sustainability

MDPI

Article

Design of a Secure Energy Trading Model Based on a Blockchain

Hoon Ko † **and Isabel Praça** *,†

Instituto Superior de Engenharia do Porto (ISEP)/Polytechnic of Porto (IPP), R. Dr. Antonio Bernardino de Almeida, 431, 4249-015 Porto, Portugal; hko@isep.ipp.pt

* Correspondence: icp@isep.ipp.pt

† These authors contributed equally to this work.

Abstract: This study proposes a Secure Energy Trading Model design based on a Blockchain is an attempt to overcome the weak security and instability of the current energy trading system. The focal point of the design lies in the user-security features of the model, such as user authentication and identification, and the blockchain that every transaction goes through. The user-security feature provides a safer system for peer-to-peer energy trade, and the blockchain technology ensures the reliability of the trading system. Furthermore, the Secure Energy Trading Model supports a decentralized data control mechanism as a future measure for handling vast amounts of data created by IoT.

Keywords: blockchain; peer-to-peer energy trade system; energy consumer; transaction

Citation: Ko, H.; Praça, I. Design of a Secure Energy Trading Model Based on a Blockchain. *Sustainability* **2021**, *13*, 1634. https://doi.org/10.3390/su13041634

Academic Editor: Eklas Hossain

Received: 2 December 2020

Accepted: 2 February 2021

Published: 3 February 2021

1. Introduction

Along with consumption, consumers have begun to take part in the overall process of the development and distribution in various industries. Simultaneously, the frontiers between suppliers and consumers are becoming more blurred [1]. Prosumer, a portmanteau of the words producer and consumer, was introduced as a futuristic concept by Alvin Toffler in 1980, and it is no longer a distant concept. In recent years, the traditional energy market system has shifted as increasing numbers of households have installed devices [1,2], such as solar panels, to generate their own electricity from renewable sources [3]. Meanwhile, a peer-to-peer energy trading system is gaining more recognition as an alternative version to the conventional energy market for consumers and producers [4,5]. The system requires a secure transaction agent for the varied types of producers and consumers. The blockchain-based Secure Energy Trade Model (SETM) proposed in this paper includes a producer/consumer module and a blockchain module that satisfies this need. The SETM consists of a transaction agent, which is a multi-interaction management agent (MiM agent), and a blockchain that contains cost information and a request/reply message. This model is connected to the consumer and the producer through an energy network. Over the course of this paper, we lay out the design of the blockchain-based secure energy trade model (SETM). In Section 2, we go through the issue statement, which is proceeded by the definition of the proposed SETM in Section 3. Then, the implementation of the SETM and a discussion with regards to the model is given in Sections 4 and 5, respectively. The paper is concluded in Section 6.

2. Background

2.1. Prosumer

Prosumer is a portmanteau of the words producer and consumer. In this case, an energy prosumer is a consumer that also generates their own energy [1]. Depending on the supply level, a prosumer can alternate between a consumer and a producer depending on a person's energy consumption and production. Various countries have different platforms that support energy trading activities between prosumers. The UK's web-based electricity trading platform "Piclo" connects electricity producers and consumers every 30 min to

trade energy [2]. The Netherlands operates "Vandebron", a web-based platform structured to accommodate interpersonal transactions. Germany operates an online platform that connects owners of solar power facilities who wish to sell their surplus energy to their neighbours [4].

2.2. Blockchain

A blockchain is a shared and distributed digital database structured by blocks chained in chronological order. Each block contains transaction data. Simply put, the structure is a ledger that includes digital transaction and data records [6]. It is a peer-to-peer distributed digital record of validated transactions. The technology is applied to establish reliability, accountability and transparency of transaction processes. It has the advantage of reducing the transaction processing cost and complexity [5]. In addition, it operates on a system based on the consensus of network users instead of a central authority that manages the system.

