BlockCom : Peer-to-Peer Commerce Model with Iterative Double Auction Mechanism Using Smart Contract

Gaurang Bansal[2], Vikas Hassija[1], Vinay Chamola[2], Neeraj Kumar[3]
[1]Department of Computer Science and Engineering, JIIT, Noida Campus, India
[2]Department of Electrical and Electronics Engineering, BITS Pilani, Pilani Campus, India
[3] Department of Computer Science and Engineering, Thapar Institute of Engineering, India.

***Abstract*—Supply chain is a complex system of organizations, people, information, and resources involved in providing services from supplier to customer. The changing technology has made the survival in commerce highly competitive and price sensitive. Blockchain technology can be the game-changer for decentralizing infrastructure and building a trust layer for business logic. BitCom is a commerce model based on the emerging technology of blockchain. It is a framework deriving its roots from both permissioned and permissionless blockchains to achieve a feasible solution to the problem of automating commerce. The model caters to need of profit maximization for suppliers and consumers using iterative auction mechanism. Parties bid to smart contract which act as auctioneer for maximizing the profit. It uses flexible smart contracts for negotiations and transactions while permissionless entry is provided to the users. Mathematical parameter named credibility score has been created to deal with trust issues in the decentralized network. BitCom provides a fresh perspective on the concept of supply chain and commerce. The objective of model remains to provide enhanced transparency, greater scalability, better security and scope of innovation. It is likely to propel the next industrial revolution, providing a new paradigm for doing business in finance, transportation, shared economy.**

***Index Terms*—Blockchain, Commerce, Double Auction, Fintech, Smart Contracts, Supply Chain**

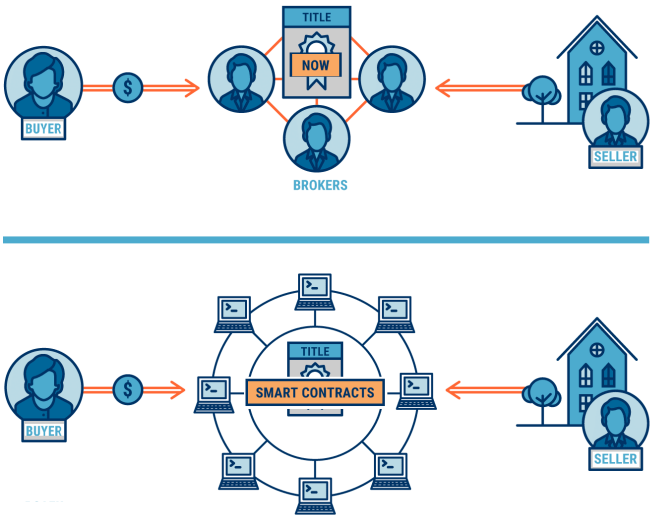

Fig. 1: (Above figure) Current distributed network of supply chain. There are middlemen involved in each link increasing system wide costs and creating a bulky supply chain. (Below figure) Proposed network using smart contracts which act as intelligent negotiator and auctioneer

I. INTRODUCTION

Supply chain can be defined as successful integration of customers, retailers, distributors and manufacturers [1]. Over the years, it has evolved to maximize service for all the involved nodes while effectively minimizing system wide costs [2]. Maintaining security is an intrinsic factor of this system. Over the years, the idea that have driven this concept is network and inventory optimization. All the companies want a clean supply chain to lower costs. Inventory optimization refers to the practice of maintaining sufficient inventory to match future consumer demands [3]. With manufacturing capacity increasing more than ever, there is need to define demand and to create sufficient inventory for catering this demand [4].

High competition, price pressures, outsourcing and shortened product cycles have revolutionized the business landscape completely. However, they have created the need for new flexible processes which can blend with the new global market and current manufacturing units [4].

Current supply chain model is based on the vertical integration of manufacturers, distributors and retailers. Manufacturers provide inventory of a given product. Retailers make the product available in the market. Distributors understand the market and retailers fill the gap between manufacturers and customers as shown in figure 1. But there are multiple problems associated with this model. Like, there are middlemen connecting two nodes together and they charge a substantial fee for their service. For example, E-commerce websites like Amazon, monetize on the same concept. In India, as of January 2019, amazon.in charges a referral fee ranging between 3 percent to 25 percent from every seller for every item sold [5]. Also it charges a closing fee based on the price range of the product. All fees is exclusive of the government taxes and referral fee is non-refundable even if the order is cancelled [5]. Secondly there is need of trusted authority such as government or notary, which has own rules and restrictions which are hindrance to e-trading. Apart from the high costs involved

in introducing different layers between the manufacturers and customers, there are various security and quality issues also involved. There have been various instances of counterfeit products and product quality issues at different levels in the existing supply chain network. The manufacturing economy of china has reported a direct loss of around 170 billion RMB per year, due to the quality issues in supply chain [**?**].

Various works have been done in regards of improving the level of transparency and security in supply chain which are discussed in next section. Nevertheless, the current models of supply chain have been insufficient to handle to personal interests of the stakeholders of supply chain. The emerging concept of blockchain, has proven itself by establishing trust, traceable transactions and minimal transaction costs without any central authority [6], [7], [8].

