blockchains

MDPI

Article

Toward a Blockchain-Based, Reputation-Aware Secure Transactive Energy Market

Peng Zhang [1], Peilin Wu [1], Yuhong Liu [2,*], Ye Chen [2], Yuanliang Li [3], Jun Yan [3] and Mohsen Ghafouri [3]

[1] College of Electronics and Information Engineering, Shenzhen University, Shenzhen 518060, China; zhangp@szu.edu.cn (P.Z.); wupeilin2021@email.szu.edu.cn (P.W.)
[2] Department of Computer Science and Engineering, Santa Clara University, Santa Clara, CA 95053, USA; ychen40@scu.edu
[3] Concordia Institute for Information Systems Engineering, Concordia University, Montréal, QC H3G 1M8, Canada; yuanliang.li@concordia.ca (Y.L.); jun.yan@concordia.ca (J.Y.); mohsen.ghafouri@concordia.ca (M.G.)
* Correspondence: yhliu@scu.edu

Abstract: The rapid expansion of transactive energy has transformed traditional electricity consumers into producers, engaging in local energy trading. In the context of distributed energy transactions, blockchain technology has been increasingly applied to facilitate transaction transparency and reliability. However, due to the challenges in collecting accurate energy transmission data from power lines, most existing studies on the blockchain-based transactive energy market are still vulnerable to security attacks, such as malicious users misreporting energy prices, refusing to pay or refusing to transmit energy. Therefore, based on the co-simulation platform PEMT-CoSim and a blockchain, we establish a blockchain-based, reputation-aware secure transactive energy market (STEM) by introducing a reputation scheme to evaluate the trustworthiness of all prosumers and designing reputation-aware, multi-round double auction and energy transmission algorithms to detect and penalize malicious attacks. Furthermore, we run comprehensive experiments for different use cases. The results show that even with malicious participants, the proposed system can guarantee the interests of the honest participants and improve the robustness and effectiveness of the energy market.

Keywords: transactive energy; trading system; double-auction; energy market; blockchain; security; reputation; trustworthiness

Citation: Zhang, P.; Wu, P.; Liu, Y.; Chen, Y.; Li, Y.; Yan, J.; Ghafouri, M. Toward a Blockchain-Based, Reputation-Aware Secure Transactive Energy Market. *Blockchains* **2024**, *2*, 61–78. https://doi.org/10.3390/blockchains2010004

Academic Editor: Keke Gai

Received: 11 January 2024
Revised: 22 February 2024
Accepted: 5 March 2024
Published: 8 March 2024

1. Introduction

The development of renewable energy has spurred the growth of microgrids. Microgrids can operate autonomously and connect to the primary grid, serving as a part of community power. The public can actively participate in microgrids, acting as either energy consumers or producers by leveraging renewable energy sources. As a result, traditional energy users can transform into energy prosumers who can either purchase energy to cover their usage or sell excessive energy generated by themselves. This dynamic involvement has injected new vitality into the energy market, leading to the new concept of transactive energy [1]. As a market-based approach, transactive energy not only provides an energy trading environment but also effectively coordinates energy generation and consumption among various entities. This alleviates the pressure on the grid and encourages community participation, boosting the penetration of renewable energy and user engagement.

However, traditional transactive energy still faces many challenges, such as centralized management, low transparency and susceptibility to manipulation. Recently, blockchain-based energy trading has been researched for its advantages in decentralization, prevention of data tampering and high transparency. Umar et al. [2] proposed a distributed microgrid energy market model that validates the effectiveness of a blockchain in the energy trading market while considering the storage structure of batteries. Esmat et al. [3] proposed a

decentralized peer-to-peer energy trading platform called Detrade, which integrates the trading market with a highly secure blockchain layer to ensure fast and real-time settlements, eliminating centralized transaction costs. Gai K et al. [4] investigated the privacy concerns in blockchain-based neighborhood energy trading systems. They employed account mapping techniques to prevent attackers from directly accessing data, and utilized virtual/partitioned accounts to alter transaction characteristics without compromising performance. Nevertheless, most of these blockchain-based solutions can only handle the transaction layer while ignoring the verification of the underneath power delivery due to the difficulties in collecting accurate energy transmission information from the power lines.

Recently, a novel concept of packetized energy was proposed [5] which provides a promising device-driven, bottom-up solution to enable power delivery in a "request-reply" way. In particular, each controllable load can request fixed-duration, fixed-power "energy packets" delivered with their source and destination specified [5,6]. By discretizing the power transmission, packetized energy-related technologies can not only make energy management easier but also provide traceability for energy delivery, providing evidence to evaluate whether a specific energy seller has successfully delivered the committed amount of energy to the buyer. Furthermore, our prior work [7] proposed the first co-simulation platform to integrate a blockchain-based energy trading system with the transactive energy simulation platform (TESP) developed by the Pacific Northwest National Laboratory (PNNL), which can synchronize different simulation modules, such as domain-specific simulation tools, sample prosumer agents, communication modules and weather modules. This work enables us to design and validate the blockchain-based transactive energy market in a more realistic way.

In this further research, we realize that there are various auction fraud issues in the process of energy trading, such as distorted bidding prices before bidding, non-payment or non-delivery after bidding [8]. These attacks will inevitably threaten the interests of honest participants and severely affect the efficiency of the trading system. Therefore, based on the Packetized Energy Management and Trading Co-Simulation (PEMT-CoSim) platform proposed in our prior work [7,9], we propose a blockchain-based, reputation-aware secure transactive energy market (STEM) by introducing a reputation scheme to calculate the reputation scores for all prosumers and designing reputation-aware, multi-round double auction and energy transmission algorithms to detect and penalize malicious participants. The major contributions of this paper are as follows:

- A multi-round double auction algorithm is proposed to prevent malicious participants involving distorted bidding prices before bidding and non-payment after bidding. Specifically, the double auction will run iteratively and only be settled when all malicious bidders are excluded, improving the robustness and effectiveness of the auction process.
- We introduce and propose a reputation scheme, where the reputation score of a prosumer is calculated according to his or her historical records stored on the blockchain to determine whether he or she has committed dishonest behaviors in prior energy transactions. Such reputation scores will be considered during the later energy auctions, together with the prosumers' bidding prices and quantities, to determine their priorities in energy bidding.
- In order to prevent malicious sellers from avoiding electricity delivery after successful bidding, we first set up an energy pool to identify the potential attackers and then design an energy transmission algorithm to maximize the benefits of buyers when malicious sellers are present.
- By integrating everything together, a secure transactive energy market (STEM) is proposed based on PEMT-CoSim and a blockchain, including energy bidding, reputation-aware, multi-round double auction, energy transmission and transaction verification. Furthermore, according to the energy delivery verification results, the reputation scores will be updated for both honest and malicious participants dynamically, and they will be taken into account for future energy auctions.

2. Related Work

This section will discuss the related work from three perspectives: transactive energy, blockchain-based energy trading and reputation schemes.

2.1. Transactive Energy

Utilizing interactive coordination and energy control methods can effectively facilitate the integration of distributed energy resources into the microgrid distribution system. Unlike traditional direct energy management models, transaction-based energy management methods indirectly coordinate energy in a community microgrid. Producers and consumers can engage in energy transactions through an energy trading system [10].

Guerrero et al. [1] focused on common microgrid features and requirements and discussed the underlying key elements of transactive energy. They integrated distributed energy resources into medium-to-low voltage networks based on the network levels and different user priorities. Nizami et al. [11] developed a two-stage energy management system to address community electricity overload and cost optimization issues, aiming to maximize profits.

In terms of the market, Faqiry et al. [12] proposed a performance evaluation framework to assess the double auction market. Bokkisam et al. [13] proposed a periodic double auction pricing mechanism to determine the settlement prices and quantity in the trading market. Lian et al. [14], based on transactive energy, explored the impact of double auction pricing and the limitations of transactive energy.

