2020-3

DEAL: Differentially Private Auction for Blockchain based Microgrids Energy Trading

Muneeb Ul Hassan
Swinburne University of Technology - Australia, muneebmh1@gmail.com

Mubashir Husain Rehmani
mubashir.rehmani@cit.ie

Jinjun Chen
Swinburne University of Technology - Australia, jinjun.chen@gmail.com

Recommended Citation

M. U. Hassan, M. H. Rehmani and J. Chen, "DEAL: Differentially Private Auction for Blockchain-Based Microgrids Energy Trading," in IEEE Transactions on Services Computing, vol. 13, no. 2, pp. 263-275, 1 March-April 2020.

DEAL: Differentially Private Auction for Blockchain based Microgrids Energy Trading

Muneeb Ul Hassan*, Mubashir Husain Rehmani§, Jinjun Chen*
*Swinburne University of Technology, Hawthorn VIC 3122, Australia
§ Cork Institute of Technology (CIT), Ireland

***Abstract*—Modern smart homes are being equipped with certain renewable energy resources that can produce their own electric energy. From time to time, these smart homes or microgrids are also capable of supplying energy to other houses, buildings, or energy grid in the time of available self-produced renewable energy. Therefore, researches have been carried out to develop optimal trading strategies, and many recent technologies are also being used in combination with microgrids. One such technology is blockchain, which works over decentralized distributed ledger. In this paper, we develop a blockchain based approach for microgrid energy auction. To make this auction more secure and private, we use differential privacy technique, which ensures that no adversary will be able to infer private information of any participant with confidence. Furthermore, to reduce computational complexity at every trading node, we use consortium blockchain, in which selected nodes are given authority to add a new block in the blockchain. Finally, we develop Differentially private Energy Auction for bLockchain-based microgrid systems (DEAL). We compare DEAL with Vickrey–Clarke–Groves (VCG) auction scenario and experimental results demonstrates that DEAL outperforms VCG mechanism by maximizing sellers' revenue along with maintaining overall network benefit and social welfare.**

***Index Terms*—Differential privacy (DP), game theoretic auction, blockchain, microgrid, smart grid (SG), VCG auction.**

I. Introduction

Microgrid technology caught attention of researchers due to increasing demand of energy from renewable energy resources. Microgrid is a distributed energy system usually equipped with more than one renewable energy resource that are used to generate green electric energy without harming the environment. Solar, wind, and biomass are commonly used energy resources by microgrids [1]. One of the major purpose of such microgrids is storage of electric energy. This stored energy is further used to benefit both the customers and utilities in various ways, such as enhancing demand side management (DSM) by dynamically adjusting prices of energy by sharing load between microgrid and fossil fuel-based energy system [2]. This stored energy is traded among different consumers depending upon their demand. In this way, a reliable energy system can be constructed that will provide seamless and uninterrupted supply of electric energy.

An important phenomenon of microgrid is trading energy mutually and with other consumers. This energy trading leads to many advantages such as increase in revenue of prosumers by supplying surplus energy to demanding customers. Energy trading phenomenon is not that simple, and it requires critical decisions, such as what will be the trading charges in accordance with per unit supplied energy? How the specific buyers will be determined from a list of buyers? Which seller to select from the list of sellers? How one will get maximum benefit/profit? How the complete network will be profitable? These mentioned decisions are crucial and require special attention before practical implementation of trading model of microgrids. If we analyse the mentioned questions critically, all these questions can be solved by developing an efficient and optimal auction phenomenon. An efficient auction phenomenon results in increase of revenue and social welfare to an optimal level in which every buyer and seller gets some advantage of participating in auction [3], [4]. This microgrid auction comes up with two critical challenges. One is to carry out a secure, user-friendly, and transparent auction, while second is to develop a game theoretic model which enhances revenue and social welfare of auction mechanism to an optimal level. In order to enhance social welfare and revenue of the network, we enhanced Vickrey–Clarke–Groves (VCG) auction mechanism and developed a new game-theoretic auction. Secondly, to overcome the need of security, we integrated blockchain technology with microgrid system because of its tamper-proof nature [5], [6].

Blockchain-based microgrid auction provides a decentralized and trusted atmosphere to buyers and suppliers in which they can freely trade without the need of a centralized trusted third-party. Despite of all these benefits, auction mechanism on blockchain is not completely secure and is actually vulnerable to certain privacy attacks. One such attack is inference attack in which the adversary tries different combinations of ask/bid in order to predict and get knowledge about the corresponding outcomes of auction [7], [8]. Another attack which require special consideration while designing an auction mechanism is the leakage of individuals' private information due to repeatability of auction. For example, microgrid energy auctions are usually repeated after a certain interval of time, thus, certain clues are always left over in form of historical records which can further be used to infer ones' private information [9], [10]. Overcoming such issues become more difficult in a transparent blockchain technology. Therefore, we used differential privacy preservation strategy in our auction mechanism which ensures that presence or absence of participant will have minimal effect over the outcome of the auction. Thus, leaving no room for adversary to infer or estimate about behaviour or any particular individual participating in auction.

In this paper, we propose DEAL, which is a Differentially private Energy Auction for bLockchain-based microgrid. DEAL not only maximizes revenue and security, but also guarantees preservation of private individual information along with protecting bid privacy. DEAL works over differentially private VCG auction algorithm deployed over blockchain-based microgrid scenario in which prosumers and customers carry out auction in order to initiate energy trading between them. We compare our results with VCG auction used by the authors in [11]. The work in [11] evaluated and proposed the use of VCG auction mechanism for microgrids energy trading.

A. *Related Work*

Auction is a well-researched topic and plenty of work have been carried out to implement and study auction behaviour in different scenarios. For example, many privacy preserving auction approaches such as encryption [12] and anonymization [13] have been proposed in literature to carry out certain optimal auctions. Similarly, certain works are available in which VCG auction is applied over smart grid energy trading scenario to maximize its revenue [14]. Moreover, certain properties and criteria of differential privacy have also been studied in literature to carry out a privacy preserving auction [15]. However, to the best of our knowledge, no work that integrates differential privacy with decentralized blockchain based microgrid auction have been carried out in the past. For more details over implementation of blockchain in smart grid, we suggest readers to study [16]. Moreover, for detailed analysis of privacy issues in blockchain and directions, we suggest our readers to consult [17].

B. *Major Contributions*

The main contributions of this paper are as follows:

- We modify VCG auction mechanism for microgrid energy trading in order to maximize revenue of the network.
- We provide moderate cost, secure, and private auction mechanism for microgrids based over consortium blockchain properties.
- We preserve bid privacy of individual participants.
- We develop DEAL algorithm to protect outcome results of VCG auction mechanism from adversaries and inferring attacks.

The remainder of paper is organized as follows: In section 2, we provide detailed description of core components of our proposed strategy. Section 3 contains the functioning and algorithmic details of DEAL strategy. Furthermore, section 4 discusses simulation results in a brief manner. Finally, section 5 concludes the article.

II. Core System Components for Private Decentralized Energy Auction

In this section, the core system components for DEAL strategy such as VCG auction mechanism, differential privacy, and consortium blockchain for DEAL are presented.

A. *VCG Auction Mechanism*

VCG auction is generally referred as a sealed-bid multiple items auction. In VCG, buyers (bidders) submit their valuations in the form of bids for every item in the auction. The allocations and payments are done by following specific rules, mention hereafter, as allocation and payment rules respectively.

1) Allocation Rule: The aim of allocation rule is to compute optimal set of bidders according to items in order to maximize social welfare along with generating a good revenue. The allocation rule is defined as [18]:

$$\mathcal{X}(b) = \underset{\upsilon \in \Lambda}{\operatorname{argmax}} \sum_{i=1}^{n} b_i(\upsilon) \tag{1}$$

where $\mathcal{X}(b)$ is the formula for allocation rule of VCG auction, b_i is specific buyer ID, υ is the valuation of each buyer (referred as bid). Here, valuations υ belong to a specific distribution Λ, this distribution will be a set of number in which buyers can bid their valuations. Getting values from a specific distribution ensures that only buyers only bid non negative bids. This distribution can further be adjusted to set minimum or maximum bid value. This equation checks all available bids for a specific item and allocates it to the highest bidder.

