Privacy-Preserving Energy Trade using Double Auction in Blockchain Offline Channels

Subhasis Thakur[1[0000−0001−6579−724X]], John Breslin[1[0000−0001−5790−050X]], and Sweta Malik[1]

National University of Ireland, Galway, Ireland
{subhasis.thakur, john.breslin, M.SWETA1}@nuigalway.ie

Abstract. Blockchain is a promising tool to implement peer-to-peer energy trade algorithms because it lowers the cost of electricity by eliminating 3rd parties such as the utility companies from energy trade and by creating a secure trade platform. However, the state of the art blockchain-based peer to peer energy trade solutions have privacy and scalability problems. In this paper, we proposed a novel method to execute double auction-based peer to peer energy trade in blockchain offline channels to enhance security, privacy and scalability of peer to peer energy trade. We prove that the proposed decentralised double auction is secure, privacy-preserving and more efficient as McAfee's double auction.

Keywords: Peer to peer energy trade · Blockchains · Blockchain Offline Channels · Bitcoin Lightning network · Double Auction

1 Introduction

Blockchains are recently used to implement peer to peer energy trade algorithms. Blockchain can reduce the cost of electricity by removing utility companies from the local electricity trade. Also, it provides a secure trade platform where parties who do not trust each other can trade electricity. There are many game-theoretic formulations of electricity trade, such as trade models based on cooperative games[10], non-cooperative games, and auctions[12]. Double auction is a popular trade model that allows the sellers and the buyers to choose their desired cost and price for electricity trade. McAfee's double auction[6] is widely used in the energy trade. In this trade model, the seller sets its asking price (minimum price at which it will sell), and the buyer sets its reservation price (maximum price that it will pay). The auction mechanism finds a price that satisfies both the seller and the buyer. The auction mechanism also needs to satisfy few economic properties such as individual rationality, budget-balancing, truth-fullness, and economic efficiency. McAfee's double auction is known to be individually rational and truthful. But it is not budget-balanced and economically efficient.

Double auction-based electricity trade algorithms implement with blockchains [12] have privacy and scalability problems. In such an auction procedure, the prosumers (who may produce and consume electricity) have to inform the auctioneer about its asking price and reservation price. It may reveal private information about the prosumers. For example, if a prosumer wants to sell electricity from 6 PM to 8 PM then, it may indicate that the prosumer may not be in his/her house during this time. Besides the physical security problem from such information, an adversary may use such information to alter electricity prices. For example, if the adversary is a utility company and it finds that its several customers who want to use electricity from peer to peer energy trade for a specific time during a day, i.e., they will not buy electricity from the grid at the price offered by the utility company at these times, then the adversary may alter price of electricity from the grid to make peer to peer energy trade economically insignificant. Hence, in this privacy-preservation problem, an adversary is the entity who wants to reveal such trade patterns of the prosumers. An adversary may control (via cyberattack) a centralised auctioneer to execute such a privacy disruption attack.

Additionally, the current blockchain implementation of double auction-based energy trade may have a scalability problem. Public blockchains have scalability problems. There are double auction-based energy trade solutions that use public blockchains. Scalability problems may prevent real-time execution of energy trade operations. For example, in the Bitcoin network it may take 10 minutes to find a new block, this means it may take up to 10 minutes to record a transaction in the blockchain. However, electricity trade windows may be as short as 5 minutes. Thus short trade operations may not be executed via public blockchains.

Further, the short window electricity trade has a very low monetary value. If blockchain transactions are created for such trade decisions, transaction fees may be too low to attract miners. Increasing the fees may increase the price for electricity in peer to peer energy trade and may defeat the purpose of the local electricity trade.

Also, blockchains (public blockchains) have a high environmental impact. It is estimated that Bitcoin has annual electricity consumption adds up to 45.8 TWh and produces 36.95 megatons of CO_2 annually. Thus the creation of blockchain transactions may increase the carbon footprint of the blockchain-based electricity trade. Hence environment-friendly energy trade should minimise the number of transactions to be created to execute the trade operation.

In this paper, we mitigate these problems with public blockchain-based electricity trade using double auction. We proposed to use blockchain-offline channels to execute the double auction procedure. Offline channels allow secure transactions without immediately updating the blockchains. It significantly reduces the number of transactions needed to execute energy trade operations. Our main contributions are as follows: (1) We present a double auction-based energy trade algorithm using offline channels. (2) We prove that the proposed auction mechanism is privacy-preserving. (3) We prove that the proposed double auction is secure as it prevents double spending of units of electricity to be sold. (3) We show that the proposed double auction is more efficient than McAfee's double auction[6].

