Blockchain-Based Distributive Auction for Relay-Assisted Secure Communications

Khan, AS, Rahulamathavan , Y, Basutli, B, Zheng, G, AsSadhan, B & Lambotharan, S.

Original citation:
Khan, AS, Rahulamathavan , Y, Basutli, B, Zheng, G, AsSadhan, B & Lambotharan, S 2019, 'Blockchain-Based Distributive Auction for Relay-Assisted Secure Communications' IEEE Access, vol. 7, pp. 95555-95568.
https://doi.org/10.1109/ACCESS.2019.2929136

DOI 10.1109/ACCESS.2019.2929136
ISSN 2169-3536
ESSN 2169-3536

Publisher: IEEE ACCESS

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 12, 2019, accepted July 9, 2019, date of publication July 16, 2019, date of current version August 2, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2929136

Blockchain-Based Distributive Auction for Relay-Assisted Secure Communications

AMJAD SAEED KHAN[1], YOGACHANDRAN RAHULAMATHAVAN[2], BOKAMOSO BASUTLI[3], (Member, IEEE), GAN ZHENG[1], (Senior Member, IEEE), BASIL AsSADHAN[4], (Member, IEEE), AND SANGARAPILLAI LAMBOTHARAN[1], (Senior Member, IEEE)

[1]Wolfson School of Mechanical, Electrical, and Manufacturing Engineering, Loughborough University, Loughborough LE11 3TU, U.K.
[2]Institute for Digital Technologies, Loughborough University London, London E15 2GZ, U.K.
[3]Electrical, Computer, and Telecommunications Engineering, Botswana International University of Science and Technology, Private bag 16, Palapye, Botswana
[4]Electrical Engineering Department, King Saud University, Riyadh 145111, Saudi Arabia

Corresponding author: Amjad Saeed Khan (a.khan@lboro.ac.uk)

This work was supported in part by the Engineering and Physical Sciences Research Council under Grant EP/R006385/1 and Grant EP/N007840/1, in part by the U.K.–India Education Research Initiative (UKIERI) under Grant UGC-UKIERI-2016-17-019, in part by the Botswana International University of Science and Technology (BIUST) under Grant R00067, and in part by the International Scientific Partnership Program (ISPP) at King Saud University under Grant ISSP134.

ABSTRACT Physical layer security (PLS) is considered as a promising technique to prevent information eavesdropping in wireless systems. In this context, cooperative relaying has emerged as a robust solution for achieving PLS due to multipath diversity and relatively lower transmission power. However, relays or the relay operators in the practical environment are unwilling for service provisioning unless they are incentivized for their cost of services. Thus, it is required to jointly consider network economics and relay cooperation to improve system efficiency. In this paper, we consider the problem of joint network economics and PLS using cooperative relaying and jamming. Based on the double auction theory, we model the interaction between transmitters seeking for a particular level of secure transmission of information and relay operators for suitable relay and jammer assignment, in a multiple source-destination networks. In addition, theoretical analyses are presented to justify that the proposed auction mechanism satisfies the desirable economic properties of individual rationality, budget balance, and truthfulness. As the participants in the traditional centralized auction framework may take selfish actions or collude with each other, we propose a decentralized and trustless auction framework based on blockchain technology. In particular, we exploit the smart contract feature of blockchain to construct a completely autonomous framework, where all the participants are financially enforced by smart contract terms. The security properties of the proposed framework are also discussed.

INDEX TERMS Physical layer security, secrecy capacity, double auction, blockchain, smart contract, network economics.

I. INTRODUCTION

Cooperative relaying is an effective method for increasing system capacity, coverage area, security, and reliability of wireless networks [1], [2], [3]. In addition, it is considered as an attractive solution for improving the energy efficiency [4]. These rewarding merits of cooperative relaying make it one of the promising techniques for future wireless systems. For example, it has been investigated as part of the project WINNER (Wireless World Initiative New Radio) [5], and has found applications in various networks including cellular, ad hoc, and wireless sensor networks.

Due to the broadcast nature of wireless channels, security and privacy are the major concerns for the future wireless technology. In this context, recently cooperative relaying has been considered as a potential technique to achieve the physical layer security (PLS), which complements the traditional cryptographic techniques employed at the upper layers of a wireless network [6], [7]. The feasibility of PLS has been first discussed by Shannon in [8], later on, its theoretical

The associate editor coordinating the review of this manuscript and approving it for publication was Md Fazlul Kader.

foundations were laid by Wyner in [9], who introduces the wire-tap channel which can achieve positive secrecy rate under the assumption that the legitimate destinations experience a better channel than eavesdroppers. Thus, relay nodes can be used to exploit the characteristic of wireless channels such as fading and noise, to transmit a message from a source to a legitimate destination while trying to keep this message confidential from eavesdropper. At present, opportunistic relaying is emerging as a promising paradigm to achieve the PLS [10], [11]. For example, the effect of single relay and multi-relay selection strategy on both the security and reliability of decode-and-forward cooperative systems was investigated in [10]. Opportunistic relaying protocols in the presence of multiple eavesdroppers were proposed in [11]. In addition to opportunistic relaying, cooperative jamming has gained significant attention as a means to further enhance the PLS [12], [13]. For example, in [12] joint relay-and-jammer selection techniques were proposed to improve the secrecy capacity of wireless networks. Moreover, a cross layer PLS design based on random linear network coding and opportunistic relaying and jamming protocols was studied in [13].

In all the aforementioned works, it is assumed that relays are always willing to cooperate with transmitters. But in reality, the relays may exhibit *selfish behaviors* and refuse to cooperate for the concerns on energy and bandwidth consumption. Thus, the relays should be given enough rewards to compensate for their resource consumption. However, more often the participants have conflicting interests. For example, transmitters would prefer to receive services at low cost, while the relays would prefer to charge high prices. Moreover, the transmitters would compete against each other for limited resources in least pricing to achieve the desired quality of service. At the same time the relays (or service providers) would compete among themselves to improve their profit. In addition, the participants may also lie or impersonate others to maximize their own benefit. Therefore, it is of paramount importance to design an unbiased, secure, and truthful incentive mechanism for reconciling the objectives of all the participants.

Game theory and mechanism design provide the basic framework to acquire solutions for resource allocation and enforcement of cooperation. For example, Stackelberg game has been exploited in [14] to investigate a distributed algorithm for the interaction between source and friendly jammers. Based on Stackelberg game a distributed relay selection and power control mechanism was proposed in [15] to achieve the PLS. Game theory is also employed in [16] for the selection of shortest distance path relay in a multi-hop cooperative communication system. In addition, game theoretic based resource allocation model for multicell D2D communication has been proposed in [17]. Moreover, a self-enforcing truth-telling mechanism was proposed in [18] for multiple relays selection to achieve PLS, while considering energy harvesting requirements. If the participants are rational, intelligent and competing, auction-based incentive strategies are quite beneficial to model in such type of situations [19]–[22]. They are simple to implement but provide effective platform for the distributed and decentralized competitive market. In addition, they provide enough structure to enable strong theoretical claims about the strategies of the participants and the optimality of solutions. Based on their bidding structures, the auctions can be classified into: forward, reverse and double auctions. In the forward auction, many potential buyers compete with each other by bidding for services (items) offered by sellers. In the reverse auction, the roles of buyers and sellers are reversed, such that, the sellers compete with each other by bidding to serve the buyers. The key objective of forward auctions is to maximize the revenue of sellers, and the objective of reverse auctions is to minimize the cost for buyers. Unlike forward and reverse auctions, double auction is a two-sided auction, such that, in double auction bidding is done by both the players (i.e., buyers and sellers) of the trading market. Auctions have recently become a topic of much interest in wireless communications literature [23]–[28]. For example, simultaneous multiple-round ascending auction mechanism were proposed in [23] as a decentralized solution for users' offloading in a heterogeneous cellular network. A single round auction was proposed in [24] as a profitable technique for selecting a mobile relay which provides the highest possible data rate, while considering the utilities of all the players including: mobile user, mobile relay and relay operator. A combinatorial auction mechanism was studied in [25] for solving the spectrum allocation problem in cognitive radio networks. Specifically, the auction was employed to approximate the NP hard optimal solution of social welfare. Optimal relay selection technique was proposed in [26] through auctioning, in multiple source-destination networks. In particular, payment mechanism for both source and relay nodes were designed to avoid selfish behavior of both the elements. In [27], double auction based relay assignment techniques were studied for both centralized and decentralized wireless networks, while considering interference due to relay transmissions. Moreover, double auction was also studied in [28] for spectrum trading between femtocell service providers and macrocell service providers, such that maximum trading fairness can be achieved.

However, these schemes are based on risk-free and trustful trading environment. In addition, they rely on a central authority (auctioneer). It is well documented that auctions contain many security risks which can lead to possible system collapses [29]–[31]. For example, buyers and sellers may collude and repudiate bids. As another possibility, the auctioneer may cheat and award the auction to someone other than the legitimate winner. Moreover, the auctioneer may disclose bidders' identities to any other trading participant or to a third party agent. Several efforts have been made to address some of these issues [32]–[36]. For example, an agent-based trust management framework was proposed in [32] that can re-evaluates users' trust values and updates access permissions dynamically. In addition to the agent-based approach, cryptographic technology was proposed in [33] to automate

and secure the auction process. Furthermore, trustworthy supervisor-based protocol was presented in [34] to address the malicious activities of the rational auctioneer. These schemes rely on a trusted third party (i.e., agents, supervisor, etc) that facilitates the development of trustful environment. Hence, it is important to have a mechanism that ensures trusted third party does not intend to collude, and also facilitates trading through explicit digital currency.