This paper proposes an architecture combining different aspects of blockchain applied to present market condition to accomplish a system of equilibrium while staying true to the inherit features of supply chain as shown in figure 1. Blockchain can act as a conceptual party that insures correctness of the network and availability while maintaining privacy of all participants. There is no intermediary fee charged by this network and no central authority monetizing on each transaction. While a public profile can be made to brand and advertise, a private key unique for each personnel is created to protect its transactions. A distributed ledger can be used to identify potential markets and demand trends. Smart Contract is created for each transaction to provide solution in case of a dispute and credibility of each node is judged based on it's history in the network.

Trading among the stakeholders involves a number of parameters such as mutual buyer trust, seller reputation or credibility score of buyer and customer. Moreover in reality, the transaction involves bidding between customer and supplier. Both the entities want to maximize their profits. So we make use of smart contracts which act as negotiator between the two parties. Smart contract is trusted entity, rather than an user which follows a set of defined rules. It calculates the best price using iterative double auction mechanism based on number of customers, number of suppliers, current demand, current supply etc. Both parties bid until they reach a point of negotiation. One's negotiation is reached, smart contract initiates generation of block into the publicly distributed ledger. At the same time smart contracts are also involved in removal of malicious nodes (buyers or suppliers) using byzantine fault tolerant consensus mechanism.

Rest of the paper is organized in following manner. In section II, we present the review of the current works in direction of using the concept of blockchain in domains other than financial services. Section III demonstrates the background of the blockchain technology and its inherent features. In section IV, we propose the framework for actually implementing a decentralized supply chain model without involving any third party governing authority. We also focus on iterative double auction mechanism to maximize the profit for both, sellers and buyers. Section V compares the proposed architecture with the current centralized model of supply chain to give a better insight on the potential of using blockchain technology. Section VI discusses the future aspects in this direction and section VII, finally concludes the paper.

II. Related Works

Supply chain use case is challenging as there is need of solving real business problems such as lack of trust, standardisation. Mutual distrust is function of multiple parameters such as credibility of supplier or customer, shipment delays, repayment delays. Moreover a large number of middleman make the things complex.

The objective is What if this could be digitized? The need for these types of intermediaries could be removed from the supply chain. The solution comes up is block chain, which is emerging technology and is under great scrutiny to solve the problem of decentralisation. [9] explains how blockchain can help in overcoming the trust issues. Blockchain technology became popular with rise of crytocurrency, solving the issues related to security [10], [11]. Blockchain is a distributed immutable public ledger. There have been a number of works that deal with creating applications based on blockchain ranging from healthcare systems [12], [13] to edge computing [14], [14], [15] presented on how the blockchain would revolutionise & would eeshape the consumer industry. [16] presented a simple supply chain model based on blockchain, to facilitate trade between a seller and buyer. However the model considered was far from reality. [17] makes use of a paid trusted third party (TTD) between the seller and buyer instead of a smart contract. This funded moderator is trusted both by seller and the buyer. This model is more expensive as the TTD needs to be paid both by the seller and the buyer. [18] enhances the commerce model in [17], by using the TTD as a moderator to solve any disputes between the seller and the buyer. However the issue of privacy and fully distributed system were not resolved. J. Matamoros et al. [19] came up with concept of trading among multiple parties without need of third parties. N. Z. Aitzhan et al., [20] furthur extended it using multi-signatures blockchain and anonymous messaging streams.

With evolution of blockchain, came the concept of smart contracts. Smart contract is set of rules that are followed during the transaction. Smart contracts provided better cooperative content delivery. [21], [22]. B. Zhang et al., [23] enhanced on model using game theoratic optimisations. S. Mahajan et al., optimised trading using stackelberg game approach [24].

Although there are various works explaining the use of blockchain in this domain, but, there is no generic framework that can be used by supply chain in real life by optimising the trade. We employ the potential of blockchain to supply chain, at the same time model an auction mechanism using smart contracts that is quite similar to real life. Model eliminates need of any intermediary and provide secure trading. The contributions of this paper are highlighted as:

1) **Iterative Auction Mechanism**
   For optimization of maximum profit for consumers and suppliers, an iterative auction mechanism is proposed. Smart Contract act as auctioneer to maximize overall profit while protecting privacy of users.

2) **Credibility Scoring**
   Each user is accessed based on credibility score, trust and reputation. Model provisions smart contract to eliminate malicious or suspicious node using byzantine fault tolerant consensus mechanism.
3) **Eliminating Middleman in Supply Chain**
   We propose a fully decentralised mechanism for providing services or trading between consumers and suppliers. This eliminates the privacy and security issues and cuts down the broker fees.

III. Background

Blockchain is the realization of the Distributed ledger technology (DLT) based on a peer to peer network [25]. It facilitates secure transaction between two groups in absence of a central authority authenticating and updating ledgers[26]. For every transaction or a group of transactions, a new immutable block is added to an already established chain of blocks, hence the name "blockchain".There are two types of blockchain models are :-

- Permissioned blockchains.
- Permissionless blockchains.

Key feature of blockchain is real time record distribution where in all the distributed ledgers are updated as transactions and other events occur. The central idea is pseudonymous nature of the user and resilience against network wide attacks.

A. Permissioned Blockchain

It is a proprietary network that governs what kind of nodes can perform transactions in a given network. If the model of permissioned blockchain were to be applied to supply chain and commerce, current nodes would be able to decide who gets to gets to participate in the network. This idea is not feasible because no seller wants more competition and hence would not allow new sellers to enter the market. Instead, everyone should be allowed to participate freely in the market.

