applied sciences

MDPI

Article

Privacy-Preserving Electricity Trading for Connected Microgrids

Oriol Alàs † and Francesc Sebé *,†

Department of Mathematics, University of Lleida, C.Jaume II, 69, E-25001 Lleida, Spain; oriol.alas@udl.cat
* Correspondence: francesc.sebe@udl.cat; Tel.: +34-973-702-713
† These authors contributed equally to this work.

Abstract: The electricity market is evolving from the traditional unidirectional model into a bidirectional one in which households also generate and sell energy. This new scenario requires technology able to manage the available energy and guarantee that all the participants pay or are paid appropriately. Unfortunately, fine-grained monitoring of energy production and consumption makes it possible to infer sensitive information about confidential aspects of people's private life. In this paper, we propose a system designed for privacy-preserving electricity trading in a connected microgrid. The system guarantees that at the end of a billing period, the distribution system operator can compute the quantity to be charged or paid to each household while being unable to trace its consumption details.

Keywords: microgrid; privacy; security

1. Introduction

In the traditional way of managing electric power, electricity is generated at power plants by large-scale energy producers (EPs). That energy is transmitted through the high-voltage network by transmission system operators (TSOs) which deliver it to regional or local distribution system operators (DSOs). Finally, DSOs distribute the energy to the households which consume it.

In the last years, technology has made it feasible for consumers to act as small-scale producers by installing, for instance, solar panels on their roofs. When their production exceeds their individual demand, households can inject the excess of energy they produce into the grid. Consequently, households do not simply act as energy consumers, but they also produce and sell electricity, becoming prosumers. Smart meters are a fundamental component of this emerging scenario. These devices continuously monitor the energy that is being consumed or injected into the grid so that prosumers can be charged or retributed accordingly.

The integration of the energy grid with Internet technology opens the door to decentralized ways of managing an electricity market in a P2P fashion. Three different P2P trading scenarios are distinguished in [1]: over-the-grid trading (consumers remain fully connected to the main grid), partly independent microgrid (a community remains grid-connected for redundancy) and fully independent microgrid (isolated self-sufficient electricity network). The amount of electricity taken off the grid for consumption, and the amount of electricity being put on the grid by electricity generation assets need to match almost perfectly. This issue is investigated in [2], where the authors classify customers by their consumption patterns and investigate the way to optimize the capacity of distributed energy sources in order to ensure a proper demand supply balance. The survey presented in [3] analyses the research topics relevant for P2P energy trading and identifies six areas: trading platform, blockchain, game theory, simulation, optimization and algorithms.

Regarding the underpinning technology, blockchain has been widely proposed as a secure medium for electricity trade data management. The survey paper [4] reviews the scientific literature focusing on the application of blockchain in smart grids. Its authors

check for updates

Citation: Alàs, O.; Sebé, F. Privacy-Preserving Electricity Trading for Connected Microgrids. *Appl. Sci.* **2024**, *14*, 1458. https://doi.org/10.3390/app14041458

Academic Editors: Doug Arent, Adam Warren and Xiaolei Yang

Received: 10 January 2024
Revised: 1 February 2024
Accepted: 9 February 2024
Published: 10 February 2024

also review research projects and products. A more recent survey [5] focuses on the security and privacy protection techniques designed for energy trading in blockchain-based public networks.

On the flip side, Internet-based energy management comes at a cost in terms of security and privacy. The authors of [6] review the existing threats in smart grid networks and propose a taxonomy composed of three categories: threats to system-level security, threats to services and threats to privacy.

A smart grid connected to the Internet is exposed to threats resulting from cyberattacks aiming to play havoc with such critical infrastructure [7]. Regarding privacy, a fine-grained and automated management of electricity consumption and production enables unlawful monitoring and profiling of prosumers not only from external attackers but from energy market service providers as well [8]. In fact, NILM (nonintrusive load monitoring) techniques make it possible to detect the activation of common electrical appliances from an aggregated consumption trace [9]. These data lead to accurate knowledge on private information such as the time people go to work, come back home, or the days they are on holidays.