Blockchain is a revolutionary technology that has recently attracted the attention of not only research community but also the interest of a wide range of stakeholders of industries related to healthcare [37], finance, real estate [38] and government sectors [39]. This is because it offers the realization of distributed, trust-free, transparent and highly secure systems [40]–[42]. In particular, smart contract based blockchain solutions offer decentralized and distributed applications where everyone is allowed to build their own arbitrary rules for agreements, transaction formats, and state transition functions [43], [44]. The smart contracts enable the blockchain system to only validate the transactions that take place under the condition of the agreed upon contract. Because of this, the blockchain has a great potential to resolve some of the issues related to lack of trust or incomplete information about the counter trading party, which conventionally required a central trusted party [45]–[48]. Note that, to the best of our knowledge, the existing work on network economics using game theory and mechanism design only consider relay(s) assignment in a single source-destination network. Thus, the key motivations of this paper are twofold: (i) To bridge the gap between existing work and the allocation problem, and propose an incentive mechanism to achieve the PLS in relay-assisted multiple source-destination networks. (ii) To exploit the blockchain features for the distributed and trust-free environment in order to address the aforementioned malicious activities in the trading process. The main contributions of the paper are summarized as follows:

1) We employ double auction theory to model the two sided interaction between transmitters and relay operators, where transmitters demand for a particular level of security while relay operators sell their services including bandwidth, and optimal relay and jamming power. In addition, we prove that the proposed model is economic robust in terms of individual rationality, budget balance, and truthfulness.
2) We exploit the features of blockchain technology to strengthen the weaknesses of the auction model, and propose a decentralized, trustless, and autonomous auction framework, where the role of a central mediator is distributed among all the trading parties (i.e., buyers and sellers). Moreover, we introduce a virtual currency system in the proposed framework for trading, and for encouraging even the non-trading agents to participate in facilitating the auction process.
3) Simulation results are presented to demonstrate the impact of malicious agent in the centralized auction environment, and how the malicious activities can be avoided by the proposed framework of blockhchain and auctioning. The detailed discussions on the security properties of the proposed framework is also provided.

The rest of the paper is organized as follows. Section II describes the system model and problem formulation, and introduces relevant notations. A detailed description of the proposed auction mechanism is provided in Section III, and its properties are analyzed. Section IV presents the proposed distributive auction framework. Results and discussions are provided in Section V followed by conclusions in Section VI.

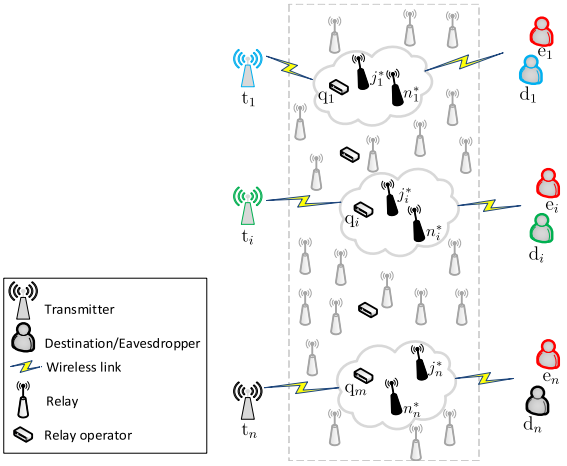

FIGURE 1. A network consisting of n transmitter-destination nodes, where each transmitter t_i wants to send a confidential message to destination d_i through cooperative relaying in the presence of an eavesdropper e_i. A set of relays are managed by a relay operator q_i. Each relay operator is responsible for suitable relay/jammer selection and resource (i.e., power and frequency sub-carrier/bandwidth) allocation.

II. SYSTEM MODEL AND PROBLEM FORMULATION

We consider a network as shown in Fig. 1, where a transmitter t_i wants to share a confidential message to destination d_i in the presence of a passive eavesdropper e_i. We assume that there is no direct link between t_i and the destination d_i, i.e., d_i can only receive signals through intermediate nodes. There are multiple intermediate nodes, such that, each node can either help in relaying the transmitter information to the legitimate destination or can cause interference to overhearing attack by the eavesdropper. We assume that the network topology contains m relay operators $\mathcal{Q} = \{q_1, q_2, \ldots q_m\}$, each relay operator q_i is associated to a group of nodes. In particular, the relay operator is responsible for selecting suitable nodes for communication services and managing available resources including subcarriers allocation and power allocation. Note that, we assume that both the operator and its corresponding relays are the members of same entity.

Each transmitter t_i desires to achieve a certain level of secure transmission of information to its destination d_i at the minimum cost of service. We assume that the relay operators are already serving regular transmitters in the network. Thus, a relay operator can only serve an additional transmitter t_i for secure communication if it contains a free subcarrier $f_i > 0$

to allocate. The relay operators can be paid for providing this additional services as a compensation for resource allocation and communication cost. This implies that the trading between a transmitter and the relay operator should meet certain requirements to benefit both parties. For example, relay operators need to be encouraged to allocate their resources, and the requirements of the transmitters should be satisfied. In particular, a relay operator cannot be paid less than the cost of its service, while the allocated resources must satisfy the transmitter's service request within the limited budget. Note that, each relay operator has complete knowledge of channel state information (CSI) of all the nodes of its group as well as the CSI of legitimate destinations and their corresponding eavesdroppers. In order to achieve secure communication at d_i, each relay operator selects the best possible pair of nodes $\{n_i^*, j_i^*\}$, such that, a relay n_i^* forwards the confidential message of t_i. At the same time, the selected jammer j_i^* generates artificial interference in order to deteriorate the eavesdropper's channel. Furthermore, we assume that all d_i's are served over orthogonal subcarriers. Note that, there are various methods available in the physical layer security literature for the selection of an appropriate relay-jammer pair [12]. Hence, the discussion on the selection procedure is avoided in this paper.

All the links connecting the nodes are assumed to be independent but not identically distributed (*i.n.i.d*) quasi-static Raleigh fading channels. The channel gain between node i and j is represented as $|h_{i,j}|^2$. Thus, the channel capacity of link connecting n_i^* and destination d_i can be defined as:

$$C_{\mathrm{d}_i} = W_i \log_2\left(1 + \frac{\rho_i |h_{n_i^*,\mathrm{d}_i}|^2}{\bar{\rho}_i |h_{j_i^*,\mathrm{d}_i}|^2 + N_0}\right), \tag{1}$$

where W_i is the channel bandwidth, N_0 represents the additive noise power, and ρ_i and $\bar{\rho}_i$ are the transmission powers of relay n_i^* and jammer j_i^*, respectively. Similarly, the channel capacity of the link connecting n_i^* and eavesdropper e_i is equal to

$$C_{\mathrm{e}_i} = W_i \log_2\left(1 + \frac{\rho_i |h_{n_i^*,\mathrm{e}_i}|^2}{\bar{\rho}_i |h_{j_i^*,\mathrm{e}_i}|^2 + N_0}\right), \tag{2}$$

For secure communication such that an eavesdropper e_i can obtain zero mutual information from the confidential message of transmitter t_i, the relay n_i^* should forwards the message with the secrecy capacity given as:

$$C_{\mathrm{se}_i} = (C_{\mathrm{d}_i} - C_{\mathrm{e}_i})^+ \tag{3}$$

where $(.)^+ = \max(., 0)$. It is assumed that all the links in the first-hop $\{\mathrm{t}_i \rightarrow n_i\}$ are of better quality than the links in the second-hop $\{n_i \rightarrow \mathrm{d}_i\}$. In addition, given that no direct links exist between t_i and e_i, security is always guaranteed in the first hop links. Thus, in the following sections, we only focus on the secrecy capacity of the second-hop links. It can be observed from (1) and (2) that both C_{d_i} and C_{e_i} are the increasing functions of relay power ρ_i. On the other hand, the channel capacities can be reduced by increasing the jamming power $\bar{\rho}_i$. We assume that each transmitter t_i demands for a specific minimum secrecy capacity $\mathcal{C}_i$. Thus, in order to achieve the required level of security, each relay operator needs to carefully allocate powers ρ_i and $\bar{\rho}_i$. Note that, the cost of communication service increases with the increase of total power allocation. We assume that each relay operator intends to provide the most cost-effective solution for a satisfactory service. For convenience, the key parameters of the system model have been sumarized in Table 1.

TABLE 1. Key parameters of the system model.

Notation	Description
t_i	Transmitter i
q_i	Relay operator i
e_i	Eavesdropper node i
d_i	Destination node i
f_i	Number of free subcarriers of i^{th} relay operator
$\mathcal{Q}$	Set of relay operators
n_i^*	Selected relay node for d_i
j_i^*	Selected jammer node for d_i
ρ_i	Allocated relay power to node n_i^*
$\bar{\rho}_i$	Allocated jamming power to node j_i^*
N_0	Additive Gaussian noise power
h_{ij}	Fading coefficient of the channel between node i and j
C_{e_i}	Channel capacity of i^{th} eavesdropper node
C_{d_i}	Channel capacity of i^{th} destination node
C_{se_i}	Secrecy capacity of i^{th} destination
$\mathcal{C}_i$	Minimum secrecy capacity requirement of t_i

Mainly, based on the number of free subcarriers, each relay operator can serve multiple transmitters t_i at the same time. Thus, the larger the number of transmitters served by a relay operator, the higher will be its utility. To maximize the benefits to both transmitters and relay operators, an incentive mechanism should be properly designed to match the relay operators' services and the transmitters' demands. However, given that we consider a highly distributed network with various parties, it is reasonable to assume that each party intends to maximize its own benefit. There are a number of malicious activities that could deter the harmony of the system. For example, a transmitter may cheat and pay less to the selected relay operator or the relay operator may not be paid with the right amount, or the relay operator may not fulfill the work as it agreed to do, etc. In order to tackle these issues related to transparency and integrity, we exploit the features of blockchain technology, which will be discussed in Section IV.

III. AUCTION MODEL AND PHYSICAL LAYER SECURITY

This section presents a general framework proposed for suitable matching between the transmitters demands of PLS and the relay operators. In particular, in addition to achieving PLS the proposed framework aims to select appropriate relay-jammer pairs for the minimum cost of service. Considering a single-round double auction mechanism for the two sided

interaction between the transmitters and the relay operators, where all the transmitters that are desirous to achieve certain level of security i.e., $C_{\mathrm{se}_i} \geq \mathcal{C}_i$, act as buyers. On the other hand, all the relay operators managing intermediate nodes for cooperation act as sellers. A control unit near to the participants can serve as an auctioneer. Note that, the selection process of auctioneer according to the proposed distributed framework will be discussed in Section IV. The auction is usually based on two stages:

1) allocation stage (also called winners determination problem): determining the best possible pairs of sellers and buyers
2) pricing stage: determining the payment to be made by each (winning) buyer and the payment to be made to each (winning) seller.