Furthermore, permissioned blockchain often and inessential creates below level trust assumptions where one node cannot trust another node [27]. Smart contracts are used as consensus mechanism . While this assumption works for cryptocurrency, in real world scenarios, trust should be established for effective and efficient supply chain [28]. Trust can be created by the quantity of interaction between two nodes or transactions in business world.

Smart contracts are generally designed to be executed on all nodes which seems oddly open for a concept based on privacy. Rather, it should be restricted to certain nodes [27].

Another subject of discussion is the inflexible nature of smart contracts. A single smart contract cannot fit the needs of every node and thus should offer adaptability while maintaining the immutable structure when added to the chain [29].

Permissioned blockchain model is insufficient to serve a platform that could benefit from distributed ledger technology.

B. Permissionless Blockchain

It is an open network accessible by all. Anybody can perform transactions here. While it seems a more appropriate for a complex network of commerce, a certain level of privacy is prerequisite for practical purposes. One manufacturer may be selling the same product to two different distributors at different prices. While an open ledger seems to provide an ideal world where everyone can acquire products at the same price, it is not feasible.

If, there are no norms (which are provided by central authorities in distributed network), there is no way of expelling fake and dishonest nodes from the network. In Bitcoin, one of the largest application of permissionless blockchain, the exchange involves cryptocurrency only. But in supply chain, goods and service exchanges are also involved. Therefore we need a way to distinguish non-credible nodes from credible nodes.

Generally, permissionless blockchain is constructed around single cryptocurrency but for business applications, such dependency is not suitable for scalability and globalization.

IV. Proposed Architecture

By combining the advantages of both permissioned and permissionless blockchains, we propose a new structure for supply chain and commerce. We present a model that derives its roots form the existing principles and propose new methods to achieve a sustainable and feasible supply chain model. We propose a network where a user can enter freely without any restrictions or peer review. Manufacturers, distributors, retailers and customers - everyone can become a part of this network. Once the user becomes a node of the network, he / she is free to assume the role of a seller or buyer. There is no specific role that a node is assigned. Everyone is a client and everyone is a service provider.

A node has pseudo privacy. It can make a public profile to advertise and still remain anonymous for transactional security. Public profile is linked to the public key generated for the node while the transactions are linked to the private key of the node.

Once the user is successfully added to the network, he can add products to the network. Proof of work (PoW) consensus will be used to add the product block to the distributed ledger [30]. All the mining would be performed by miners who will receive incentives in form of cryptocurrency for maintaining the network. All the terms of agreement will be preserved in a smart contract that is accessible only by the nodes involved. We emphasize on using a flexible smart contract that can be modified to cater a node's need but still be immutable after the signature of the participating nodes [31] [32]. In here, we have used smart contracts for optimization of trade profit and acting as mediating contract between consumers and suppliers.

Once a smart contract is signed by the agreeing parties, it will be added to the network and be identified by the mutual key of the concerned nodes. A block containing information about the product sold will be added to the distributed ledger. This information is available to all the nodes for market analysis [33].

To help develop trust in the network, we introduce a mathematical parameter named credibility score for each node.

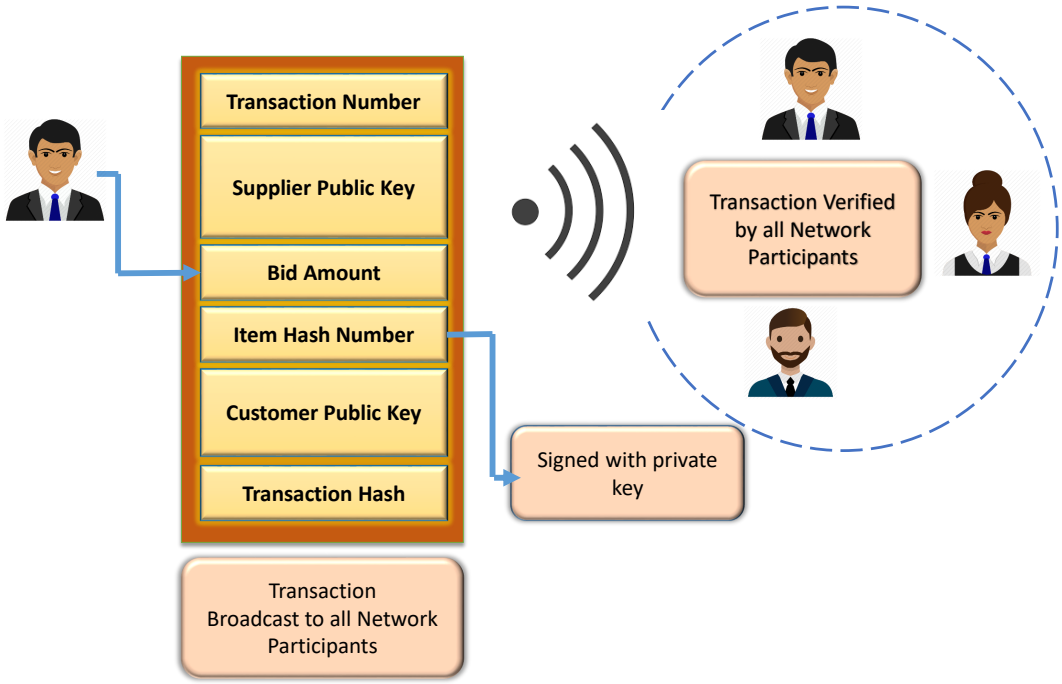

Fig. 2: Description of the block created once the transaction between consumer and supplier is made. The block is propagated to all the nodes, where the consensus is achieved using proof of work

It is a factor meant to help nodes trust each other while performing transactions. It will be calculated by the successful and unsuccessful transactions performed by the node and will be visible to rest of the nodes.

