $v_H$ and $v_L$




(a) Buyers choose seller (b) Sellers choose quality (c) Buyers submit feedback

Fig. 1: An example round. Red-dotted arrows and green-dashed arrows denote low and high quality respectively

respectively. We use $t$ to denote the current round and $i$ to denote a round in general. We denote the fraction of sales made by seller $s$ in round $i$ that got a feedback of high quality by $I_Q(s,i)$. $\mathbb{1}_T(s,i)$ is the indicator function for whether seller $s$ made any sales in round $i$. We associate a *public perception vector* $Q^t$ with a round $t$, indexed by sellers, i.e, $Q^t(s)$ denotes the public perception of seller $s$ in round $t$. We denote the time dampening factor for past feedback by $\delta_M \in (0.5, 1)$. At the current round $t$, the information from a past round $i < t$ is given a weight of $\delta_M^{t-i-1}$.

We need two more indicator variables: $\mathbb{1}_Q(s,b,i)$ is the indicator function for whether or not seller $s$ gave buyer $b$ a high quality product in round $i$ and $\mathbb{1}_T(s,b,i)$ is the indicator function for whether or not seller $s$ supplied to buyer $b$ in round $i$. We denote the default rating for a seller who has not yet sold any product by $\xi$, i.e, $Q^1(s) = \xi, \forall s$. We denote the price charged by seller $s$ in round $t$ by $p^t(s)$. The discounting factor of a seller $s$ is denoted by $\sigma_s$ and signifies his patience. We assume that the sellers do not have buyer specific strategies[1]. We use the terms public perception and rating interchangeably.

The public perception vector for the round $t$ is defined as:

$$Q^t(s) = \frac{\sum_{i=1}^{t-1} \delta_M^{t-i-1} I_Q(s,i) + \xi \Pi_{i=1}^{t-1}(1 - \mathbb{1}_T(s,i))}{\sum_{i=1}^{t-1} \delta_M^{t-i-1} \mathbb{1}_T(s,i) + \Pi_{i=1}^{t-1}(1 - \mathbb{1}_T(s,i))} \quad (1)$$

Each buyer $b$ maintains a personal history vector $h_b^t$ which captures the time discounted average number of times the sellers have supplied a high quality product to buyer $b$ up to round $t$. For sellers with whom the buyer has never transacted, $\xi$ is the initial perception. The computation of $h_b^t$ is given by

$$h_b^t(s) = \frac{\sum_{i=1}^{t-1} \delta_b^{t-i-1} \mathbb{1}_Q(s,b,i) + \bar{\xi}(s) \Pi_{i=1}^{t-1}(1 - \mathbb{1}_T(s,b,i))}{\sum_{i=1}^{t-1} \delta_b^{t-i-1} \mathbb{1}_T(s,b,i) + \Pi_{i=1}^{t-1}(1 - \mathbb{1}_T(s,b,i))} \quad (2)$$

Here, $\bar{\xi}(s)$ is $\xi$ in round $t$ if $\xi \geq Q^i(s), \forall i = 1, \cdots, t$ else is $Q^t(s)$. Buyer's dampening factor $\delta_b \in (0.5, 1)$ is private information of the buyer. At the start of each round, a buyer $b$ will compute the personal perception vector as follows:

$$q_b^t(s) = \theta_b h_b^t(s) + (1 - \theta_b) Q^t(s) \quad (3)$$

where $\theta_b$ is the type of the buyer that signifies the relative importance that $b$ assigns to personal history in comparison to public perception. The estimated utility of a buyer from a seller $s$ is $q_b^t(s) v_H + (1 - q_b^t(s)) v_L - p^t(s)$. Each buyer chooses a seller who maximizes the buyer's estimated utility. If there are multiple such sellers, then the buyer chooses the seller who most recently gave a high quality product, if any; otherwise, chooses randomly among them.

**Punishment**: Repeated games[2] enable punishing buyers for not cooperating. In our setting, sellers cooperate by giving good quality products, and buyers by giving honest feedback. As discussed, the feedback submitted by the buyers aggregates to form the ratings, and further influences the seller chosen by a buyer in future rounds. A buyer may believe that by giving a seller poor feedback, she would decrease his rating, hence, ensuring that he provides good quality to increase it. Similarly, a short-sighted seller, may decide to provide low-quality goods in order to save on the production cost. To deal with such behavior, punishment comes into play.