2.2. Blockchain-Based Transactive Energy

Blockchain technology originates from the Bitcoin protocol in 2008[15]. Due to its unique advantages in non-repudiation, traceability, decentralization and transparency, blockchains have frequently been adopted in energy trading research [16]. Recently, Wong et al. [17] explored the application and impact of blockchain technology on distributed energy trading in terms of three aspects: scalability, security and decentralization. Gai et al. [18] proposed an edge model based on the smart grid, which aids in detecting inappropriate energy usage behaviors to reduce/prevent energy-related attacks. AlSkaif et al. [19] proposed two strategies for implementing bilateral transaction coefficients in a blockchain-based peer-to-peer energy market. These strategies aim to ensure maximum freedom and autonomy for prosumers in their transactions. Khalid et al. [20] designed a hybrid peer-to-peer energy trading market with a consortium blockchain, using smart contracts to manage local transactions in the market, but they did not discuss the security aspects. Doan et al. [21] studied a peer-to-peer energy trading system using a dual auction-based game theory approach, where buyers can adjust the energy purchase quantity based on electricity prices to maximize their benefits. The study also incorporated privacy protection for participant bidding information.

2.3. Reputation Schemes

Reputation schemes play a crucial role in establishing trust among various entities. They are widely applied in decentralized systems, such as peer-to-peer networks, wireless sensor networks and e-commerce systems [22]. This effectively reduces the participation and impact of malicious users and reduces fraudulent activities, boosting profits for honest users. Traditional feedback-based reputation schemes [23] rely on users to provide ratings for each other. However, these ratings may not be evidence-based or can be easily manipulated [24]. By leveraging smart contracts on blockchains, distributed reputation systems can effectively solve these challenges. For example, Ahmed et al. [25] introduced five fundamental requirements that a reputation system should have when established within a smart contract and proposed a reliable trust and reputation calculation framework based on Ethereum.

When applied in energy trading, reputation schemes can effectively limit dishonest behaviors conducted by either buyers or sellers, making it easier to create a more equitable

environment for auctions and transactions. Wang et al. [26] introduced a reputation scheme into peer-to-peer energy trading, creating a positive incentive for prosumers to participate in energy transactions. Simultaneously, a fairness metric was employed to quantify the fairness of energy trading. Ullah et al. [27] introduced a new mutual reputation index as a product distinction to consider the bilateral energy trading intentions of both buyers and sellers. This was aimed at enhancing the reliability and stability of the energy market through peer-to-peer energy sharing.

In the existing studies, the reputation scores of users were mainly based on other users' ratings, but we update them based on readings from smart meters, which is more objective and evidence-based.

3. System Overview

Based on PEMT-CoSim and a consortium blockchain, a blockchain-based reputation-aware secure transtive energy market (STEM) is proposed in this paper, where PEMT-CoSim is employed for energy management, energy bidding and reputation management, while the consortium blockchain utilizes smart contracts for double auction pricing in energy transactions and stores transaction data and reputation values on chains. In this section, we first describe the general framework and the attack model considered by the STEM. The key notations are described in Table 1.

Table 1. The definitions of key notations.

Notation	Definition
B_i	Buyers participating in the auction
S_i	Sellers participating in the auction
P_{Si}	Energy transmitted by seller i
P_{Bi}	Energy obtained by buyer i
P_{sum}	The total amount of energy in the energy pool
R_{t_n}	Reputation value at time t_n
$Price_{t_n}$	Clearing price at time t_n
$Quantity_{t_n}$	Clearing quantity at time t_n
Q_i	The number of bids in the current auction
P_i	The bid price in the current auction
$R_{t_n}^{+}$	Positive feedback reputation value at time t_n
$R_{t_n}^{-}$	Negative feedback reputation value at time t_n
α_{t_n}	Reputation decay factor at time t_n
R_d	Price difference between two bidders
R_n	Total reputation value
R_{min}	Reputation threshold for participating in transactions
C_S	Successful seller set
C_B	Successful buyer set
FC_S	Candidate seller set
FC_B	Candidate buyer set
$Rank_{auction}$	Double auction ranking criteria for bidders
$P_{C_S}^{avg}$	Average price for successful seller
$P_{C_B}^{avg}$	Average price for successful buyer
S_{ca}	Reputation scaling factor

3.1. The General Framework

The general framework of the STEM is shown in Figure 1, including four stages: energy bidding, multi-round double auction, energy transmission, and transaction verification, which will be described in Section 4 in detail. The energy market is running as the core, interacting with different prosumers, which are simulated in PEMT-CoSim. The management of prosumers and their transactions relies on the consortium blockchain. The main components are described below.

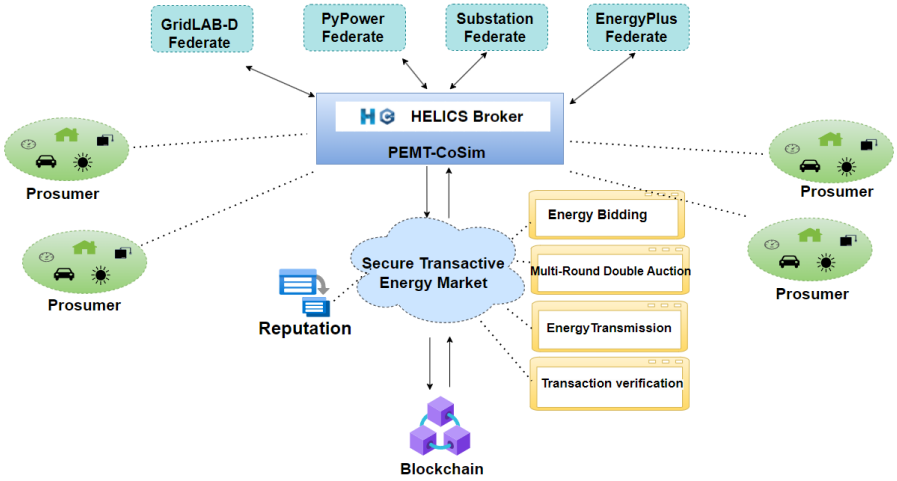

Figure 1. The general framework of the secure transactive energy market.

- PEMT-CoSim: PEMT-Cosim developed in our prior work [9], incorporates packetized energy (PE) technologies and provides a flexible approach to packetized energy management (PEM) and packetized energy trading (PET). In particular, the Helics framework is employed to synchronize and coordinate communication among different federates, including GridLAB-D, PyPower, EnergyPlus, and Substation. It facilitates the management, distribution and trading of energy through the PEM and PET modules. More importantly, the adoption of this co-simulation platform enables the proposed framework to collect accurate energy delivery information, which serves as evidence for the proposed reputation management.
- Prosumers: Prosumers are the primary participants in the microgrid. In our system, prosumers manage various electricity loads and productions at the residential level, including base loads and controllable loads (e.g., HVAC or a dishwasher), along with solar panels and batteries. Prosumers determine their roles in the energy trading market (buyer, seller or non-participant) by forecasting residential photovoltaic generation and house load consumption. Based on the forecasted values, prosumers, acting as participants in energy trading, submit bidding information during the auction phase of the energy market to maximize their own interests.
- Blockchain: In the double auction phase, after the clearing price and quantity are determined, a shared wallet on the blockchain is established to store buyers' prepayments and sellers' default penalties. In the phase of transaction verification, all transaction information and updated reputation scores are stored on a blockchain. This helps achieve traceability and transparency in monitoring the credibility of transactions participants.

3.2. The Attack Model

In this paper, we mainly focus on potential attacks from malicious participants in the process of energy trading.

- Attack 1: Misreporting of Electricity Prices

Any prosumer, on principle, can intentionally quote unreasonable electricity prices and not participate in subsequent transactions to disrupt the auction results. In severe cases, the efficiency of the system and the fairness of transactions will be significantly affected.