The detailed description of the auction framework is described as follows:

A. AUCTION FRAMEWORK

Before the auction process starts, it is assumed that all the parties are well informed about the buyers demands of security requirements (i.e., $\mathcal{C}_i$). We consider that each buyer has different valuations of the sellers. This is because of different quality of communication (e.g., channel conditions) between the buyers t_i and the sellers q_j. Similarly, given that each buyer t_i has distinct security requirements, and because of different channel conditions between cooperative relays and receivers $R_i \in \{\mathrm{d}_i, \mathrm{e}_i\}$, each seller has its own cost of delivery for destination d_i. We refer seller's bids as asks to differentiate them from that of a buyer. Thus, each buyer has different bids for sellers, and each seller has different asks for buyers. By considering a sealed bid auction, both buyers and sellers submit their respective offers to the auctioneer in a private manner. Once all the traders have submitted their offers, the auctioneer identifies suitable pairs of buyers and sellers according to the proposed double auction mechanism (Algorithm 1). The final result of the auction consists of: winning buyers set $\mathcal{B}_\mathrm{b} \subseteq \mathcal{U} = \{\mathrm{t}_1, \mathrm{t}_2, \ldots \mathrm{t}_n\}$, winning seller set $\mathcal{S}_\mathrm{s} \subseteq \mathcal{Q} = \{\mathrm{q}_1, \mathrm{q}_2, \ldots \mathrm{q}_m\}$, payment vector $\mathbf{P}^\mathrm{b}$ containing payments $p^\mathrm{b}_{i,j}$ that winning buyers t_i are charged by sellers q_j, and price vector $\mathbf{P}^\mathrm{s}$ containing prices $p^\mathrm{s}_{i,j}$ that winning sellers q_j are rewarded by t_i.

The utility of a buyer t_i can be defined as its true valuation minus the price it pays to the winning seller q_j, given as:

$$U^\mathrm{b}_{\mathrm{t}_i} = \sigma_{i,j}\mathcal{C}_i - p^\mathrm{b}_{i,j}$$

where, $\sigma_{i,j}$ represents the gain for a unit of secrecy capacity such that $\sigma_{i,j} = \alpha_{\mathrm{t}_i,\mathrm{q}_j} d^{-a_{\mathrm{t}_i,\mathrm{q}_j}}_{\mathrm{t}_i,\mathrm{q}_j}$ with $\alpha_{\mathrm{t}_i,\mathrm{q}_j}$ being a positive constant, and $d_{\mathrm{t}_i,\mathrm{q}_j}$ and $a_{\mathrm{t}_i,\mathrm{q}_j}$ are the Euclidean distance and the path loss exponent between node t_i and q_j, respectively. Note that, the communication cost (i.e., energy spent by t_i per secrecy bit) between t_i and q_j is proportional to the term $d^{-a_{\mathrm{t}_i,\mathrm{q}_j}}_{\mathrm{t}_i,\mathrm{q}_j}$. This implies that, larger the value of $d^{-a_{\mathrm{t}_i,\mathrm{q}_j}}_{\mathrm{t}_i,\mathrm{q}_j}$ higher will be the communication cost, which also reduces the utility of buyer t_i. The utility of seller q_j can be defined as the total payments it receives from the winning buyers minus the total cost of its services. Mathematically, it can be expressed as:

$$U^\mathrm{s}_{\mathrm{q}_j} = \sum_{i=1}^{n} [p^\mathrm{s}_{i,j} - c(\rho_i, \bar{\rho}_i)] I_{i,j}$$

where, $I_{i,j} \in \{0, 1\}$ is an indicator function such that $I_{i,j} = 1$ if seller q_j is paired with buyer t_i, otherwise $I_{i,j} = 0$. In addition, $c(\rho_i, \bar{\rho}_i)$ is the cost of delivering secure communication, and it can be defined as:

$$c(\rho_i, \bar{\rho}_i) = \eta_{i,j}(\rho_i + \bar{\rho}_i) + \varepsilon_{i,j} \tag{4}$$

where, $\eta_{i,j}$ is the unit cost of relay and jamming power, and $\varepsilon_{i,j}$ represents the commission which the auctioneer charges the seller for facilitating the auction. We assume that the auctioneer commission is a percentage cost of relay and jamming power allocation, which is only charged to the winning seller. Thus for winning seller we can define $\varepsilon_{i,j} = \kappa \times \eta_{i,j}(\rho_i + \bar{\rho}_i)$, where $0 \leq \kappa \leq 1$ is the percentage value.

Given that, each relay operator is intended to offer minimum cost of service as discuss in Section II. Therefore, before submitting an offer for buyer t_i each seller employs (5) to minimize its cost.

B. RESOURCE ALLOCATION MODEL

For fixed values of $\eta_{i,j}$ and κ, the minimum cost of communication can be achieved by solving the following optimization problem:

$$\min_{\rho_i,\ \bar{\rho}_i} c(\rho_i, \bar{\rho}_i) \tag{5}$$

$$\text{subject to:} \quad C_{\mathrm{se}_i} \geq \mathcal{C}_i, \tag{6}$$

$$\rho_i \leq \rho_{\max}, \tag{7}$$

$$\bar{\rho}_i \leq \rho_{\max}, \tag{8}$$

where, $\rho_{\max}$ represents the maximum transmission power of an intermediate node. Given that the constraint (6) is not convex, the optimization problem is clearly non convex.

Lemma 1: The cost minimization problem (5) can be transformed into Geometric Programming (GP) optimization problem.

Proof: For notational convenience, let us first define $\gamma_{i,j} = \frac{\rho_i}{N_0}|h_{i,j}|^2$ as the instantaneous SNR of the link between node i and j, where ρ_i represents the transmission power. In addition, by comparing (1) and (2) with Shannon's capacity formula, we obtain $\phi_{\mathrm{d}_i} = \gamma_{n^*_i \mathrm{d}_i}/(\gamma_{j^*_i \mathrm{d}_i} + 1)$, $\phi_{\mathrm{e}_i} = \gamma_{n^*_i \mathrm{e}_i}/(\gamma_{j^*_i \mathrm{e}_i} + 1)$. Thus, (6) can be re-formulated as:

$$\begin{aligned} \phi_{\mathrm{d}_i} &\geq \tau_{\mathrm{d}_i}, \\ \phi_{\mathrm{e}_i} &\leq \tau_{\mathrm{e}_i}, \\ \tau_{\mathrm{d}_i} - \tau_{\mathrm{e}_i} &\geq \tau_i, \end{aligned}$$

where $\tau_i = 2^{\mathcal{C}_i} - 1$. Consequently, after substitutions and mathematical manipulations the optimization problem can be

expressed as:

$$\min_{\tau_{\mathrm{D}},\tau_{\mathrm{E}}} c(\rho_i, \bar{\rho}_i) \tag{9}$$

$$\text{subject to:} \quad \tau_{\mathrm{d}_i}\gamma_{j_i^*\mathrm{d}_i}\gamma^{-1}_{n_i^*\mathrm{d}_i} + \tau_{\mathrm{d}_i}\gamma^{-1}_{n_i^*\mathrm{d}_i} \leq 1, \tag{10}$$

$$\frac{\gamma_{n_i^*\mathrm{e}_i}\tau^{-1}_{\mathrm{e}_i}}{\gamma_{j_i^*\mathrm{e}_i}+1} \leq 1, \tag{11}$$

$$\tau_{\mathrm{e}_i}\tau^{-1}_{\mathrm{d}_i} + \tau_i\tau^{-1}_{\mathrm{d}_i} + \tau_i\tau^{-1}_{\mathrm{d}_i}\tau_{\mathrm{e}_i} \leq 1, \tag{12}$$

$$\rho_i\rho^{-1}_{\max} \leq 1, \tag{13}$$

$$\bar{\rho}_i\rho^{-1}_{\max} \leq 1, \tag{14}$$

where the constraints (10), (12), (13) and (14) are in the posynomial form. However, (11) is not posynomial since the ratio of monomial by posynomial is non-posynomial [49]. To deal with this issue, we approximate the denominator of (11) with monomial function by employing widely known arithmetic geometric mean approximation [50], as follows:

$$\frac{1}{\gamma_{j_i^*\mathrm{e}_i}+1} = \left(\frac{\gamma_{j_i^*\mathrm{e}_i}(t)}{\alpha(t)}\right)^{-\alpha(t)}\left(\frac{1}{\beta(t)}\right)^{-\beta(t)}, \tag{15}$$

where $\alpha(t) = \frac{\gamma_{j_i^*\mathrm{e}_i}(t-1)}{\gamma_{j_i^*\mathrm{e}_i}(t-1)+1}$ and $\beta(t) = \frac{1}{\gamma_{j_i^*\mathrm{e}_i}(t-1)+1}$. Thus, using (15) we can approximate (11) into a posynomial form related to each iteration, as follows:

$$\gamma_{n_i^*\mathrm{e}_i}\tau^{-1}_{\mathrm{e}_i}\left(\frac{\gamma_{j_i^*\mathrm{e}_i}(t)}{\alpha(t)}\right)^{-\alpha(t)}\left(\frac{1}{\beta(t)}\right)^{-\beta(t)} \leq 1. \tag{16}$$

This completes the proof ■

Once the optimization problem is transformed into a GP problem, the solution can be obtained using the CVX toolbox [49].

C. DESIRABLE PROPERTIES OF DOUBLE AUCTION

In order to encourage participation of all buyers and sellers, the auction mechanism should satisfy some of the desired economic requirements, as follow:

1) INDIVIDUAL RATIONALITY

According to this property, the payment made by a buyer should be less than or equal to its bid, and the price received by a seller should be greater than or equal to its ask price. In other words, this property ensures that no one should lose by joining the auction.

2) BUDGET BALANCE

According to this property, the payments of the buyers must be entirely transferred to the sellers, i.e., the total payment charged to winning buyers should be equal to total price rewarded to winning sellers. In other words, the auctioneer does not lose or gain (except fixed percentage commission) money during the trade.

3) TRUTHFULNESS

Truthfulness is the most fundamental property of auctions. All the buyers and sellers are usually rational and selfish, they can manipulate their bids and asks to maximize their own utility. Therefore, this property ensures that neither the seller nor the buyer can improve its utility by misreporting its true valuations.

