BlockCom: A Blockchain based Commerce Model for Smart Communities using Auction Mechanism

Vikas Hassija[1], Gaurang Bansal[2], Vinay Chamola[2], Vikas Saxena[1], Biplab Sikdar[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 Electrical and Computer Engineering, National University of Singapore, Singapore

***Abstract*—Smart Communities seeks to thrive in a context of broadband economy, its engine and reason for being. The success of any community is a function of its economic backbone or the supply chain. A supply chain can be defined as the integration of customers, retailers, distributors and manufacturers. 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. BlockCom is a commerce model based on the emerging technology of blockchain. This paper presents a double auction scheme for energy trading between customers and suppliers. A smart contract implements a distributed algorithm to maximize individual participating profit. Parties bid to smart contract which act as auctioneer for maximizing the profit. Mathematical parameter named credibility score has been created to deal with trust issues in the decentralized network using byzantine fault tolerant mechanism. BlockCom provides a fresh perspective on the concept of supply chain and commerce.**

I. Introduction

Smart communities seeks balance between the local economy and globalization. Regardless of the size of the community, whether large or small, the objective is to improve its competitiveness in trade and global economy. Information and communications technology is used to build efficient trade mechanism or supply chain.

Supply chain over the year has evolved to maximize service for all the involved nodes while effectively minimizing system wide costs [1]. Maintaining security is an intrinsic factor of this system. Over the years, the idea that has driven this concept is network and inventory optimization. With manufacturing capacity increasing more than ever, there is need to define demand and to create sufficient inventory for catering this demand [2]. 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 [2].

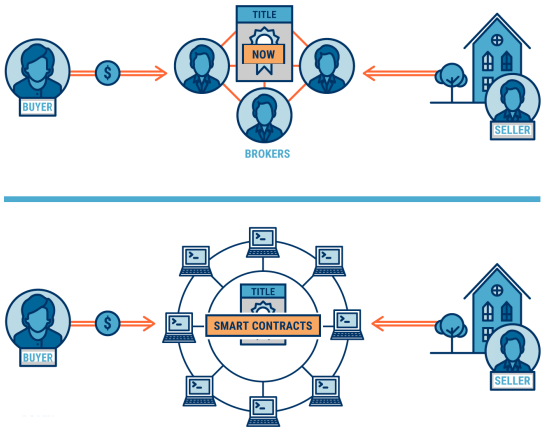

Fig. 1. (Top) Current distributed network of supply chain. (Bottom) Proposed network using smart contracts which act as intelligent negotiator and auctioneer

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 Fig. 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. 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. 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

978-1-7281-2373-8/19/$31.00 ©2019 IEEE

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.

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 Fig. 1.

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. In section III, 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, namely the sellers and the buyers. Section V discusses the proposed architecture with the current centralized model.

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 (i.e. middlemen) 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. [3] explains how blockchain can help in overcoming the trust issues. Blockchain technology became popular with rise of crytocurrency, solving the issues related to security [4], [5]. 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 [6], [7] to edge computing [8],[9], [10].

[11] presented on how the blockchain would revolutionise & would reshape the consumer industry. [12] 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. [13] 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. [14] enhances the commerce model in [13], 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. [15] & [16] came up with concept of trading among multiple parties without need of third parties. N. Z. Aitzhan et al., [17] 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 [18]. GS Aujla et al., [19] also presented trading with dynamic pricing model.

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. The proposed model eliminates need of any intermediary and provide secure trading. The contributions of this paper are highlighted as:

1) **Double Auction Mechanism**
   For optimization of maximum profit for consumers and suppliers, an iterative auction mechanism is proposed. Smart Contract acts as an auctioneer to maximize overall profit while protecting privacy of users. In here, smart contract is a trusted third entity that executes the code and is visible to all the nodes in the blockchain network.
2) **Credibility Scoring**
   Each user is accessed based on credibility score, trust and reputation. The proposed model provisions smart contract to eliminate the malicious or suspicious nodes 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.

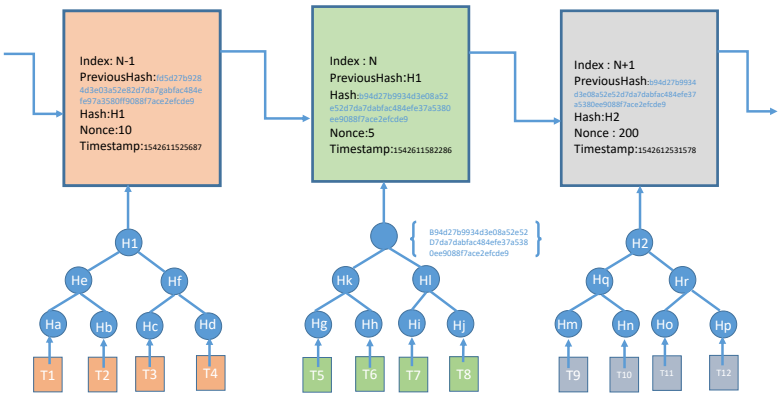

Fig. 2. Description of the block created once the transaction between consumer and supplier is made. The block is propagated to all the nodes, where the consensus is achieved using proof of work. Each block contains multimle transactions.