Our setup punishes buyers by means of a monitoring protocol and the smart contract deployed to enforce the same. Every infraction by a buyer, detected by the monitoring protocol, is penalized by a fee[3]. This fee is selected as the maximum utility a buyer may receive across all further rounds, with a discounting factor of $1 - \nu$ for future payoffs with $\nu$ being a positive quantity extremely close to 0. We also ensure that our protocol does not detect dishonesty when the buyer has given honest feedback.

Hence, in our setup, sellers do not actively punish the buyers, and we do not discuss any punishment strategies for sellers. Buyers, on the other hand, can follow various punishment strategies to penalize sellers for providing bad quality goods. To this effect, we study traditional punishment strategies, like tit for tat, which are implemented on an individual level by buyers for having received poor quality in some recent round. We also study punishment at a market-wide level as well, where a seller is punished by all buyers in the market, if his public rating drops below a threshold value (this model is inspired by [21]). Additionally, we assume that all buyers follow the same punishment strategy. The next section analyzes this model under different pricing rules and punishment strategies.

### A. Analysis with Homogeneous Pricing

We first consider the setting where each seller sells his product at price $p$. This setting is both an important building block for the settings discussed subsequently, and is of independent interest, capturing perfectly competitive markets [22]. In this, the homogeneous pricing model, we assume buyers value a high quality product at $v$ and a low-quality one at 0. As discussed, each seller incurs a cost $c$ to produce a high quality product and incurs a cost 0 to produce a low quality one, with $v > p > c > 0$. We assume standard quasi-linear utility. Thus, the payoff matrix for a *single* transaction will be:

| | $H$ | $L$ |
|---|---|---|
| Buy | $v - p, p - c$ | $-p, p$ |

[1]This implies that seller is indifferent to the business he receives from the buyers, but this does not contradict the requirement of anonymity of buying patterns. The lack of buyer-specific strategies is in fact a result of the anonymity of buying patterns achieved by the regulation protocols.

[2]Refer to [20] for an introduction to repeated games and their analysis.

[3]The fee is chosen to ensure that on giving dishonest feedback, the buyer will incur a loss greater than any utility she can receive from further purchasing in the market

This pricing rule ensures that buyers choose the seller providing the best quality, as all sellers charge the same price. The monitoring protocol ensures that buyers are honest in their feedback. We analyze different punishment strategies in an attempt to induce honest behavior from sellers.

*Punishment Model: Local Punishment*

Under local punishment, a buyer penalizes a seller who has given her low quality products, by blacklisting the seller in future rounds. The duration of the blacklisting is determined by the type of strategy chosen. As it is unreasonable to punish those deemed incapable of giving high-quality, $b$ punishes seller $s$, only if $q_b^t(s) > 0$. In any given round, a buyer will only consider sellers who are not being punished in that round and chooses the one who maximizes her estimated utility. We discuss several candidate punishment strategies in this case.

*1) Grim Trigger:* Under this punishment strategy, on receiving low quality, a buyer blacklists the seller for all future rounds. Let $H^*$ and $L^*$ respectively denote the strategies that a seller supplies only high and low quality products to a buyer. Thus, the seller's utility from $H^*$ is $\frac{p-c}{1-\sigma_s}$. On the other hand, the seller's utility from not cooperating (giving low quality) is only $p$, as the buyer blacklists the seller in future rounds. Thus, $s$ will follow $H^*$ if

$$\frac{p-c}{1-\sigma_s} > p \Rightarrow c < \sigma_s p.$$

If $c > \sigma_s p$, a seller has no incentive to delay giving a low quality product. Also, as sellers only follow either $H^*$ or $L^*$ with all buyers, buyers cannot lie. As the buyer tries to maximize his estimated utility in each round, if a buyer does not switch to a different seller it implies that the seller supplied high quality products. This leads us to the following theorem.

**Theorem 1.** *Under grim trigger strategies, if $c < \sigma_s p$, then a seller will follow $H^*$, else will follow $L^*$.*

*2) Tit for Tat:* Under this punishment strategy, on receiving a low quality product, the seller is blacklisted for exactly one round. If all sellers follow $H^*$, then after the first round, a seller will neither gain nor lose a buyer. After the first round, the value of $q_b^t(s) = 1\ \forall s, b$.