2) Payment Rule: In VCG dynamic price auction, the payment that each bidder has to pay is calculated on the basis of "harm" his/her presence causes to other participant bidders. It can be simplified by saying as the difference between the accumulative sum of bids of other bidders without the winner and the accumulative sum of bids of other bidders when the winner is included in the allocation rule [19]. This payment is also known as "social cost". In our blockchain-based VCG auction, the payments can be calculated as:

$$\mathcal{P}_i(b) = \underbrace{\max_{\upsilon \in \Lambda} \sum_{j \neq i} b_j(\upsilon)}_{\substack{(A) \\ without\ winner\ i}} - \underbrace{\sum_{j \neq i} b_j(\upsilon^*)}_{\substack{(B) \\ with\ winner\ i}} \tag{2}$$

In the above equation, υ^* is the outcome of the winner chosen in Eq. 1, j serves as iterative factor that iterates through all the values except for winner i. It is worthy to note that $\mathcal{P}_i(b)$ will always yield a nonnegative socially optimal number. In the above equation, part (B) is the sum of winning bids, while part (A) is sum of valuations/bids of all participants that would win if bidder i was not bidding. This can also be termed as, the difference between optimal social welfare of all participating players (if i is not the participant) and welfare of all participating from the selected result (in which i is participating).

Definition** 1: **(Truthfulness) Truthfulness is always a dominant strategy in VCG auction. Moreover, the allocation rule $(\mathcal{X}(b))$ and payment rule $(\mathcal{P}(b))$ provides maximum revenue and significantly good social welfare if the bids are truthful. In VCG mechanism, *Revenue* is the total finalised payment that sellers will get at the end of auction mechanism. Furthermore, *utility* can be termed as the difference between the valuation of buyer and the hammer price (selected price $\mathcal{P}(b)$ after payment rule). Similarly, the sum of utilities of all participants of auction is referred as *social welfare*, which will indicate the total amount of profit that is generated in the market because of that specific auction mechanism [20]. It is compulsory for an auction mechanism to have nonnegative utility for every buyer, which means that no buyer will be allocated any slot with a price more than its valuation. This positive utility ensures that every participant is satisfied which in turn motivates other agents as well to participate in the auction. The utility U_i of VCG auction is referred as quasilinear utility, which is given as follows [18]:

$$U_i = S_i(\upsilon) - \mathcal{P}_i(b) \tag{3}$$

In Eq. 3, $S_i(\upsilon)$ represents the true valuation of bidder i and $\mathcal{P}_i(b)$ represents the payment that specific bidder will pay [21]. By substituting the value of Eq. 2 in Eq. 3, we get:

$$U_i = S_i(\upsilon) - [\max_{\upsilon\in\Lambda} \sum_{j\neq i} b_j(\upsilon) - \sum_{j\neq i} b_j(\upsilon^*)] \tag{4}$$

After substituting the value of utility in Eq. 4, the following result is obtained:

$$S_i(\upsilon) - \mathcal{P}_i(b) = S_i(\upsilon) - [\max_{\upsilon\in\Lambda} \sum_{j\neq i} b_j(\upsilon) - \sum_{j\neq i} b_j(\upsilon^*)] \tag{5}$$

This can further be rearranged as follows:

$$S_i(\upsilon) - \mathcal{P}_i(b) = \underbrace{S_i(\upsilon) + \sum_{j\neq i} b_j(\upsilon^*)}_{\substack{(A)\\ combined\ valuations}} - \underbrace{[\max_{\upsilon\in\Lambda} \sum_{j\neq i} b_j(\upsilon)]}_{\substack{(B)\\ bids\ without\\ winner\ i}} \tag{6}$$

In Eq. 6, part (B) is a constant term, which is independent of bid of bidder (i). Therefore, bidder i will not be able to increase or decrease its payment by reporting a lie. The only possible change that will take place by varying bidder i bid is in part (A) of Eq. 6, although this change will only have effect of the value of combined social welfare. Hence, bidder i will be keener to enhance term (A), which in turn will lead to truthful reporting of valuation. It can also be said in a way that lying or false bid will not change the overall outcome, however, the utility of i depends upon its bidding. Therefore, bidder i is not left with any other option except truthful bidding.

B. Differential Privacy

The term "Differential Privacy" was first introduced by C. Dwork in 2006 to protect the privacy of statistical datasets [22]. Differential privacy ensures that a result of an observers' query should not reveal too much amount of personal information about a particular individual present in the dataset [16], [23].

Definition** 2: **(Differential Privacy) A mechanism $\mathbb{F}$ provides (ε, δ)-differential privacy protection for every set having an output range Ω, and for any two neighboring datasets $\mathbb{D}$ and $\mathbb{D}'$.

$$Pr[\mathbb{F}(\mathbb{D}) \in \Omega] \leq \exp(\varepsilon) \cdot Pr[\mathbb{F}(\mathbb{D}') \in \Omega] + \delta \tag{7}$$

This mechanism states that for a particular output range Ω, e^{ε} bounds the ratio between two probabilities. Similarly, if the value of δ = 0, then the randomized mechanism provides ε-differential privacy according to its strictest definition. However, (ε, δ)-differential privacy relaxes the strict ε-differential privacy definition for certain events requiring low probability. ε-differential privacy is generally said to be *pure differential privacy*, however, the form (ε, δ)-differential privacy having $\delta > 0$ is referred as *approximate differential privacy* [24].

In Definition 2, the symbol ε represents the parameter called privacy budget, which further controls the level of guarantee that differentially private mechanism $\mathbb{F}$ provides [25]. Smaller value of ε ensures stronger privacy guarantee, therefore in practice, the value of ε is usually set less than unity "1".

The term $sensitivity$ determines the amount of perturbation which is required to protect the data from adversary. Sensitivity will calibrate the volume/amount of noise for the mechanism $\mathbb{F}(\mathbb{D})$. It can formally be defined as follows:

Definition 3: (Sensitivity) Suppose a random query is given to the mechanism $\mathbb{F}(.)$, then the value of sensitivity $\Delta\mathbb{F}_S$ can be defined as:

$$\Delta\mathbb{F}_S = \max_{\mathbb{D},\mathbb{D}'} ||\mathbb{F}(\mathbb{D}) - \mathbb{F}(\mathbb{D}')|| \tag{8}$$

1) Laplace Mechanism: Laplace mechanism is basically based over addition of controlled amount of Laplacian noise to the analyst query output. The noise is calculated by sampling it via Laplace distribution, in which μ acts as a centre point and σ acts as a scaling factor [26]. The formula for basic Laplace mechanism is:

$$Lap(b) = \frac{1}{2\sigma} exp(-\frac{|b|}{\sigma}) \tag{9}$$

Definition 4: (Laplace Mechanism) Let $\mathcal{F}$ be a function, $\mathbb{D}$ be a dataset in a range $\mathbb{R}$, the mechanism $\mathbb{L}$ is ε-differentially private if it adds Laplacian noise using the given formula on the basis of Eq. 7 as follows:

$$\mathbb{L}(\mathbb{D}) = \mathcal{F}(\mathbb{D}) \frac{\Delta\mathcal{F}}{\varepsilon} \tag{10}$$

2) Exponential Mechanism: A powerful method to execute differential privacy in a game-theoretic auction is Exponential mechanism. In this mechanism, a selection probability is assigned to every possible outcome in accordance to a utility function (also named as score function), which maps input and output pairs to a utility score.

Definition 5: (Exponential Mechanism) Let $\mathcal{N}(\mathbb{D}, \Phi)$ be a utility (score) function of input data $\mathbb{D}$ which calculates the output Φ in a range $\mathbb{P}$ $(\Phi \in \mathbb{P})$, then the Exponential mechanism $\mathbb{F}$ will be ε-differentially private if

$$Pr[\mathbb{F}(\mathbb{D}, \mathcal{N}, \mathbb{P}) = \mathcal{N}] \propto exp(\frac{\varepsilon\mathcal{N}(\mathbb{D}, \Phi)}{2\Delta\mathcal{N}}) \tag{11}$$

C. Consortium Blockchain for DEAL

The concept of blockchain flourished after the introduction of Bitcoin in 2008 by S. Nakamoto [27], [28]. Generally, blockchain is divided into three further types; private, public,