III. 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 [20], [21]. 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 [22] [23]. 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 [24].

To help develop trust in the network [25], we introduce a mathematical parameter named credibility score for each node. 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

Algorithm 1 Incoming user to network

function $Addnode()$
  initialize: $User$;
  if $UserAlreadyExists$ **then**
    Login to the network
  else
    initialize: $User = NewUser$;
    initialize: $Address = GenerateAddress()$;
    initialize: $Passord = SetPassword()$;

    public key, private key = Key generation()
    $Credibility\_Score = credibiltyscore(User)$;
  end if
end function

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. Description of adding a node to network is explained in algorithm 1.

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 consumer and supplier. The smart contract acts as an 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 or we refer as aggregator (AG) facilitates trading and can communicate with any entity (E) to establish a real-time trading market.

The set of consumers is denoted by $\phi_C = (C_i^n | i \in \mathbb{N}), \mathbb{N} = \{0, 1, 2, \ldots, I\})$. We denote the set of suppliers by $\phi_S = (D_j^n | j \in \mathbb{N}_\supset), \mathbb{N}_\supset = \{0, 1, 2, \ldots, J\}$

The demand of consumer is denoted in form of vector by C_i^n. $c_i^{n,\min}$ & $c_i^{n,\max}$ are minimum and maximum requirement of the consumer. AG must provide atleast $c_i^{n,\min}$ for normal trading. c_{ij}^n is demand of consumer C_i^n from D_j^n supplier. For the supplier,the supply vector for i^{th} consumer is denoted by ${D_{ji}}^n$. The total demand of consumer is given in Eqn. 1. Also, the total supply by the supplier is given in Eqn. 2. Using Eqn. 1, trade satisfaction (U_i) for i^{th} consumer is presented in Eqn. 3.

$$\mathbf{C_i^n} \triangleq \{c_{ij}^n | j \in \mathbb{Z}\} \tag{1}$$

$$\mathbf{D_j^n} \triangleq \{d_{ji}^n | i \in \mathbb{R}\} \tag{2}$$

$$U_i(\mathbf{C_i^n}) = \tau \ln \left(\sum_{j=1}^{J} c_{\mathrm{ij}}^n - (c_i^{n,\min} + 1) \right) \tag{3}$$

Here, τ is considered as a constant > 0. The maximum supply for a supplier is $D_j^{n,\max}$. The cost function for a supplier D_j^n given by

$$L_j(\mathbf{D_j^n}) = l_1 \sum_{i=1}^{I} (d_{\mathrm{ji}}^n)^2 + \psi \sum_{i=1}^{I} d_{\mathrm{ji}}^n \tag{4}$$

l_1 & ψ are constant cost factors > 0 which are fixed for a supplier depending on the trust value of the supplier.

AG, 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[26]. Sellers are expecting maximum profit, whereas the buyers are looking for the minimum cost. To achieve an equilibrium in the market, AG, provides a solution that maximizes the mutual profit for both sellers and buyers. Total satisfaction and cost function is calculated as following. Eqn. 7 gives the problem formulation which auctioneer has to maximise.

The bid price vector for i^{th} consumer is $\mathbf{B_i^n} \triangleq \{b_{\mathrm{ij}}^n | j \in \mathbb{Z}\}$. For all consumers, $\mathbf{B^n} \triangleq \{\mathbf{B_i^n} | i \in \mathbb{C}\}$. The optimal bidding for consumer would be

$$CB : \max_{\mathbf{B_i^n}} [U_i(\mathbf{C_i^n}) - pay_i(\mathbf{B_i^n})] \tag{5}$$

where $pay_i(\mathbf{B_i^n})$ is payment made by the consumer, and $Rew_j(\mathbf{S_j^n})$ be the profit of the supplier. Similarly, the bid price vector for j^{th} supplier is $\mathbf{S_j^n} \triangleq \{s_{\mathrm{ji}}^n | i \in \mathbb{C}\}$. Aggregate for all suppliers is $\mathbf{S^n} \triangleq \{\mathbf{S_j^n} | j \in \mathbb{Z}\}$. The optimal bidding for supplier is

Algorithm 2 Functioning of smart contract

Input: Set of customers (ϕ_C), Set of suppliers (ϕ_S), demand of consumer, bid price vector of consumer, bid price vector of supplier

Output: Negotiated Price, consumer & buyer identity

1: **while** (true) **do**
2: Calculating optimum value of OPT_{max} using bid price vector of consumer and supplier.
3: **if** ($\left|b_{\mathrm{ij}}^{n^{(t)}} - b_{\mathrm{ij}}^{n^{(t-1)}}\right| == 0$) **then**
4:
5: return $b_{\mathrm{ij}}{}^{n}$, i, j
6: **end if**
7: **end while**

$$ES : \max_{\mathbf{S_j^n}} [Rew_j(\mathbf{S_j^n}) - L_j(\mathbf{D_j^n})] \tag{6}$$