The credibility score thus calculated can be used to remove dishonest nodes form the network. A modified version of Byzantine Fault Tolerance will be used to reach to consensus. If the credibility score falls below a threshold score, network will pose a challenge whether to remove the node or not and all the nodes that have had interaction with the faulty node (validating nodes) will participate in the consensus.

A. *Adding users to the network*

When a user wants to enter the network, the network checks whether it is a new or an already existing user. Existing user can directly login to the network. In case of a new user, a unique address is generated for the network and two keys namely - public key and private key are generated using the key generation algorithm (KGA). Two random and large prime numbers m, n are choosen in a way that $k = p*q$. Further, an integer (b) is chosen from $\left[1,\phi(k)\right]$, where $\phi(k)$ is the euler function. The great common multiple of b and $\phi(k)$ is 1. Now, to generate the public and private keys, KGA calculates a new parameter g, such that, $g*b = 1(modk)$. Ones this is done, b, is assigned as the private key and g is assigned as the pubic key of a user.

The generating function uses SHA256 cryptographic hash. Password is created for future logins. After this, node has been added to the network. Also the node is asked to create a public profile that is visible throughout the network. This public profile is linked to the public key of the node while the private key is designated to be used for future transactions. Creating a public profile is a one time task.

Supply chain is a public distributed ledger of goods that a seller wants to sell. After being added to the network, a buyer can browse for products while a seller can introduce his products to the network. One product will be entered at a time. A block will be created for every product and will contain its identification number, name, description, time stamp, date of expiry. The supplier encrypts the block with its private key.

B. *Transactions*

This section presents the process of actual dealing between the supplier and the buyers. Since there are multiple buyers and multiple sellers in the network, every entity would like to increase its profits. The seller wants to sell the goods at maximum price available, while consumer would like to buy at the cheapest cost. Moreover the entities participating are not assumed to be trusted. So we introduce a smart contract which acts mediator between the consumers and suppliers. The smart contract act as auctioneer, where the customers try to bid the least price to get the stakes. On the other hand sellers want to maximise the profit. The problem formulation of trading is explained in the following section.

C. *Auctioning Problem formulation*

This section presents the problem formulation for dynamic pricing and to maximize the overall profit for the sellers and the buyers. The smart contract (SC) facilitates trading and can communicate with any entity (E) to establish a real-time trading market.

The set of consumers is denoted by $C = (C_i | i \in \mathbb{N}), \mathbb{N} = \{0, 1, 2, \ldots, I\})$. While, the set of suppliers is denoted by $S = (S_j | j \in \mathbb{N}_\supset), \mathbb{N}_\supset = \{0, 1, 2, \ldots, J\}$

We calculate the trade satisfaction (U) for customer and trade dissatisfaction (L) of suppliers in the system. In this scenario, we have considered that there are multiple customers and multiple buyers that are bidding to buy a particular item. The maximum price that seller can sell is capped at η (imposed based on government restrictions). Customers want to minimise the cost they have to pay. So the utility of customer is how much less they pay from market price η. $U(C)$ according to utility theory can be modelled as:

$$U(\mathbf{C}) = \left(\sum_{i=1}^{I} \sum_{j=1}^{J} \ln(\eta - c_{\mathrm{ij}}) \right) \tag{1}$$

Suppliers want to maximise their profit. Trade dissatisfaction for supplier is a function of how far is actual selling value from market price. Using utility theory, trade dissatisfaction $L(S)$ is given by:

$$L(\mathbf{S}) = \sum_{i=1}^{I} \sum_{j=1}^{J} (\eta - s_{\mathrm{ji}})^2 \tag{2}$$

Thus the overall utility problem is presented by $\mathbf{P}$

$$\mathbf{P} : \max_{\forall(\mathbf{c}_{\mathrm{ij}}, \mathbf{s}_{\mathrm{ji}})} (U(\mathbf{C}) - L(\mathbf{S})) \tag{3}$$

$$\mathbf{P} : \max_{\forall(\mathbf{c}_{\mathrm{ij}}, \mathbf{s}_{\mathrm{ji}})} \left(\sum_{i=1}^{I} \sum_{j=1}^{J} \ln(\eta - c_{\mathrm{ij}}) - \sum_{i=1}^{I} \sum_{j=1}^{J} (\eta - s_{\mathrm{ji}})^2 \right)$$

$$Constraints : \sum_{i=1}^{I} s_{\mathrm{ji}} \leq \eta \sum_{i=1}^{I} (\delta_{ij}), \forall j \in \mathbb{S},$$

$$s_{\mathrm{ji}} = c_{\mathrm{ij}}, \forall i \in \mathbb{C}, \forall j \in \mathbb{S},$$

$$c_{\mathrm{ij}} \geq 0, \forall i \in \mathbb{C}, \forall j \in \mathbb{S}$$

$$\frac{\partial \mathbf{P}}{\partial c_{ij}} = \frac{-1}{(\eta - c_{\mathrm{ij}})}$$

$$\frac{\partial}{\partial c_{ij}} \left(\frac{\partial \mathbf{P}}{\partial c_{ij}} \right) = \frac{-1}{(\eta - c_{\mathrm{ij}})^2}$$

$$\frac{\partial \mathbf{P}}{\partial s_{ji}} = -2(\eta - s_{ji})$$

$$\frac{\partial}{\partial s_{ji}} \left(\frac{\partial \mathbf{P}}{\partial s_{ji}} \right) = 2$$