On the other hand, when all other sellers follow $H^*$, if seller $s$ gives a low quality product to a buyer $b$, $b$ will punish $s$. As monitoring protocol ensures honest feedback, buyer $b$ will give negative feedback and $s$ will lose all customers in the next round. In the subsequent round, where $s$ is no longer blacklisted by $b$, as the value of $q_b(s)$ will have decreased, $b$ does not ever return to $s$. Thus, if at round $t$, seller $s$ has $n$ customers, then by giving only $b$ a low quality product in this round, the seller will lose all the customers in the next round, nonetheless. Thus, $s$ will give low quality products to all the customers. Hence, seller $s$ will deviate from $H^*$ if:

$$p > \frac{p-c}{1-\sigma_s} \Rightarrow c > \sigma_s p$$

Even if two sellers have $c < \sigma_s p$, the same reasoning will compel them to follow $H^*$ in equilibrium. For a seller $s$, if $c > \sigma_s p$, there is no reason to delay supply low quality products, and hence $s$ will follow $L^*$.

**Theorem 2.** *If $c < \sigma_s p$, for at least two of the sellers, then the subgame perfect equilibrium for these sellers is to follow $H^*$ and the others sellers to follow $L^*$.*

We now consider when would supplying a low quality product become a subgame perfect equilibrium strategy for all sellers. If all sellers follow $L^*$, then $Q^t(s) = 0\,\forall t > 1$ and initially buyers buy once from each seller, till $h_b^t(s) = 0\ \forall b \in B,\ s \in S$, after which each buyer randomly selects a seller in each round. Thus, a single deviation by seller $s$ to $H$ will result in all buyers buying from sellers $s$ in every round they are not punishing $s$. Thus, for all sellers playing $L^*$ to be a subgame perfect equilibrium, we need that for all sellers:

$$p + \frac{n_B p \sigma_s}{n_S(1-\sigma_s)} > p - c + \frac{\sigma_s n_B p}{(1-\sigma_s^2)}$$

$$\Rightarrow c > p\sigma_s n_B \left(\frac{1}{1-\sigma_s^2} - \frac{1}{n_S(1-\sigma_s)}\right)$$

In this condition, $L^*$ is not only an equilibrium strategy but also a dominant strategy. The sellers have no motivation to give even a single high quality product, even if it means that they will get all the buyers henceforth. Hence, any seller, for whom $c > p\sigma_s n_B \left(\frac{1}{1-\sigma_s^2} - \frac{1}{n_S(1-\sigma_S)}\right)$, irrespective of the strategies of other buyers, $L^*$ yields a higher utility. Therefore, we have the following theorem.

**Theorem 3.** *If $c > p\sigma_s n_B \left(\frac{1}{1-\sigma_s^2} - \frac{1}{n_S(1-\sigma_s)}\right)$, for a seller, then $L^*$ is a dominant strategy.*

In the case when neither $H^*$ nor $L^*$ can be a subgame perfect equilibrium, we find that no other pure strategy subgame perfect equilibrium is possible for any punishment strategy followed in the homogeneous pricing model.

**Theorem 4.** *No pure strategy subgame perfect equilibrium exists for homogeneous pricing other than $H^*$ and $L^*$.*

The proof is rather involved and consequently, we only give an outline. It is proven by first considering a particular set of strategies, deriving the conditions necessary for them to form an equilibrium and showing that those conditions can never be met, irrespective of the punishment strategy followed. We then show that it is sufficient to show that no equilibrium exists for these strategies to prove the theorem.

Along with the characterization of pure strategy subgame perfect equilibria, for the tit for tat setting, we also infer that **competition** and **profit margin** are the major driving factors in the quality offered by sellers. If at least $n_S - 1$ sellers have $c > \sigma_s p$ and exactly one seller has the highest $\frac{\sigma_s p}{c}$ ratio, then this seller has a monopoly, and will follow the strategy that maximizes his utility[4]. This strategy also ensures that all buyers in the market return to him, whenever they are not punishing him. This completes the characterization of equilibrium behaviour of pure strategy equilibria in this

[4]This strategy will loosely be the one where he produces only the minimum amount of high quality goods needed to maintain his monopoly.

setting. We now study the effect of increasing the duration of blacklisting.

*3) Limited Punishment:* In limited punishment, duration of blacklisting is $\alpha \in \mathbb{N}\backslash\{0\}$ rounds. Proofs here are similar to those in tit for tat.

**Theorem 5.** *If $c < \sigma_s p$, for at least two of the sellers, then the subgame perfect equilibrium for these sellers is to follow $H^*$ and the other sellers to follow $L^*$.*

**Theorem 6.** *If $c > p\sigma_s n_B \left(\frac{1}{1-\sigma_s^{\alpha+1}} - \frac{1}{n_S(1-\sigma_s)}\right)$, for a seller, then $L^*$ is a dominant strategy.*

Clearly, increasing the duration of the blacklisting reduces the incentive to supply low quality products. As discussed earlier, no other pure strategy subgame perfect equilibrium is possible. This analysis completes the characterization of subgame perfect equilibria under traditional punishment strategies. We now explore punishment strategies implemented market-wide.