Algorithm 1 Double Auction

All the sellers employ (5) to calculate asks
All the buyers calculate bids corresponding to each seller
The auctioneer employes the following procedure:
Input: All bids $\mathcal{B}$, All asks $\mathcal{A}$, Sellers resources $\mathcal{R}$
Output: sellers set $\mathcal{S}_{\mathrm{s}}$, buyers set $\mathcal{B}_{\mathrm{b}}$, sellers price vector $\mathbf{P}^{\mathrm{s}}$, and buyers payment vector $\mathbf{P}^{\mathrm{b}}$
Shortlist asks which are greater than or equal to their corresponding bids, that is, $\mathcal{A}_{\mathrm{c}} = \{a_{\mathrm{t}_i,\mathrm{q}_j} | a_{\mathrm{t}_i,\mathrm{q}_j} \geq b_{\mathrm{t}_i,\mathrm{q}_j}\}$
Shortlist bids, such that, $\mathcal{B}_{\mathrm{c}} = \{b_{\mathrm{t}_i,\mathrm{q}_j} | a_{\mathrm{t}_i,\mathrm{q}_j} \geq b_{\mathrm{t}_i,\mathrm{q}_j}\}$
Sort all the elements of $\mathcal{A}_{\mathrm{c}}$ in ascending order
Arrange the elements of $\mathcal{B}_{\mathrm{c}}$ according to elements in $\mathcal{A}_{\mathrm{c}}$
Initialize: $\mathcal{B}_{\mathrm{b}} = \emptyset$, $\mathcal{S}_{\mathrm{s}} = \emptyset$, $\mathbf{P}^{\mathrm{b}} = \emptyset$, $\mathbf{P}^{\mathrm{s}} = \emptyset$, $i = 1$
while $\mathcal{A}_{\mathrm{c}} \neq \emptyset$ **do**
  if $f_i > 0$ **then**
    $\mathcal{B}_{\mathrm{b}} \leftarrow \mathcal{B}_{\mathrm{b}} \cup \{\mathrm{t}_i\}$, $\mathcal{S}_{\mathrm{s}} \leftarrow \mathcal{S}_{\mathrm{s}} \cup \{\mathrm{q}_i\}$
    $p^{\mathrm{b}}_{i,j} = \min(b_{\mathrm{t}_i,\mathrm{q}_i}, a_{\mathrm{t}_i,\mathrm{q}_{i+1}})$, $p^{\mathrm{s}}_{i,j} = p^{\mathrm{b}}_{i,j}$
    $\mathbf{P}^{b} \leftarrow \mathbf{P}^{\mathrm{b}} \cup \{p^{\mathrm{b}}_{i,j}\}$, $\mathbf{P}^{\mathrm{s}} \leftarrow \mathbf{P}^{\mathrm{s}} \cup \{p^{\mathrm{s}}_{i,j}\}$
    $f_i = f_i - 1$
Update $\mathcal{A}_{\mathrm{c}}$ by removing asks corresponding to buyer t_i
Update $\mathcal{B}_{\mathrm{c}}$ by removing all the remaining bids of t_i
  else
    if $f_i \leq 0$ **then**
      $\mathcal{A}_{\mathrm{c}} \leftarrow \mathcal{A}_{\mathrm{c}} \setminus \{a_{\mathrm{t}_i,\mathrm{q}_i}\}$
      $\mathcal{B}_{\mathrm{c}} \leftarrow \mathcal{B}_{\mathrm{c}} \setminus \{b_{\mathrm{t}_i,\mathrm{q}_i}\}$
    end if
  end if
  $i = i + 1$
end while
Return: $\mathcal{B}_{\mathrm{b}}$, $\mathcal{S}_{\mathrm{s}}$, $\mathbf{P}^{\mathrm{b}}$, $\mathbf{P}^{\mathrm{s}}$

D. PROPOSED ALGORITHM

This section describes the proposed double auction mechanism in detail in Algorithm 1. We start by representing a bid $b_{\mathrm{t}_i,\mathrm{q}_j}$ as the maximum price that a buyer t_i is willing to pay for a seller q_j, and denote $a_{\mathrm{t}_i,\mathrm{q}_j}$ as the price that q_j asks for its service to t_i. In addition, we consider that each seller q_j has f_j subcarriers to allocate as discussed in Section II. Thus, a pair $\{\mathrm{t}_i, \mathrm{q}_j\}$ can be defined as feasible for matching iff $b_{\mathrm{t}_i,\mathrm{q}_j} \geq a_{\mathrm{t}_i,\mathrm{q}_j}$ and $f_j > 0$. We assume that all the non-zero asks are collected in a set $\mathcal{A} = \{a_{\mathrm{t}_1,\mathrm{q}_1}, \ldots, a_{\mathrm{t}_m,\mathrm{q}_n}\}$. Similarly, the respected bids are also collected in a set $\mathcal{B} = \{b_{\mathrm{t}_1,\mathrm{q}_1}, \ldots, b_{\mathrm{t}_m,\mathrm{q}_n}\}$. In the allocation stage, all the feasible elements of $\mathcal{A}$ are first added into the candidate set, i.e., $\mathcal{A}_{\mathrm{c}} \leftarrow \mathcal{A}$ with $\mathcal{A}_{\mathrm{c}} = \{a_{\mathrm{t}_i,\mathrm{q}_j} | b_{\mathrm{t}_i,\mathrm{q}_j} \geq a_{\mathrm{t}_i,\mathrm{q}_j}\}$. Likewise, $\mathcal{B}_{\mathrm{c}} \leftarrow \mathcal{B}$ with $\mathcal{B}_{\mathrm{c}} = \{b_{\mathrm{t}_i,\mathrm{q}_j} | b_{\mathrm{t}_i,\mathrm{q}_j} \geq a_{\mathrm{t}_i,\mathrm{q}_j}\}$. Afterward, elements of $\mathcal{A}_{\mathrm{c}}$ are sorted in ascending order of their values such that $a_{\mathrm{t}_i,\mathrm{q}_j} \geq a_{\mathrm{t}_i,\mathrm{q}_{j+1}}$. For point-to-point (bid-ask) association, the elements of $\mathcal{B}_{\mathrm{c}}$ are also arranged in accordance with $\mathcal{A}_{\mathrm{c}}$. At this stage, the order of elements in $\mathcal{A}_{\mathrm{c}}$

also determines the priority of sellers, such that, highest priority will be given to seller who has the minimum ask. However, if two or more elements in $\mathcal{A}_c$ are equal, then priority will be given to seller who is offered by the highest bid.

Thus, in order to determine winning buyer-seller pairs (from Line 10 to 26 in Algorithm 1), we start from the first (highest priority) element in $\mathcal{A}_c$ and check for the availability of free subcarrier (Line 12). A pair $\{t_i, q_j\}$ will be considered as valid if $f_j > 0$. The winning buyer and seller are then added into winning sets, such that: $\mathcal{B}_b \leftarrow \mathcal{B}_b \cup \{t_i\}$ and $\mathcal{S}_s \leftarrow \mathcal{S}_s \cup \{q_j\}$ (Line 13). Note that, a buyer may be feasible for more than one seller, therefore, all the remaining elements (asks) in $\mathcal{A}_c$ that are linked to t_i are deleted (Line 17). Similarly, elements of $\mathcal{B}_c$ that are related to t_i are also deleted (Line 18). In the pricing stage, in order to satisfy the desirable property of individual rationality, the payment $p^b_{i,j}$ which the buyer $t_i \in \mathcal{B}_b$ needs to pay is the best unsuccessful offer $\min(\mathbf{a}_{t_i,-q_j})$ as long as it is lower than the successful bid b_{t_i,q_j}. Otherwise, the winning buyer will be charged equal to its bid. Mathematically, it can be expressed as: $p^b_{i,j} = \min(b_{t_i,q_j}, \min(\mathbf{a}_{t_i,-q_j}))$, where $\mathbf{a}_{t_i,-q_j}$ represents the asks of sellers except q_j.

Lemma 2: The proposed auction mechanism satisfies individual rationality.

Proof: According to the proposed auction, the payment $p^s_{i,j}$ such that $q_j \in \mathcal{S}_s$ is always greater than or equal to a_{t_i,q_j}, i.e., $p^s_{i,j} \geq a_{t_i,q_j}$. On the other hand, the payment $p^b_{i,j}$ with $t_i \in \mathcal{B}_b$ is always less than or equal to b_{t_i,q_j}, i.e., $p^b_{i,j} \leq b_{t_i,q_j}$. Thus, both the winning sellers and buyers do not lose from joining the auction, which completes the proof. ■

Lemma 3: The proposed auction mechanism is budget balanced.

Proof: After the winning determination stage, each winning buyer $t_i \in \mathcal{B}_b$ has only one winning seller $q_j \in \mathcal{S}_s$. This implies that $|\mathcal{B}_b| = |\mathcal{S}_s|$. Moreover, for each winning pair $\{t_i, q_j\}$, the payment $p^b_{i,j}$ made by t_i is equal to the price $p^b_{i,j}$ received by q_j. Thus, it is clear to express that:

$$\sum_{i=1}^{n}\sum_{j=1}^{m} p^b_{i,j} = \sum_{i=1}^{n}\sum_{j=1}^{m} p^s_{i,j}. \tag{17}$$

This completes the proof. ■

Lemma 4: The proposed auction mechanism is truthful for both the sellers and the buyers.

Proof: In the proposed method, a winning seller q_j is always rewarded with payment less than or equal to ask of seller who loses the trade, also termed as critical ask for q_j. However, the seller will be removed form the list of winning set if it changes its offer to a value greater than the second minimum ask i.e., $a_{t_i,q_j} > \min(\mathbf{a}_{t_i,-q_j})$. Therefore, likewise the VCG mechanism [19], being truthful will be the dominant strategy for the sellers. On the other hand, given that a buyer t_i can only win if $b_{t_i,q_j} \geq a_{t_i,q_j}$, therefore, a_{t_i,q_j} can be referred as the critical bid for buyer t_i, if it loses by submitting $b_{t_i,q_j} < a_{t_i,q_j}$, given others submission remain unchanged. In addition, the winner will be charged $a_{q_{j+1}}$ if $b_{t_i,q_j} \geq a_{t_i,q_{j+1}}$, otherwise it will be charged equal to its bid. However, for a particular seller q_j, the highest priority will be given to the buyer who offers the highest bid. This produces a tradeoff for the buyer t_i, that is, either it can win and increase its profit by bidding just above the critical bid (if it exceptionally knows the value) but lower than its true value, or it can lose the trade and achieves zero benefit. Thus, given that a buyer is always charged less than or equal to its bid, truthful bidding will be the dominant strategy for him/her. This completes the proof. ■

E. THE NEED FOR BLOCKCHAIN

There are many fundamental risks of adopting the plain sealed bid auction. For example, in the proposed scheme, only a single element (auctioneer) is responsible for all the decisions and the transactions. In particular, the auctioneer receives all the sealed bids from both the trading parties, and declares clearing prices which the buyers have to pay for their desirous PLS. The auctioneer is regarded as part of the auction mechanism, and it is assumed that he abides by the protocol. Given that only the auctioneer sees the bids and reveals the auction outcome, there could be a possibility that it may misbehave by inserting fictitious bids or by removing bids or by declaring false results to maximize his personal benefit. Thus because of its personal benefits the auctioneer may ruin the network performance for other transmitters. For example, as will be shown in Section VI-A, that the network will suffer by loss of data and high power consumptions if there is a corrupted auctioneer who only ignores the lowest ask prices. On the other hand, both sellers and buyers can also cheat by submitting multiple bids using multiple fake identities. This way the sellers can achieve maximum profit out of their services, and the buyers can acquire their desired service at the lowest possible price. Moreover, a seller or a buyer can also deviate from the standard trade process. For example, after receiving payment the seller doesn't provide the requested security service as he agreed to do, or after acquiring the service the buyer doesn't respond or transfer the money. This leads to reduced trust between all the parties including bidders and auctioneer, potentially decreasing the number of participants as well as the level of bidding competition.