AG performs multiple iterations of double auction mechanism based on the input bid price. The sellers and buyers update bid price vectors. The auctioneer solves the following optimal allocation problem OPT_{max}.

$$OPT_{max} : \max_{\mathbf{C^n},\mathbf{D^n}} \sum_{i=1}^{I}\sum_{j=1}^{J} [b_{\mathrm{ij}}^n \ln(c_{\mathrm{ij}}^n) - s_{\mathrm{ji}}^n d_{\mathrm{ji}}^n] \tag{7}$$

The problem OPT_{max} is similar to $Profit_{max}$ problem defined above.

$$\nabla_{c_{\mathrm{ij}}^n} OPT_{max} = \frac{b_{\mathrm{ij}}^n}{c_{\mathrm{ij}}^n} - \eta\alpha_i + \eta\beta_i - \lambda_{\mathrm{ij}} - \mu_{\mathrm{ij}} = 0, \tag{8}$$

$$\nabla_{d_{\mathrm{ji}}^n} OPT_{max} = -s_{\mathrm{ji}}^n + \gamma_j + \lambda_{\mathrm{ij}} = 0. \tag{9}$$

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

Based on Eqn. (8) & (9) under KKT conditions [27] there exist linear correlations for the maximum mutual profit. The function of smart contract is descriped in algorithm 2.

$$b_{\mathrm{ij}}^n = \frac{c_{\mathrm{ij}}^n}{\left(\sum_{j=1}^{J} c_{\mathrm{ij}}^n - c_i^{n,\min} + 1\right)} \tag{10}$$

$$s_{\mathrm{ji}}^n = 2l_1 d_{\mathrm{ji}}^n + \psi. \tag{11}$$

D. Mechanism of blockchain for 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 Fig. 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.

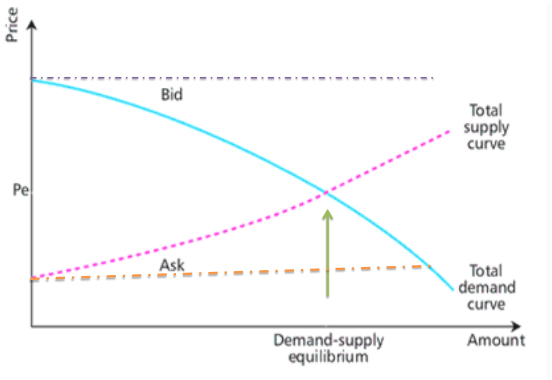

Fig. 3. Result

IV. Results

Figure 3 depicts how bidding price change for customer and supplier. Price refers to selling cost (Ask) of supplier. While amount refers to bidding cost (Bid) of customer. The double auction mechanism tries to optimise the maximum profit of both by reaching at demand-supply equilibrium. P_e is the optimal bidding price for customer. Auction mechanism tries to converge to this equilibrium point. Blue line denotes that as variation of total demand curve, while pink line is total supply curve. Figure 5 depicts customers profit is maximised using auction mechanism rather that trading without auction (depicted by purple line). On other hand for supplier as the demand for supply increases auction mechanism increases the profit of supplier. The amount of profit for supplier increased from orange line to total supply curve.

This model is an enhancement to provide secure smart communities by 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 [28] with profit maximisation using double auction mechanism.

V. Acknowledgement

We gratefully acknowledge the support of NVIDIA Corporation with the donation of the Titan Xp GPU used for this research.

VI. Conclusion

Buyer & supplier relationship forms the backbone of any community. Smarter community means smarter economic backbone. Our model sets a pioneer of applying blockchain in commerce. Model provides improved transparency, better scalability and security. We have emphasized on use of flexible smart contracts 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 which helps the nodes trust each other. 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] http://lcm.csa.iisc.ernet.in/scm/supply_chain_intro.html.

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

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

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] V. Chamola, C.-K. Tham, and G. S. Chalapathi, "Latency aware mobile task assignment and load balancing for edge cloudlets," in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*. IEEE, 2017, pp. 587–592.

[10] 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.

[11] 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.

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

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

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

[15] 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.

[16] S. A. Abeyratne and R. P. Monfared, "Blockchain ready manufacturing supply chain using distributed ledger," 2016.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] G. Bansal, A. Dua, G. S. Aujla, M. Singh, and N. Kumar, "SmartChain: a smart and scalable blockchain consortium for smart grid systems," in *2019 IEEE International Conference on Communications Workshops (ICC Workshops)*, 2019.

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

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

[24] 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.

[25] V. Chamola, B. Krishnamachari, and B. Sikdar, "An energy and delay aware downlink power control strategy for solar powered base stations," *IEEE Communications Letters*, vol. 20, no. 5, pp. 954–957, 2016.

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

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

[28] 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.