- Attack 2: Refusing to Pay
  In one scenario, the seller successfully bids but fails to provide the prepayment portion due to insufficient funds in his or her wallet, resulting in the transaction's failure. In another scenario, the buyer successfully bids but refuses to pay the token for the purchased energy, leading to failure of the transaction. These behaviors can affect the execution of auction results and the efficiency of the trading system.
- Attack 3: Refusing to Transmit Energy
  When a seller is a malicious user, he or she may participate in transaction bidding but not transmit energy. Although we lock the seller's default penalty in a smart contract before energy transmission, this does not prevent him or her from engaging in malicious behavior in subsequent transactions. Such behavior significantly affects the valid interest of buyers and results in a negative experience for buyers.

4. Reputation-Aware Secure Transtive Energy Market

Considering the mentioned fraudulent attacks in energy trading, we propose a secure transactive energy market (STEM) to enhance security and robustness by introducing a reputation scheme. In this section, we will provide a detailed explanation of the four stages of the STEM: energy bidding, reputation-aware multi-round double auction, energy transmission, and transaction verification. The process of the secure transactive energy trading system is shown in Figure 2.

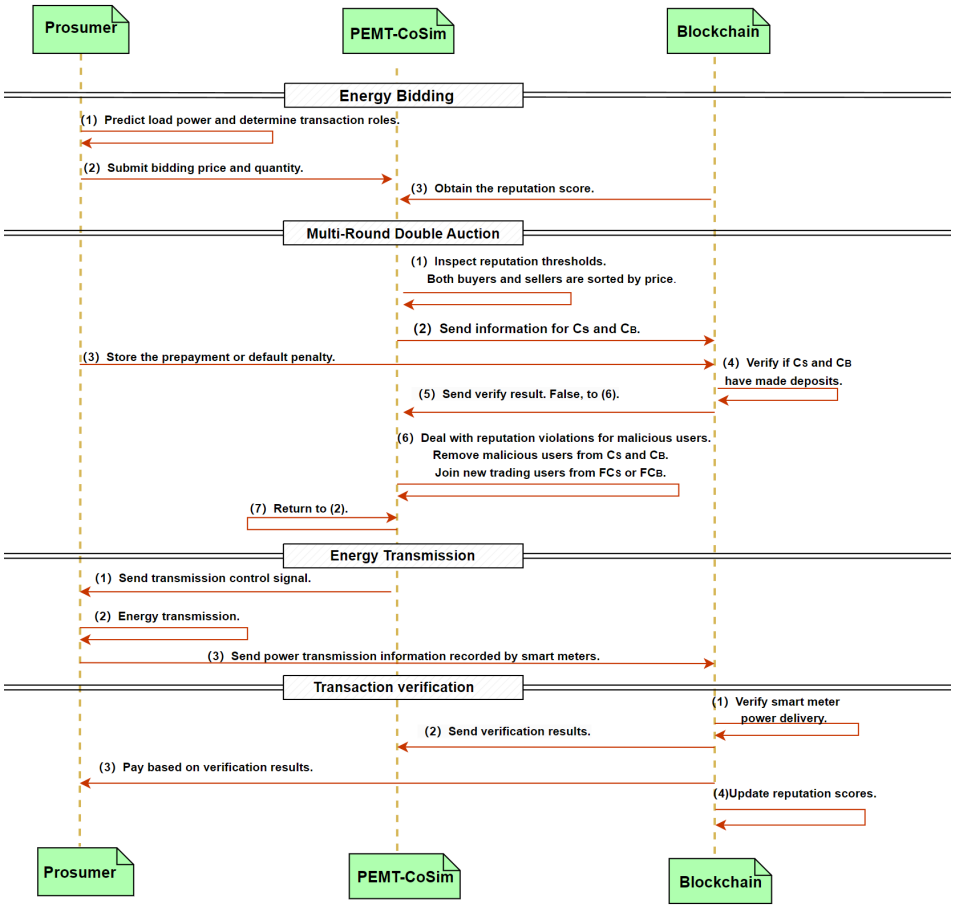

Figure 2. The process of the secure transactive energy market.

4.1. Energy Bidding

When PEMT-Cosim initiates a market cycle, prosumers forecast the next stage of residential photovoltaic generation and house load consumption. Based on the predictions, if the prosumers have surplus electricity, then they act as sellers and participate in market trading. Prosumers with insufficient electricity act as buyers and participate in market trading or may choose not to participate. At the same time, sellers and buyers evaluate market bidding information (price, quantity, and reputation score) for double auctioning, and the reputation scores are calculated by the following reputation scheme.

The Reputation Scheme

Specifically, we define a reputation array $\{R_{t_1}, R_{t_2}, \cdots, R_{t_n}\}$ for a time period n, where R_{t_i} denotes the reputation feedback value at certain times. Furthermore, the clearing price and quantity at time t_n are denoted by $Price_{t_n}$ and $Quantity_{t_n}$, respectively.

If a user is honest, then we define a positive feedback coefficient $R^+_{t_n}$:

$$R^+_{t_n} = \frac{Price_{t_n}}{P^{avg}_{C_S} + P^{avg}_{C_B}} \cdot \frac{Q_i}{Quantity_{t_n}} \in [0, 1) \tag{1}$$

which represents the positive feedback reputation value of the transaction at time t_n. $P^{avg}_{C_S}$ and $P^{avg}_{C_B}$ are the average seller's price in C_S and the average buyer's price in C_B, respectively.

Likewise, if a user is malicious, then we define a negative feedback coefficient:

$$R^-_{t_n} = -\frac{Price_{t_n}}{P^{avg}_{C_S} + P^{avg}_{C_B}} \cdot \frac{Q_i}{Quantity_{t_n}} \in [0, 1) \tag{2}$$

which represents the negative feedback reputation value of the transaction at time t_n.

Thus, this allows us to obtain the reputation values of users at a specific moment in time with the following equation:

$$R_{t_n} = \begin{cases} \alpha_{t_n} \cdot R^+_{t_n}, & Honest \quad User \\ \alpha_{t_n} \cdot R^-_{t_n}, & Malicious \quad User \end{cases} \tag{3}$$

where α_{t_n} represents the reputation decay factor at at time t_n, with values in the range of $(0, 1)$.

From Equations (1) and (2), we can see that (1) an honest behavior will receive a positive feedback coefficient while a malicious one will receive a negative coefficient, and (2) the absolute coefficient value is determined by both the trading price and quantity. Such a design will lead to a faster reputation increase for honest active users who committed higher amounts of energy trades, which can encourage users' further participation. Meanwhile, this also demotivates on-off attacks, a major reputation manipulation attack [28] where malicious users obtain economic profits by accumulating a greater reputation through a set of small transactions to prepare them for committing large amounts of fraud transactions.

By utilizing the least recently used (LRU) algorithm [29], we select the least recently used value for eviction and eliminate the historical reputation feedback values beyond the time period n. The total reputation value R_n at time t_n is represented as follows:

$$R_n = \frac{\sum_{i=1}^{n} R_{t_i}}{S_{ca}} \in (0, 1), \tag{4}$$

where S_{ca} represents the scaling factor for the total reputation value and R_n has a range of values in $(0, 1)$.

In the phase of double auctioning, if a user's reputation R_n is less than a threshold R_{min}, then we will not allow that user to participate in this auction. We calculate the total scores of the buyers in the transaction as follows and arrange them in descending order:

$$Rank_{auction} = P_i \cdot R_n \in (0, P_i), \tag{5}$$

where P_i represents the buyers's bidding price in the current auction.

We calculate the total scores of the sellers in the transaction as follows and arrange them in ascending order:

$$Rank_{auction} = P_i \cdot (1 - R_n) \in (0, P_i), \tag{6}$$

where the price represents the seller's bidding price in the current auction.

4.2. Reputation-Aware Multi-Round Double Auction

The attack of misreporting electricity prices can happen in this phase. A direct manifestation of a buyer misreporting prices in an auction is their inability to pay the bidding price, resulting in financial losses for other participating buyers in this round of transactions. Therefore, we employ a multi-round double auction to address this issue and minimize its impact as described in Algorithm 1.