2.3. Problem Definition

Currently, energy is traded on an unreliable e-trade system that lacks security and stability. Despite its registration process, the system is prone to forgery and price tampering by its participants [7]. Without a user-security step, the blockchain can be accessed and opened for anyone to join a transaction. This means that the trade system is vulnerable to participants exploiting the system by trying to modify/block/interrupt transactions. In addition, the system's centralized data handling process is inadequate to keep up with the vast amount of data created by the ever increasing IoT [8]. A secure energy trading platform that can also process big data must be devised [9]. In response to the issue, an energy trading model with the integration of blockchain technology is proposed as a secure and stable platform that conforms to modern standards in the field. In [10], the authors suggest a blockchain-based secure service mechanism for IoT with a blockchain. The service code is protected by unreliable servers that are implicated in the seamless on-board computer network and with a blockchain [11]. The efficiency of the system for resource constrained devices is evaluated by the results of the simulation. However, neither a service charging mechanism nor a security mechanism for secure communication is considered. In [10], in the commercial warranty system, systems that do not fix security issues are vulnerable to data hijacking. A transparent computing network for a deportation system with a centralized and distributed architecture would be used for cost-effective communication. The servers are distributed in order to provide a necessary service and to arrive at the location. However, efficient deployment of servers that can enable IoT caching techniques is not considered. The authors introduced a blockchain based on Vehicular Network, which allows for the development of a distributed network in large vehicles [12]. However, a trust management system is required to ensure dependable communication. Generally, in V2V, each ID is used for communication purposes. However, it is vulnerable to privacy leakage problems.

3. Secure Energy Trading Model (SETM)

In this section, Figure 1 shows the SETM which explains the model configuration, including consumers, producers, request time, price of the transaction and the definition of an authentication and identification method of user security.

3.1. SETM Structure

In Figure 1, SETM consists of a consumer, a producer, a blockchain module, a multi-interaction management agent (MiM agent) and a blockchain for reliable multilateral transactions. The producer and the consumer in the model are a representation of a user interconnected in multiple forms. A prosumer may alternate between these two roles depending on the need. Users are granted roles only after authentication through a trusted server, such as *uA* and *uI*. Users are linked to each other in a grid, and they share the energy

they need or the energy they want to trade. Using the shared information, users request to buy the amount they need, and the seller receives these purchase requests. The energy transaction between these users with different roles is stored in a blockchain.

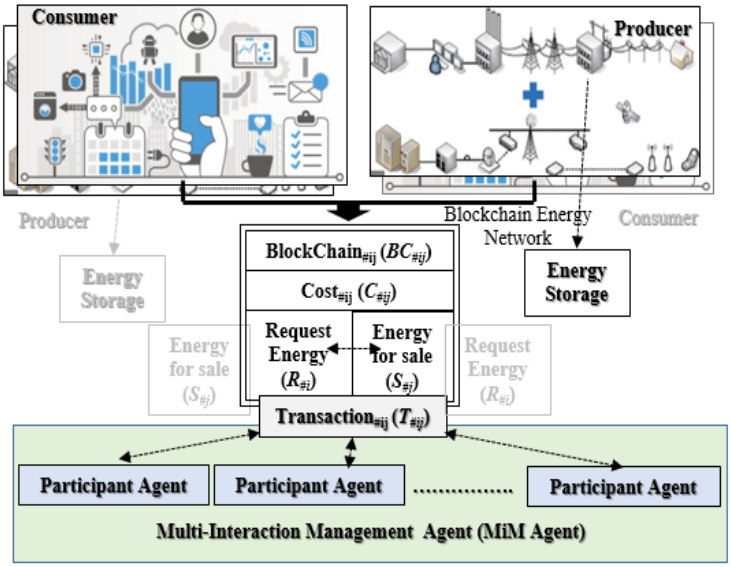

Figure 1. Secure Energy Trade Model (SETM) Structure.

3.2. Energy Market Mechanism

The SETM is connected to a blockchain energy network (BEN). The customer and/or the producer such as smart factories, energy companies, home solar systems, wearable devices, smart IoT devices, smart vehicles and personal offices are also connected to the BEN together (Figure 2). There is also a multi-interaction manager agent (MiM agent), which consists of the Web, customer service, a blockchain I/F and operation system. The MiM agent functions as a manager of the energy trade in the SETM. Each customer and each producer consist of a controller, device I/F, user I/F, blockchain module and operation system. In Figure 2, the energy company only produces energy. The home solar system can be either a consumer or a producer. A personal office, a smart factory, wearable devices, smart IoT devices and smart vehicles are customers. Generally all participants contact an MiM agent to monitor the current information. If one of the customers wish to buy energy, the customer contacts the MiM agent by sending 'request message'. If a producer wants to sell energy, the producer sends 'share message'. The 'share message' contains [available energy and cost]. Consumers have the option of choosing from these offers.