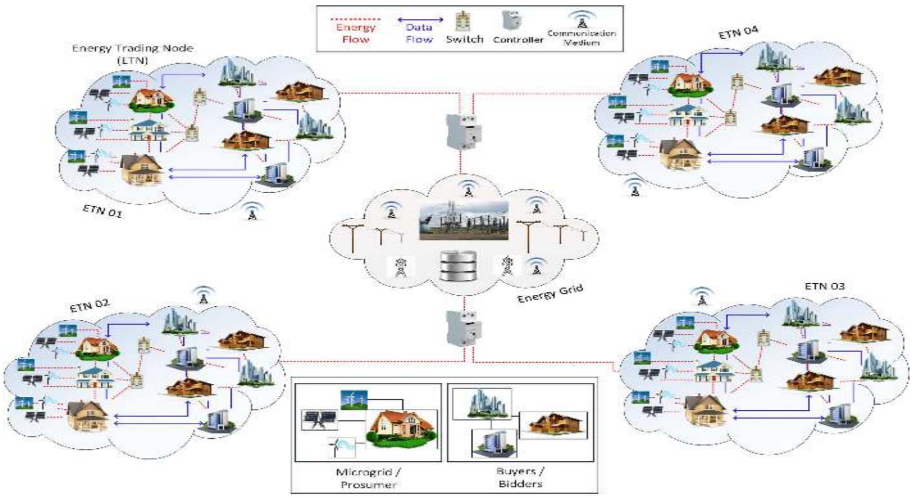


Fig. 1: System model of DEAL strategy describing the complete auction scenario between microgrid, buyers, energy power grid, and ETNs, along with information representation of energy and data flow.

and consortium [29], [30]. In this paper, we use the third type named as consortium blockchain, that is special type of blockchain in which consensus is carried out using some pre-selected nodes (energy trading nodes (ETNs) in our case). The controlling nodes (ETNs) are authorized to mine a new block in the network by carrying out consensus process. Major reason behind use of consortium blockchain is to facilitate such nodes which does not have high computational power. So that, the nodes that cannot solve complex cryptographic puzzle can also take part in the trading process.

1) "Blocks" Data Storage Entity: Blockchain network maintains uninform record of transactions in form of data storage entities named as "blocks" [31]. These blocks are fault-tolerant, append-only, shared, and distributed among all consensus carrying nodes of blockchain [32]. In DEAL strategy, ETNs are the consensus nodes which are responsible for addition of blocks in the network. A brief illustration of ETNs, and their connection with microgrid, and blockchain network is provided in Fig. 2. Mining and storing a new block in the network require high computational power. Therefore, we chose ETNs as authoritative nodes, which control the process of consensus. ETNs collect, handle, manage, and audit their local transactional records. ETNs collect records, audit them (with help of consensus), and then structure these records into blocks after encryption. Once a block gets added in the blockchain network (through consensus mechanism, defined hereafter), it becomes publicly accessible to all blockchain nodes (i.e. microgrid users, sellers, buyers, and ETNs), however, this record is tamper-proof, therefore these nodes can only view the data and cannot change it.

2) DEAL Coin: DEAL coin is a trading entity for our proposed mechanism, which is used to carry out trading, provide incentives, and charge penalties to participating nodes. Each blockchain node will have a cryptographic wallet to store and manage these energy coins. Actual value of this energy coin can be controlled by ETNs or can also be hard coded in the genesis node.

3) Consensus Mechanism: In this paper, we use proof of work (PoW) consensus algorithm, which is also the backbone of Bitcoin technology. Consensus nodes (also known as ETNs) are chosen by mutual agreement between all participating nodes. These nodes are not permanent and can be changed afterwards if some node does not follow the legal rules.

*a) **Proof-of-Work Consensus**:* We are using PoW consensus mechanism in our DEAL strategy because it ensures a healthy competition among mining nodes and every miner gets a reward after successfully mining a block. Moreover, PoW is less prone to security attacks as compared to other consensus mechanisms, because attacker require to control minimum of 51% computational power in order to hack complete network. In order to add new transactional record in blockchain, all ETNs in the network will carry out consensus. PoW consensus ensures the appending of legitimate data in the blockchain along with a guarantee that there is no conflict in the transaction and historical records of data [33], [34]. PoW used for ETNs in our strategy is similar to the mechanism used in Bitcoin technology, in which a unique hash value is generated every time along with a certain puzzle for every new block that needs to be mined in blockchain. This specific unique hash value serves as a link between the newly appended block and the prior block in that chain. ETNs solve a puzzle (by finding valid PoW) in order to mine a block in the network, and thus, they do also compete with each other to add the blocks as quick as possible. Similarly, this competition turns out to be in favour the fastest ETN which gets rewards in the form of DEAL coin every time a new block is added in blockchain. During consensus process, an ETN audits the auction records, structure these records in the form of a new block to verify the block from other ETNs during the PoW consensus process.

Similarly, the microgrids with maximum contribution in the network do also gets incentives in the form of DEAL coins from their respective ETNs. These incentives serve as a reward that will encourage more microgrids to take part in the auction process and to contribute more energy to the grid network.

These rewards are given on the basis of energy recorded by smart meter.

III. Differentially Private Auction Model

In this section, we discuss motivation, system model, design goals, and adversary model of DEAL mechanism.

A. Motivation of DEAL

The motivation of our DEAL strategy is as follows:

- Traditional smart grid auctions are usually carried out via some intermediary of centralized auction authority, which leads to lack of trust in the network. Our proposed blockchain based DEAL strategy ensures that every participant gets its fair share and no intermediary can alter with auction mechanism.
- Conventional VCG auction is not inclined towards maximizing revenue of sellers. However, in DEAL we modified VCG auction to provide maximum possible revenue to sellers.
- Typical auction approaches does not consider any privacy parameter and are prone to certain privacy attacks, such as inference attack. In our proposed DEAL strategy, we integrated differential privacy to ensure bidding privacy of bidders participating in decentralized auction.

B. Problem Definition

Problem definition of our proposed work consists of three major points which are defined as follows:

- How to maximize revenue and utility of sellers and buyers respectively in order to motivate more microgrid sellers to participate in auction process?
- How to provide a secure and transparent auction mechanism?
- How to preserve true valuations of bidders in VCG auction mechanism in order to protect their privacy and trust?

C. System Model of DEAL

DEAL consist of three major entities, i.e., microgrids (integrated with homes), buyer homes/buildings, and blockchains' distributed ledger. Microgrid can be a smart home or a network of homes that are capable of producing energy from different renewable energy resources such as solar, wind, biomass, etc. Microgrids are autonomous and can power the connected homes, and even surplus electricity can be traded into the network. Each microgrid has storage capacity where it can store its surplus energy which can be used for trading or usage at the time of need. Similarly, these microgrids are also connected with certain other homes and building that are not autonomous and require a continuous supply of electricity (which usually comes from electric grid station). These buildings/homes can request microgrids to sell its extra energy to earn some profit. This trading leads to the formation of an auction strategy, which is used to carry out a type of trading in which every participant will be happy and gets some benefits.

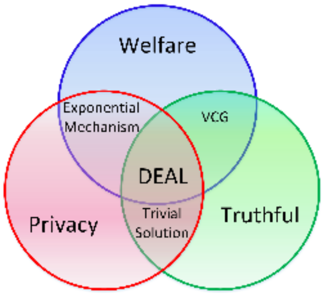


Fig. 2: Venn diagram based visual illustration of DEAL

Traditional auctions are usually carried out using an intermediary or centralized auctioneer. However, central auctioneer has certain disadvantages and may cause trust, security, and privacy leakages especially when using VCG auction (discussed in Section III). Here, the next entity of our DEAL strategy comes over which is blockchain-based distributed ledger. As discussed earlier, blockchain is a decentralized distributed ledger which ensures the correctness of records throughout the network. This step is carried out with the help of ETNs, which work as brokers to provide access to buyers and microgrids in order to trade energy. Each microgrid send a request to ETN about their excessive electric energy along with minimum selling price. ETNs announces the available amount of energy to buyers in the network. Energy buyers then submit their bids to network, and ETN carry out auction process and match energy trading pairs of microgrids and energy buyers. Nevertheless, integration of consortium blockchain in microgrid auction has solved certain security and trust issues, but due to its public nature it also raises large number of privacy threats. In order to overcome this, our DEAL strategy integrated differential privacy protection strategy with blockchain-based microgrid auction.

The dynamic nature of differential privacy ensures that adversary may not be able to infer any private information about auctions' participants. Despite of public availability of auction results, differential privacy is one of the most optimal strategy which preserves auction privacy. Furthermore, DEAL ensures the truthfulness and revenue maximization of the network using VCG auction mechanism. In order to make DEAL understandable for generalist audience, we also developed a pseudocode based algorithm which is given in Algorithm 1. A graphical illustration of our system model is given in Fig. 1.