The paper is organised as follows: in section 2 we discuss related literature, in section 3 we define the auction problem, in section 4 we discuss the offline channel-based double auction for energy trade, in section 5 we discuss economic properties of the auction, in section 6 we present experimental evaluation on efficiency of the proposed energy trade, and we conclude the paper in section 7.

2 Related Literature

Blockchains are recently used to implement trade algorithms for peer to peer energy trade. In [10] authors have used coalitional game theory in peer to peer energy trade which also includes electric vehicles. In [11, 14] the authors used coalitional game theory to model blockchain-based energy trade. Double auction is a popular trade mechanism for peer to peer energy trade. In [12] the authors used double auction for peer to peer energy trade using blockchains. In [2] the authors used continuous double auction for peer to peer energy trade. In this paper, we investigated double auction-based energy trade. The Bitcoin lightning network was proposed in [8] which allows peers to create and transfer funds among them without frequently updating the blockchain. Similar networks are proposed for Ethereum [1] and credit networks [4]. Blockchain is a suitable platform for peer to peer energy trade. In [3] authors have analysed the suitability of blockchain network in terms of network size, communication delay, etc on recording transactions for the energy trade. In [13], the authors used blockchain offline channels to implement a cooperative game-based peer to peer energy trade.

In this paper we used proof of work-based blockchains. Proof of work-based blockchains was proposed in [7]. There are several variations of blockchains in terms of consensus protocols. Offline channels for Bitcoin, i.e., Bitcoin Lightning network was proposed in [8] which allows peers to create and transfer funds among them without frequently updating the blockchain. Similar networks were proposed for Ethereum [1] and credit networks [5]. [5, 9] proposed a landmark-based routing protocol for fund transfer in a credit network. We advance the state of the art in double auction-based energy trade as follows: (1) We proposed a privacy-preserving double auction which prevents an adversary from identifying the trading parties. (2) We proposed to use blockchain offline channels which allows us to build a high scale double auction protocol.

3 Energy trade problem

A double auction for peer to peer energy trade can be described as follows:

Definition 1. *The double auction for the trade window t_i to t_{i+1} is as follows:*

- *A be a distinguished entity acting as the auctioneer. All prosumers know A and have a secure communication method with A.*
- *Asking prices: $\{P^x_{i-\epsilon}\}$ be the set of asking prices of the sellers received by the auctioneer A at most ϵ time before time instance t_i and not after t_i. $\{p^x_{i-\epsilon}\}$ be amount of electricity a prosumer wants to sell for the time duration t_i to t_{i+1}.*

Table 1: Notations used to model the energy trade problem.

$\{p_i\}$	A set of n prosumers(who may buy and (or) sell electricity from each other.) A prosumer may be a house with renewable energy generator such as asolar panel.
$\{t_i\}$	discrete time instances dt time apart.
D_i^j and S_i^j	Energy demand and energy supply (through its own energy generators, i.e., solar panels) of the prosumer p_i at time t_j until time t_{j+1} or for time duration dt. The energy requirement at p_i at time t_j is $E_i^j = D_i^j - S_i^j$. A positive value of E_i^j means prosumer p_i has surplus energy (i.e., it is generating more than its own consumption) and a negative value of E_i^j will mean the prosumer has an energy deficiency for next dt time duration.
$d^{i,j}$	the distance between prosumer p_i and p_j w.r.t the distribution lines.

- *Bids:* $\{Q^x_{i-\epsilon}\}$ *be the set of bids of the sellers received by the auctioneer* A *at most* ϵ *time before time instance* t_i *and not after* t_i. $\{q^x_{i-\epsilon}\}$ *be amount of electricity a prosumer wants to buy for the time duration* t_i *to* t_{i+1}.
- *Outcomes: A set of messages to the prosumers* (W_i^x, C_i^x) *such that* W_i^x *is the amount of electricity* x *will buy or sell (i.e., they will be paid or receive fund for only this amount of electricity) at the price or cost* C_i^x. W_i^x *is positive means* p_x *will sell* W_i^x *electricity (in kWh) and it will receive fund* C_i^x *per unit of electricity (kWh).* W_i^x *is negative means* p_x *will buy* W_i^x *electricity (in kWh) and it will lose fund* C_i^x *per unit of electricity (kWh).*