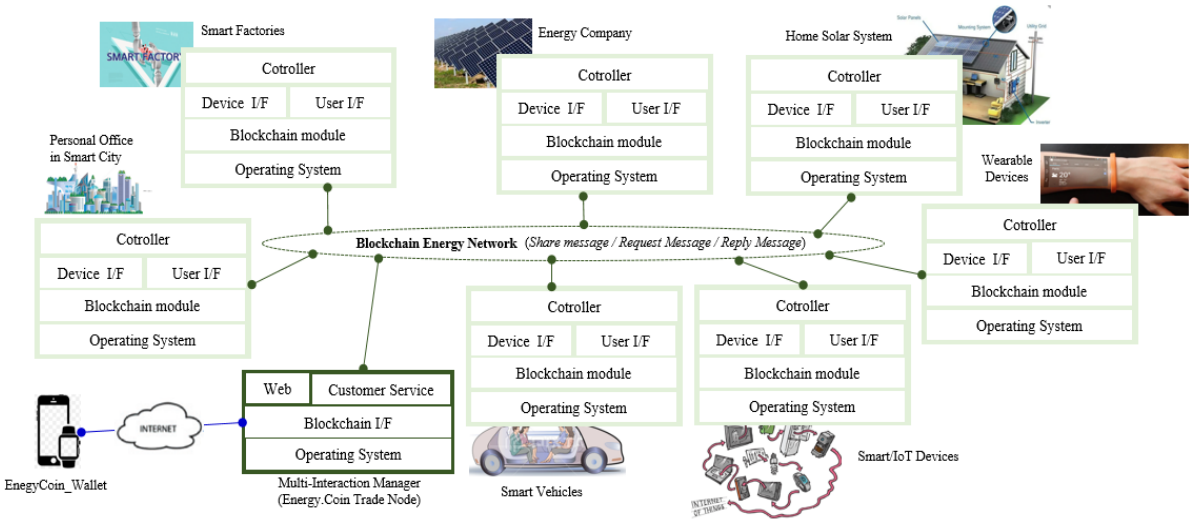

Figure 2. Blockchain energy market mechanism.

3.3. Messages Flow in SETM

All messages are sent through the energy network (Figure 3). The flow begins with participants, who have to go through the user.security step, user.Authentication *uA* and *uI*. As part of the model, user's security is a formal registration procedure a user must authenticate in order to participate in a transaction. The blockchain guarantees the safety/reliability of transactions, and the dependability of the decentralized database of each user is relatively weak. Each user is given a unique key that is stored on the server, and a mutual key is bestowed to users in a transaction (Figure 4). The mutual key verifies the reliability of the other party. Those that wish to sell on the SETM must enter their amount of energy and cost by sending a SHARE message to the model. Figure 3, depicts energy generators such as the solar system and the home solar system sending a SHARE message. Depending on supply levels, at times, the home solar system can sell surplus energy and vice versa. To buy the energy, buyers send a (request message) to acquire [available cost, amount available] from the SETM. With the (reply message) from the SETM, the buyer receives information, and the trade proceeds in the SETM. Figure 5 shows the process by which each transaction is linked to the blockchain. Each block contains information on the transaction. Information on the transaction includes information on energy shared by each vendor, information on buyers' purchases and information on each cost. The transaction information (*TI: 1, ..., n*) is defined as shown in Figure 5.