Algorithm 1 Reputation-aware multi-round double auction.

procedure MULTI-ROUND DOUBLE AUCTION(bidding information)
  Initialize: $flag = 0$
  while $flag = 0$ **do**
    for each $B_i, i \in (1, \ldots l)$ **do**
      Bid energy prices P_i , quantities Q_i and reputation scores R_n.
    end for
    for each $S_i, i \in (1, \ldots l)$ **do**
      Bid energy prices P_i , quantities Q_i and reputation scores R_n..
    end for
    Match auction participants based on the descending order of buyer bid prices and the descending order of seller bid prices.
    Obtain the sets of successful sellers C_S and buyers C_B.
    Obtain the sets of failed sellers FC_S and buyers FC_B.
    Sort FC_S in ascending order and FC_B in ascending order of price.
    Create a shared wallet SW for C_S and C_B.
    for each $B_i \in C_B$ **do**
      Deposit the bidding amount $Price_{t_n} \cdot Quantity_{t_n}$ into the shared wallet.
      The smart contract updates $flag_{B_i} = 1$ based on the wallet records.
    end for
    for each $S_i \in C_S$ **do**
      Deposit the default penalty into the shared wallet.
      The smart contract updates $flag_{S_i} = 1$ based on the wallet records.
    end for
    The smart contract updates $flag = \prod_{B_i} flag_{B_i} \prod_{S_i} flag_{S_i}$.
    if $flag = 0$ **then**
      The smart contract checks the value of $flag$, and users with a flag value of false are removed from group C_B or C_S.
      Add the first user of FC_S to C_S or the first user of FC_B to C_B.
    end if
  end while
end procedure

In the first round of the double auction, when there is a price difference within a threshold X between two bidders in the buyer set, we use Equation (5) to calculate the ranking scores for the two adjacent price bidders. Similarly, when there is a price difference within the threshold X between two bidders in the seller set, we use Equation (6) to calculate

the ranking scores for the two adjacent price bidders. The ranking scores of the participating buyers are arranged in descending order, and the ranking scores of the sellers are arranged in ascending order, based on which the clearing price and quantity are determined.

After the first round of the double auction, we determine the set of successful bidding buyers C_B and the set of successful bidding sellers C_S. Shared wallets are created for the successful bidders. The buyers in set C_B are required to deposit an advance payment into the shared wallet, while the sellers C_S need to deposit the default penalty (*Pays*) in advance into the shared wallet. To encourage honest users to participate in the transactions and deter malicious users from participating, we calculate the default penalty amount as follows:

$$Pays = P_i \cdot Q_i \cdot (1 - R_n) \tag{7}$$

In this round, the buyers or sellers who failed in bidding will be placed in the backup collections FC_B in descending order or FC_S in ascending order, respectively.

The smart contract checks whether each participating buyer and seller has deposited the tokens according to the wallet deposit records. If a buyer has not deposited the prepayment, then the auction for this round is invalidated, and the buyer is removed from C_B. Then, the smart contract will add the first candidate buyer in FC_B to C_B, and the other auctioneer information in C_B remains unchanged. Similarly, if a seller has not deposited the default penalty in advance, then the current auction round becomes invalid, and the seller is removed from C_S. Subsequently, the smart contract adds eligible candidate buyers from FC_S to C_S, while the bidding information of other participants in C_S remains unchanged. Energy transmission is then initiated only after the shared wallet receives the tokens pre-deposited by all participants.

4.3. Energy Transmission

When a seller is a malicious user, he or she may participate in the transaction bidding but not transmit energy. The previous work [7] could not detect who the malicious seller was. Therefore, we introduce an energy pool for energy transactions. The input represents the energy transmitted by the sellers, while the output represents the energy obtained by the buyers. PEMT-CoSim collects the total energy quantity in the energy pool.

As described in Algorithm 2, if the current total energy quantity in the pool is less than the amount of the matched quantity at the end of the auction, then this suggests that a malicious seller has not transmitted electricity. If the current total energy quantity in the pool is sufficient, then the buyers will receive the clearing quantity of energy from the energy pool.

Algorithm 2 Energy transmission.

for each seller S_i **do**
    Control the discharge of S_i at P_{Si} $kw \cdot h$
    Update the total sum of current electricity $P_{sum} = \sum P_{Si}$
end for
for each buyer B_i **do**
    if $P_{sum} \leq 0$ **then**
        Set $P_{Bi} = 0$
        Control the charge of P_{Bi} $kw \cdot h$ for B_i
    end if
    if $P_{sum} < P_{Bi}$ **then**
        Control the charge of P_{sum} $kw \cdot h$ for B_i
    else
        Control the charge of P_{Bi} $kw \cdot h$ for B_i
    end if
    Update $P_{sum} = P_{sum} - P_{Bi}$
end for

4.4. Transaction Verification

Once the energy transmission is completed, all participants involved in this energy transaction will have their smart meters record the details of the energy transmission on PEMT-CoSim and the blockchain, and the seller will receive the corresponding transaction amount. By querying the smart meter readings on the blockchain, we can distinguish honest users and malicious users and update the reputation scores according to Equation (3).

5. Experiments and Analysis

In this section, we compare the experiment results for several case studies running on the co-simulation platform for energy trading to demonstrate the effectiveness of the proposed transactive energy market.

5.1. Simulation Set-Up

We implemented the proposed secure transactive energy market (STEM) on a computer with an Intel(R) Core(TM) i5-9500 CPU at 3.00 GHz and 16 GB of RAM using GO (go 1.15.8 Linux/amd64, Google, Mountain View, CA, USA), Python (Python 3.8.10, Python Software Foundation, Portland, OR, USA) and Node.js (v10.19.0, Node.js Foundation, Portland, OR, USA). We used the consortium chain Fabric (V 2.2.3) as the distributed ledger to store transaction information, electricity meter usage and reputation values.

Hyperledger Fabric is an open-source blockchain framework developed by IBM, comprising a world state and transaction logs. The world state is the database of the ledger. We stored transaction information, electricity meter usage and reputation values in the world state in the form of key-value pairs. Smart contracts in Fabric are also called chaincode. When external programs interact with Fabric, the smart contracts are invoked using command line interface (CLI) commands or the Software Development Kit (SDK, V 2.2.3) [30]. We used a Javascript interface written in Node.js to access the smart contracts published in Fabric.

Due to Fabric being a permissioned blockchain, although it supports tokens, it does not facilitate the issuance of commercial cryptocurrencies. To enable users holding Fabric tokens to make purchases outside the Fabric network, we opted for Ethereum. By utilizing a cross-chain exchange protocol [31], asset exchange between Fabric tokens and Ether can be achieved, catering to the broader purchasing needs of users.

The co-simulation used in the experiments was developed based on the Transactive Energy Simulation Platform (TESP V1.0.0). We initialized 32 houses for simulations, including an Unresponsive_Buyer (meaning an urgent need for electricity). The market cycle of the simulation was 300 s.

In these experiments, the reputation threshold R_{min} for user participation in the auction was set to $R_{min} = 0.1$. The value of the time period n was set to 5 and initialized as $\{0.05, 0.05, 0.05, 0.05, 0.05\}$ to ensure that the total reputation value R_n of honest users was greater than R_{min}. The reputation decay factor array was set to $\{0.1, 0.2, 0.4, 0.6, 0.8\}$. The value of S_{ca} was set to 0.1. In the double auction, if the price difference R_d between two bidders was less than USD 0.00001, then $Rank_{auction}$ was used to calculate the bidding scores. Please note that this price difference was quite small due to the sensitive energy unit price adopted in the simulation. In practice, this value can be adjusted to fit the system.

When the user participates in the energy trading market for the first time, user initialization smart contracts are used to authenticate the user's identity, register the wallet and register the smart meter ledger [7]. In addition, the user is initialized with the reputation value described above.

5.2. A Normal Case

This section presents a electricity trading situation without malicious users. Tables 2 and 3 display the sellers' and buyers' bidding information, respectively. The reputation values exceeding the auction reputation threshold $R_{min} = 0.5$ indicate that the participating houses in this round met the auction requirements.