Thus, in order to deter all the parties from cheating and to develop a trustful environment, and also to fully harness the benefits of the proposed auction mechanism, it is vital that there exists a decentralized way for all the decisions to be made. In addition, it is important that the participants' identities as well as their corresponding transactions are to be verified distributively. For this purpose, we exploit the blockchain technology for the development of a distributed auction framework. The key use of the blockchain-based framework has two folds: 1) employing the smart contract facility to validate the transactions and 2) settle the payments to buyers and sellers. The detailed description of the proposed framework is presented in the following sections.

IV. BLOCKCHAIN-BASED DISTRIBUTIVE AUCTION FRAMEWORK

The proposed system contains several distrusting parties i.e., transmitters, sellers, relay-jammer pairs who intend to work together for a common goal. In this section, we introduce a public blockchain framework that interconnects all the distrusting parties without a central authority. To build a blockchain framework, on top of the parties mentioned above, we also introduce *miners* who verify the transactions and update the blockchian to build a trustless system by enabling transparency, integrity and validity. Note that, miners are usually separate entities who are equipped with enough computational power to perform transaction verification and validation.

Given that, one of the key objectives of this work is the development of fully distributed, cheat-free and trustless framework, therefore, we adopt Ethereum based permissionless blockchain instead of permissioned blockchain. This is because permissioned blockchain relies on trusted nodes which consequently establishes a partially centralized trust in the network [51]. In this case the performance of the network can be easily degraded if the trusted nodes collude by themselves or being attacked by external elements. Moreover, Instead of Bitcoin, the reason behind the choice of Ethereum to support the decentralized network and handling financial transactions is to minimize the mining process. For example, bitcoin framework has a mining window of 10 minutes, which is longer for the underlying relay wireless channel. On the other hand, Ethereum framework can support a mining window of up to 12 seconds [52], which is more suitable for the considered framework. It is important to note that, increasing the mining window from 12 seconds to 10 minutes will also increase the risk of double spending by a factor of at least fifty. Given that, our model is based on Ethereum blockchain, therefore, *Ether* will be considered as virtual currency for all types of payments. It enables all the parties in the system to make and receive payments. Moreover, Ether can also be exchanged with other popular coins [53]. Let us briefly introduce the important building blocks required for the proposed blockchain.

A. BUILDING BLOCKS OF BLOCKCHAIN

1) ASYMMETRIC CRYPTOGRAPHY

Each new party, when they join the relay-auction system, generates new pair of public and private keys using popular asymmetric crypto systems such as ECC (Elliptic-curve cryptography) [54]. The private key is used to protect the virtual wallet of the party. The public keys are public and anyone can obtain other's public keys and it can be used for identification purposes. Asymmetric cryptography can be used to encrypt messages using public key and the encrypted messages can be decrypted by the private key. The same keys can be used to sign a message which is explained in the following section.

2) DIGITAL SIGNATURE SCHEME

The digital signatures can be used to prove the provenance or the owner of the messages communicated between two parties. This can be achieved by the same public-private key pairs generated using the asymmetric cryptography. For example, if Alice wants to generate a signature for a message, then she can encrypt the message using the private key. The encrypted message can be decrypted by the corresponding public key which is known to Bob. If Bob can decrypt the message sent by Alice using Alice's public key then Bob can ensure that the message was indeed sent by the Alice.

The digital signature scheme is vital for all blockchain systems. Every time the buyers and sellers exchange messages (bids or ask price), miners will use the digital signature scheme to verify the identity of the sender.

3) CRYPTOGRAPHIC HASH FUNCTION

Cryptographic hash functions can be used to generate a message digest with a fixed length regardless of the size of the message. There are several algorithms such as *SHA-256* can be exploited for this purpose. The advantage of the hash function is that it will produce unique message digest for the message as long as the message is not altered. Even if the message is altered by one bit, the output of the hash function will be completely different. Hash functions are easy to compute and it is infeasible to find two different messages that produce the same message digest.

4) SMART CONTRACT

Smart contract is a software program that executes an agreement between distrusting parties automatically in the digital domain [55]–[57]. Smart contract can be used to transfer valuables between distrusting parties without the need for a middleman. The important property of a smart contract is that if one party agrees to pay a certain amount of money for a given service then the party can neither deny payment after receiving the service nor tamper the smart contract [58].

5) MINERS AND MINING BLOCKS

In the public blockchain, since there is no central authority, the role of miners is important. The miners ensure that no one in the system can cheat by verifying the transactions, executing the smart contracts to make the payments and record all the activities in a public ledger (blockchain). To ensure that miners are not cheating the systems, the public blockchain has several protocols [59] such as *proof-of-work*, *proof-of-stake*, *proof-of-burn*, etc. These protocols ensure that a miner which is approving a transaction has negative benefit if it is trying to cheat the other parties in the distributed network. In Bitcoin blockchain, the time required for the proof-of-work is set to 10 minutes, while in Ethereum it is set to 12 seconds, as mentioned before. Note that, Proof-of-Work algorithm in Ethereum is also known as Ethash which is a modified version of a precursor algorithm known as

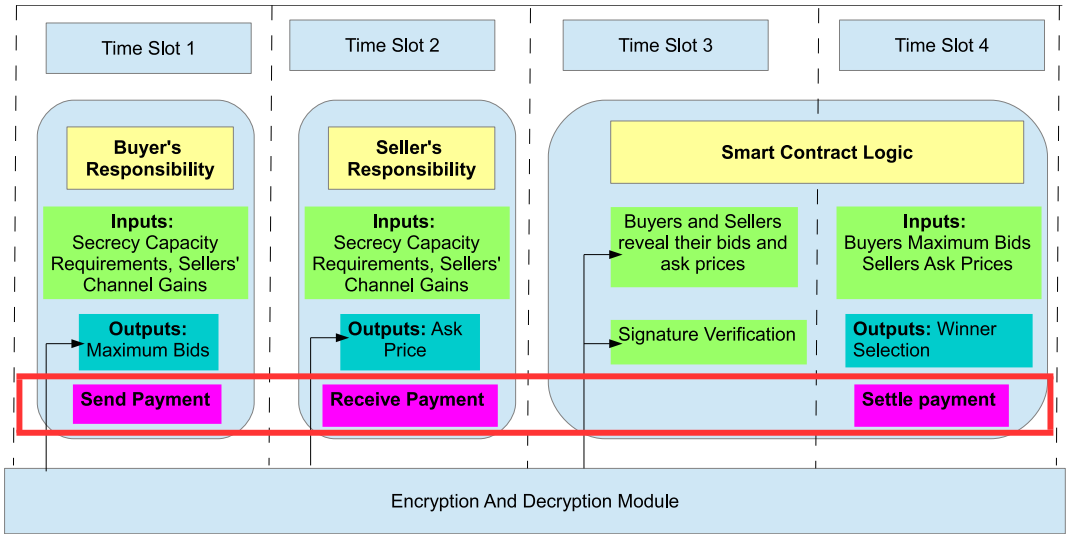

FIGURE 2. Block diagram of the proposed framework.

Dagger-Hashimoto [60]. However, because of scalability, speed and energy consumption issues of Ethash, recently, proof-of-stake also known as Casper in Ethereum is emerging as a potential approach for the next generation of Ethereum blockchain.

6) SYSTEM INITIALIZATION

Initially, each party generates their own public and private key pair. Denote the number of buyers, sellers and miners active on a particular session as n_B, n_S, and n_M, respectively. Denote the public and private key pairs for party i as $\{pk_i, sk_i\}$. Each party has a number of Ethers in the digital wallet. Denote the cth Ether coin belongs to ith party wallet as $ETH_{c,i}$ which is a $256-bit$ long serial number. This coin is registered against party ith public key pk_i and if a party wants to send this coin to another party then it will use the private key for validation. For example, let us consider two parties, Alice and Bob, whose public-private key pairs are $\{pk_A, sk_A\}$ and $\{pk_B, sk_B\}$. Now, let us suppose, Alice wants to pay 1 Ether (serial number ETH_{c,pk_A}) to Bob. To do that, Alice prepare the following transaction:

$$T_{Alice->Bob} = Enc_{sk_A}(ETH_{c,pk_A}||pk_B)||ETH_{c,pk_A}||pk_B,$$

where $Enc_{sk_A}(.)$ denotes asymmetric key encryption algorithm and $||$ denotes concatenation operation. Transaction $T_{Alice->Bob}$ contains the serial number of Ether, Bob's public key, and digital signature of transaction to prove that this is indeed generated by Alice. This transaction may contain other parameters such as date and serial number. Most importantly, Alice obtains the digital signature of this transaction by encrypting the transaction using sk_A. Now the transaction and the corresponding signature is sent to the network. This transaction can be verified by the miners by checking the following:

$$Dec_{pk_A}(ETH_{c,pk_A}||pk_B) = ETH_{c,pk_A}||pk_B,$$

where $Dec_{pk_A}()$ denotes the asymmetric key decryption algorithm. The miner first checks whether the message is actually sent by Alice using the pk_A. If the above verification is successful then the miners will search the past transactions from the blockchain and check who actually owns the coin ETH_{c,pk_A}. If the last owner of the coin is indeed Alice then the miners can approve the transaction by creating a new block where the ownership of the coin is transferred to Bob. Based on this fundamental principle, the following subsections define the steps of the blockchain architecture.

7) AUTHENTICATION

Since our model is built on top of the Etherium framework, the authentication of transactions will use the default settings, e.g., it relies on public-private key pairs, the properties of public key encryption, and digital signature as described in Section IV-A.2. As described in Section IV-A.6, each party has a pseudo identity known by its public key (pk_i). This public key is linked to their wallet, such that, anyone can verify the balance in the wallet. Since it is a distributed system, there is no restriction for a new party to join the system. When a new party joins the system, as described in Section IV-A.6, the party will generate its own public and private key. The public key will be announced to the system.