D. Design Goals

Previous technical works over microgrid auction, differentially private auction, and blockchain-based auction considered certain problems on either topic individually, but none of the work from past literature considered preservation of individuals and bidding privacy in blockchain-based microgrid scenario using differential privacy protection. In order to visualize DEAL strategy from truthfulness, privacy, and social welfare perspective, we made a Venn diagram based illustration, which is given in Fig. 2. Our developed DEAL strategy has following design goals:

- Integrating consortium blockchain technology with microgrid energy trading system by using ETNs as authoritative nodes.
- Ensuring security during bidding by using cryptographic encryption of blockchain technology.
- Maintaining a decentralized and distributed ledger in auction to ensure transparency in the network.
- Achieving complete bid privacy and individual record privacy using differential privacy so that nobody may be able to estimate about future bids or auction outcomes.
- Enhancing revenue and social welfare of auction mechanism to ensure that every auction participant gets benefit from participating in the auction.

E. Adversary Model

In DEAL, owners of energy buying homes and buildings submit their truthful valuations to auctioneer in order to carry out VCG auction. However, the value of a specific energy slot is very private information in the sight of buyers. Similarly, if someone gets to know the final output prices of VCG auction, then it can easily infer the valuations and bidding prices of winners and other bidders because it is a sealed bid auction. So, revealing of valuations of energy buyers will directly put these bidders at the risk of disclosure of their sensitive information. Therefore, we aim to protect this sensitive bidders' information from different adversaries within or outside the decentralized blockchain network. Contrary to this, if bidders have a risk of leakage of their valuations, then they will not report their truthful valuations to the mechanism. Which will lead to the denial of truthfulness of VCG mechanism, along with the reduction in social welfare and revenue of the auction. In order to overcome all this situation, we propose a decentralized differentially private auction mechanism that preserves the valuations of bidders by using the concept of dual differential privacy as demonstrated in the next sections.

IV. Private Decentralized Energy Auction using DEAL Strategy

In this section, operational details, and functioning of DEAL strategy is discussed as follows:

A. Operation Details of DEAL

DEAL works over the principle of integration of differential privacy in VCG auction operating over consortium blockchain.

1) Parameter and Roles Initialization: In DEAL, each bidder and seller is formed a legitimate entity after a formal registration over a trusted authority, i.e. smart grid base station controlled by government authorities. During registration, the agent declares that whether it wants to join as buyer or seller. The assigned roles cannot be changed during an auction process, and one have to re-register itself with a new one if there comes any change. Once an agent joins the blockchain network, it gets its public and private key to carry out cryptographic transactions in the network. Similarly, we use elliptic curve digital signature algorithm in order to carry out cryptographic transactions in the network, as demonstrated in [35]. Each agent in the network is identified using its true identity, public key, and private key generated by authorities. Moreover, in order to carry out transactions and trade DEAL coins, agents do require x number of cryptographic wallet addresses $(WAD_{i,j})$, which the agents (A_i) can request to authorities after joining the blockchain network. In here, i is the node identity and j is the specific address ID within that wallet. The governing authority is responsible to provide every agent with an appended list of public key, private key, and wallet address $(PBK_i, PRK_i, [WAD_{i,j}]_{j=1}^{x})$. This mapping list, especially the wallet addresses can be used to carry out auction and trading after authorization by ETN of that area. A memory pool, which is further connected to decentralized distributed ledger stores the record of every auction and transaction in the network. This record is uniformly updated over the distributed ledger via ETNs.

2) Collecting Bids and Pre-Requisites of Auction: After parameters and roles initialization, the next step is to advertise the available energy slots and collect bids, which is carried out by the use of ETNs. ETN collects the information about available energy from all microgrids with respect to a pre-decided geographical distance, this can also be distance dependent and concept of Energy Internet can be used in order to route energy in the most optimal manner. Afterwards, ETNs broadcast this energy to all available buyers in the network. The buyers then check the available energy and provide their responses back to ETNs. ETNs collects the bids and carry out auction using our proposed DEAL strategy.

3) Carrying out Auction: Auction mechanism in the network is carried out using the DEAL strategy, in which all available nodes participate, and winners are determined in accordance with their bids and available energy slots. As ETN has collected all the bids of buyers, it carries out VCG auction and then modify it further to enhance the privacy using differential privacy and maximize the revenue using our proposed methodology. The detailed elaboration of DEAL mechanism is given in Section III. Similarly, after a specific period of time, the microgrids that have provided maximum amount of energy are incentivized in the form of DEAL coins. Along with this, the ETN winning the consensus mechanism is rewarded with certain DEAL coins according to the strategy.

4) Paying and Auditing Transactions: After completion of auction, all buyers pay the calculated amount to microgrids through wallet address of the specific microgrid. The buyers transfer DEAL coins from their wallet to the wallet of microgrid, which further collects the amount and verify it by using digital signature. These digitally signed approved transaction records are further sent to ETNs for auditing.

5) Carrying out PoW consensus: After a specific interval of time, ETNs collect all energy and coin transaction records of their local network, encrypt them, and then protect them by using digital signature. This encryption and signature process is carried out to ensure the accuracy, authenticity, and immutability of data. These transaction records are then combined to form a block like structure which do also contains the address of previous block in the chain. Furthermore, ETN calculates the hash value of this block over a random nonce value (e.g., x) to mine it in the chain using PoW consensus. Consensus is carried out similar to the method of Bitcoin consensus, in which timestamp, hash value and Merkle root of transaction is used to determine the hash value in accordance with difficulty, such as $HashValue(x+P_{data}) <$ *ConsensusDifficulty*) [36]. The speed of mining and block addition depends upon the *ConsensusDifficulty* which is a variable entity and is varied accordingly by authorities to control block mining rate. In our DEAL mechanism, consensus difficulty is varied to make sure that every block gets mined at least after 10 minutes.

6) Appending and Verifying the Block using Consensus: The fastest ETN to achieve PoW becomes the leader of that consensus process. This leader further broadcasts the compiled block to all authorized ETN nodes, which audit this block to ensure the verification and mutual supervision in the network. These ETNs broadcast their report in the network after auditing the received block. After this, each ETN compare their result with the result of other ETNs in the network. This comparison result is further sent to the network along with the signature of each ETN. The leader then does a statistical analysis of data to ensure that there is not conflict in the block. If the block is free from conflict, then the block is appended in the blockchain network in chronological order. The total time required to reach the consensus is 10 minute, which is independent of the size of nodes in the network [37]. However, if there arises any conflict or any ETN disapproves the block, then leader analyse all results in a comprehensive manner and broadcast the disputed block again to all ETNs for re-auditing. After this, the same process is carried out again, and the results are analysed again for all ETNs along with their ring signatures. This correspondence between ETNs help out to reach the compromised ETN, which is held accountable afterwards.

B. Functioning and Problem Formalization of DEAL

In this section, we propose DEAL mechanism to carry out differentially private δ-revenue maximizing auction operating over decentralized blockchain network for microgrids energy trading. The mechanism is used to determine the winner, winning price, and system utility and revenue. The detailed pseudo code based functioning of DEAL mechanism is presented in Algorithm 1.

1) Preliminaries of DEAL:

a) ***Microgrids****:* Microgrids send their available energy slots, along with its time and available energy to auctioneer. The energy slot vector for i^th slot of total n number of slots is $\mathbf{S_i^n} = \{S_i^n | j \in \mathbb{M}\}$. The aim of every microgrid agent is to maximize its revenue, and in order to increase its revenue, the auctioneer solves a problem based over DEAL auction algorithm. The combined revenue of microgrids is accumulated at the end of auction in order to determine the total revenue generation in the network. The aim of our DEAL mechanism is to enhance the revenue so that more sellers participate in the auction. The problem for revenue calculation sums up all payments (P_i) for m number of buyers, the formula is given as follows:

$$\text{Total Revenue } (R) = \sum_{i}^{m}(P_i) \tag{12}$$

Algorithm 1 Algorithmic Implementation of DEAL

Input: Set of Bidders **N**, buyers bids **V**, set of available energy slots **S**, sensitivity S_p, Laplace privacy budget ε_1, Exponential privacy budget ε_2
Output: Set of Winners $\mathcal{W}$, Differentially private final price Pf

```
    (1) Carrying out VCG Auction
for i ← 1 to $S_{max}$ do
    for j ← 1 to $N_{max}$ do
        Calculate Winner for $i^{th}$ slot according to allocation rule
        $\mathcal{W}_i(b) = \text{argmax}_\upsilon \sum_{j \in N} b_j(\upsilon)$
        // $\mathcal{W}_i(b_j)$ is the winner of slot $S(i)$
    end for
    for k ← 1 to $N_{max}$ do
        Compute VCG payment for $k^{th}$ bidder assigned $i^{th}$ slot
        $\mathcal{VP}_i(k) = \max_\upsilon \sum_{j \neq i} b_j(\upsilon) - \sum_{j \neq i} b_j(\upsilon^*)$
    end for
    Link Winners with their allocated slots and payments in form of a Matrix
    $\mathcal{W}[S_i, \mathcal{VP}_i]$
end for
    (2) Generate Payment Groups using Laplace Differential Privacy
for i ← 1 to $\mathcal{W}_{max}$ do
    Base price = bp ← $\mathcal{VP}_i$
    Bid of winner $i$ = bv ← $V(\mathcal{W}_i)$
    Difference = dv = bv - bp
    Calculate mean ($\mu$) and noise scale ($sc$)
    $\mu = dv/2$
    $sc = \sqrt{\frac{(sd)\varepsilon_1^2}{2N_x}}$
    Generate random Laplacian noise using normal probability distribution
    // Our mechanism will generate random Laplacian noise between [($\mu - sc$) to
    ($\mu + sc$)], here $sc$ depends upon privacy budget $\varepsilon_1$.
    X ← group size
    for j ← 1 to $X$ do
        $\vec{LP}_i(append) = bp + Lap(\mathbb{F}; \mu, sc)$
    end for
    // After this, we get a group of prices of length $X$ for $i^{th}$ winner.
end for
    (3) Computing probability distribution via Exponential DP
for $i$ ← 1 to $LP_{max}$ do
    $q(\vec{LP}, P_s) \leftarrow \vec{LP}(Ps)$
    $\Delta q \leftarrow S_p$
    $P_r(\mathbb{F}(q, LP, P_s) = Ps) \leftarrow$
        $\frac{\exp(\frac{\varepsilon_2 . q(LP, P_s)}{2\Delta q})}{\sum_{P_s' \in LP(P_s)} \exp(\frac{\varepsilon_2 . q(LP, P_s')}{2\Delta q})}$
end for
$P_s \leftarrow \mathbb{F}(q, LP, P_s)$ // Probability distribution
$P_f$ ← final selected price via probability distribution
//$Pf$ is the price $i^{th}$ bidder ($\mathcal{W}_i$) will pay for selected slot.
return $\mathcal{W}, P_f$
```

b) ***Buyers (homes, buildings)****:* Buyers analyse the available energy slots and place their bids for every slot in the form of a bid vector for every buyer. It is a requirement of VCG auction that the buyer has to bid for every available slot, however, if some buyer does not bid for some specific energy slot, then its bid will be counted as zero and that buyer will never be allocated that specific slot, because the utility of buyers always needs to be positive. Individual valuations of i^th buyers in vector form $B_i^n = \{b_i^n \in \mathbb{N}\}$ are sent to auctioneer which further processes these valuations and carry out auction. The aim of buyers is to maximize their utility, for which they have to solve the following problem:

$$\text{Utility } (U_i) = \underset{B_i^n}{\text{argmax}} \ (B_i – \mathcal{P}_i) \tag{13}$$

The above equation computes utility U_i of DEAL mechanism for buyers by subtracting each bid B_i from the payment P_i for that specific buyer. The sum of all utilities of buyers is called as social welfare of the network which is denoted as follows:

$$\text{Social Welfare } (SW) = \sum_{i}^{n} \ (\underset{B_i^n}{\text{argmax}} \ (B_i - \mathcal{P}_i)) \tag{14}$$

c) Auctioneer: Auctioneer is responsible to carry out decentralized differentially private VCG auction along with maximizing the network revenue and social welfare. In our scenario, auctioneer collects the bids and energy information from buyers and sellers respective and determine the winners and winning price. After completion of auction, the auctioneer does solves the problem to calculate total revenue and social welfare of the network. Here, we formed a new variable named as "*Network Benefit* (NB)", which shows the accumulative sum of revenue and social welfare of the network. The aim of auctioneer is to maximize NB, in order to attract more buyers and sellers to participate in the auction. The problem for calculation of NB is given as follows:

$$\text{NB} = \sum_{i}^{m} \ (P_i) \ + \ \sum_{i}^{n} \ (\underset{B_i^n}{\text{argmax}} \ (B_i - \mathcal{P}_i)) \tag{15}$$

Eq. 15 computes network benefit by adding payment received by seller $(\sum_i^m \ (P_i))$ and utility of buyers $(\sum_i^n \ (\text{argmax}_{B_i^n} \ (B_i - \mathcal{P}_i)))$ which is also given in Eq. 14.

2) Problem Formalization: In DEAL strategy, homes or building who require energy act as buying entities, and the microgrid smart homes act as selling entities. Sellers will submit their available energy and time slots to auctioneer, which is advertised afterwards, and the buyers will submit their bids after viewing the advertised energy slots. After successful collection of bids, the auctioneer will carry out auction using the allocation and payment rule provided in Section 2. In further equations, "i" will denote the buyer number ($i \in n$) and "j" ($j \in m$) will denote the seller. In order to proceed further, we assume that there are "n" number of buyers ($i = \{1, 2, 3...n\}$) and "m" ($j = \{1, 2, 3...m\}$) number of sellers in the blockchain environment. Since we want everyone to participate in the auction, we make an assumption that microgrid sellers will always provide the energy cheaper than the actual energy grid which is controlled by government. Furthermore, we assume that the number of buyers is always greater than or at least equal to number of sellers ($n \geq m$). We further divided the energy trading into slots, which demonstrates the exact time period at which the supply of energy will be available, we denoted it with T ($T = \{1, 2.3...t\}$). The slots can be decided by the mutual agreement, for example there may be 24 hourly slots in a day, or 12 slots of 2 hours, etc. Once the allocation and VCG payment is calculated, the auctioneer further proceeds to make the payments differentially private by using the revenue maximizing DEAL algorithm proposed in this paper. Finally, a matrix *WM* is formed which will indicate the buyer id, allocated slot number, seller of slot, and the payment decided for that slot. The matrix will look as follows:

$$WM = \begin{bmatrix} b_i & t_i & s_i & p_i \\ \vdots & \vdots & \vdots & \vdots \\ b_n & t_i & s_i & p_i \end{bmatrix} \tag{16}$$

3) Differentially Private Pricing Strategy: One of the major purpose of DEAL strategy is to optimize revenue of VCG mechanism while preserving the bids privacy. It is because in VCG mechanism, is one gets to know about the actual price that a buyer is paying, and the adversary has a complete record of prices from some previous auctions, it can easily infer the private information of specific buyers, such as their private valuations for a specific energy slot, valuations for specific time, etc. Therefore, to preserve bid privacy, we use the concept of differential privacy in decentralized auctions scenario. In this section, we start the discussion from part (2) of Algorithm 1. We assume that auctioneer has calculated VCG payments and has decided the winners of specific slots and only the calculation of final price is left II-A. We use dual differential privacy mechanism, in which we use both Laplacian mechanism and Exponential mechanism to make our pricing strategy more private. At first, the Laplacian mechanism collects data from step (1) and calculates mean and noise scale (sc) on the basic of VCG price (also called as base price). The intensity of noise scale is controlled by the privacy parameter ε_1 which in turn controls the amount of noise generated by Laplacian mechanism. The formulas used are as follows [1]:

$$\mu = dv/2 \tag{17}$$

$$sc = \sqrt{\frac{(sd)_{\varepsilon}{}_{1}^{2}}{2N_x}} \tag{18}$$

After calculation of mean and noise scale, Laplacian mechanism is used to generate a group of number in accordance with noise scale and mean value. As discussed earlier, ε_1 controls the intensity of noise, and it can be varied to increase or decrease the level required privacy. In this experiment, we use $\varepsilon_1 = 1$, but this can be changed depending up the demand and need of application. Afterwards, Laplace mechanism generates a random number using the basic differentially private Laplacian mechanism, which is given as follows:

$$f\left(x; \mu, \sqrt{\frac{(sd)_{\varepsilon}{}_{1}^{2}}{2N_x}}\right) = \frac{1}{2\sqrt{\frac{(sd)_{\varepsilon}{}_{1}^{2}}{2N_x}}} . e^{\left(-\frac{|x-\mu|}{\sqrt{\frac{(sd)_{\varepsilon}{}_{1}^{2}}{2N_x}}}\right)} \tag{19}$$