The objective function in is strictly concave. Therefore, using Karush-Kuhn-Tucker (KKT) [34] conditions, an optimal and unique solution always exists. The following Lagrangian is obtained by carrying out the relaxation of constraints. The optimal solution is given by

$$\begin{aligned} OPT_s = \quad & U(\mathbf{C}) - L(\mathbf{S}) \\ & + \sum_{i=1}^{I} \beta_i \left(\eta \sum_{j=1}^{J} c_{\mathrm{ij}} - c_i^{\max} \right) \\ & + \sum_{j=1}^{J} \gamma_j \left(\sum_{i=1}^{I} s_{\mathrm{ji}} - \eta \sum_{i=1}^{I} (\delta_{ij}) \right) \\ & - \sum_{j=1}^{J} \sum_{i=1}^{I} \mu_{\mathrm{ij}} c_{\mathrm{ij}}. \end{aligned}$$

where $\boldsymbol{\beta}, \boldsymbol{\gamma}, \boldsymbol{\mu}$ are lagrange multipliers under stationary conditions. Taking the derivatives, we get

SC performs multiple iterations of double auction mechanism based on the input supply and demand curve (vector) given in eq. 2 & 3. The sellers and buyers update bid price vectors after every round. The auctioneer solves the following optimal allocation problem OPT_{max}. For every iteration of algorithm, smart contract generates a transaction with confirmed supplier and buyer, with the agreed price for a quantity. Buyers ans sellers update their bid price vector for further iterations based on current information. b_{ij} be the bid for next iteration for i_{th} customer to j_{th} supplier. $P(C_i)$ be total amount that customer i has to pay. Similarly, k_{ji} be the bid for next iteration for supplier j to i_{th} customer. $A(S_j)$ be total amount that supplier gets. SC, as a broker not only decides for the suitable seller and buyer on the basis of consumer's demand, but also tries to maximize their profits[35]. Sellers are expecting maximum profit, whereas the buyers are looking for the minimum cost. To achieve an equilibrium in the market, SC, provides a solution that maximizes the mutual profit for both sellers and buyers. Total satisfaction and cost function is calculated as following. Using [36] we form the problem formulation which auctioneer has to maximise.

$$OPT_{max} : \max_{\mathbf{b}_{ij}, \mathbf{k}_{ji}} \sum_{i=1}^{I} \sum_{j=1}^{J} \left[\frac{1}{b_{\mathrm{ij}}} \ln(\eta - c_{\mathrm{ij}}) + \eta k_{\mathrm{ji}} (\ln s_{\mathrm{ji}}) \right] \tag{4}$$

The problem OPT_{max} is similar to OPT_s problem defined above with same constarints. Applying KKT,

$$\nabla_{c_{\mathrm{ij}}} OPT_{max} = \frac{1}{-b_{\mathrm{ij}}\eta - c_{\mathrm{ij}}} + \beta_i - \mu_{\mathrm{ij}},$$

$$\nabla_{s_{\mathrm{ji}}} OPT_{max} = \frac{\eta k_{\mathrm{ji}}}{s_{ji}} + \gamma_j$$

where $\boldsymbol{\beta}, \boldsymbol{\gamma}, \boldsymbol{\mu}$ are positive lagrange multipliers.

There exist linear correlations for the maximum mutual profit for a single transaction and overall profit of system. So equating the differentials to get the bid for next iteration for consumer and supplier.

$$\frac{1}{b_{\mathrm{ij}}} = \frac{\eta - c_{\mathrm{ij}}}{\left(J\eta - \sum_{j=1}^{J} c_{\mathrm{ij}} \right)}$$

Algorithm 1 Functioning of smart contract

Input: Set of customers (ϕ_C), Set of suppliers (ϕ_S), demand of consumer (δ_{ij}), bid price vector of consumer (b_{ij}), bid price vector of supplier (k_{ji})

Output: Negotiated Price, consumer & buyer identity

1: **while** δ_{ij} != 0 **do**:
2: Calculating optimum value of OPT_{max} using bid price vector of consumer and supplier.
3: return b_{ij}, i, j
4: Make a transaction between i^{th} customer and j^{th} supplier with b_{ij} as bid amount for Δ_{ij} supplies.
5: δ_{ij} = δ_{ij} - Δ_{ij}
6: Input (New Bids from Suppliers and Customers)

$$k_{\text{ji}} = l_1 \frac{(\eta - s_{\text{ji}})s_{ji}}{\eta}$$

The algorithm for the smart contract is given in algorithm **??**. It takes set of customers, set of suppliers, demand of consumer, bid price vector of consumer, bid price vector of supplier as input and outputs customer and buyer with the final bid price.

D. Mechanism of blockchain for commerce trading

After the consumer and supplier are decided by the negotiator. Once both the seller and buyer are satisfied, the smart contract creates block that is digitally signed by key of both the parties. The structure of transaction block is presented in figure 2. Negotiator then creates block with quantity, discount amount, date of dispatch, period of arrival, mode of transport, initial payment, repayment period. Payment is done in form of cryptocurrency and a block showing the transaction is added to the network. A new block is added for every transaction and proof of work is used as the consensus mechanism. Proof-of-Work (PoW) is based on the fact that work must be feasibly hard to compute but easy to verify. It also provides protection against spam or DoS attacks where every node is forced to do some computational task. Before a new block of transactions is inserted into block chain list, PoW is carried out for consensus mechanism. Each mining node competes to validate the block and validating node is rewarded as an incentive.