The economic characterisation of a double auction are as follows:

- Individual rationality: No prosumer should pay more than its bid, no prosumer should get less than its asking price, no prosumer will trade without participating in the auction.
- Balanced Budget: The auctioneer A will collect fund from prosumers who wants to buy and it will pay the prosumers who wants to sell. Using the outcome (W_i^x, C_i^x), we can calculate the fund at the auctioneer as $B^i = \sum_{x \in n: W_i^x > 0} W_i^x \times C_i^x + \sum_{x \in n: W_i^x < 0} W_i^x \times C_i^x$. We will say the double auction is strong budget-balanced if $B^i = 0$ and we will say the double auction weak budget-balanced if $B^i > 0$.
- Truthfulness: We will say a double auction is Nash equilibrium incentive compatible if it is a Nash equilibrium for the prosumers to report true bid or asking price.
- Economic efficiency: We will define economic efficiency in terms of amount of electricity can be traded using the auction. It can be defined as:

$$EE^i = (\sum_{x \in N} p_i^x - \sum_{x \in N: W_i^x > 0} W_i^x) \qquad + (\sum_{x \in N} q_i^x + \sum_{x \in N: W_i^x < 0} W_i^x) \tag{1}$$

EE^i is the amount summation of the electricity which could not be sold by the auction and the amount of electricity that can not be bought from the double auction.

Further, we can characterise the double auction with privacy-preservation properties. An adversary in a double auction wants to know the asking price, bids, and outcome of a double auction. We assume that the adversary can control a fraction of nodes of the blockchain network which is computing the double auction procedure.

4 Energy Trade with Decentralised Double Auction

Briefly, the auction procedure is as follows: (1) There are two types of nodes in the offline channel network, one is the set prosumers, and another is the set of nodes controlled by the DSOs (any of these nodes can be the auctioneer). (2) Each prosumer randomly chooses an auctioneer node to buy or sell electricity on its behalf. (3) The chosen auctioneer can either find a matching prosumer who also wants to buy or sell via it. If there is no such prosumer, then another auctioneer may buy or sell electricity from it. (4) We designed a protocol that allows each auctioneer to buy electricity from other prosumers with the assurance that if it cannot sell the electricity then it can sell it to either another auctioneer or the first prosumer.

4.1 Unidirectional Offline Channel

Blockchain offline channels [8] uses multi-signature addresses to open an offline channel among peers of the blockchain. This offline channel[8] is bidirectional and potentially infinite, i.e., it can execute the infinite number of transfers between two peers provided they do not close the channel and each of them has sufficient funds. We construct an offline channel for proof of work-based public blockchain with the following properties: (1) We construct a uni-directional channel between two peers, i.e., only one peer can send funds to another peer of this channel. (2) We construct a uni-directional channel which can be used for a finite number of transfers from a designated peer to another peer.

The procedure for creating the uni-directional channel from A to B (A transfers token to B)is as follows: Let A and B are two peers of the channel network H. $M_{A,B}$ is a multi-signature address between A and B. This is a unidirectional channel from A to B.

1. A creates a set of k (k is a positive even integer) random strings $S_A^1, \ldots, S_A^k$. Using these random strings A creates a set of Hashes $H_H^1 = H(S_B^1), H_B^2 = H(S_B^1) \ldots, H_B^k = H(S_B^k)$ where H is Hash function (using SHA256). A creates a Merkle tree order λ using these Hashes. Thus there are k leaf nodes and $k-1$ non-leaf nodes of this Merkle tree. We denote the non-leaf nodes as $H'^1_A, \ldots, H'^(k-1)_A$.
2. B creates a set of $k1$ random strings $S^1, \ldots, S^k$ and corresponding Hashes $H_B^1, \ldots, H_B^k$.
3. A sends the Merkle tree to B and B sends the set of Hashes $H_B^1, \ldots, H_B^k$ to A.