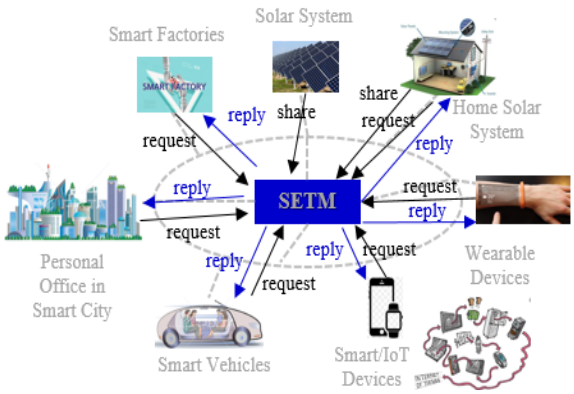

Figure 3. SETM flow in a blockchain energy network.

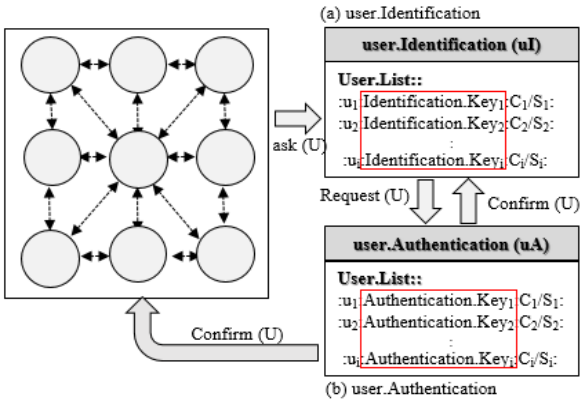

Figure 4. User Identification and user authentication.

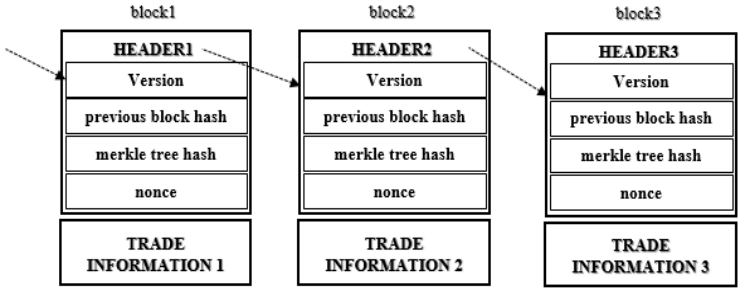

Figure 5. Blockchain structure of SETM.

4. Implementation

4.1. Case Study

For this case study, we use data from a local energy market with seven stakeholders ranging from consumers (both domestic and industrial), industrialists and producers. Each party has a usage and generation profile. In Table 1, we can see each member's min bid and max bid for energy.

Table 1. Case study.

Name	Days for Forecasting	min bid Euro/MWh	max bid Euro/MWh
personal consumer 1 (Home solar system)	9	34	46
personal consumer 2 (Wearable Devices)	4	34	46
personal consumer 3 (Smart Devices)	9	36	48
personal consumer 4 (Smart Vehicles)	18	36	48
personal consumer 5 (Personal Office)	8	38	48
industrial consumer 1 (Smart Factories)	1393	36	50
generation 1 (Solar System)	342	40	52

4.2. SETM Sequence Diagram

Figure 6 represents the sequence diagram for the SETM. In the figure, there are five personal consumers, one industrial consumer and one generation. The first transaction is initialized with the generation's SEND *Energy(x kW)* to personal customer 1. The SEND *Energy(x kW)* message contains *g*, *ep*, *message(1 kW)*. As soon as the message is sent, the *(Genesisblock Hash())* is created and treated as the first *hashblock*. Upon Personal Customer 1's

receipt, the process is ready for the next procedure, Initial.Tran(). Then, *message.Energy(xx kW)* is sent as a *forgeryblockhash*. *Initial.Tran()* now contains *g1* and *c1* data. Meanwhile, Customer 2 wants to partake in the transaction by processing the User Security Process. Generation 1 sends the same message *Energy (xx kW)* to Customer 2. Now, Personal Customer 2 can join the transaction by computing *blockhash* Figure 7. Industrial Customer 1 takes the same steps and the transaction is set at *Tran(g1, c1, c2, ic1*. In this model, we define *energy.Producer(eP), energy.Consumer(eC), energy.Request Time(eRT), energy.Price(ePr), Agreement Time(AT), user.Authentication(uA), and user.Identification(uI)* Algorithm 1 and in Algorithm 2. The TI_1 is considered the first blockchain of this block, followed by TI_2 as the next blockchain. put simply, TI_n is the nth block chain value. Price (Pr) is expressed in equations when there are two producers (g1, g2). Consumers are provided with the option to select from the variety of supply created by producers nearby. The resulting outcome of this variety leaves consumers to acquire energy at a competition reduced rate.