*Punishment Model: Threshold Punishment*

In this punishment model, the market as a whole blacklists a seller for $\alpha$ rounds if his rating falls below a threshold value. The motivation for this model is to give room to sellers to not be punished for every infraction. Buyers still select the seller who maximizes their estimated utility, based on $q_b$ values. A seller is blacklisted only if the value of $Q^t(s)$ is less than the specified threshold. A blacklisted seller is reintroduced to the market after $\alpha$ rounds with the threshold value as his rating.

The threshold for homogeneous pricing is $p/v$, the value below which the estimated utility would be negative. Analysis is similar to that of the *local punishment* model.

**Theorem 7.** *If $c < \sigma_s p$, for at least two of the sellers, then the subgame perfect equilibrium for these sellers is to follow $H^*$ and the others sellers to follow $L^*$, and the buyers to give honest feedback.*

**Theorem 8.** *If $c > \frac{\sigma_s p n_B}{(1-\sigma_s^{\alpha+1})}\left(1 - \frac{\sigma_s^{\alpha+1}}{n_S}\right)$, for a seller, then $L^*$ is a dominant strategy.*

While the pure strategy equilibria in this model do not leave room for buyers to buy from sellers who infrequently supply low quality products, the mixed strategy equilibria would do so. This is due to the fact that for mixed strategy equilibria to arise in this setting, giving either $H^*$ or $L^*$ consistently should be infeasible for the sellers. So in this setting, there would be room for sellers to alternate between high quality and low quality without losing buyers.

By comparing the conditions for $L^*$ to be a dominant strategy, we can infer that threshold punishment disincentivizes low quality better than local punishment. Consequently, we assume threshold punishment for further analysis. We next explore a more generalized model, namely, binary pricing.

### *B. Analysis with Binary Pricing*

Here, sellers of a given product may either belong to a high price category or low price category. The price category to which the seller belongs to is often an indicator of the quality of the product provided by him. We abstract this situation into the binary pricing model as follows. We assume that each buyer has value $v_L$ and $v_H$ for low quality and high quality respectively, with $v_H > v_L > 0$. In this model, goods can be sold at either $p_H$ or $p_L$, with the cost of producing a high quality and a low quality product as $c$ and 0 respectively. We assume (a) $p_H > p_H - c > p_L > p_L - c > 0$ and (b) $v_H - p_L > v_H - p_H > v_L - p_L > 0 > v_L - p_H$. Let $S_H$ and $S_L$ be the set of sellers selling at $p_H$ and $p_L$ respectively. Thus, $S = S_H \cup S_L$. Let $n_H = |S_H|$ and $n_L = |S_L|$.

The punishment threshold for sellers in $S_H$ is $p_H/v_H$, similar to the homogeneous pricing model. For sellers in $S_L$, it is $\epsilon$ such that $0 < \epsilon << 1$ and is introduced to demotivate $L^*$ becoming an equilibrium strategy.

Within binary pricing, we consider two pricing models: (i) Non-adaptive binary pricing: The sets $S_H$ and $S_L$ do not change and (ii) Adaptive binary pricing: The prices charged by the sellers depend on their public perception.

*1) Non-adaptive Binary Pricing:* This models markets where the prices offered by a seller are constant over time. On analysis, we find that this pricing rule reduces to different instances of the homogeneous pricing model, under different conditions. Throughout the game, sellers in $S_H$ charge $p_H$, and those in $S_L$ charge $p_L$. In this model, we assume initial perception of a seller, $\xi$ to be the same irrespective of the price charged. As the estimated likelihood of getting a high quality product is the same for all sellers, in the first round, a buyer randomly chooses a seller in $S_L$.

Buyers estimate a utility of $\xi v_H + (1-\xi)v_L - p_H$ from sellers in $S_H$. Thus, as long as at least one seller in $S_L$ has estimated utility at least $\xi v_H + (1-\xi)v_L - p_H$ then buyers never buy from a seller in $S_H$. If $c < \sigma_s p_L$ for at least two sellers in $S_L$, then the buyers get a utility of $v_H - p_L$ from these sellers and will continue to buy from these sellers. Similarly, any equilibrium which gives a utility of at least $\xi v_H + (1-\xi)v_L - p_H$ can be sustained, and no buyer will ever buy from a seller in $S_H$.