4. A sends a Hashed time-locked contract $HTLC_A^1$ to B as follows:
   (a) From the multi-signature address $M_{A,B}$, 1 token will be given to A after time T if B does not claim these tokens before time T by producing the key to $H_A'^1$ and 0 token will be given to A if it can produce the key to H_B^1.
   (b) A sends $HTLC_A^1$ to B.
5. Now, A sends 1 token to $M_{A,B}$. A includes the Merkle tree and $H_B^1, \dots, H_B^k$ in this transaction. This records the Merkle tree and $H_B^1, \dots, H_B^k$ in the blockchain and any other peer can verify the existence of these Hashes by checking transactions of the public blockchain. Also, at this stage, A's funds are safe as it can get the tokens from $M_{A,B}$ after time T as B does not know $H_A'^1$.
6. Next to send another $(1/k)$ tokens to B, A sends S_A^1 to B and B sends H_B^1 to A. Then A forms the following HTLC:
   (a) From the multi-signature address $M_{A,B}$, $1-1/k$ token will be given to A after time T if B does not claim these tokens before time T by producing the key to $H_A'^2$ and $1/k$ token will be given to A if it can produce the key to H_B^2.
   (b) A sends $HTLC_A^2$ to B.
7. This process continues until all keys of the Hashes of non-leaf nodes are revealed by A.

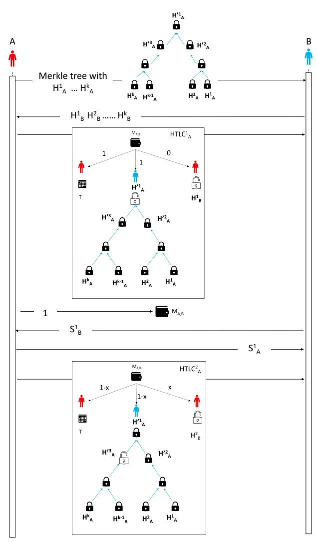


Fig. 1: Procedure of creating unidirectional offline channels.

In this model of the unidirectional channel, A is sequentially releasing the keys of the Merkel tree of the HTLCs. Its fund in this channel is decreasing with time. It can not prevent B from obtaining the tokens as only B can publish the HTLCs. B will publish the HTLC where it gets the maximum value. A path-based fund transfer (PBT) is possible in this uni-directional channel network along paths in the channel network. For example, three nodes p_x, p_y, p_z can facilitate token transfer from p_x to p_z as follows:

1. p_z will create a lock H_z and inform p_x about H_z.
2. A sequence of two HTLCs will be created. The first HTLC will transfer fund of 1 token from p_x to p_y if p_y can present the key to H_z before time 10 seconds. The second HTLC will transfer fund of 1 token from p_y to p_z if p_z can present the key to H_z before time 8 seconds.
3. p_z will initiate the execution of these HTLCs by revealing key to H_z to p_y. And, p_y will use the same key to take 1 token from p_x.

4.2 Double auction using offline channels

We will a blockchain network with $m > n$ peers consisting of prosumers, DSOs, and miners. We assume that the blockchain network uses Bitcoin-like proof of work-based blockchains and there is an offline channel network using a unidirectional network as described in the previous section. The blockchain network will consist of a set of distinguished and recognised (possibly the miners of the blockchain network) as the auctioneers. We denote these peers as the set $\{d_i\}$. A prosumer may establish a uni-directional channel with a subset of auctioneers. Auctioneers may establish a uni-directional channel among themselves. We will denote the channel network as a directed graph $G = (V, E)$ where V is the peers of the channel network and E is the channels. $W(E)$ will denote channel balances, i.e., $W(p_i, p_j)$ is the amount of fund p_i can send to p_j using the channel $p_i \rightarrow p_j$. The blockchain network will also consist of a set of nodes $\{D_i\}$ representing the DSOs of the electricity management networks. They are regulators and their objective is to ensure the integrity of the energy trade and security of the electricity grid. They need to ensure that one unit of electricity to be sold to only one prosumer asking for one unit of electricity.

Asking Price and Bids: The channel from the prosumer p_i to the auctioneer node d_j will be used for payment for electricity to be used by p_i. The channel to the prosumer p_i from the auctioneer node d_j will be used to pay p_i for its surplus electricity to be sold to other prosumers. The bid and asking price announcement process is shown in Fig. 2(a) and it is as follows:

1. A prosumer can submit its bid to any auctioneer node (with whom it has a offline channel) by creating a HTLC as follows:
   (a) Let p_a wants to submit a bid to d_1. The HTLC will state that p_a will pay d_1 if d_1 can prove that the offered electricity is unique as it will not be sold to another prosumer.
2. Let p_x wants to sell electricity it can submit its asking price as follows:

(a) p_x contacts a DSO node D_1 for a token to be used as a unique identity to its offer to sell electricity for the next trade window (if p_x asks it at time t_i then its trade window is from t_i to $t_i + dt$.). D_1 will inform p_x about a set of the locks $H_{D1}, H_{D2}, H_{D3}, H_{D4}$ (number of such locks is equal to the total number of auctioneer + 1) to be used to uniquely identify p_x's asking price for the trade window from t_i to $t_i + dt$.