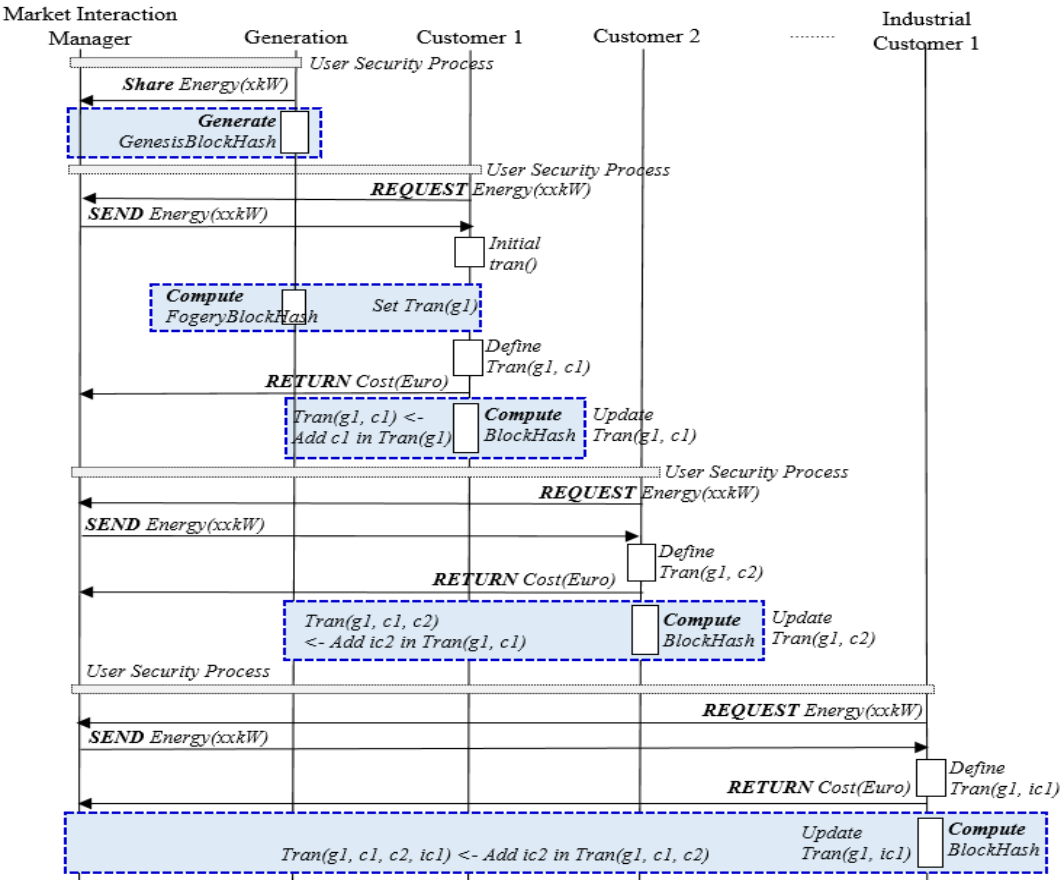

Figure 6. SETM sequence diagram.

Figure 7. Result of blockhash value.

Algorithm 1 user.SecurityAlgorithm

procedure USER.SECURITYALGORITH(a, b)
  for *Everytimeinablock* **do**
    $ask(U) \leftarrow user.Identification(uI)$
    $request(CONFIRM(U)) \leftarrow user.Authentication(uA)$
    $confirm(U)$ ▷ for askU and for the blockchain member
    if (**then**$\Delta h\_user \neq (uI \cdot uA)$)
      $Message(Thisiswronguser.)$
      $cancel(user.SecurityAlgorithm)$
      $returnERROR$
    end if
  end for
  $confirm(U)$ ▷ for askU and for the blockchain member
end procedure

5. Discussion

5.1. Model Compare

Unlike previous models, blockchain technology is integrated into the suggested SETM to ensure more secure energy transactions and privacy protection. The privacy of the payment system in the traditional model relies on the trust confirmation of a third party. Problems may occur in the traditional privacy model by attempts made to break the flow of information in some places. [Figure 8]. In comparison, the blockchain of the blockchain-based privacy model [Figure 9] involves the transaction information and all participants' information to do the payment.