If a seller in $S_L$ cannot sustain a strategy that gives the buyers a utility of at least $\xi v_H + (1-\xi)v_L - p_H$, then they give out $L$ from the very first round. In the case that all sellers in $S_L$ are in this state, only then buyers will proceed to buy from sellers in $S_H$.

Thus, once buyers start buying from sellers in $S_H$ as long as at least one of the sellers can give an estimated utility of at least $v_L - p_L$, buyers will continue to buy from sellers in $S_H$, else will switch back to sellers in $S_L$ and never again buy from sellers in $S_H$. All sellers who cannot sustain a strategy that guarantees an estimated utility of $v_L - p_L$ and avoids going into isolation will follow $L^*$. If the buyers switch from buying from sellers in $S_H$ to buying from sellers in $S_L$, the game reduces to that of the homogeneous pricing model with threshold punishment at $p_L$.

*2) Adaptive Binary Pricing:* We now model markets where prices are not constant over time, such as with new technology. Initially, all sellers charge a high price in order to indicate quality, but may later reduce the price. We abstract this situation into an adaptive binary pricing model. The sellers

switch their states based on their rating. All sellers start at price $p_H$. If $Q^t(s) < \frac{p_H}{v_H}$, the seller is isolated for $\alpha$ rounds, after which the seller joins $S_L$ and charges $p_L$, with $Q^t(s) = \max(\epsilon, Q^{t-\alpha-1}(s))$. The seller is upgraded to price $p_H$ once the estimated utility, based on the rating crosses $v_H - p_H$, thus when $Q^t(s) \geq 1 - \frac{p_H - p_L}{v_H - v_L}$. The reason for having all sellers start at the same price, is that if sellers cannot sustain giving high quality at a higher price, they will not be able to do so at a lower price.

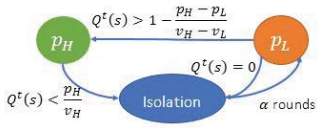



Fig. 2: Adaptive Binary Pricing: Price update Rule

All those sellers who cannot sustain a strategy that avoids isolation will follow $L^*$. If there is at least one seller who can avoid isolation, then the game reduces to the homogeneous pricing case at $p_H$ with the sellers who can avoid isolation. If there are no such sellers, then the game reduces to that of homogeneous pricing at price $p_L$ with all the sellers.

As both the pricing rules in binary pricing reduce to various cases of homogeneous pricing, we conjecture that other discrete pricing models with multiple prices also do the same. Intuitively, it appears that such models will not achieve anything more than exploding the state space.

## IV. Regulation Protocols for Implementation

The key takeaway from the previous section is that trusted visibility of seller ratings results in a desirable equilibrium behaviour of strategic buyers and sellers across a spectrum of pricing and punishment strategies. In this section, we present privacy preserving computation of the ratings and feedback monitoring protocol, ensuring their reliability, on a permissioned blockchain network. The regulation protocols carry out a distributed simulation of an oracle's solution for the aggregation of feedback vectors, while satisfying the constraints listed in Section I-A. They are executed as smart contracts on the blockchain network (refer [23] for preliminaries).

A more intuitive approach would be to have a single software agent receive the feedback vectors of every buyer, by means of a smart contract, and compute the ratings vector and check for dishonesty. However this approach has two critical problems. Firstly, it creates a point of centralization in the setup, which is not only against the inherent philosophy of blockchains, but also makes the system more vulnerable to attacks. An attacker need only target the software agent to gain access to all the feedback. More importantly, the existence of an entity with access to the feedback vectors of all the agents, whilst knowing correctly which agent each feedback vector belongs to is a violation of the first constraint. As a result, the task of meeting the anonymity constraints is non-trivial, thus requiring multiple agents for the system to be truly anonymous a relatively more carefully designed setup is required.