Table 2. Normal seller bidding information in ascending order.

Seller	Quantity (kw · h)	Price (USD/kw· h)	Reputation
H22	3.0	0.00986157	0.368
H24	4.0	0.00994884	0.4972
H0	4.0	0.01026626	0.4970
H23	3.0	0.01029680	0.3869
H05	3.0	0.01036818	0.3869
H16	3.0	0.01042923	0.3869
H13	4.0	0.01084566	0.3743
H26	4.0	0.01085052	0.3785
H20	4.0	0.01089693	0.3048
H19	4.0	0.01091098	0.2747
H12	4.0	0.01091497	0.1763
H17	4.0	0.01101028	0.2621
H11	3.0	0.01102611	0.2898
H10	4.0	0.01141691	0.1767
H02	4.0	0.01147908	0.2252
H15	4.0	0.01173408	0.105

Table 3. Normal buyer bidding information in descending order.

Buyer	Quantity (kw· h)	Price (USD/kw· h)	Reputation
Unresponsive_Buyer	6.0	1.0	
H04	8.0	0.02744484	0.547
H28	5.0	0.02465901	0.4968
H01	8.0	0.02372708	0.6819
H07	5.0	0.01953452	0.5655
H18	5.0	0.01932851	0.6389
H03	5.0	0.01424168	0.8479
H14	5.0	0.01229886	0.7925
H21	5.0	0.01085663	0.105

Table 2 shows the detailed bidding information from all participating sellers. In particular, we highlighted two rows of data in red. Without reputation values, the price of H12 was higher than that of H19, and the auction ranking of H12 should have been above H19. However, with the introduction of the reputation scheme, the prices of H19 and H12 satisfied the adjacent price threshold *rd*. The set value *rd* not only ensured that the price remained the primary bidding sorting parameter but also considered the reputation values of the participants when the price was insufficient as the main parameter for bid sorting. This encourages users to engage in honest transactions. Consequently, we utilized Equation (6) to calculate $Rank_{auction}$ for H19 and H12. Subsequently, we rearranged their bidding order based on the ranking scores. Thus, as shown in Table 2, the auction ranking of H19 was higher than that of H12.

Subsequently, a double auction market clearance was conducted, and we obtained the market clearing prices and quantity from Figure 3. Based on the clearing results of the double auction, H10, H2 and H15 did not successfully bid in this round and were placed into the seller backup set FC_S. Similarly, H21 did not successfully bid in this round and was placed into the buyer backup set FC_B. The successful sellers and buyers in the auction were placed into sets C_S and C_B, respectively.

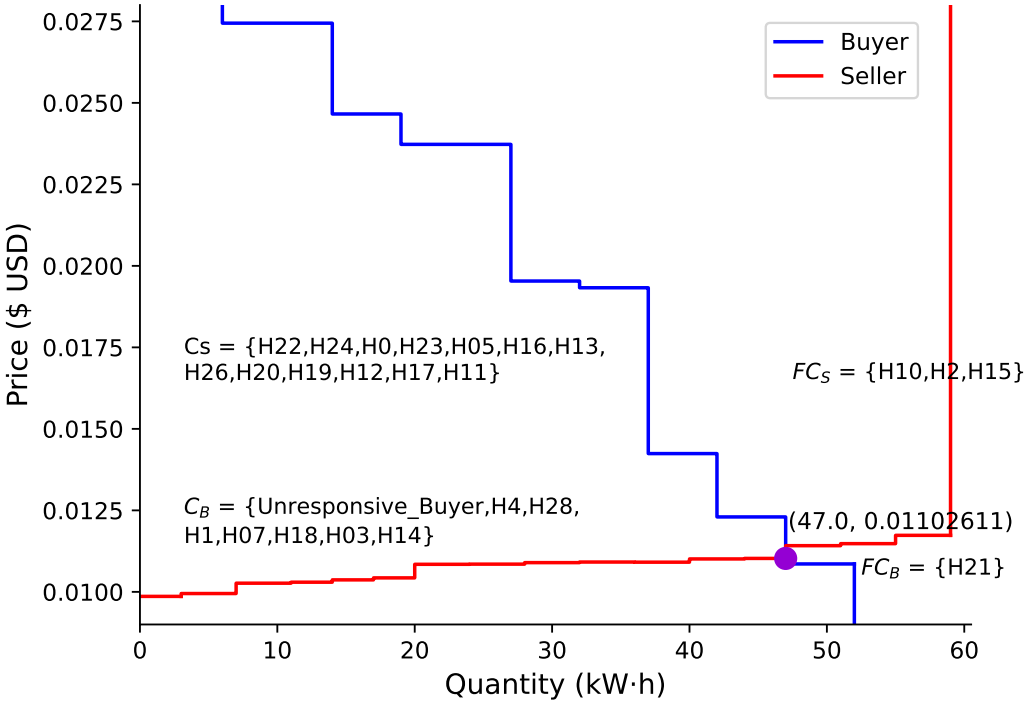

Figure 3. Market clearing price and quantity in the normal case.

5.3. Case of Misreporting of Electricity Prices

In this case, houses gather, organize electricity consumption and generate data to participate in energy bidding. During the energy trading auction phase, there is a risk of malicious users misreporting prices to disrupt the integrity of the transaction. In this auction scenario, we assumed that buyer H21 intentionally inflated the price to secure a favorable position in the seller rankings, and seller H15 intentionally reduced the price to secure a favorable position in the buyer rankings. The highlighted entries in Table 4 depict instances where H15 submitted a reduced price during the bidding phase to secure the top position among all participating sellers. Similarly, the highlighted entries in Table 5 illustrate cases where H21 submitted an increased price during the bidding phase to secure a high position among all participating buyers.

Following the market clearing in Figure 4, we observed noticeable changes in the clearing price and quantity compared with those in Figure 3. The results unequivocally indicate that the deceptive pricing actions of H15 and H21 impacted the clearing price and quantity, causing severe disruption to the transaction market.

According to Algorithm 1, after the smart contract detected H15 and H21's inability to pay the corresponding default penalty or prepayments, H15 and H21 should have been allocated to the seller backup set FC_S and buyer backup set FC_B, respectively. Following the rules of a double auction, new sellers and buyers were then supplemented from FC_B and FC_S, initiating a new round of a double auction. The second round of market clearance, as illustrated in Figure 3, aligned with the normal market clearance process, effectively thwarting this particular attack. Notably, the attack did not result in transaction failure, as the multi-round auction ensured the robustness of the transactions.

Table 4. Seller bidding information in ascending order with attack 1, having one seller attacker and a buyer attacker.

Seller	Quantity (kw· h)	Price (USD/kw· h)	Reputation
H15	4.0	0.00815842	0.105
H22	3.0	0.00986157	0.368
H24	4.0	0.00994884	0.4972
H0	4.0	0.01026626	0.4970
H23	3.0	0.01029680	0.3869
H05	3.0	0.01036818	0.3869
H16	3.0	0.01042923	0.3869
H13	4.0	0.01084566	0.3743
H26	4.0	0.01085052	0.3785
H20	4.0	0.01089693	0.3048
H19	4.0	0.0109109	0.2747
H12	4.0	0.01091497	0.1763
H17	4.0	0.01101028	0.2621
H11	3.0	0.01102611	0.2898
H10	4.0	0.01141691	0.1767
H02	4.0	0.01147908	0.2252

Table 5. Buyer bidding info in ascending order with attack 1, having one buyer attacker.

Buyer	Quantity (kw· h)	Price (USD/kw·h)	Reputation
Unresponsive_Buyer	6.0	1.0	
H21	5.0	0.028085663	0.105
H04	8.0	0.02744484	0.547
H28	5.0	0.02465901	0.4968
H01	8.0	0.02372708	0.6819
H07	5.0	0.01953452	0.5655
H18	5.0	0.01932851	0.6389
H03	5.0	0.01424168	0.8479
H14	5.0	0.01229886	0.7925

Based on the clearance results, we compared the seller's income and buyer's cost of our current round of transactions with the BCTE scheme proposed by Chen et al. [7]. Figures 5 and 6 illustrate the differences between the two schemes in terms of the seller's revenue and buyer's cost, respectively. When a false price reporting attack occurred, it can be observed that the proposed STEM yielded a higher average income and smaller variance compared with BCTE, where the average income of the buyers was higher due to malicious bidding leading to successful bids. However, malicious buyers can disrupt the energy trading market, causing harm to the respective interests of both buyers and sellers.