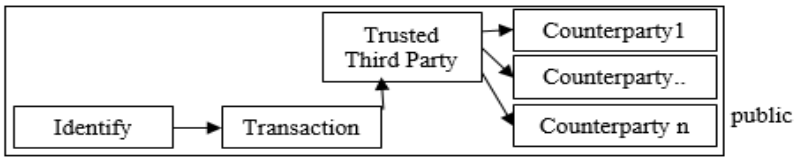

Figure 8. Traditional Privacy Model.

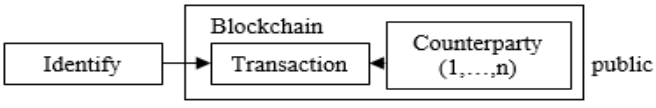

Figure 9. Blockchain-based privacy model.

The security of transactions is impossible compromise. Data Unforgeability is the decentralized nature of the consortium blockchain, which combined with digitally signed transactions, ensures that no adversary is able to pass as each node to corrupt the network. The digital signature of a node cannot be forged, nor can an adversary gain control over the majority of the network resources. The energy coin relies on digital signatures to prove ownership and public history of transactions to prevent double-spending. The transaction histories are going to be shared in the P2P network and will be conform to the proof-of-work methods. Digital Wallet Security, without corresponding keys and certificates, no adversary can open a prosumers (consumer and producer)' wallet and steal energy coins from the wallet. As each node has a unique wallet corresponding to its energy coin account. We use multiple wallet addresses as pseudonyms of this wallet for privacy protection.

Last, with the removal of the trusted intermediary, in our energy blockchain, each node trades energy in a P2P manner, which is unlike traditional centralized trading relying on a globally trusted intermediary. All nodes have the equal right to trade energy with the help of authorized prosumers. The energy blockchain is robust and scalable without the involvement of a globally trusted intermediary.

5.2. Security Analysis

Table 2 shows the comparison with existing research for security analysis. The security problem in [13] is that Unknown people can infer a user's electricity usage habits based on the data. The suggested model integrates the private blockchain and smart meters as a main technology and uses the market auction mechanism. In [14], they used a blockchain, smart meters and smart contract with a market auction mechanism; however, if the cost of each auction can be retrieved in the blockchain, the subsequent auction may be affected. There are lots of main technologies in [15] such as a blockchain, multiple signatures, and anonymous encrypted information flow. However, the multiple signatures would be an unnecessary process because the hash process in the blockchain can replace the signature. In [16], they include private information in all transactions, which can potentially pose a security problem. our suggested SETM uses a blockchain and IoT, and as the pricing mechanism, we defined negotiable energy prices and a multi-agent usage. In the security analysis, because the SETM has the *user.security* step, such as *user.authentication*n and *user.identification*, the SETM contains stronger privacy policy than existing studies Algorithm 2.

Table 2. Security analysis.

Ref.	Main Technologies	Pricing Mechanism	Security Analysis
[13]	private blockchain, smart meters	market auction mechanism	Unknown people can infer a user electricity usage habits based on the data.
[14]	blockchain, smart meters, smart contract	market auction mechanism	In case, the cost of each auction can be retrieved in the blockchain, the subsequent auction may be affected.
[15]	blockchain, multiple signatures, anonymous encrypted information flow	negotiate energy prices anonymously	Achieved many security and privacy requirements.
[5]	blockchain, IoT	adjust prices of electric energy according to the trading situation	nothing
[16]	blockchain	distributed pricing mechanism	include the private information in the transaction
SETM	blockchain, IoT	negotiable energy prices, multi-agent used	use the user security (user authentication and user identification