In above equation, we take $N_x = 1$ for single sample and it can be varied according to sample size. Similarly, the value of x is generated using the random Laplace mechanism of simulation environment. After simplification, the above equation can be re-written for noise calculation as

$$\underset{t}{noise} = \frac{1}{(\sqrt{2})(sd)_{\varepsilon 1}} . e^{\left(-\frac{\sqrt{2}|x|}{\sqrt{(sd)_{\varepsilon}{}_{1}^{2}}}\right)} \tag{20}$$

Once, the group is generated, we further generate the final output group to be fed into exponential mechanism. The final noise array is generated by appending all values and adding the base price value to them individually using the following formula.

$$\vec{LP}_i(append) = bp + Lap(\mathbb{F}; \mu, sd) \tag{21}$$

Here, our section (2) of algorithm completes up and the output result is fed to section (3), in which Exponential mechanism is used to decide the differentially private price of energy slot. In this part of algorithm, the group size of calculated Laplacian price is used to determine the size of probability distribution of Exponential mechanism. Two privacy controlling parameters are used in exponential mechanism, one is Δq (also known as sensitivity), and second is ε_2 (also called as privacy budget). It is worth to remind that in Laplacian mechanism, we used privacy budget value as 1 ($varepsilon_1 = 1$). However, in Exponential mechanism, we will vary the privacy budget according to the experimental setup. Similarly, the value of Δq also depends upon the requirement of privacy and it can vary accordingly. Different researchers calculate *sensitivity* via different methods, so it depends upon the discretion of the researcher implementing it up. An important function of Exponential mechanism is "$scorefunction[q(\vec{LP}, P_s)]$". The score function explains that how good is the output P_s is for the given dataset LP. Similarly, the choice of a good score function also depends upon the requirement of application, in our mechanism, we use formal Exponential score function in order to carry out optimal price selection using differential privacy mechanism. After getting Laplacian price group, Exponential mechanism generate a probability distribution of the group prices using the mechanism as follows [38]:

$$P_r(\mathbb{F}(M) = Ps) \propto \frac{\exp(\frac{\varepsilon_2 . q(LP, P_s)}{2\Delta q})}{\sum_{P_s' \in LP(P_s)} \exp(\frac{\varepsilon_2 . q(LP, P_s')}{2\Delta q})} \quad (22)$$

In above equation, $M = (q, LP, P_s)$.
After generating Exponential probability distribution, a temporary price is selected using the random mechanism, which is further checked for all the constraints such as the selected price should provide non-negative utility, positive revenue, etc. If the selected price fulfils all the requirements, then the price is finalized and is considered to be selling price (P_f) that i^{th} buyer has to pay for selected slot. As true valuation of bidder is the base price which is used to determine this differentially private price, so our proposed strategy guarantees that price selection is completely random. This randomness ensures that no adversary can get to know the original valuation of buyer/bidder. Therefore, DEAL mechanism provides 100% privacy guarantee to participating bidders.

***Theorem** 1: (DEAL satisfies ε-differential privacy)*
For any two set of bidders valuations $B = (b_1, b_2, ...b_n)$ and $B' = (b_1, b_2, ...b_n)$ having a difference of only one valuation. The output probability distribution of DEAL mechanism determined using Eq. 22 ($\varepsilon_2 = \varepsilon$). So, in accordance with the differential privacy definition, for a similar output x, we get the following result [38].

$$\frac{P_r[DEAL(B) = x]}{P_r[DEAL(B') = x]} = \frac{\frac{\exp(\frac{\varepsilon . q(B, x)}{2\Delta q})}{\sum_{i \in N} \exp(\frac{\varepsilon . q(B, x)}{2\Delta q})}}{\frac{\exp(\frac{\varepsilon . q(B', x)}{2\Delta q})}{\sum_{i \in N} \exp(\frac{\varepsilon . q(B', x)}{2\Delta q})}} \leq \exp(\varepsilon) \quad (23)$$

According to proof of differential privacy in [39], the equation 23 satisfies ε-differential privacy, as if the input is data varied by only one element, then the output varies no more than $\exp(\varepsilon)$. This can formally be written as:

$$P_r[DEAL(B) = x] \leq P_r[DEAL(B') = x]. \exp(\varepsilon) \quad (24)$$

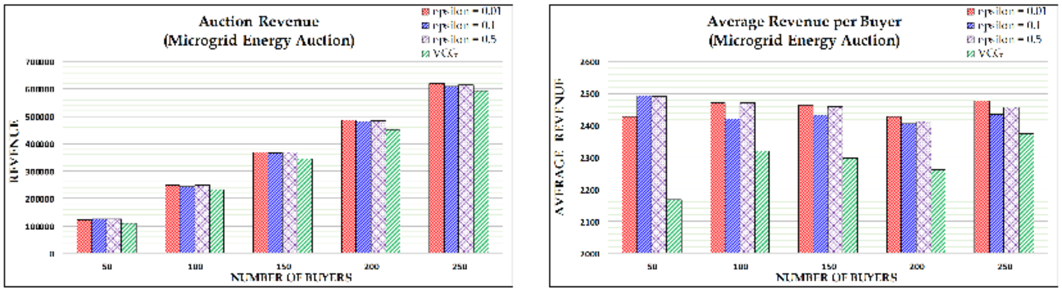
Keeping in view all above discussion, we can conclude that our proposed DEAL mechanism satisfies ε-differential privacy condition.

V. Performance Evaluation

In order to evaluate the performance of DEAL, we consider three parameters named as revenue (R), buyers utility (BU), and network benefit (NB). We compare our results with VCG auction used by the authors in [11]. In order to carry out experiments, we use Pandas v0.24 and NumPy v1.14 libraries over Python 3.0 and iterated our auction for 50, 100, 150, 200, and 250 buyers. In every auction simulation, we took the data set of n buyers and n-1 sellers. We generate output results by dealing with five different parameters named as revenue, utility, NB, average utility per buyer, and average revenue per seller. Furthermore, one of the most important factor in differentially private preservation strategy is the change in output by varying value of ε, which is ε_2 in our case for exponential privacy preservation according to Algorithm 1. In our experiments, we conducted auction by varying ε_2 at three different privacy levels such as 0.01, 0.1, and 0.5. Furthermore, we assumed that the sellers will always sell their electricity in a price less than the energy price from smart grid. This further leads to two important points, (i) if the price of energy is greater than the price of smart grid energy, then there is no reason left for buyers to participate in auction as they can simply purchase the energy at lower cost directly from grid station. (ii) hence, buyers are getting energy at low cost as compared to price of grid station, so the major objective is to encourage more and more microgrid sellers to participate and this can only be done by maximizing their revenue. The detailed description of auction, it's functioning, and privacy preservation according to selected parameters is given below in this section.

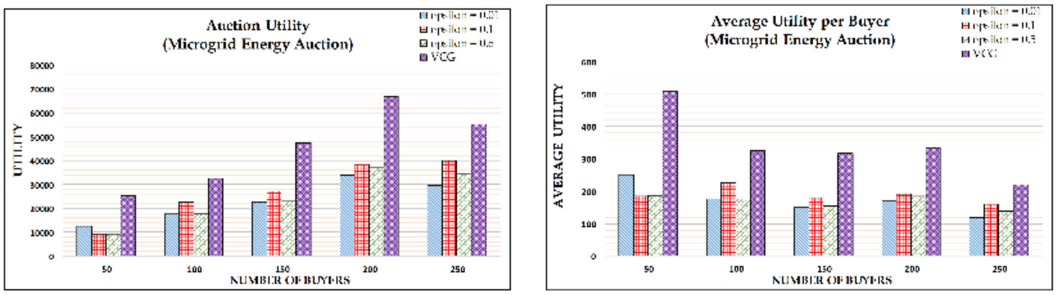
A. Differentially Private Revenue Maximization

During decentralized energy trading, maximizing revenue is the most important objective. Revenue is termed as the total amount of cash collected. In our scenario, the total amount that a seller gets after completion of auction is the revenue of that seller, and the accumulated sum of all revenues is the total revenue of our system. Furthermore, we evaluated average seller revenue, which is a ratio that demonstrates the average revenue a seller will generate if he/she participates in the auction mechanism. In order to maximize revenue, we modified the payment rule of VCG mechanism and ensured that our differentially private auction generates more revenue as compared to VCG mechanism. The graphical illustration of outcomes of DEAL auction in comparison with VCG auction is presented in Fig. 3. In Fig. 3a, the graph demonstrates revenues of DEAL strategy in comparison with VCG auction. We categorized graph in two way, first one is the change of revenue with respect to privacy parameter ϵ and the second one



(a) (b)