V. RELAY SMART CONTRACT

This section describes the Ethereum-based smart contract for the proposed work. As shown in the "contract Relay" pseudo code in Fig. 3, the smart contract has a number of public and private functions. These functions can be invoked by sellers, buyers and the smart contract itself. Let us explain responsibilities of sellers, and buyers as well as the smart contract logic below. We also split the whole process into four time periods, as shown in Fig. 2.

```
contract Relay {
  /*buyers invoke buyerPlaceBid function to send
their requirements such as secracy capacity require-
ments, hash bids, etc */
      function buyerPlaceBid() public { }
  /*buyer invokes buyerMakeDefaultPayment func-
tion to make default payments to the smart contract.
*/
      function buyerMakeDefaultPayment() public{ }
  /*seller invokes sellerPlaceBid functions to place
ask price in the form of hash value */
      function sellerPlaceBid() public { }
  /*Once the bidding period is over, the buyer in-
vokes buyerRevealBid function to reveal the bid and
random values used to generate hash value*/
      function buyerRevealBid() public{ }
  /*At the end of Time Slot 1 the Smart contract
broadcasts that buyer has completed a bidding and
sellers can submit the ask prices*/
      event BuyerBidComplete();
  /*Once the bidding period is over, the seller in-
vokes sellerRevealBid function to reveal the ask price
and random values used to generate hash value*/
      function sellerRevealBid() public { }
  /*At the end of Time Slot 2 the Smart contract
broadcasts that sellers has submitted the ask prices
and now buyers and sellers can reveal their bids and
ask price*/
      event SellerBidComplete();
      /*Now the smart contract executes the private
function verifyBidsAndAskPrice to check if the bids
and ask prices are correct*/
      function verifyBidsAndAskPrice() private { }
  /*The smart contract executes the private function
paymentToSeller to select the winner and make pay-
ment to the seller*/
      function paymentToSeller() private { }
  /*The smart contract executes the private function
balanceToBuyer to make the remaining balance to the
buyer*/
      function balanceToBuyer() private { }
}
```

FIGURE 3. Pseudocode code of the proposed Relay smart contract.

A. BUYER'S RESPONSIBILITIES

Initially, the buyer performs its own calculation using the channel gain information of the seller and calculates the required secrecy capacity and the amount it is willing to pay for the service. Once this calculation is performed, the buyer invokes function **buyerPlaceBid**() to create a new bidding process. The input parameters for this functions are unique transaction identification number (tx_{id}), the requirements, time stamp and digital signature of the transaction. Let us denote this as $T_{Buyer->Blockchain\ Network}$ where

$$T_{Buyer->Blockchain\ Network} = data_1||data_2||data_3,$$

where

$$\begin{aligned} data_1 &= Secrecy\ capacity||tx_{id}||pk_{Buyer}||Time,\\ data_2 &= H(bids||nonce||capacity||tx_{id}||pk_{Buyer}||Time),\\ data_3 &= Enc_{sk_{Buyer}}(data_2||data_1), \end{aligned}$$

where $H(.)$ denotes hashing operation using SHA256 algorithm. Note that the bid value is hidden inside the hash value in $data_2$. Digital signature of the transaction is in $data_3$. To randomise the hash operation, the buyer is adding a random *nonce* during the hash computation. Since the range of bids is small, this *nonce* will secure the bid from miners during Time Slot 1. During Time Slot 3, *bid* and *nonce* will be revealed by the buyer. The buyer will also make a default payment to the smart contract by invoking function **buyerMakeDefault**(). The default payment must be fixed and much higher than the bid. Given that the bid value is protected by its hash, therefore, the default payment can be public.

B. SELLER'S RESPONSIBILITIES

At the end of Time Slot 1, the smart contract broadcasts the bidding through "event" function. This is to notify all the sellers about the new bidding. Once sellers receive $T_{Buyer->Blockchain\ Network}$ in Time Slot 1, they extract *capacity* requirements and based on the channel gains, sellers calculate the ask prices for different buyers, and then invoke function **sellerPlaceBid**() using the following arguments as input in Time Slot 2:

$$T_{Seller->Blockchain\ Network} = data_4||data_5||data_6,$$

where,

$$\begin{aligned} data_4 &= tx_{id}||pk_{Seller}||pk_{Buyer}||Time,\\ data_5 &= H(ask\ price||nonce||tx_{id}||pk_{Seller}||pk_{Buyer}||Time),\\ data_6 &= Enc_{sk_{Buyer}}(data_4||data_5). \end{aligned}$$

The transaction $T_{Seller->Blockchain\ Network}$ contains the same tx_{id} and public key of the seller and buyer. This transaction signed by the sellers private key ($data_6$). Instead of transmitting this message to the network, the seller obtains a hash value ($data_5$) of the transaction which is again randomised by *nonce*. It should be noted that there is a predefined period for the first time slot and all the bids must be submitted within the time slot. During Time Slot 3, *ask price* and *nonce* will be revealed by the seller.

C. SMART CONTRACT LOGIC

At the beginning of Time Slot 4, the smart contract will invoke the private function **verifyBidsAndAskPrice**() by inputting hash values of bids, ask price, and the corresponding nonce. This function first verifies the signature as follows:

$$Dec_{pk_{Buyer}}(data_3) = data_2||data_1.$$

If it is correct then it proceeds to perform the same operation to validate the seller's ask prices transactions. If any party is malicious and propagating false data then it can be identified by the miner and the reputation of that party will be damaged. Then to check whether bids and ask prices are correct by checking the following equations for all buyers and sellers:

$$\begin{aligned} H(bids||nonce||data_1) &= data_2,\\ H(ask\ price||nonce||data_4) &= data_5. \end{aligned}$$

If there is no cheating then the smart contract declares the winners by executing Algorithm 1. Afterward, it will

invoke function **paymentToSeller**() and function **balanceToBuyer**() to settle payments.

VI. PERFORMANCE EVALUATION

In this section, we present simulation results and demonstrate the effect of rational agent in the centralized based auction model. We also discuss the security properties of the proposed blockchain based distributed auction framework.

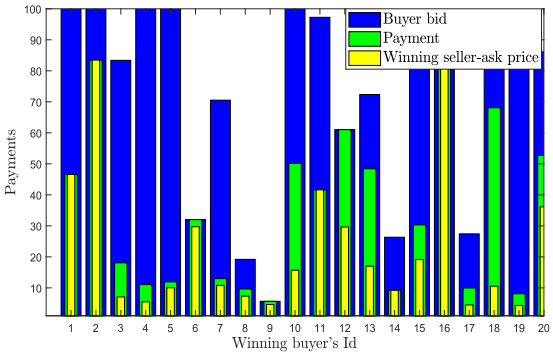

FIGURE 4. The comparison of payments, offers (bids) and ask prices under the proposed double auction mechanism, when $n = 20$, $m = 15$, and $f_i = 3$.

A. SIMULATION RESULTS

This section exhibits the performance of the proposed auction mechanism in terms of individual rationality. In addition, it shows the impact of a rational auctioneer in a centralized mediated model. Note that, there are many malicious activities as discussed in Section III-E, which could directly affect the network performance. However, in order to demonstrate the effect of malicious insider, we only take into account an example of malicious auctioneer (termed as selfish auctioneer) in which it always ignores the lowest ask price for each buyer. A Monte Carlo simulation platform representing the system model was developed in MATLAB. For simulation setting, unless otherwise stated we consider $C_{\text{th}} = \mathcal{C}_i \geq 0.2$, that is, all the transmitters t_i are desirous to achieve the same minimum level of secure transmission. In addition, they are randomly located according to a uniform distribution, such that values of $d_{\text{t}_i,\text{q}_j}$ are chosen within the range of (0, 1]. The path loss exponent is set to $a = a_{\text{t}_i,\text{q}_j} = 3$, and $\kappa = 0.1$, and the values of $\alpha_{\text{t}_i,\text{q}_j}$ and $\eta_{i,j}$ are drawn randomly according to a uniform distribution over the range (0, 30] and [20, 100], respectively. Moreover, all the intermediate relays are located randomly over the uniform distribution such that their channel qualities to destination d_i and e_i are selected within the range of (0, 1]. Fig. 4 shows the bids of winning buyers, asks of winning sellers and payments made, when there are $n = 20$ buyers and $m = 15$ sellers, each seller can only support up to 3 buyers, i.e., $f_i = 3$. Clearly, it is evident that each winning seller is rewarded with a payment not less than its ask, while each winning buyer is charged by the payment not greater than its bid. This implies that the winning transmitters t_i and the relay operators q_i that are successfully matched have gained positive utilities. Thus, the agents have sufficient incentive to participate in the trade.

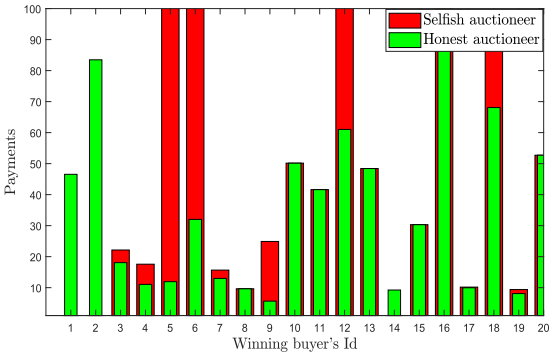

FIGURE 5. The comparison of payments made by winning buyers under both the honest and the selfish auctioneer, when the parameters are set as $m = 20$, and $f = f_i = 4$.

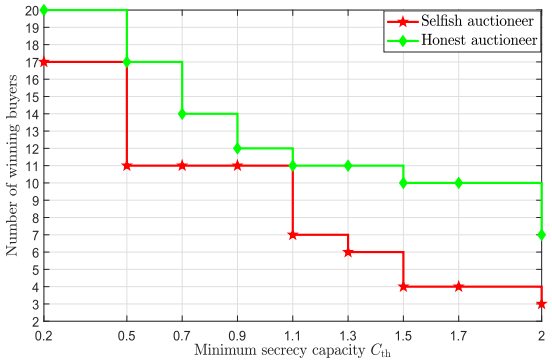

FIGURE 6. Minimum desired secrecy capacity versus the number of winning buyers under both the honest and the selfish auctioneer, when $n = 20$, $m = 15$, and $f = f_i = 3$.