Algorithm 2 SETM.Transaction Algorithm

procedure TRANSACTION(a, b)
  $c \leftarrow consumer$
  $g \leftarrow generation$
  $ic \leftarrow industrialcustomer$
  $ic \leftarrow generation$
  $eP \leftarrow energy.Producer$
  $ec \leftarrow energy.Consumer$
  $eRT \leftarrow energy.RequestTime$
  $ePr \leftarrow energy.Price$
  $AT \leftarrow AgreementTime$
  $uA \leftarrow user.Authentication$
  $uI \leftarrow user.Identification$
  $Manager \leftarrow Energy.amount(kW)$ ▷ Keep continue
  if $REQUEST \leftarrow c.Amount(kW)$ **then**
    $c \leftarrow MiM.Amount(kW)$
    CASE1: $Initial.Transaction(g_i)$
      $COMPUTE(Fogery.BlockHash())$
      $GOTO\ payment.Transaction(g_i)$
    CASE2: $Define.Transaction(g_i)$
      $DEFINE(g_i, c_i)$
      $COMPUTE(BlockHash())$
      $ADD\ c_i\ to\ Define.Transaction(g_i)$
      $GOTO\ payment.Transaction(g_i, c_i)$
    CASE3: $Update.Transaction(g_i, c_i)$
      $COMPUTE(BlockHash())$
      $ADD\ c_i + 1\ to\ Define.Transaction(g_i, c_i)$
      $GOTO\ payment.Transaction(g_i, c_i, c_i + 1)$
  end if
  $Label : payment.Transaction$
  while $\int_{t=0} \infty (eP_i \cdot Pr_i)(eP_j \cdot Pr_j)$ **do**
    $Pi = (ti \cdot Pr_i)_1 (t_{i+1} \cdot Pr_{i+1})_1 \cdots$
    $P_{i+1} = (t_{i+1} \cdot Pr_{i+1})_{i+1} (t_{i+1} \cdot Pr_{i+1})_{i+1} \cdots$
    $Trade_i.SET = Negotiation.Pr(C_i, C_{i+1}, ..., C_{i+...})$
    $C_i set = Consumer.SET(C_i)$
  end while
  $h.SET_i = (Block_1(Version||hash \leftarrow merkle.tree.hash||nonce)$
  $block_i = (h.SET_i||Trade_i.SET)$
  $endLabel : payment.Transaction$
end procedure

We defined the security problems of the existing model in the Section 2.3 problem definition. We define how the SETM overcomes the security problems in Table 3, which is a security strength of SETM. In Table 3, there are four security problem definitions and security of strength was also analysed for each security problem.

Table 3. Security strength of SETM.

Security Problem	Security Strength
Lack security and stability	SETM applied *user.security = [uA, uI]* to all participants, so without *user.security*, no one can join the trade system. The *user.security* can keep the security in stability.
Vulnerable to forgery and price tampering	A blockchain in SETM prevents the forgery and the tampering in the transactions.
Vulnerable to participants exploiting the system by trying to modify/block/interrupt the transactions	If someone who has joined the trade system, modified the transaction, then the rules of the blockchain are broken. If the rules are broken, the trade system will be blocked.
Centralization of the data handling process is inadequate to keep track of the vast amount of data.	Basically, a blockchain is a peer-to-peer distributed digital record of validated transactions, not the centralized data handling.

6. Conclusions

In this paper, we have thoroughly reviewed the structure, the system and, specifically, the safeguards of the SETM. The security features integrated in the model make it more reliable than the conventional market and any other models suggested from existing studies. The structure of the SETM consists of a multi-interaction management agent (MiM agent) and a blockchain which contains the cost data, request and reply messages. The model is connected to the consumer party and the producer party through an energy network. The system begins with the producer registering the available energy amount for sale along with the price to the model. Consumers can choose and buy from these sellers. However, the model needs further adjustments. Despite the security and stability of the model, the applications of this model are yet unfit for bi-directional trades. Interested stakeholders' role in the model is confined to either as a consumer or a producer, and cannot be both, specifically a prosumer, for energy trade.