(b) D_1 will check with all DSO nodes if p_x has applied for another such identifier at the same or overlapping trade window. In such a case D_1 will not issue the unique offer identifier to p_x.

(c) We assume that all prosumers are permission-ed, as their identity, location, smart-meter identification numbers are verified by the DSO nodes. This means prosumers can not create a false identity to participate in this trade with multiple identities.

(d) Next, p_x will create a random path among all auctioneer nodes and inform all of them about H_{D1}.

(e) All auctioneer node will inform p_x about the Hash in the Merkle tree for the unidirectional channel between pairs of auctioneer nodes according to the path among the auctioneer node created by p_x which can transfer fund equal to the asking price of p_x. As shown in Fig. 2(a) such Hashes are H_1, H_2, H_3, and H_4.

(f) Now, p_x will facilitate the creation of sequence $HTLC$s from itself to the auctioneer nodes and finally to itself using the Hashes of the Merkle tree of the channel among the auctioneers. As shown in Fig. 2(a), first HTLC states that d_1 will give p_x .1 token if p_x can produce key to H_1. The second HTLC states that d_2 will given d_1 .1 token if d_1 can reveal H_2 and H_{D1}, H_{D2} before time 8. And so on until p_x gives d_3 .1 tokens before time 10 for keys to all hashes H_4, and $H_{D1}, H_{D1}, H_{D2}, H_{D3}, H_{D4}$. The time mentioned in these HTLCs are just examples, in practice, these times will be few seconds but constantly increasing.

(g) After creating these HTLCs, d_2 will reveal key to H_2 to p_x, and d_3 will reveal key to H_3 to p_x.

(h) Next, p_x will reveal key to H_2 to d_1, key to H_3 to d_2, and key to H_4 to d_3.

(i) Now, the auctioneer d_1 will buy the electricity from p_x as follows: d_1 reveals the key of H_1 to p_x as it purchases the surplus electricity from p_x. d_1 can either sell the electricity to any other prosumer who has submitted a bid to d_1 or sell to d_2 if there is no such prosumer.

(j) Similarly, d_2 can purchase the electricity it from d_1 and may sell it to any prosumer who had submitted a bid to d_2 or sell it to d_3 otherwise. This process can continue to p_x. This means an auctioneer node can always purchase electricity from another auctioneer or a prosumer as it can always resale it.

(k) Thus, using the above protocol p_x can submit asking prices to the auctioneer. Its asking price will be evaluated by the auctioneer in a random sequence chosen by p_x. Any rational auctioneer, say d_1 may be able to sell this electricity from p_x to another prosumer such as p_a if bid of p_a

is more or equal to the asking price of p_x. Otherwise it will resale the electricity to another auctioneer d_2.

(l) It is possible that the asking price p_x is more than any other bid submitted by other prosumers. In this case, no rational auctioneer will be able to sell electricity from p_x and initial fund given to p_x will be taken from p_x by d_3. Thus if it is not possible to sell electricity from p_x then p_x does not get paid.

Trade uniqueness: However, in the given protocol it may be possible to double-spend the electricity as follows:

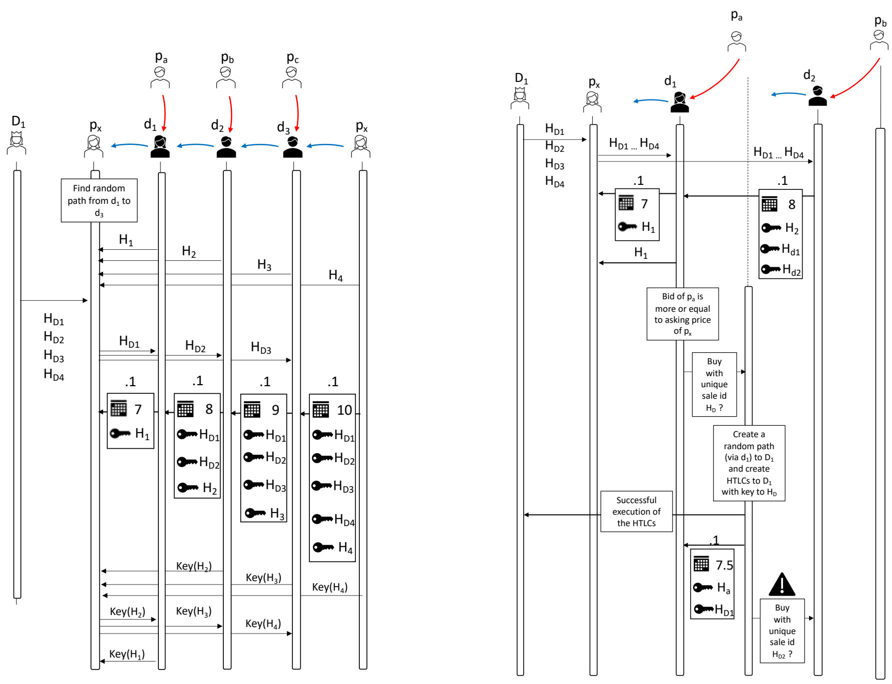
1. It is possible that d_1 finds a prosumer p_a whose bid is more than the asking price of p_x.
2. d_1 will sell electricity from p_x to p_a and also, resale the electricity to the next auctioneer d_2. Thus d_1 will be able to sell the electricity at least twice.
3. All such auctioneer may do the same and resale the electricity multiple times.

Thus it is necessary to maintain uniqueness of the electricity trade. We allow the prosumer to trade a uniform amount of electricity per its asking price and bid. We solve the uniqueness problem of electricity trade as follows:

1. As shown in Fig. 2(b), before submitting the bid, p_x needs to collect a unique offer identifier from a DSO node D_1. Let D_1 informs p_x about the unique offer identifiers $H_{D1}, H_{D2}, H_{D3}, H_{D4}$.
2. p_x will inform all auctioneer about this unique offer identifier.
3. After forming the HTLCs for asking prices, an auctioneer d_1 may find a prosumer p_a whose bid is more than the asking price of d_1.
4. p_a will pay d_1 if d_1 can prove uniqueness of the trade offer.
5. d_1 will inform p_a that unique offer identifier is H_{D1} and it is issued by the DSO node D_1.
6. p_a can create and execute a PBT from p_a to D_1 via d_1 with lock H_{D1}. In such a transfer D_1 will execute the PBT by revealing the key to H_D. Key to H_{D1} will eventually reach p_a and d_1 after successful execution of the PBT.
7. If such PBT in unsuccessful then it will prove that the proposed trade is not unique and p_a will not d_1.
8. Hence if d_1 will not be able to sell electricity from p_x multiple times.

5 Analysis

Theorem 1. *If a prosumer p_x trades electricity with another prosumer p_a then an adversary may not know the trade between p_x and p_a unless the adversary controls all parties in the path from p_x to p_a. For example, such a path will include $p_x \rightarrow d_1 \rightarrow p_a$.*



(a)

(b)

Fig. 2: (a)Double auction procedure: Sequence of key distribution and HTLC formation, (b) Double auction procedure: Procedure to ensure uniqueness of a trade.

Proof. Note that, submission of bids and asking prices are executed via exchange of HTLCs. For example, as shown in Fig. 2(a), p_x will receive an updated HTLC from d_1 as it submits its asking price to d_1. Similarly, d_1 will receive an updated HTLC from p_a as p_a submits a bid to d_1. The updated HTLCs are not visible by other parties and hence the adversary needs to control all entities in a path between two parties who are trading electricity.

Theorem 2. *It is not possible to double-spend the electricity in the proposed double auction protocol.*