E. Removing a node from the network

Trust is a pillar for commerce. To introduce it to our model, we use the concept of credibility score of each node. For every successful transaction, credibility score of a node increases and for every unsuccessful transaction, credibility score of the node decreases. In a case where the node has been performing badly for many transactions, his score would fall below a present threshold. In such a case, network will pose a challenge asking the users whether a given node should be expelled from the network or not. We will use modified version of Byzantine Fault Tolerance (BFT) consensus i.e. the concept of majority to attain an answer [37]. Consensus mechanism provides correctness of the shared data in the network and fault tolerance in case a node fails to participate in the decision making [38].

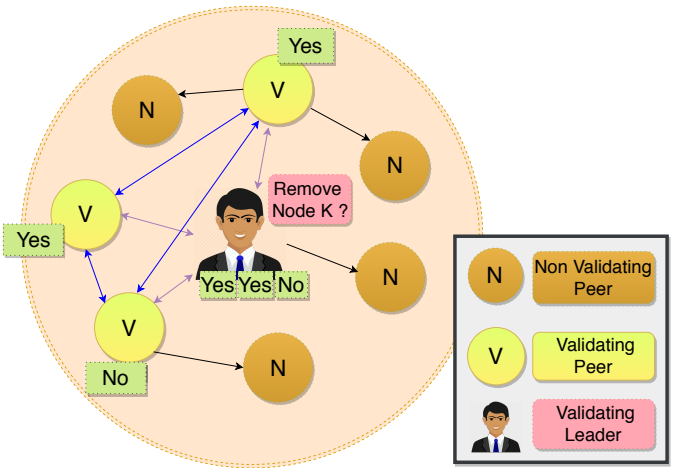

Fig. 3: Byzantine fault tolerant consensus mechanism. A validating leader (smart contract) initiates the request to remove the malicious node. It sends message to all the validating nodes. Based on received messages it takes the decision to remove the node or not.

Only those users who have transacted with the node (validating node) in question will be asked if they were satisfied with their transaction or not. If negative reviews exceed the positive reviews, node will be removed from the network. This function has been added to remove dishonest nodes from the network and increase trust within the nodes as shown in figure 3.

F. Credibility score calculation

Trust is factor of supply chain that is often overlooked by most of the proposed frameworks of commerce. Trust and commitment are critical factors for a company to build competitive advantage in the market [39].In order to introduce it into our model, we propose a mathematical parameter named credibility score. It can be computed using equation 5 [40].

The credibility score of a node can assume a value in the range of 0 to 1. When a user first enters the network, it will be equal to 0.5. There is no definite way of ensuring that a node will never betray the network. But we can say that credibility score is the probability of a node behaving appropriately in future [40].

$$Trust_n = \frac{1}{1 + e^{-}\alpha(\#good - \#bad)} \tag{5}$$

Alpha is the step size and calculated by the amount of cryptocurrency involved in a particular transaction. Credibility score will be calculated after every transaction and will be visible to every node in the network.

V. Results & Discussion

Fig. 5 depicts how the auction algorithm functions. In Fig 5, there are 6 suppliers and 1 buyer (red line). Buyer and Seller bids their prices for different quantity forming the demand curve and supply curve. Smart contract acts as an auctioneer and finds, The double auction mechanism tries to optimise the maximum profit of both by reaching at demand-supply