Fig. 5 demonstrates the impact of a selfish auctioneer on the payments of winning buyers. It can be seen that due to the selfish auctioneer some of the buyers are charged extra payments as compared to the payments made under the honest auctioneer. Moreover, some of the legitimate destinations also suffer by lost of data. For example, the buyers q_1, q_2 and q_{14} are not served due to the selfish auctioneer. This is because of the reason that after removing the lowest ask prices, there are no matching options left for the buyers demands, or, the matched sellers have already allocated their resources (i.e., subcarrier) to other buyers. This can also be exhibited in Fig. 6, where the number of winning buyers also depends on their level of security requirement. Thus, from both Fig. 5 and Fig. 6, it is apparent that the buyers and their corresponding destinations are always substantially suffered because of the selfish auctioneer. Figure. 7 shows the relationship between the number of sellers and the network cost in terms of total power consumption for security services. As expected, the selfish auctioneer causes extra power dissipation. It can be observed that for a small number of sellers there is a huge gap between the two curves. This is due to the fact that for fewer number of sellers there are lower number of options for suitable seller-buyer matching, and as a result, selfish

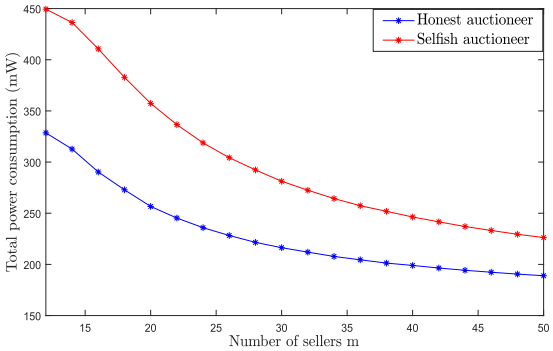

FIGURE 7. The amount of total power consumption in order to satisfy the security requirements of all the buyers, when $n = 20$, and $f = f_i = 2$.

auctioneer will remarkably affect the network performance. However, the number of matching options increases with the increase of the number of sellers, which effectively reduces the impact of the selfish auctioneer and thus decreases the gap between the curves.

B. SECURITY PROPERTIES OF THE PROPOSED FRAMEWORK

The aim of the blockchain based framework is to remove the central authority (i.e., auctioneer) in traditional systems where the auctioneer in traditional system can manipulate the bidding system to increase his own profit. However, distributed system like the one proposed in this paper could be vulnerable to attacks such as replay, manipulation and repudiation. In this subsection, we describe how each of these attacks are mitigated in our proposed framework.

1) REPLAY ATTACKS

Given that, in our proposed double auction framework, for the transparency, the bids should be revealed to everyone in the network. This will lead to replay attacks. For example, in Time Slot 1, it is possible for an adversary to replay the transactions (unsuccessful) announced in the past. This will be a problem if there are no counter measures to mitigate this e.g., the legitimate buyer will loss money for something he didn't ask. However, the proposed protocol mitigate this issue by incorporating two parameters: time and transaction id. Even though it is possible for the adversary to change time and transaction id in $data_1$ and $data_2$, it is not possible for generating legitimate signature $data_3$. We used the same technique to protect the sellers transaction.

2) MANIPULATION ATTACKS

Since our protocol follows sequential approach, it is possible for the buyers to manipulate their bids once they knew the ask price of sellers or the sellers can increase their ask price if they knew the bids in advance. We mitigated this problem by incorporating hashing operation in Time Slot 1 and Time Slot 2. During these slots, buyer and seller commit their bid and ask price via a simple hashing operation. In Time Slot 3, they will reveal the values. Since hash functions, like SHA256, are one-way function, it is infeasible for buyer or seller to find another bid (smaller than committed) or ask price (bigger than committed) so that they could generate the same hash values in $data_2$ or $data_5$.

3) BRUTE FORCE ATTACK BY SELLER

The range of bids are limited e.g., 0 to 10000 (i.e., 14 bits). Even though we use one way hashing function to hide the buyers' bid in $data_2$ during Time Slot 1, if we don't add *nonce*, the seller can easily obtain bids by computing all possible (i.e., there only 2^{14} possibilities) values for bids. In order to avoid this problem, we added 2048−bit long *nonce*. This will increase the complexity from 2^{14} into 2^{2048} (computing all possibilities would require several hours).

4) REPUDIATION ATTACK

Similar to traditional bidding systems, buyers may deny their commitments if the winning price is substantial or want to change their mind. Since our model follows asymmetric key based digital signature and invokes smart contract, buyers cannot prove that he didn't generated a particular winning bid. Similarly, since our model uses smart contracts, the payment will be taken from the buyer wallet automatically. However, since the smart contract is a software program, buyers can terminate their device before the transaction is signed by the buyers' private key. However, terminating the smart contract will put the buyer on danger of bad reputation and the Ethers stored in buyers wallet become unusable i.e., the miner will blacklist all the Ethers under the particular buyers public key and update the blockchain.

VII. CONCLUSION

In this paper, we proposed a double auction mechanism to bridge network economics need and transmitters requirements of PLS using cooperative relaying and jamming. Through theoretical analysis, we proved that the proposed double auction is individual rational, budget balance and truthful. Our analyses demonstrate that if the the proposed model is employed by the traditional centralized auction framework, a selfish auctioneer can ruin the network performance in terms of data loss and extra power dissipation. In addition, the winning buyers can be suffered by extra payments. Thus, in order to address the malicious activities of participants, we developed a decentralized, cheat-proof, and autonomous auction framework, based on smart contract features of blockchain. Moreover, a virtual currency system was introduced for all the transactions, where a node that contributes to a successful delivery can obtain a reward. We analyzed that the proposed framework can also mitigate many security attacks including replay attack, manipulation attack, brute force attack, and repudiation attack.

REFERENCES

[1] A. K. Sadek, Z. Han, and K. J. R. Liu, "Distributed relay-assignment protocols for coverage expansion in cooperative wireless networks," *IEEE Trans. Mobile Comput.*, vol. 9, no. 4, pp. 505–515, Apr. 2010.

[2] N. Marchenko, T. Andre, G. Brandner, W. Masood, and C. Bettstetter, "An experimental study of selective cooperative relaying in industrial wireless sensor networks," *IEEE Trans. Ind. Informat.*, vol. 10, no. 3, pp. 1806–1816, Aug. 2014.

[3] A. S. Khan and I. Chatzigeorgiou, "Non-orthogonal multiple access combined with random linear network coded cooperation," *IEEE Signal Process. Lett.*, vol. 24, no. 9, pp. 1298–1302, Sep. 2017.

[4] R. Madan, N. B. Mehta, A. F. Molisch, and J. Zhang, "Energy-efficient cooperative relaying over fading channels with simple relay selection," *IEEE Trans. Wireless Commun.*, vol. 7, no. 8, pp. 3013–3025, Aug. 2008.

[5] W. Mohr, "The WINNER (wireless world initiative new radio) project-development of a radio interface for systems beyond 3G," *Int. J. Wireless Inf. Netw.*, vol. 14, no. 2, pp. 67–78, Jul. 2007.

[6] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 574–583, Mar. 2015.

[7] G. Chen, Z. Tian, Y. Gong, Z. Chen, and J. A. Chambers, "Max-ratio relay selection in secure buffer-aided cooperative wireless networks," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 4, pp. 719–729, Apr. 2014.

[8] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[9] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[10] J. Zhu, Y. Zou, B. Champagne, W. P. Zhu, and L. Hanzo, "Security–reliability tradeoff analysis of multirelay-aided decode-and-forward cooperation systems," *IEEE Trans. Veh. Technol.*, vol. 65, no. 7, pp. 5825–5831, Jul. 2016.

[11] V. N. Q. Bao, N. Linh-Trung, and M. Debbah, "Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 12, no. 12, pp. 6076–6085, Dec. 2013.

[12] I. Krikidis, J. S. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5011, Oct. 2009.

[13] A. S. Khan and I. Chatzigeorgiou, "Opportunistic relaying and random linear network coding for secure and reliable communication," *IEEE Trans. Wireless Commun.*, vol. 17, no. 1, pp. 223–234, Jan. 2018.

[14] Z. Han, N. Marina, M. Debbah, and A. Hjørungnes, "Physical layer security game: Interaction between source, eavesdropper, and friendly jammer," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, p. 11, Dec. 2009.

[15] B. Wang, Z. Han, and K. J. R. Liu, "Distributed relay selection and power control for multiuser cooperative communication networks using stackelberg game," *IEEE Trans. Mobile Comput.*, vol. 8, no. 7, pp. 975–990, Jul. 2009.

[16] K. R. Reddy and A. Rajesh, "Best relay selection using co-operative game theory: MANETs," in *Proc. IEEE Int. Conf. Commun. Signal Process. (ICCSP)*, Melmaruvathur, India, Apr. 2016, pp. 1347–1351.

[17] J. Huang, Y. Yin, Y. Sun, Y. Zhao, C.-C. Xing, and Q. Duan, "Game theoretic resource allocation for multicell D2D communications with incomplete information," in *Proc. IEEE Int. Conf. Commun. (ICC)*, London, U.K., Jun. 2015, pp. 3039–3044.

[18] M. R. Khandaker, K.-K. Wong, and G. Zheng, "Truth-telling mechanism for two-way relay selection for secrecy communications with energy-harvesting revenue," *IEEE Trans. Wireless Commun.*, vol. 16, no. 5, pp. 3111–3123, May 2017.

[19] W. Vickrey, "Counterspeculation, auctions, and competitive sealed tenders," *J. Finance*, vol. 16, no. 1, pp. 8–37, 1961.

[20] E. H. Clarke, "Multipart pricing of public goods," *Public Choice*, vol. 11, no. 1, pp. 17–33, Sep. 1971.

[21] R. B. Myerson and M. A. Satterthwaite, "Efficient mechanisms for bilateral trading," *J. Econ. Theory*, vol. 29, no. 2, pp. 265–281, Apr. 1983.

[22] R. P. McAfee and J. McMillan, "Auctions and bidding," *J. Econ. Literature*, vol. 25, no. 2, pp. 699–738, Apr. 1987.

[23] B. Basutli, J. M. Chuma, and S. Lambotharan, "Network capacity enhancement in HetNets using incentivized offloading mechanism," *IEEE Access*, vol. 6, pp. 39307–39323, 2018.

[24] B. S. Khan, S. Jangsher, and F. Bhatti, "Profitable relay selection in cooperative cellular network with mobile relays," in *Proc. IEEE Veh. Technol. Conf. (VTC)*, Toronto, Canada, Sep. 2017, pp. 1–5.

[25] M. Dong, G. Sun, X. Wang, and Q. Zhang, "Combinatorial auction with time-frequency flexibility in cognitive radio networks," in *Proc. IEEE INFOCOM*, Orlando, FL, USA, Mar. 2012, pp. 2282–2290.

[26] D. Yang, X. Fang, and G. Xue, "HERA: An optimal relay assignment scheme for cooperative networks," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 2, pp. 245–253, Feb. 2012.

[27] B. Cao, G. Feng, Y. Li, and M. Daneshmand, "Auction-based relay assignment in cooperative communications," in *Proc. IEEE Global Commun. Conf.*, Dec. 2014, pp. 4496–4501.

[28] R. Zong, X. Gao, and X. Feng, "Truthful double auction of spectrum trading for femtocell service provision," *Wireless Commun. Mobile Comput.*, vol. 16, no. 17, pp. 2924–2938, Dec. 2016.