Proof. As discussed in the previous section, a prosumer has to collect a unique offer identifier from a DSO node before it can submit its asking price. DSO nodes want to secure the electricity grid, and hence they will not allow multiple offer identifiers to the same prosumer for overlapping trade window. This is because multiple prosumers may consume electricity simultaneously if there is a double-spending of electricity offered by a prosumer. This will imbalance the electricity grid. Further, as mentioned before, prosumers are permission-ed nodes, i.e., DSO will check their location and identity to ensure that each prosumer has only one node in the blockchain. Thus a prosumer can't use multiple identities to sell the same unit of electricity. Further, before buying electricity a prosumer will seek proof of uniqueness from the DSO using the offer identifier provided by the auctioneer. The DSO node will reveal the key to such an offer identifier. For example, (Fig. 2(b)) p_a may verify offer identifier H_{D1} by creating a PBT from p_a to the DSO node D_1 with the lock H_{D1}. D_1 will reveal the key to this Hash to p_a and p_a will use it to execute a PBT to D_1. If D_1 has already revealed the key to H_{D1} then it will not participate in such a PBT, and failure of this PBT will cause p_a not to buy electricity from d_1. Further, if d_1 tries to resale electricity to another auctioneer d_2 then p_b (who had submitted the bid to d_2) will check if the trade offer is unique by creating a PBT to the DSO node D_1. Again D_1 can ensure offer uniqueness. And, p_b will not buy if the offer is not unique. Hence D_2 will not buy the electricity from D_1 as it can not resale the electricity.

Theorem 3. *The proposed auction is individually rational, weakly budget balanced, and have the same economic efficiency compared with McAfee's double auction[6].*

Proof. The proposed auction is individually rational because

1. a prosumer does not pay more than its bid,
2. a prosumer does not receive less than its asking price,
3. and, if the surplus electricity of a prosumer can not be sold by the auction then the prosumer does not get paid.

(1) and (2) hold because a rational auctioneer d_1 will only buy electricity from p_x if it can sell it to another prosumer p_a whose bid is higher than the asking price of p_x. Otherwise, the auctioneer will lose funds. (3) holds because using the set of HTLCs as shown in Fig. 2(a), if electricity from p_x can not be sold then although p_x initially gets paid by d_1 but p_x pays back the fund to d_3.

The proposed double auction is weakly budget-balanced as the auctioneer will only pay the prosumer such as p_x if it can sell electricity from p_x at the price at least equal to the asking price of p_x.

The proposed double auction has at least the same economic efficiency as McAfee's double auction because the asking price of p_x is sequentially compared will all bids and it is matched (i..e., corresponding electricity is sold) as soon as there is a bid more than asking price of p_x. Any asking price which is matched with a bid (i.e., the bid is more than the asking price) by McAfee's algorithm will also be matched in the proposed double auction method.

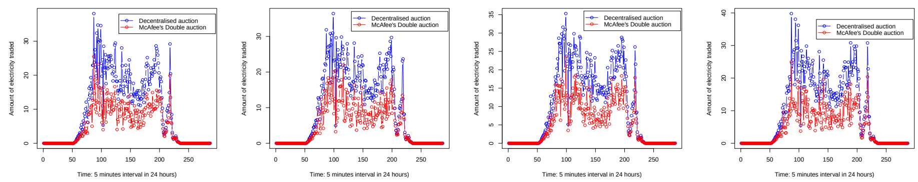
The proposed auction can significantly reduce the number of transactions needed to be recorded in the blockchain. A unidirectional channel can be used a finite number of times without updating the blockchain. If such a number of channel updates is k then it can reduce $k-1$ transactions needed to be recorded in the blockchain (one transaction is needed to open then offline channel). Auctioneers will have a non-negative revenue from the proposed auction. This will attract investment in building the blockchain network to execute the energy trade.

6 Experimental Evaluation

We used prosumer energy demand and PV generation data from [12] to evaluate proposed decentralised double auction. The data contains energy demand and PV generation data of 100 prosumers for 24 hours (data recorded in every 5 minutes). We used the blockchain simulator developed in [3] to simulate a proof-of-work-based blockchain network and offline channels. First, we used agent-based modelling to implement a centralised double auction and then we implemented the decentralised double auction in the blockchain simulator. In each set of experiments, we executed simulated peer to peer energy trade among these prosumers. We execute four sets of simulations. In each set, first we execute the energy trade simulation for centralised auction, and then, we execute the the energy trade simulation for the decentralised auction with identical asking price and bid data(in the range $[0, 1]$). In these experiments we measured the amount of electricity traded as an indicator of energy trade efficiency. Fig. 3 show that the decentralised auction is more efficient than centralised double auction as more electricity is traded with decentralised double auction.