Author Contributions: H.K. leads this paper by suggesting the idea and has performed the implementation and I.P. managed the whole paper work. Both the authors have read and agreed to the published version of the manuscript.

Funding: This work has received funding from FEDER Funds through COMPETE program and from National Funds through FCT under the project SPET–PTDC/EEI-EEE/029165/2017.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

Abbreviations

The following abbreviations are used in this manuscript:

SETM	Secure Energy Trade Model
IoT	Internet of Things
5G	5 Generation

References

1. Kosnik, E. Production for consumption: Prosumer, citizen-consumer, and ethical consumption in a postgrowth context. *Econ. Anthropol.* **2018**, *5*, 123–134. [CrossRef]
2. Zafar, R.; Mahmood, A.; Razzaq, S.; Ali, W.; Naeem, U.; Shehzad, K. Prosumer based energy management and sharing in smart grid. *Renew. Sustain. Energy Rev.* **2018**, *82*, 1675–1684. [CrossRef]
3. Zhang, S.; Lee, J.H. A Group Signature and Authentication Scheme for Blockchain-Based Mobile-Edge Computing. *IEEE Internet Things J.* **2019**, *7*, 4557–4565. [CrossRef]
4. Hwang, J.; Choi, M.i.; Lee, T.; Jeon, S.; Kim, S.; Park, S.; Park, S. Energy prosumer business model using blockchain system to ensure transparency and safety. *Energy Procedia* **2017**, *141*, 194–198. [CrossRef]
5. Park, L.W.; Lee, S.; Chang, H. A sustainable home energy prosumer-chain methodology with energy tags over the blockchain. *Sustainability* **2018**, *10*, 658. [CrossRef]
6. Andoni, M.; Robu, V.; Flynn, D.; Abram, S.; Geach, D.; Jenkins, D.; McCallum, P.; Peacock, A. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renew. Sustain. Energy Rev.* **2019**, *10*, 143–174. [CrossRef]
7. Sultana, T.; Almogren, A.; Akbar, M.; Zuair, M.; Ullah, I.; Javaid, N. Data sharing system integrating access control mechanism using blockchain-based smart contracts for IoT devices. *Appl. Sci.* **2020**, *10*, 488. [CrossRef]
8. Yan, Z.; Lee, J.H. The road to DNS privacy. *Future Gener. Comput. Syst.* **2020**, *112*, 604–611. [CrossRef]
9. Guan, Z.; Lu, X.; Wang, N.; Wu, J.; Du, X.; Guizani, M. Towards secure and efficient energy trading in IIoT-enabled energy internet: A blockchain approach. *Future Gener. Comput. Syst.* **2020**, *110*, 686–695. [CrossRef]
10. Madhav, B.V.; Balu, S.B.; Laxman, W.S. Time Efficient Secure Negotiation in E-Trading. *IRE J.* **2019**, *2*.
11. Sharma, P.K.; Park, J.H. Blockchain based hybrid network architecture for the smart city. *Future Gener. Comput. Syst.* **2018**, *86*, 650–655. [CrossRef]
12. Liu, D.; Lee, J.H. CNN based Malicious Website Detection by Invalidating Multiple Web Spams. *IEEE Access* **2020**, *8*, 97258–97266. [CrossRef]
13. Mengelkamp, E.; Notheisen, B.; Beer, C.; Dauer, D.; Weinhardt, C. A blockchain-based smart grid: Towards sustainable local energy markets. *Comput. Sci. Res. Dev.* **2018**, *33*, 207–214. [CrossRef]
14. Hahn, A.; Singh, R.; Liu, C.C.; Chen, S. Smart contract-based campus demonstration of decentralized transactive energy auctions. In Proceedings of the 2017 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 23–26 April 2017; pp. 1–5.
15. Aitzhan, N.Z.; Svetinovic, D. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Trans. Dependable Secur. Comput.* **2016**, *15*, 840–852. [CrossRef]
16. Cheng, S.; Zeng, B.; Huang, Y. *Research on Application Model of Blockchain Technology in Distributed Electricity Market*; IOP Conference Series: Earth and Environmental Science; IOP Publishing: Bristol, UK, 2017; Volume 93, p. 012065.