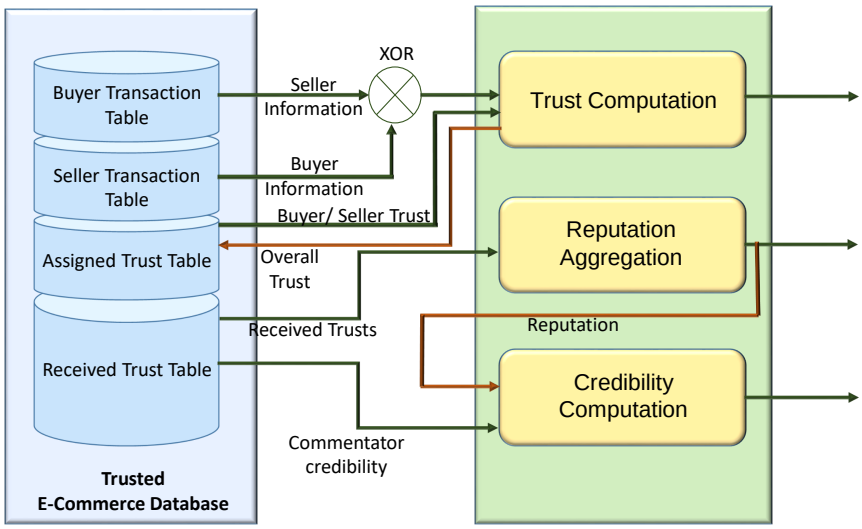

Fig. 4: Description of credibility score calculation using trust and reputation

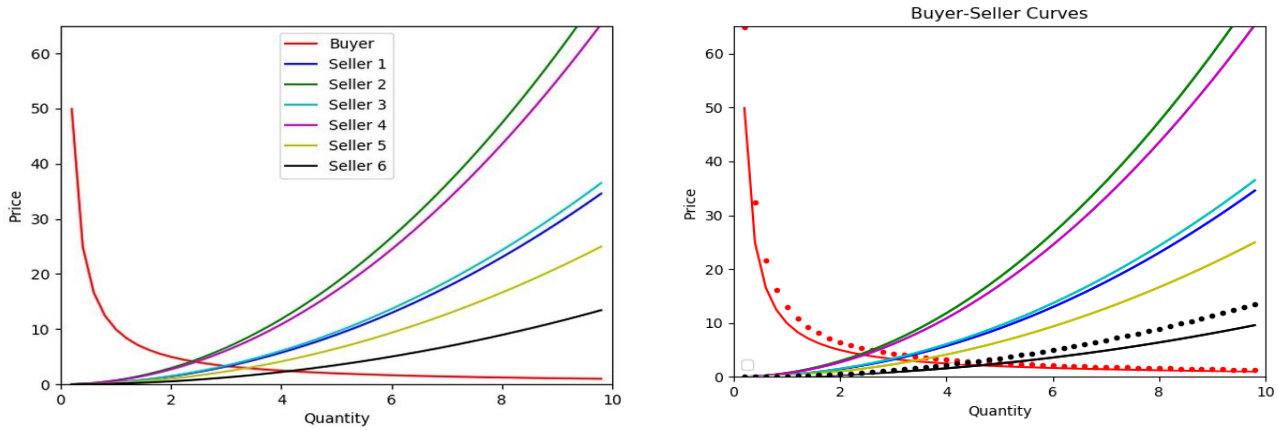

Fig. 5: Iterative Double Auction Mechanism: (a) depicts the initial iteration for single buyer and multiple sellers. (b) depicts how bids change after an iteration of auction mechanism. Dotted red line is new bid of buyer from red solid in previous iteration. Black dotted line is new bid of seller in new transaction.

equilibrium. Once the deal is made, it makes a transaction between i^{th} buyer and j^{th} supplier in blockchain. In the next iteration, buyer increases the bid based on previous iteration. In fig 5(b), buyer shifts his bid in next iteration, and supplier lowers his bid based on b_{ij} & k_{ij} values.

This model is an amalgamation of the current supply chain with technology to achieve a realistic platform for commerce powered by blockchain. It advocates transparency of the transactions and non-falsifiable nature of the distributed ledger [41]. Supply chain is a dynamic framework that alters with time. Customer demands and suppliers' capacity to meet that demand are the key factors affecting it [2].

Current supply chain includes a facility to trust another facility without any prior knowledge. This concept is faulty and often leads to dishonest claims and frauds. Information sharing helps reduce behaviour uncertainty and results in significant boost in trust [42]. Our system provides a mathematical measure named credibility score to solve this problem. It is calculated by the successful and unsuccessful transactions of a node and helps a user decide the credibility of that node. It helps achieve a model where trust is not blind but proven by history of a node. Furthermore, if the credibility score of a node falls below a certain threshold, he can be expelled from the network with permissioned consensus. This feature can be used to identify fake companies and products and remove them from the network. The model for trust, reputation and credibility computation is presented in figure 4. Network has a trusted e-commerce database, which is accessible to smart contract. Except smart contract no entity has the write to modify and read the database. Network after every transaction calculates the credibility score, trust and reputation parameters based on transaction table of buyer and seller.

VI. Conclusion

This paper uses concept of blockchain for commerce trading. We model the problem scenario of trade using iterative double auction mechanism. Model provides improved transparency, better scalability and security. Smart contracts provides an alternative solution to provide peer to peer auctioning without need of trusted party. To establish trust in the network, we introduce a mathematical parameter named credibility score. Credibility score being the measure of credibility of seller and buyer. This model is a step further in integrating technology with the current commerce setup providing decentralizing infrastructure and business logic trust among stakeholders.

References

[1] https://www.investopedia.com/terms/s/scm.asp.

[2] http://lcm.csa.iisc.ernet.in/scm/supply_chain_intro.html.

[3] https://www.avidxchange.com/inventory-optimization-role-businesses/.

[4] https://www.sdcexec.com/sourcing-procurement/news/10358095/six-key-trends-changing-the-supply-chain-management-today.

[5] https://sellercentral.amazon.in/gp/help/external/help.html_?itemID=200336920ref=efph_200336920_cont_G2.

[6] D. Katz, M. Bommarito, and J. Zelner, "The trust machine," *The Economist, October*, 2015.

[7] S. Chen, R. Shi, Z. Ren, J. Yan, Y. Shi, and J. Zhang, "A blockchain-based supply chain quality management framework," in *2017 IEEE 14th International Conference on e-Business Engineering (ICEBE)*. IEEE, 2017, pp. 172–176.

[8] S. Ramamurthy, "Leveraging blockchain to improve food supply chain traceability," *IBM Blockchain Blog, Nov*, 2016.

[9] E. Karaarslan and E. Adiguzel, "Blockchain based dns and pki solutions," *IEEE Communications Standards Magazine*, vol. 2, no. 3, pp. 52–57, 2018.

[10] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in industrial internet of things," *IEEE transactions on industrial informatics*, vol. 14, no. 8, pp. 3690–3700, 2018.

[11] Z. Guan, G. Si, X. Zhang, L. Wu, N. Guizani, X. Du, and Y. Ma, "Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities," *IEEE Communications Magazine*, vol. 56, no. 7, pp. 82–88, 2018.