Table 6 presents bidding information in an auction where two sellers, attackers H15 and H02, misreported electricity prices. As all buyers participated in the transactions, the bidding information for the buyers remained as presented in Table 5. From Figure 7, it can be observed that the equilibrium price changed in a scenario where two sellers and one buyer acted as attackers. Due to the false reporting of electricity prices by H02, their ranking in the auction was higher, leading to a situation where, with unchanged buyer demand, H11 and H10 failed to successfully bid in this round. In comparison with a scenario involving one seller and one buyer as attackers, the scenario with two sellers and one buyer as attackers resulted in more severe disruptions to market transactions.

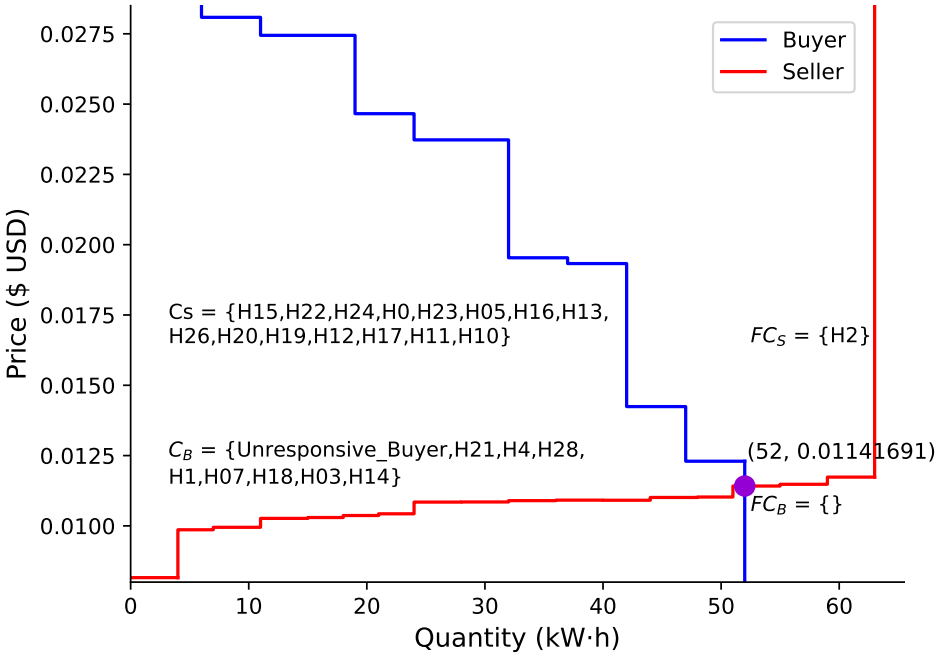

Figure 4. Market clearing price and quantity in the case of attack 1, with one seller attacker and one buyer attacker.

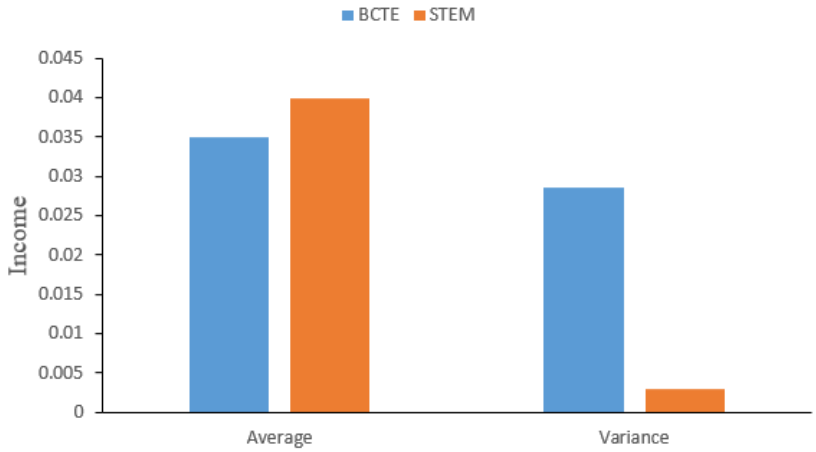

Figure 5. Seller income analysis and comparison.

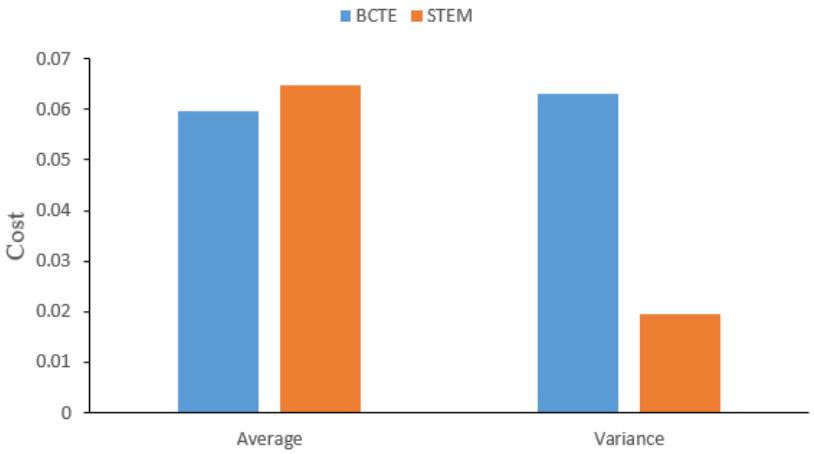

Figure 6. Buyer cost analysis and comparison.

Table 6. Seller bidding information in ascending order with attack 1, having two seller attackers.

Seller	Quantity (kw·h)	Price (USD/kw·h)	Reputation
H15	4.0	0.00815842	0.504
H02	4.0	0.00859642	0.2252
H22	3.0	0.00986157	0.368
H24	4.0	0.00994884	0.4972
H0	4.0	0.01026626	0.4970
H23	3.0	0.01029680	0.3869
H05	3.0	0.01036818	0.3869
H16	3.0	0.01042923	0.3869
H13	4.0	0.01084566	0.3743
H26	4.0	0.01085052	0.3785
H20	4.0	0.01089693	0.3048
H19	4.0	0.0109109	0.2747
H12	4.0	0.01091497	0.1763
H17	4.0	0.01101028	0.2621
H11	3.0	0.01102611	0.2898
H10	4.0	0.01141691	0.1767

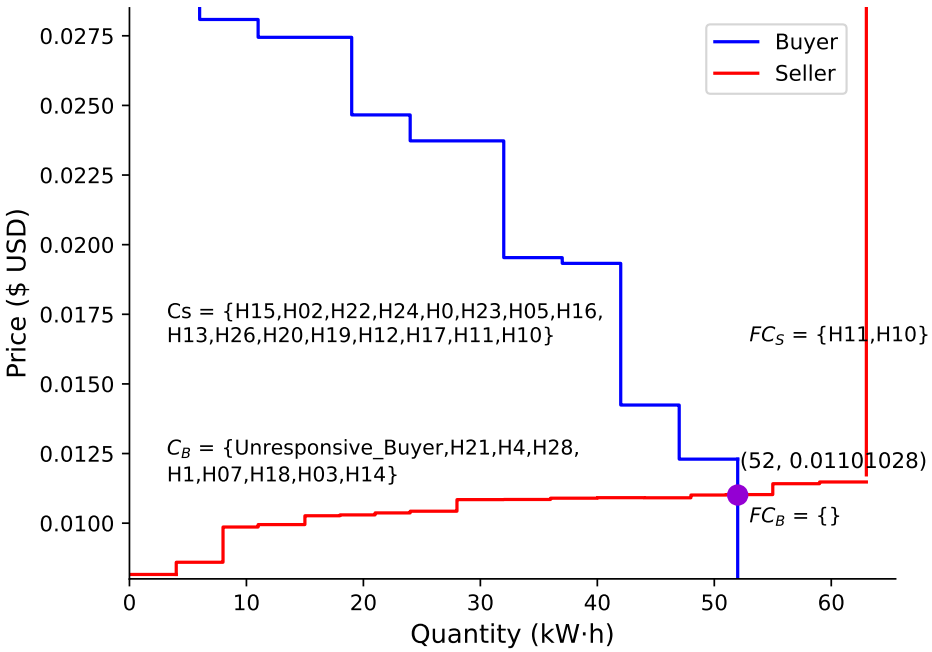

Figure 7. Market clearing price and quantity in the case of attack 1, with two seller attackers and one buyer attacker.