[29] W. Wang and Z. Hidvégi, and A. B. Whinston, *Shill Bidding in English Auctions*. New York, NY, USA: MIMEO, 2001.

[30] D. A. Graham and R. C. Marshall, "Collusive bidder behavior at single-object second-price and English auctions," *J. Political Economy*, vol. 95, no. 6, pp. 1217–1239, Dec. 1987.

[31] R. Zeithammer, "Research note–strategic bid-shading and sequential auctioning with learning from past prices," *Manage. Sci.*, vol. 53, no. 9, pp. 1510–1519, Sep. 2007.

[32] H. Xu, S. M. Shatz, and C. K. Bates, "A framework for agent-based trust management in online auctions," in *Proc. IEEE Int. Conf. Inf. Technol. New Generat. (ITNG)*, Las Vegas, NV, USA, Apr. 2008, pp. 149–155.

[33] X. Yi and C. K. Siew, "Secure agent-mediated online auction framework," *Int. J. Inf. Technol.*, vol. 7, no. 1, pp. 1–14, Apr. 2001.

[34] B. Catane and A. Herzberg, "Secure second price auctions with a rational auctioneer," in *Proc. IEEE Int. Conf. Security Cryptogr. (SECRYPT)*, Reykjavik, Iceland, Jul. 2013, pp. 1–12.

[35] J. Trevathan, H. Ghodosi, and W. Read, "An anonymous and secure continuous double auction scheme," in *Proc. IEEE Hawaii Int. Conf. Syst. Sci.*, Kauia, HI, USA, Jan. 2006, pp. 125b–125b.

[36] M. Wooldridge, *An Introduction to MultiAgent Systems*. Hoboken, NJ, USA: Wiley, 2009.

[37] W. Suberg. (2015). *Factom's Latest Partnership Takes on us Healthcare*. [Online]. Available: http://cointelegraph.com/news/factoms-latestpartnership-takes-on-us-healthcare

[38] A. Mizrahi, "A blockchain-based property ownership recording system," in *A Blockchain-based Property Ownership Recording System*. ChromaWay, 2015. [Online]. Available: https://chromaway.com/papers/A-blockchain-based-property-registry.pdf

[39] M. Walport, *Distributed Ledger Technology: Beyond Blockchain*. London, U.K.: Government Office for Science, 2016.

[40] A. Wright and P. De Filippi. (2015). *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*. [Online]. Available: https://ssrn.com/abstract=2580664

[41] S. Underwood, "Blockchain beyond Bitcoin," *Commun. ACM*, vol. 59, no. 11, pp. 15–17, 2016.

[42] J. M. Graglia and C. Mellon, "Blockchain and property in 2018: At the end of the beginning," *Innov. Technol., Governance, Globalization*, vol. 12, no. 2, pp. 90–116, Jul. 2018.

[43] V. Buterin. (2014). *A Next-Generation Smart Contract and Decentralized Application Platform*. [Online]. Available: https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf

[44] S.-C. Cha, J.-F. Chen, C. Su, and K.-H. Yeh, "A blockchain connected gateway for ble-based devices in the Internet of Things," *IEEE Access*, vol. 6, pp. 24639–24649, 2018.

[45] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized blockchain for IoT," in *Proc. 2nd Int. Conf. Internet-Things Design Implement.*, Pittsburgh, PA, USA, Apr. 2017, pp. 173–178.

[46] A. Stanciu, "Blockchain based distributed control system for Edge computing," in *Proc. 21st Int. Conf. Control Syst. Comput. Sci. (CSCS)*, Bucharest, Romania, May 2017, pp. 667–671.

[47] M. Conoscenti, A. Vetro, and J. C. De Martin, "Peer to peer for privacy and decentralization in the Internet of Things," in *Proc. 39th IEEE Int. Conf. Softw. Eng. Companion*, Buenos Aires, Argentina, May 2017, pp. 288–290.

[48] Y. Rahulamathavan, R. C.-W. Phan, M. Rajarajan, S. Misra, and A. Kondoz, "Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption," in *Proc. IEEE Int. Conf. Adv. Netw. Telecommun. Syst. (ANTS)*, Bhubaneswar, India, Dec. 2017, pp. 1–6.

[49] S. Boyd, S.-J. Kim, L. Vandenberghe, and A. Hassibi, "A tutorial on geometric programming," *Optim. Eng.*, vol. 8, no. 1, p. 67, Mar. 2007.

[50] G. Xu, "Global optimization of signomial geometric programming problems," *Eur. J. Oper. Res.*, vol. 233, no. 3, pp. 500–510, 2014.
[51] M. Valenta and P. Sandner, *Comparison of Ethereum, Hyperledger Fabric and Corda*. Frankfurt, Germany: Frankfurt School, 2017.
[52] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in *Proc. 19th Int. Conf. Adv. Commun. Technol.*, Feb. 2017, pp. 464–467.
[53] K. Kotobi and S. G. Bilen, "Secure blockchains for dynamic spectrum access: A decentralized database in moving cognitive radio networks enhances security and user access," *IEEE Veh. Technol. Mag.*, vol. 13, no. 1, pp. 32–39, Mar. 2018.
[54] J. W. Bos, J. A. Halderman, N. Heninger, J. Moore, M. Naehrig, and E. Wustrow, "Elliptic curve cryptography in practice," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, 2014, pp. 157–175.
[55] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
[56] T. Dickerson, P. Gazzillo, M. Herlihy, and E. Koskinen, "Adding concurrency to smart contracts," in *Proc. ACM Symp. Principles Distrib. Comput.*, Mar. 2019, pp. 303–312.
[57] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on Ethereum smart contracts (SoK)," in *Proc. Int. Conf. Principles Secur. Trust*, 2017, pp. 164–186.
[58] R. Modi, *Solidity Programming Essentials: A Beginner's Guide to Build Smart Contracts for Ethereum Blockchain*. Birmingham, U.K.: Packt Publishing Ltd, 2018.
[59] L. S. Sankar, M. Sindhu, and M. Sethumadhavan, "Survey of consensus protocols on blockchain applications," in *Proc. 4th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, Jan. 2017, pp. 1–5.
[60] D. Vujičić, D. Jagodić, and S. Ranđić, "Blockchain technology, bitcoin, and ethereum: A brief overview," in *Proc. 17th Int. Symp.*, East Sarajevo, Bosnia, Mar. 2018, pp. 1–6.

AMJAD SAEED KHAN received the B.Eng. degree in computer engineering from the COMSATS Institute of Information Technology, Pakistan, in 2010, and the M.Sc. degree in digital signal processing and intelligent systems and the Ph.D. degree in communication systems from Lancaster University, U.K., in 2013 and 2018, respectively. He is currently a Research Associate in signal processing for 5G networks with the Wolfson School of Mechanical, Electrical, and Manufacturing Engineering, Loughborough University, U.K. His research interests include 5G networks, network coding, secure wireless communication, digital signal processing, nonorthogonal multiple access, embedded systems design, machine learning, and blockchain technology.

YOGACHANDRAN RAHULAMATHAVAN received the B.Sc. degree (Hons.) in electronic and telecommunication engineering from the University of Moratuwa, Sri Lanka, in 2008, and the Ph.D. degree in signal processing from Loughborough University, U.K., in 2011. He received a scholarship from Loughborough University to pursue his Ph.D. degree. In 2008, he was an Engineer with Sri Lanka Telecom, Sri Lanka, and from 2011 to 2012, he was a Research Assistant with the Advanced Signal Processing Group, School of Electronic, Electrical, and Systems Engineering, Loughborough University, U.K. He was a Research Fellow with the Information Security Group, School of Engineering and Mathematical Sciences, City University London, U.K. He is currently a Faculty Member with Loughborough University. His research interests include signal processing, machine learning, blockchain technology, and information security and privacy.

BOKAMOSO BASUTLI (M'11) received the Ph.D. degree in electronic, electrical, and systems engineering from Loughborough University, U.K., in 2016. From 2008 to 2010, he was an Installation Engineer and a Lead Engineer with Singapore Technologies Electronics (Info-Software Systems). He was a Senior Telecommunications Engineer with the Civil Aviation Authority of Botswana, from 2010 to 2012. He joined the Botswana International University of Science and Technology (BIUST) as a Founding Teaching Instructor, in 2012, where he is currently a Lecturer with the Department of Electrical, Computer, and Telecommunications Engineering. He is currently leading the Signal Processing, Networks, and Systems Research Group, BIUST. His research interests include convex optimization, resource allocation, wireless communications, and game theory.

GAN ZHENG (S'05–M'09–SM'12) received the B.Eng. and M.Eng. degrees in electronic and information engineering from Tianjin University, Tianjin, China, in 2002 and 2004, respectively, and the Ph.D. degree in electrical and electronic engineering from The University of Hong Kong, in 2008. He is currently a Reader of signal processing for wireless communications with the Wolfson School of Mechanical, Electrical, and Manufacturing Engineering, Loughborough University, U.K. His research interests include machine learning for communications, UAV communications, mobile edge caching, full-duplex radio, and wireless power transfer. He was a first recipient of the 2013 IEEE Signal Processing Letters Best Paper Award, the 2015 GLOBECOM Best Paper Award, and the 2018 IEEE Technical Committee on Green Communications and Computing Best Paper Award. He currently serves as an Associate Editor for the IEEE Communications Letters.

BASIL AsSADHAN received the M.S. degree in electrical and computer engineering from the University of Wisconsin and the Ph.D. degree in electrical and computer engineering from Carnegie Mellon University. He is currently an Assistant Professor with the Electrical Engineering Department, King Saud University. His research interests include cybersecurity, network security, network traffic analysis, and anomaly detection.

SANGARAPILLAI LAMBOTHARAN (SM'06) received the Ph.D. degree in signal processing from Imperial College London, London, in 1997, where he was a Postdoctoral Research Associate, until 1999. He was a Visiting Scientist with the Engineering and Theory Centre, Cornell University, USA, in 1996. From 1999 to 2002, he was with the Motorola Applied Research Group, U.K., where he investigated various projects including physical link layer modeling and performance characterization of GPRS, EGPRS, and UTRAN. He was with King's College London and Cardiff University as a Lecturer and Senior Lecturer, respectively, from 2002 to 2007. He is currently a Professor of digital communications and the Head of the Signal Processing and Networks Research Group, Wolfson School of Mechanical, Electrical, and Manufacturing Engineering, Loughborough University, Loughborough, U.K. His current research interests include 5G networks, MIMO, radars, smart grids, machine learning, network security, and blockchain technology. He has authored more than 200 journals and conference articles in these areas.