### A. Monitoring Protocol

Dishonesty must be detected in the system when a buyer's observed behavior is not consistent with her feedback history and the ratings. We define monitors that are distinguished set of entities (auditors) to constantly monitor the feedback submitted by buyers corresponding to a seller for potential dishonesty. Let the set of buyers as $B = \{b_1, b_2, ..., b_{n_B}\}$. For the sake of simplicity, let a monitor be associated with at most one buyer and hence the number of monitors is at least the number of buyers. For the purpose of the protocol, we consider the availability of pairwise private channels and a broadcast channel using blockchain among the buyers. Since monitors are audit entities, we assume that monitors are honest and do not collude with corrupt buyers. The description of the protocol is as follows:

[A] Each $b_i, i \in [n_B]$ must be assigned a monitor randomly to maintain the anonymity constraint. To obtain such a mapping, all buyers run a GenerateRandom routine in the network of buyers as follows: (i). Each $b_i, i \in [n_B]$ chooses a random $r_{ij} \in \{0,1\}^\kappa$, $j \in [n_B]$, computes hash $z_{ij} = \mathsf{H}(r_{ij})$ and broadcasts $\{\mathsf{H}(r_{ij})\}_{j \in [n_B]}$ using blockchain. Finally, $b_i$ must obtain a random value $r_i = \oplus_{j \in [n_B]} r_{ji}$. (ii). To construct each $b_i$'s random value $r_i$, each $b_j, j \neq i$ broadcasts $r_{ji}$. Now, $b_i$ verifies if $z_{ji} = \mathsf{H}(r_{ji})$. If not, $b_i$ chooses a default value for $r_{ji}$ and so do all buyers. Finally, $b_i$ computes $\{r_i\} = \{\oplus_{j \in [n_B]} r_{ji}\}$, $z_i = \mathsf{H}(r_i)$ and broadcasts $z_i$. (iv). $b_i$ uses the randomness $r_i$ to derive a random index value $t_i$ in $[m]$ where $m$ is the number of monitors available and $m \geq n_B$.

[B] To connect with the assigned monitor $M_{t_i}$, $b_i$ samples a random $a$ from a multiplicative group of integers modulo $p$ with $g$ as a primitive root of $p$. $b_i$ sends $(pk_i, g^a)$ encrypted under $M_{t_i}$'s public key to $M_{t_i}$. Similarly, $M_{t_i}$ also chooses a random $w$ from the group and sends $g^w$ encrypted under $pk_i$ to $b_i$ where $pk_i$ was received as part of encrypted message from $b_i$.

[C] Both $b_i$ and $M_{t_i}$ compute $K = (g^w)^a$ and $K = (g^a)^w$ respectively to agree on the key $K$. In each round, $b_i$ now encrypts its feedback vector, $f_{b_i}$ as: $c = \mathsf{Enc}_K(r_i, z_i, f_{b_i})$ and sends to $M_{t_i}$. $M_{t_i}$ decrypts $(r_i, z_i, f_{b_i}) = \mathsf{Dec}_K(c)$, verifies if $z_i = \mathsf{H}(r_i)$ and uses it for monitoring. For the very first round, $M_{t_i}$ sends $r_i$ to all buyers for cross verification of $r_i$ associated with $b_i$.

[D] $M_{t_i}$ uses $f_{b_i}$ as its input to monitor and compute public perception vector. A monitor constantly observes its buyer's feedback after every purchase. If the observed behavior is inconsistent with the feedback given by the buyer and the public perception, $M_{t_i}$ identifies that $b_i$ is corrupt and sends $(\textit{Corrupt}, r_i, z_i)$ to all the buyers. Each $b_j, (j \neq i) \in [n_B]$ checks $z_i$ with its own set of $\{z_j\}_{j \in n_B}$ to identify the buyer $b_i$, thus unanimously identifying $b_i$ to be corrupt and the penalty is enforced by the system. A penalty is then paid by $b_i$.

### B. Public Perception Protocol

The purpose of the monitoring protocol is to ensure that the ratings vector computed is reliable. The public perception protocol computes this vector while preserving anonymity of

feedback. This protocol is run amongst the monitors using the feedback they receive. The dampening factor $\delta_M$ necessary in each round $t$ can be computed using a protocol similar to as described in GenerateRandom protocol. We assume that $\delta_M$ and trusted setup (common reference string) necessary for key generation in threshold fully homomorphic encryption(FHE) is generated using an MPC protocol.

[A] All monitors involved in the computation run the threshold *Key Generation* protocol of threshold FHE ( [24]) to obtain their corresponding public key, private key $(pk_i, sk_i)$ pair. The public keys of all the monitors are consolidated as part of the key generation protocol to obtain the common public key $pk^*$ that will be used to perform homomorphic encryption and operation on the encrypted data homomorphically.

[B] For $j \in [m], i \in [n_B]$, each monitor $M_j$ consolidates the feedback for the sellers that it received from the assigned buyer using a vector $f_{b_i}$=$(f_{s_1}, \cdots, f_{s_{n_S}})$ where $f_{s_1}, \cdots, f_{s_{n_S}}$ indicate the feedback values corresponding to all $n_S$ sellers $s_1$, ..., $s_n$ respectively. The feedback is -1 for low and 1 for high if a purchase is made from $s_j$. Otherwise, $f_{s_j} = 0$.