Fig. 3: Revenue evaluation on the basis of DEAL mechanism and VCG auction mechanism
(a) Accumulative Revenue of Network (b) Average Revenue per Buyer



(a) (b)

Fig. 4: Utility evaluation of buyers on the basis of DEAL mechanism and VCG auction mechanism
(a) Accumulative Utility of Network (b) Average Utility per Buyer

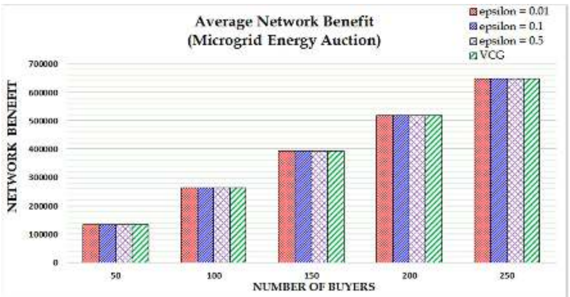


Fig. 5: Network benefit of participating agents according to DEAL and VCG mechanism

is the change in revenue by varying number of buyers/bidders. From ε point of view, a slight increase in the revenue can be observed when value of ε is varied from 0.01 to 0.1. However, the value of utility does not really change when this value is raised to 0.5. Since, lower value of epsilon (such as 0.01) is demanded, therefore it can be said that there is a slight decrease in revenue with the decrease in privacy level. However, if we compare these values with VCG auction revenue, we can see a clear difference that DEAL auction strategy outperforms VCG auction mechanism, because of modifications made in the payment rule. Similarly, from the point of view of number of buyers, it can be observed that the revenue increases with the increase in buyers, this is because the number of sales also increase with the number of bidders. However, the clear difference between revenues of DEAL and VCG can be observed even with the increase in number of buyers. Another important parameter that is normally used to determine the efficiency of an auction mechanism is the average revenue per seller. We calculate average revenue for all our scenarios and presented its graphical illustration in Fig. 3b. From the figure, it can be observed that revenue of DEAL mechanism always outclasses the revenue of VCG auction. *Keeping of view all the discussion, we can conclude that DEAL maximized revenue of VCG mechanism along with preserving the privacy of bidders.*

B. Buyers Utility

Enhancing utility of buyers and having non-zero utility is also an important objective of any auction mechanism. In DEAL mechanism, we ensured that no should have negative utility and the level of satisfaction or social welfare is always positive. Similarly, in our scenario, revenue and utility are linked with each other as revenue is the degree of happiness of sellers and utility is the degree of satisfaction of buyers. So, there is always a trade-off between both of them. However, we tried to enhance the revenue of buyers along with not decreasing utility to a larger extent. The payment values are selected using differential privacy Laplacian and Exponential distribution, and thus, this payment ensured that the revenue always gets maximized, therefore the slight decrease in utility can be observed in our simulation results as compared to VCG

mechanism. The detailed graphs showing the auction utility is given in Fig. 4.
Graph in Fig. 4a demonstrate the trend of utility with respect to variation in privacy parameter (ε) and number of buyers. It can be observed that utility value increases with the increase in number of buyers, because it is the accumulative sum of all utilities. However, the privacy parameter has varied effect over utility values. For example, the value of utility with 100 buyers is maximum with ε = 0.1, same goes with other presented graphs as well. This is because the trade-off between revenue and utility supports the utility maximization at ε = 0.1. However, from the presented graphs, we can visualize that if we decrease the value of ε, we will increase the level of privacy, but utility will decrease. Similarly, in Fig. 4b, the average utility per buyers also demonstrates the similar output and ensures that the level of social welfare of buyers is always satisfactory. This utility is actually the buyers' utility also named as social welfare, so it should not be mixed with the usefulness (utility) of data which is usually referred in differential privacy papers. In DEAL, the utility reflects the level of satisfaction of buyers according to their valuation and payment, and it should not be mixed with the privacy value or data usefulness. *By viewing all graphs, it can easily be concluded that DEAL provides satisfactory utility ratio for all its bidders and encourages bidders to participate in auction because of non-negative utility.*

C. Network Benefit

We introduced a new parameter named as network benefit. The value of network benefits is the sum of total revenue and utility of the network in that particular scenario. We calculated the network benefit of VCG and DEAL auctions for different buyers and different privacy preservation scenarios. The graph showing the comparison of network benefit is provided in Fig. 5. It can be seen from the graph that the value of network benefits is exactly the same for both DEAL and VCG auction. This shows that the overall performance of DEAL is equal to optimal VCG mechanism. Though, the trade-off between revenue and utility is adjusted because of the requirement of maximizing of revenue. Besides, DEAL mechanism also ensures bid privacy by using modern differentially private privacy preservation. However, basic VCG mechanism in the presented paper do not ensures the privacy of bids and any adversary can infer private information of buyers by analysing winning price and comparing it with previous data. Furthermore, DEAL also provides decentralized energy trading that ensures the security and transparency in auction mechanism, which further increases the trust of participating agents. *By analysing all graphical values from perspective of participants, it can be concluded that DEAL outperforms VCG mechanism by maximizing auction revenue along with enhancing utility and overall network benefit.*

D. Privacy Analysis

Final price in DEAL mechanism is picked by dual differential privacy mechanism; first random string is generated using Laplace differential privacy and afterwards, exponential privacy protection mechanism is used to pick a completely random price according to chose distribution. In order to carry out privacy analysis, we thoroughly compared randomly picked price with theoretic bounds of differential privacy presented in Theorem 1 and Definition 2. *After careful analysis, we can say that our proposed DEAL mechanism fulfils all theoretical implications of differential privacy and is one of the most suitable mechanism to preserve bidding privacy for microgrids auction.*

VI. Conclusion

Microgrids are capable of generating, storing, and distributing energy to the network in the time of need using solar, wind and similar renewable energy resources. Usually microgrids produce more than the required amount of energy and trade the surplus energy in order to generate some profit. This trading works in accordance with the rules provided by governing authorities. The trading is not completely secure and private; therefore, researchers are working over formulation of latest technologies to make it more efficient. Nowadays, modern trading technologies do also discuss the use of blockchain in trading due to its decentralized, timestamped, transparent, and immutable nature. However, blockchain in not an all one solution to all auction/trading problems as it can easily cause leakage of because of its transparent nature. In this paper, we propose a decentralized auction strategy for microgrid energy trading and preserved bid privacy by using differential privacy protection operating over consortium blockchain technology. To be more precise, we develop **D**ifferentially private **E**nergy **A**uction for b**L**ockchain-based microgrid systems (DEAL) mechanism, which preserves the privacy of participants of auction by effectively preserving the data using Laplacian and Exponential privacy protection. We further evaluated DEAL in different auction scenarios and compared it with optimal VCG auction mechanism. The results from experimental evaluations show that DEAL outperforms VCG mechanism by providing maximizing revenue and enhancing utility and network benefit to a satisfactory level. As a plan of our future work, we intend to develop a prototype of decentralized private auction with the help of DApp platform and smart contract.

References

[1] M. U. Hassan, M. H. Rehmani, R. Kotagiri, J. Zhang, and J. Chen, "Differential privacy for renewable energy resources based smart metering," *Journal of Parallel and Distributed Computing*, vol. 131, pp. 69–80, 2019.

[2] M. H. Rehmani, M. Reisslein, A. Rachedi, M. Erol-Kantarci, and M. Radenkovic, "Integrating renewable energy resources into the smart grid: Recent developments in information and communication technologies," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 7, pp. 2814–2825, July 2018.

[3] X. Wang, L. Huang, H. Xu, and H. Huang, "Social welfare maximization auction for secondary spectrum markets: A long-term perspective," in *13th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, 2016, pp. 1–9.

[4] C. Zhihua, W. Yechuang, C. Xingjuan *et al.*, "A pigeon-inspired optimization algorithm for many-objective optimization problems," *SCIENCE CHINA Information Sciences*, 2019. [Online]. Available: https://doi.org/10.1007/s11432-018-9729-5

[5] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, "The blockchain as a decentralized security framework [future directions]," *IEEE Consumer Electronics Magazine*, vol. 7, no. 2, pp. 18–21, 2018.

[6] D. Puthal, S. P. Mohanty, P. Nanda, E. Kougianos, and G. Das, "Proof-of-authentication for scalable blockchain in resource-constrained distributed systems," in *IEEE International Conference on Consumer Electronics (ICCE)*, 2019, pp. 1–5.