5.4. Case of Refusing to Pay

In this scenario, when the double auction bidding concludes, PEMT-CoSim stores the double auction market clearing results on the blockchain. Simultaneously, a smart contract on the blockchain is responsible for creating a shared wallet for buyers and sellers in sets C_S and C_B, respectively, and checks whether the buyers and sellers in sets C_S and C_B have stored the corresponding prepayment and default penalty on the blockchain. The successful bidders in C_S and C_B are expected to deposit the specified bidding amount or default penalty into the shared wallet to proceed smoothly to the following energy transmission phase. However, a malicious participant among the successful bidders may refuse to pay the bidding amount or default penalty, disrupting the transactions.

Assume that H24 in C_S is malicious. When the smart contract queries and identifies that H24 has failed to deposit the default penalty into the shared wallet, the next round of the double auction starts. From Figure 8, we can observe the results of the second round,

where H24 was removed from the buyer bidding set C_S. Simultaneously, since the price of H14 was higher than that of H10, H10 would be substituted into the buyer bidding set C_S from FC_S.

In cases where H24 acts as a malicious seller without adopting our scheme, the absence of any penalty constraints may result in H24 facing no substantive repercussions when failing to transmit energy during the energy transfer phase. The lack of our scheme could potentially incentivize sellers to refrain from energy transmission while still receiving a prepayment from the buyer. This poses a significant threat to the robustness of the transaction market.

The results demonstrate an effective defense against refusal to pay attacks, ensuring the transaction's robustness against potential financial defaults by individual users and safeguarding the interests of other users. Simultaneously, it facilitates the smooth progression of transactions without interruptions.

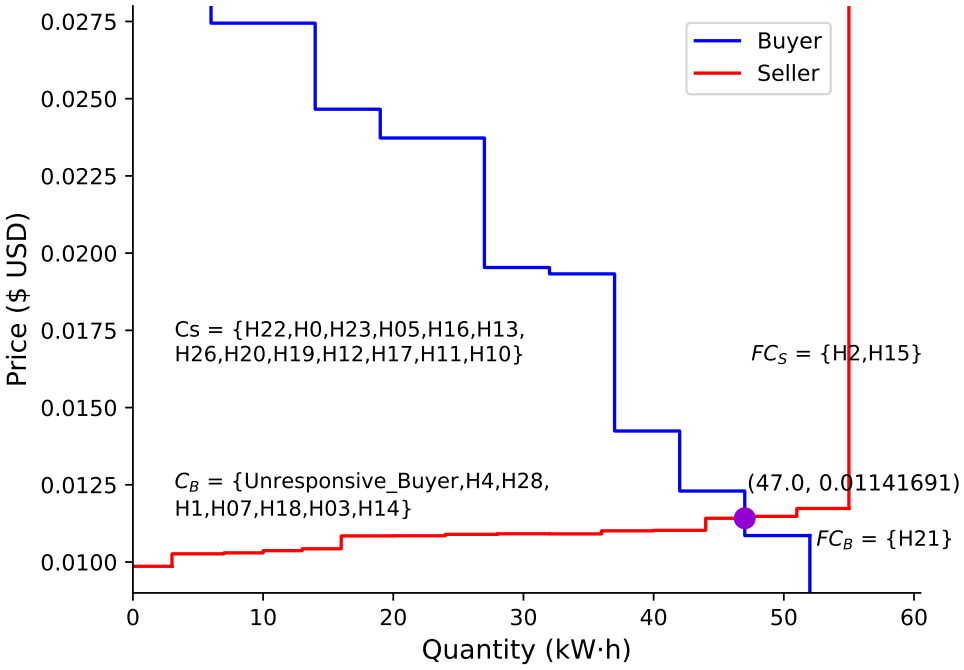

Figure 8. Market clearing price and quantity in the case of attack 2.

5.5. Case of Refusing to Transmit Energy

After completing the bidding phase and asset verification stage, the sellers in C_S need to transmit the energy quantity from the double auction bidding to the buyers in C_B. Although the sellers have already deposited the relevant default penalty into the shared wallet, some malicious sellers refuse to transfer the energy, disrupting the transaction. We assumed such an attack where H23 did not transmit energy.

Specifically, the energy transmitted by H23 was zero, and the smart meter of H23 uploaded the energy transmission result to the blockchain. During the transaction verification stage, the smart contract detected no related energy transmission information for H23 on the blockchain, identifying H23 as a malicious seller. Simultaneously, using Equation (2), the reputation of H23 was updated and stored on the blockchain. As a result, H23 would be penalized and might not be qualified to participate in future auctions. Figure 9 shows the energy transmission from the sellers in set C_S.

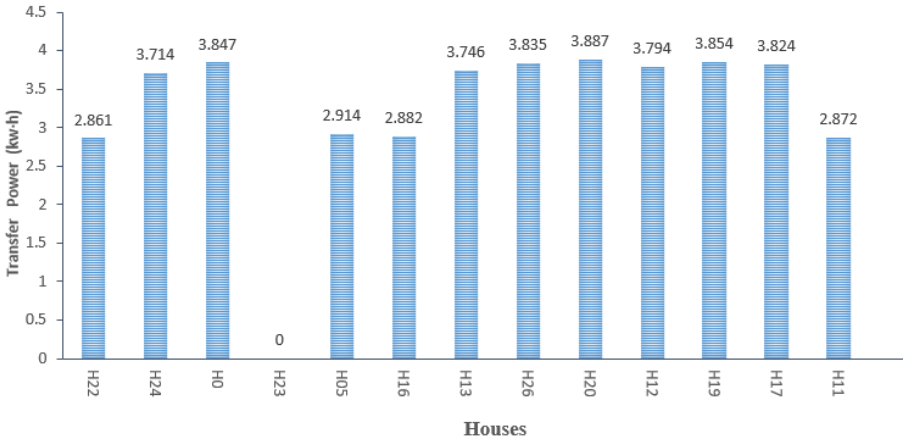

Figure 9. Energy transmission quantity of sellers.

6. Conclusions

Considering malicious attacks such as users misreporting electricity prices, refusing to pay and refusing to transmit energy in energy market transactions, we established a blockchain-based, reputation-aware secure transactive energy market (STEM) on top of the co-simulation platform PEMT-CoSim. We measured user credibility using a reputation scheme based on historical feedback and integrated the reputation scores into a double auction to incentivize honest user participation and restrict malicious user involvement. The market auction's robustness and security were improved through a backup mechanism employing a reputation-aware, multi-round double auction. Additionally, the combination of smart meters and a blockchain ensured that electricity transmission and consumption data recorded by smart meters were uploaded to the blockchain for subsequent transaction verification, preventing malicious attacks where sellers refused to transmit electricity.