[C] Each $M_j$ encrypts her feedback vector $f_{b_i}$ using the consolidated public key $pk^*$ to obtain the ciphertext $c_j$ and sends the ciphertext to all the other monitors. Monitors homomorphically consolidate the vectored ciphertexts $c_j$ as rows in order to compute the matrix $F$.

[D] To separate the positive and negative feedback, the following operations are performed:

$$F_H = \frac{1}{2}(F + |F|)\,,\; F_L = \frac{1}{2}(|F| - F) \tag{4}$$

Here $|F|$ denotes the matrix $F$ with absolute values of the entries. The resulting matrices $F_L$ and $F_H$ contain 1-entries (in encrypted form) at positions where the feedback is low and high respectively. Each column sum of $F_L$ would give the sum of all sales made by corresponding seller with feedback of $-1$ denoted as $sum_L^p$, $p \in [n_S]$. Each column sum of $F_H$ would give the sum of all sales made by the corresponding seller with feedback of 1 denoted as $sum_H^p$, $p \in [n_S]$. Total sales made by each seller $s_p$ is obtained as: $sum_{s_p} = sum_L^p + sum_H^p$ Thus, the fraction of sales made in round a $t$, $I_Q(s_p, t)$ = $sum_H^p / sum_{s_p}$ is obtained in encrypted form.

[E] Monitors together perform distributed threshold homomorphic decryption to obtain $I_Q$ for round $t$. Each monitor locally computes the public perception vector $Q^t$, using $\delta_M$ and verifies the resulting values are consistent, through consensus on blockchain. Each monitor $M_j$ sends $Q^t$ to all buyers.

The Public Perception protocol may be instantiated using the threshold multi-key fully homomorphic encryption schemes that utilize separate public key and secret keys held by the parties as well.

### C. Properties of the Regulation Protocols

The regulation protocols discussed above ensure that the honesty constraint is always met and the anonymity constraints are met in all cases except a few corner cases.

*1) Honesty of Feedback:* A monitor knows the rule deployed by buyers for selecting sellers and has access to the public perception vector $Q^t$. If the feedback is honest, then it is the same as her personal history. In the two pricing models studied, it is found on analysis that the private values of the buyers are not influential in their choice of seller. Consequently, the monitor can correctly predict which seller the buyer should choose to buy from next. If this prediction proves to be incorrect, it would indicate that the buyer has been dishonest. As the buyers will be fined when caught, buyers will choose to report their feedback honestly.

*2) Anonymity of Buying Patterns:* Each monitor is mapped to exactly one buyer whose identity is concealed from the monitor. As a result, the monitor can only decipher that a particular seller made a sale in that round, which is always publicly known. The cases in which a buying pattern may be deciphered is when in a given round, exactly one or two sellers make sales. When there are exactly two such sellers, only these sellers are able to decipher who bought from whom. With exactly one seller making a sale in a given round, it becomes public knowledge that all buyers bought from that seller. These two corner cases are unfortunately unavoidable in our framework.

*3) Anonymity of Feedback:* As the monitors remain unaware of the identity of the buyers whose feedback they monitor, anonymity is preserved. The feedback used in the public perception protocol is encrypted and aggregated homomorphically. As a result, buyers have no access to the feedback vector of any other buyer. The only case in which the feedback may be revealed to the seller is when his rating is either 0 or 1. This would be a consequence of all buyers giving the same feedback. This is, sadly, unavoidable within our setup. The only way to circumvent this would be to introduce noise in the ratings, which would make the system less reliable and cause non-deterministic behavior.

Our framework can easily accommodate other participants who need not be part of the secure computation protocol, such as logistics providers providing shipment status of the products. This information is recorded on the ledger for visibility, but not used in any computation.

## V. Conclusions

In this paper, we have attempted to build a trusted B2B platform that is attractive to enterprise buyers and sellers and induces honest behavior. The proposed platform uses a permissioned blockchain that executes smart contracts designed using a game theoretic model of the interactions between buyers and sellers. The platform uses cryptographic protocols that ensure the needed transparency as well as enforce privacy of business sensitive information. We believe this is just a first step towards building blockchain enabled collaborative business networks.

## Acknowledgment

The first author wishes to thank IBM Research, Bangalore, for providing a research internship opportunity during May-July 2017 and for many thought provoking discussions.