[7] H. Jin, L. Su, B. Ding, K. Nahrstedt, and N. Borisov, "Enabling privacy-preserving incentives for mobile crowd sensing systems," in *IEEE 36th International Conference on Distributed Computing Systems (ICDCS)*, 2016, pp. 344–353.

[8] X. Cai, Y. Niu, S. Geng, J. Zhang, Z. Cui, J. Li, and J. Chen, "An under-sampled software defect prediction method based on hybrid multi-objective cuckoo search," *Concurrency and Computation Practice and Experience*, 2018. [Online]. Available: https://doi.org/10.1002/cpe.5478

[9] Y. Li, H. Yu, B. Song, and J. Chen, "Image encryption based on a single-round dictionary and chaotic sequences in cloud computing," *Concurrency and Computation: Practice and Experience*, p. 5182, 2019. [Online]. Available: https://doi.org/110.1002/cpe.5182

[10] Z. Cui, Y. Cao, X. Cai, J. Cai, and J. Chen, "Optimal leach protocol with modified bat algorithm for big data sensing systems in internet of things," *Journal of Parallel and Distributed Computing*, vol. 132, pp. 217–229, 2019. [Online]. Available: https://doi.org/10.1016/j.jpdc.2017.12.014

[11] W. Zhong, K. Xie, Y. Liu, C. Yang, and S. Xie, "Auction Mechanisms for Energy Trading in Multi-Energy Systems," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 4, pp. 1511–1521, April 2018.

[12] J. Wang and S. S. Chow, "Secure strategyproof ascending-price spectrum auction," in *IEEE Symposium on Privacy-Aware Computing (PAC)*, 2017, pp. 96–106.

[13] C.-C. Chang and Y.-F. Chang, "Efficient anonymous auction protocols with freewheeling bids," *Computers & Security*, vol. 22, no. 8, pp. 728–734, 2003.

[14] H. R. Varian and C. Harris, "The vcg auction in theory and practice," *American Economic Review*, vol. 104, no. 5, pp. 442–45, 2014.

[15] R. Zhu, Z. Li, F. Wu, K. Shin, and G. Chen, "Differentially private spectrum auction with approximate revenue maximization," in *Proceedings of the 15th ACM international symposium on mobile ad hoc networking and computing*, 2014, pp. 185–194.

[16] M. U. Hassan, M. H. Rehmani, and J. Chen, "Differential Privacy Techniques for Cyber Physical Systems: A Survey," *IEEE Communication Surveys and Tutorial (Submitted).*, 2019.

[17] ——, "Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions," *Future Generation Computer Systems*, vol. 97, pp. 512–529, 2019.

[18] J. D. Hartline and T. Roughgarden, "Simple versus optimal mechanisms," in *Proceedings of the 10th ACM conference on Electronic commerce*, 2009, pp. 225–234.

[19] Q. Wu, M. Zhou, Q. Zhu, and Y. Xia, "VCG auction-based dynamic pricing for multigranularity service composition," *IEEE Transactions on Automation Science and Engineering*, vol. 15, no. 2, pp. 796–805, 2018.

[20] Y. Zhang, C. Lee, D. Niyato, and P. Wang, "Auction approaches for resource allocation in wireless systems: A survey," *IEEE Communications surveys & tutorials*, vol. 15, no. 3, pp. 1020–1041, 2013.

[21] A. Roth, "Algorithmic Game Theory," Lectures, 2017, uRL: https://www.cis.upenn.edu/aaroth/courses/agtS17.html.

[22] C. Dwork, "Differential privacy," in *Automata, Languages and Programming*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 1–12.

[23] P. Wang, J. Huang, Z. Cui, L. Xie, and J. Chen, "A gaussian error correction multi-objective positioning model with nsga-ii," *Concurrency and Computation: Practice and Experience*, p. e5464, 2019. [Online]. Available: https://doi.org/10.1002/cpe.5464

[24] A. Beimel, K. Nissim, and U. Stemmer, "Private learning and sanitization: pure vs. approximate differential privacy," in *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*. Springer, 2013, pp. 363–378.

[25] A. Haeberlen, B. C. Pierce, and A. Narayan, "Differential privacy under fire." in *USENIX Security Symposium*, 2011.

[26] T. Zhu, G. Li, W. Zhou, and P. S. Yu, *Preliminary of Differential Privacy*. Cham: Springer International Publishing, 2017, pp. 7–16.

[27] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *[Online] http://bitcoin.org/bitcoin.pdf*, 2008.

[28] W. Chen, Z. Zhang, Z. Hong, C. Chen, J. Wu, S. Maharjan, Z. Zheng, and Y. Zhang, "Cooperative and distributed computation offloading for blockchain-empowered industrial internet of things," *IEEE Internet of Things Journal, in Press*, 2019.

[29] D. Puthal and S. P. Mohanty, "Proof of authentication: IoT-friendly blockchains," *IEEE Potentials*, vol. 38, no. 1, pp. 26–29, 2018.

[30] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, "Everything you wanted to know about the blockchain: Its promise, components, processes, and problems," *IEEE Consumer Electronics Magazine*, vol. 7, no. 4, pp. 6–14, 2018.

[31] W. Wang, D. T. Hoang, Z. Xiong, D. Niyato, P. Wang, P. Hu, and Y. Wen, "A survey on consensus mechanisms and mining management in blockchain networks," *arXiv preprint arXiv:1805.02707*, 2018.

[32] Y. Yahiatene, A. Rachedi, M. A. Riahla, D. E. Menacer, and F. Nait-Abdesselam, "A blockchain-based framework to secure vehicular social networks," *Transactions on Emerging Telecommunications Technologies*, vol. 30, no. 8, p. e3650, 2019, e3650 ett.3650. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.3650

[33] J. Garay, A. Kiayias, and N. Leonardos, "The bitcoin backbone protocol: Analysis and applications," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2015, pp. 281–310.

[34] Z. Li, Z. Yang, and S. Xie, "Computing resource trading for edge-cloud-assisted internet of things," *IEEE Transactions on Industrial Informatics, in Press*, 2019.

[35] 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.

[36] I. Alqassem and D. Svetinovic, "Towards reference architecture for cryptocurrencies: Bitcoin architectural analysis," in *IEEE International Conference on Internet of Things (iThings), and Green Computing and Communications (GreenCom), IEEE and Cyber, Physical and Social Computing (CPSCom)*, 2014, pp. 436–443.

[37] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, "A secure sharding protocol for open blockchains," in *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, 2016, pp. 17–30.

[38] C. Dwork, A. Roth *et al.*, "The algorithmic foundations of differential privacy," *Foundations and Trends® in Theoretical Computer Science*, vol. 9, no. 3–4, pp. 211–407, 2014.

[39] F. McSherry and K. Talwar, "Mechanism design via differential privacy," in *48th Annual IEEE Symposium on Foundations of Computer Science, FOCS'07.*, 2007, pp. 94–103.

Muneeb Ul Hassan received his Bachelor degree in Electrical Engineering from COMSATS Institute of Information Technology, Wah Cantt, Pakistan, in 2017. He received Gold Medal in Bachelor degree for being topper of Electrical Engineering Department. Currently, he is pursuing the Ph.D. degree from Swinburne University of Technology, Hawthorn VIC 3122, Australia. His research interests include privacy preservation, blockchain, game theory, and smart grid.

Mubashir Husain Rehmani (M'14-SM'15) received the B.Eng. degree in computer systems engineering from Mehran University of Engineering and Technology, Jamshoro, Pakistan, in 2004, the M.S. degree from the University of Paris XI, Paris, France, in 2008, and the Ph.D. degree from the University Pierre and Marie Curie, Paris, in 2011. He is currently working as Assistant Lecturer at Cork Institute of Technology (CIT), Ireland. He worked at Telecommunications Software and Systems Group (TSSG), Waterford Institute of Technology (WIT), Waterford, Ireland as Post-Doctoral researcher from Sep 2017 to Oct 2018. He served for five years as an Assistant Professor at COMSATS Institute of Information Technology, Wah Cantt., Pakistan. He is currently an Area Editor of the IEEE Communications Surveys and Tutorials. He served for three years (from 2015 to 2017) as an Associate Editor of the IEEE Communications Surveys and Tutorials.

Dr. Jinjun Chen is a Professor from Swinburne University of Technology, Australia. He is Deputy Director of Swinburne Data Science Research Institute. He holds a PhD in Information Technology from Swinburne University of Technology, Australia. His research interests include scalability, big data, data science, data systems, cloud computing, data privacy and security, health data analytics and related various research topics. His research results have been published in more than 160 papers in international journals and conferences, including various IEEE/ACM Transactions.