Author Contributions: Methodology, P.Z., P.W. and Y.L. (Yuhong Liu); software, P.Z., P.W. and Y.L. (Yuanliang Li); formal analysis, P.Z. and Y.C.; resources, Y.C., Y.L. (Yuanliang Li), J.Y. and M.G.; writing—original draft, P.Z.; writing—review and editing, P.Z., P.W. and Y.L. (Yuhong Liu); supervision, P.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research has been partially supported by IEEE Blockchain Enabled Transactive Energy Initiative, and in part by Science and Technology Program Project of Shenzhen under Grant SZWD2021012.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Guerrero, J.; Gebbran, D.; Mhanna, S.; Chapman, A.C.; Verbič, G. Towards a transactive energy system for integration of distributed energy resources: Home energy management, distributed optimal power flow, and peer-to-peer energy trading. *Renew. Sustain. Energy Rev.* **2020**, *132*, 110000. [CrossRef]
2. Umar, A.; Kumar, D.; Ghose, T. Blockchain-based decentralized energy intra-trading with battery storage flexibility in a community microgrid system. *Appl. Energy* **2022**, *322*, 119544. [CrossRef]
3. Esmat, A.; de Vos, M.; Ghiassi-Farrokhfal, Y.; Palensky, P.; Epema, D. A novel decentralized platform for peer-to-peer energy trading market with blockchain technology. *Appl. Energy* **2021**, *282*, 116123. [CrossRef]
4. Gai, K.; Wu, Y.; Zhu, L.; Qiu, M.; Shen, M. Privacy-preserving energy trading using consortium blockchain in smart grid. *IEEE Trans. Ind. Inform.* **2019**, *15*, 3548–3558. [CrossRef]
5. Espinosa, L.A.D.; Almassalkhi, M. A packetized energy management macromodel with quality of service guarantees for demand-side resources. *IEEE Trans. Power Syst.* **2020**, *35*, 3660–3670. [CrossRef]
6. Almassalkhi, M.; Espinosa, L.D.; Hines, P.D.H.; Frolik, J.; Paudyal, S.; Amini, M. Asynchronous coordination of distributed energy resources with packetized energy management. In *Energy Markets and Responsive Grids: Modeling, Control, and Optimization*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 333–361.

7. Chen, Y.; Wu, P.; Li, Y.; Zhang, P.; Yan, J.; Ghafouri, M.; Liu, Y. A Blockchain-based Co-Simulation Platform for Transparent and Fair Energy Trading and Management. In Proceedings of the 5th ACM International Symposium on Blockchain and Secure Critical Infrastructure, Melbourne, VIC, Australia, 10–14 July 2023; pp. 95–104.
8. Trevathan, J. Getting into the mind of an "in-auction" fraud perpetrator. *Comput. Sci. Rev.* **2018**, *27*, 1–15. [CrossRef]
9. Li, Y.; Hou, L.; Du, H.; Yan, J.; Liu, Y.; Ghafouri, M.; Zhang, P. PEMT-CoSim: A Co-Simulation Platform for Packetized Energy Management and Trading in Distributed Energy Systems. In Proceedings of the 2022 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Singapore, 25–28 October 2022; IEEE: New York, NY, USA, 2022; pp. 96–102.
10. Zou, Y.; Xu, Y.; Feng, X.; Naayagi, R.; Soong, B.H. Transactive energy systems in active distribution networks: A comprehensive review. *Csee J. Power Energy Syst.* **2022**, *8*, 1302–1317.
11. Nizami, M.S.H.; Hossain, M.J.; Fernandez, E. Multiagent-based transactive energy management systems for residential buildings with distributed energy resources. *IEEE Trans. Ind. Inform.* **2019**, *16*, 1836–1847. [CrossRef]
12. Faqiry, M.N.; Das, S. Double auction with hidden user information: Application to energy transaction in microgrid. *IEEE Trans. Syst. Man Cybern. Syst.* **2018**, *49*, 2326–2339. [CrossRef]
13. Bokkisam, H.R.; Acharya, R.M.; Selvan, M. Framework of transactive energy market pool for community energy trading and demand response management using an auction-theoretic approach. *Int. J. Electr. Power Energy Syst.* **2022**, *137*, 107719. [CrossRef]
14. Lian, J.; Ren, H.; Sun, Y.; Hammerstrom, D.J. Performance evaluation for transactive energy systems using double-auction market. *IEEE Trans. Power Syst.* **2018**, *34*, 4128–4137. [CrossRef]
15. Nakamoto, S.; Bitcoin, A. A peer-to-peer electronic cash system. *Bitcoin* **2008**, *4*, 15.
16. Abdella, J.; Tari, Z.; Anwar, A.; Mahmood, A.; Han, F. An architecture and performance evaluation of blockchain-based peer-to-peer energy trading. *IEEE Trans. Smart Grid* **2021**, *12*, 3364–3378. [CrossRef]
17. Wongthongtham, P.; Marrable, D.; Abu-Salih, B.; Liu, X.; Morrison, G. Blockchain-enabled Peer-to-Peer energy trading. *Comput. Electr. Eng.* **2021**, *94*, 107299. [CrossRef]
18. Gai, K.; Wu, Y.; Zhu, L.; Xu, L.; Zhang, Y. Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks. *IEEE Internet Things J.* **2019**, *6*, 7992–8004. [CrossRef]
19. AlSkaif, T.; Crespo-Vazquez, J.L.; Sekuloski, M.; van Leeuwen, G.; Catalao, J.P. Blockchain-based fully peer-to-peer energy trading strategies for residential energy systems. *IEEE Trans. Ind. Inform.* **2021**, *18*, 231–241. [CrossRef]
20. Khalid, R.; Javaid, N.; Almogren, A.; Javed, M.U.; Javaid, S.; Zuair, M. A blockchain-based load balancing in decentralized hybrid P2P energy trading market in smart grid. *IEEE Access* **2020**, *8*, 47047–47062. [CrossRef]
21. Doan, H.T.; Cho, J.; Kim, D. Peer-to-peer energy trading in smart grid through blockchain: A double auction-based game theoretic approach. *IEEE Access* **2021**, *9*, 49206–49218. [CrossRef]
22. Govindaraj, R.; Govindaraj, P.; Chowdhury, S.; Kim, D.; Tran, D.T.; Le, A.N. A Review on Various Applications of Reputation Based Trust Management. *Int. J. Interact. Mob. Technol.* **2021**, *15*, 87–102.
23. Hendrikx, F.; Bubendorfer, K.; Chard, R. Reputation systems: A survey and taxonomy. *J. Parallel Distrib. Comput.* **2015**, *75*, 184–197. [CrossRef]
24. Hîrţan, L.A.; Dobre, C.; González-Vélez, H. Blockchain-based reputation for intelligent transportation systems. *Sensors* **2020**, *20*, 791. [CrossRef]
25. Almasoud, A.S.; Hussain, F.K.; Hussain, O.K. Smart contracts for blockchain-based reputation systems: A systematic literature review. *J. Netw. Comput. Appl.* **2020**, *170*, 102814. [CrossRef]
26. Wang, T.; Guo, J.; Ai, S.; Cao, J. RBT: A distributed reputation system for blockchain-based peer-to-peer energy trading with fairness consideration. *Appl. Energy* **2021**, *295*, 117056. [CrossRef]
27. Ullah, M.H.; Park, J.D. Peer-to-peer energy trading in transactive markets considering physical network constraints. *IEEE Trans. Smart Grid* **2021**, *12*, 3390–3403. [CrossRef]
28. Chae, Y.; DiPippo, L.C.; Sun, Y.L. Trust management for defending on-off attacks. *IEEE Trans. Parallel Distrib. Syst.* **2014**, *26*, 1178–1191. [CrossRef]
29. Dan, A.; Towsley, D. An approximate analysis of the LRU and FIFO buffer replacement schemes. In Proceedings of the 1990 ACM SIGMETRICS Conference on Measurement and Modeling of Computer Systems, Boulder, CO, USA, 22–25 May 1990; pp. 143–152.
30. Liu, H.; Han, D.; Li, D. Fabric-IoT: A blockchain-based access control system in IoT. *IEEE Access* **2020**, *8*, 18207–18218. [CrossRef]
31. Herlihy, M. Atomic cross-chain swaps. In Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing, Egham, UK, 23–27 July 2018; pp. 245–254.