## REFERENCES


[1] I. Spectrum, "Special issue on blockchain technology," *IEEE Spectrum*, October 2017.

[2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," https://bitcoin.org/bitcoin.pdf, 2008.

[3] Y. Haghpanah, "A trust and reputation model for supply chain management," in *International Joint Conference on Artificial Intelligence*, vol. 22, no. 3, 2011, pp. 2814–2820.

[4] S. Jiang, "Towards the design of robust trust and reputation systems." in *IJCAI*, 2013, pp. 3225–3226.

[5] A. Kiayias, E. Koutsoupias, M. Kyropoulou, and Y. Tselekounis, "Blockchain mining games," in *Proceedings of the 2016 ACM Conference on Economics and Computation*. ACM, 2016, pp. 365–382.

[6] Y. Lewenberg, Y. Bachrach, Y. Sompolinsky, A. Zohar, and J. S. Rosenschein, "Bitcoin mining pools: A cooperative game theoretic analysis," in *Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems*. International Foundation for Autonomous Agents and Multiagent Systems, 2015, pp. 919–927.

[7] B. Fisch, R. Pass, and A. Shelat, "Socially optimal mining pools," in *Web and Internet Economics*, 2017, pp. 205–218.

[8] X. Liu, W. Wang, D. Niyato, N. Zhao, and P. Wang, "Evolutionary game for mining pool selection in blockchain networks," in *IEEE Wireless Communications Letters*, 2018.

[9] O. Schrijvers, J. Bonneau, D. Boneh, and T. Roughgarden, "Incentive compatibility of bitcoin mining pool reward functions," in *International Conference on Financial Cryptography and Data Security*. Springer, 2016, pp. 477–498.

[10] I. P. Fainmesser, "Community structure and market outcomes: A repeated games-in-networks approach," in *American Economic Journal: Microeconomics*, vol. 4, no. 1. American Economic Association, 2012, pp. 32–69.

[11] J. Levin, "Reputation in repeated interaction," 2006, accessed: 2017-05-18.

[12] A. Wolitzky, "Communication with tokens in repeated games on networks," in *Theoretical Economics*, vol. 10, no. 1. Wiley Online Library, 2015, pp. 67–101.

[13] G. P. Cachon and M. Fisher, "Supply chain inventory management and the value of shared information," in *Management science*, vol. 46. INFORMS, 2000, pp. 1032–1048.

[14] I. Dobos and M. Pintér, "Cooperation in supply chains: A cooperative game theoretic analysis," https://core.ac.uk/download/pdf/12354823.pdf, 2010.

[15] M. Ganesh, S. Raghunathan, and C. Rajendran, "Distribution and equitable sharing of value from information sharing within serial supply chains," in *IEEE Transactions on Engineering Management*, vol. 61, no. 2. IEEE, 2014, pp. 225–236.

[16] R. S. Gazzale and T. Khopkar, "Remain silent and ye shall suffer: seller exploitation of reticent buyers in an experimental reputation system," in *Experimental Economics*, vol. 14, no. 2. Springer, 2011, pp. 273–285.

[17] G. Bigi, A. Bracciali, G. Meacci, and E. Tuosto, "Validation of decentralised smart contracts through game theory and formal methods," in *Programming Languages with Applications to Biology and Security*, 2015.

[18] Y. Wang, A. Bracciali, T. Li, F. Li, X. Cui, and M. Zhao, "Randomness invalidates criminal smart contracts," in *Information Sciences*, vol. 477. Elsevier, 2019, pp. 291–301.

[19] C. Cachin, "Architecture of the hyperledger blockchain fabric," in *Workshop on Distributed Cryptocurrencies and Consensus Ledgers*, 2016.

[20] M. J. Osborne, *An Introduction to Game Theory*. Oxford university press New York, 2004, vol. 3, no. 3.

[21] Y. Zhang and M. van der Schaar, "Reputation-based incentive protocols in crowdsourcing applications," in *Proceedings of IEEE International Conference on Computer Communications*. IEEE, 2012, pp. 2140–2148.

[22] R. Lipsey and A. Chrystal, *Economics*, 13th ed. Oxford University Press, 2015.

[23] J. Katz and Y. Lindell, *Introduction to Modern Cryptography, Second Edition*. CRC Press, 2014.

[24] G. Asharov, A. Jain, A. López-Alt, E. Tromer, V. Vaikuntanathan, and D. Wichs, "Multiparty computation with low communication, computation and interaction via threshold FHE," in *Advances in Cryptology-31st Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 2012, pp. 483–501.