[12] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K.-K. R. Choo, "Blockchain: A panacea for healthcare cloud-based data security and privacy?" *IEEE Cloud Computing*, vol. 5, no. 1, pp. 31–37, 2018.

[13] P. K. Vairam, G. Mitra, C. Rebeiro, B. Ramamurthy, and K. Veezhinathan, "Approxbc: Blockchain design alternatives for approximation-tolerant resource-constrained applications," *IEEE Communications Standards Magazine*, vol. 2, no. 3, pp. 45–51, 2018.

[14] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When mobile blockchain meets edge computing," *IEEE Communications Magazine*, vol. 56, no. 8, pp. 33–39, 2018.

[15] J.-H. Lee and M. Pilkington, "How the blockchain revolution will reshape the consumer electronics industry [future directions]," *IEEE Consumer Electronics Magazine*, vol. 6, no. 3, pp. 19–23, 2017.

[16] https://dappsforbeginners.wordpress.com/tutorials/two-party-contracts/ .

[17] https://blog.localethereum.com/how-our-escrowsmart-contract-works/ .

[18] https://www.openbazaar.org/features/.

[19] J. Matamoros, D. Gregoratti, and M. Dohler, "Microgrids energy trading in islanding mode," in *2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 2012, pp. 49–54.

[20] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 5, pp. 840–852, 2018.

[21] B. Barua, M. Matinmikko-Blue, Y. Zhang, A. A. Abouzeid, and M. Latva-aho, "On contract design for incentivizing users in cooperative content delivery with adverse selection," *IEEE Transactions on Wireless Communications*, vol. 17, no. 12, pp. 8418–8432, 2018.

[22] K. Zhang, Y. Mao, S. Leng, Y. He, S. Maharjan, S. Gjessing, Y. Zhang, and D. H. Tsang, "Optimal charging schemes for electric vehicles in smart grid: A contract theoretic approach," *IEEE Transactions on Intelligent Transportation Systems*, no. 99, pp. 1–13, 2018.

[23] B. Zhang, C. Jiang, J.-L. Yu, and Z. Han, "A contract game for direct energy trading in smart grid," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 2873–2884, 2018.

[24] S. Maharjan, Q. Zhu, Y. Zhang, S. Gjessing, and T. Basar, "Dependable demand response management in the smart grid: A stackelberg game approach," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 120–132, 2013.

[25] A. Collomb and K. Sok, "Blockchain/distributed ledger technology (dlt): What impact on the financial sector?" *Digiworld Economic Journal*, no. 103, 2016.

[26] A. Deshpande, K. Stewart, L. Lepetit, and S. Gunashekar, "Distributed ledger technologies/blockchain: Challenges, opportunities and the prospects for standards," *Overview report The British Standards Institution (BSI)*, 2017.

[27] M. Vukoli_'c, "Rethinking permissioned blockchains," in *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts*. ACM, 2017, pp. 3–7.

[28] I.-W. G. Kwon and T. Suh, "Trust, commitment and relationships in supply chain management: a path analysis," *Supply chain management: an international journal*, vol. 10, no. 1, pp. 26–33, 2005.

[29] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *2016 IEEE symposium on security and privacy (SP)*. IEEE, 2016, pp. 839–858.

[30] R. Qin, Y. Yuan, and F.-Y. Wang, "Research on the selection strategies of blockchain mining pools," *IEEE Transactions on Computational Social Systems*, no. 99, pp. 1–10, 2018.

[31] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *Ieee Access*, vol. 4, pp. 2292–2303, 2016.

[32] https://www.coindesk.com/information/ethereum-smart-contracts-work.

[33] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. Kishigami, "Blockchain contract: Securing a blockchain applied to smart contracts," in *2016 IEEE International Conference on Consumer Electronics (ICCE)*. IEEE, 2016, pp. 467–468.

[34] S. Boyd and L. Vandenberghe, *Convex optimization*. Cambridge university press, 2004.

[35] D. Friedman, *The double auction market: institutions, theories, and evidence*. Routledge, 2018.

[36] F. P. Kelly, A. K. Maulloo, and D. K. Tan, "Rate control for communication networks: shadow prices, proportional fairness and stability," *Journal of the Operational Research society*, vol. 49, no. 3, pp. 237–252, 1998.

[37] M. Castro, B. Liskov *et al.*, "Practical byzantine fault tolerance," in *OSDI*, vol. 99, 1999, pp. 173–186.

[38] A. Baliga, "Understanding blockchain consensus models," in *Persistent*, 2017.

[39] Y. Yuan, B. Feng, F. Lai, and B. J. Collins, "The role of trust, commitment, and learning orientation on logistic service effectiveness," *Journal of Business Research*, vol. 93, pp. 37–50, 2018.

[40] G. Zyskind, O. Nathan *et al.*, "Decentralizing privacy: Using blockchain to protect personal data," in *2015 IEEE Security and Privacy Workshops*. IEEE, 2015, pp. 180–184.

[41] S. Apte and N. Petrovsky, "Will blockchain technology revolutionize excipient supply chain management?" *Journal of Excipients and Food Chemicals*, vol. 7, no. 3, p. 910, 2016.

[42] I.-W. G. Kwon and T. Suh, "Factors affecting the level of trust and commitment in supply chain relationships," *Journal of supply chain management*, vol. 40, no. 1, pp. 4–14, 2004.