7 Conclusion

In this paper, we proposed a secure and privacy-preserving decentralised double auction using blockchain offline channels. The proposed method will be useful if energy trade is executed in public blockchains. Public blockchains have scalability problems, and there is a significant carbon footprint for creating a transaction in public blockchains such as Bitcoin or Ethereum. However, these public blockchains can be valuable platform to implement decentralised energy



(a) (b) (c) (d)

Fig. 3: (a)It shows the performance of the proposed decentralised double auction and centralised McAfee's double auction, (b) It shows the performance of the proposed decentralised double auction and centralised McAfee's double auction, (c) It shows the performance of the proposed decentralised double auction and centralised McAfee's double auction, (d) It shows the performance of the proposed decentralised double auction and centralised McAfee's double auction.

trade due their easy access and high token valuation. Our solution implements decentralised energy trade with a minimum number of transactions. Hence it is not only a highly scalable solution but also reduces the carbon footprint of using public blockchains.

Acknowledgement

This publication has emanated from research conducted with the financial support of Science Foundation Ireland (SFI) under Grant Number SFI/12/RC/2289, co-funded by the European Regional Development Fund.

References

1. Raiden network. http://raiden.network/, accessed 2018.
2. Chen, K., Lin, J., Song, Y.: Trading strategy optimization for a prosumer in continuous double auction-based peer-to-peer market: A prediction-integration model. Applied Energy **242**, 1121–1133 (2019). https://doi.org/https://doi.org/10.1016/j.apenergy.2019.03.094, https://www.sciencedirect.com/science/article/pii/S0306261919305045
3. Hayes, B., Thakur, S., Breslin, J.: Co-simulation of electricity distribution networks and peer to peer energy trading platforms. International Journal of Electrical Power & Energy Systems **115**, 105419 (2020). https://doi.org/https://doi.org/10.1016/j.ijepes.2019.105419, http://www.sciencedirect.com/science/article/pii/S0142061519302972
4. Malavolta, G., Moreno-Sanchez, P., Kate, A., Maffei, M.: Silentwhispers: Enforcing security and privacy in decentralized credit networks. IACR Cryptology ePrint Archive **2016**, 1054 (2016)
5. Malavolta, G., Moreno-Sanchez, P., Kate, A., Maffei, M.: Silentwhispers: Enforcing security and privacy in decentralized credit networks. IACR Cryptology ePrint Archive **2016**, 1054 (2016)

6. McAfee, R.: A dominant strategy double auction. Journal of Economic Theory **56**(2), 434–450 (1992). https://doi.org/https://doi.org/10.1016/0022-0531(92)90091-U, https://www.sciencedirect.com/science/article/pii/002205319290091U
7. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system. www.bitcoin.org (2008)
8. Poon, J., Dryja, T.: The Bitcoin Lightning Network:Scalable Off-Chain Instant Payments https://lightning.network/lightning-network-paper.pdf
9. Roos, S., Moreno-Sanchez, P., Kate, A., Goldberg, I.: Settling payments fast and private: Efficient decentralized routing for path-based transactions. CoRR **abs/1709.05748** (2017), http://arxiv.org/abs/1709.05748
10. Thakur, S.: A unified model of peer to peer energy trade and electric vehicle charging using blockchains. IET Conference Proceedings pp. 77 (6 pp.)–77 (6 pp.)(1), https://digital-library.theiet.org/content/conferences/10.1049/cp.2018.1909
11. Thakur, S., Breslin, J.G.: Peer to peer energy trade among microgrids using blockchain based distributed coalition formation method. In: Technol Econ Smart Grids Sustain Energy. vol. 3 (2018). https://doi.org/https://doi.org/10.1007/s40866-018-0044-y
12. Thakur, S., Hayes, B.P., Breslin, J.G.: Distributed double auction for peer to peer energy trade using blockchains. In: 2018 5th International Symposium on Environment-Friendly Energies and Applications (EFEA). pp. 1–8 (Sep 2018). https://doi.org/10.1109/EFEA.2018.8617061
13. Thakur, S., Breslin, J.G.: Real-time peer to peer energy trade with blockchain offline channels. In: 2020 IEEE International Conference on Power Systems Technology (POWERCON). pp. 1–6 (2020). https://doi.org/10.1109/POWERCON48463.2020.9230545
14. Tushar, W., Saha, T.K., Yuen, C., Azim, M.I., Morstyn, T., Poor, H.V., Niyato, D., Bean, R.: A coalition formation game framework for peer-to-peer energy trading. Applied Energy **261**, 114436 (2020). https://doi.org/https://doi.org/10.1016/j.apenergy.2019.114436, http://www.sciencedirect.com/science/article/pii/S0306261919321245