We claim that in order to preserve prosumers' privacy, the information collected and available to the electricity company should enable it to compute the bills while it must not be possible to infer detailed consumption or production traces from it.

In this paper, we present a privacy-preserving system for trading locally produced electricity in a scenario composed of geographically close prosumers in which production and consumption demands are matched. Such microgrid is connected to the global grid so that when the local production cannot meet the local demand, additional energy is fed. Furthermore, the microgrid can export energy in case of generation surplus. The proposal aims to minimize the information about production and consumption that can be inferred from the data exchanged during the trading process.

Since energy has to be paid for, energy offers and requests have to be processed in such a way that at the end of the billing period, the DSO can charge those prosumers who consumed more energy than produced and pay those who generated more than consumed. Obviously, the charged (or paid) sum has to be computed from the difference between the consumed energy and the produced one.

In our proposal, as in [10], electricity is traded through small pieces of energy that are paid by means of Chaum's [11] e-coin system. Anonymous energy offers and anonymous demands are continuously monitored by the DSO who makes the matchings. For each matching, the consumer makes a micropayment to the producer in the form of an anonymous digital cash transaction. The identity of the participants in each transaction is not revealed by the protocol.

At the end of the billing period, households are required to deposit the e-coins they are in possession of. Then, they will be charged (or paid) the sum of money corresponding to the difference between the withdrawn and the deposited e-coins. This is the only identified information learnt by the DSO about households.

Section 1 has introduced the paper. Next, Section 2 reviews existing related work and highlights the strong points of the new proposal. After that, Section 3 provides details on the assumptions made while designing the system. Then, Section 4 briefly introduces the employed cryptographic tools. The new proposal is detailed in Section 5, its privacy and security features are analysed in Section 6, while Section 7 presents some performance figures obtained from a simulator. Finally, Section 8 concludes the paper.

2. Related Work

The scientific literature has plenty of research papers addressing security and/or privacy issues in smart metering [12] and decentralized energy trading [13].

The authors in [10] present a proposal in which smart-grid users purchase electricity tokens (Chaum's e-coins) and use them to pay for the electricity they consume when submitting their measurement reports. Privacy requires trust in a third party, an aggregator,

who acts as an intermediary between smart meters and the utility provider. The proposal also enables the utility provider to purchase energy from users, but it does not consider trading among users.

Chaum's anonymous e-coin payments are also used in [14] in a system designed for customer-to-electricity-provider payments. Privacy preservation requires the presence of a trusted aggregator who prevents the operation centre from learning user consumption details. After analysing the proposal in depth, one can see that the proposal includes an additional actor, the bank, who can learn the consumption profile of every household from the e-coin withdrawal queries it receives.

This review continues by addressing proposals allowing energy trading among users.

The authors of [15] present a blockchain-based electricity trading platform. It includes the functionality to withdraw financial assets from an account managed by the DSO into anonymous addresses on the blockchain, where they can be transferred among addresses as a result of trade operations. Financial assets from the blockchain can later be deposited into an account. This solution prevents households from learning the real identity of the participants involved in each transaction. Unfortunately, all the identities are available to the DSO who is able to trace all the transactions carried out by each participant.

In [16], a decentralized privacy-preserving TTP-free energy trading system based on a broadcast channel for message interchange is proposed. Payments are made using the Bitcoin cryptocurrency. The system is designed to provide privacy by means of the use of pseudonyms that hide the real identity of the parties involved in each transaction. Unfortunately, Bitcoin payments make the system vulnerable to Bitcoin value fluctuations caused by events unrelated to the electricity market. In fact, those households that usually consume more electricity than they produce will regularly run out of Bitcoins and will need to acquire them through third parties at a difficult-to-predict price. Last but not least, blockchain-based cryptocurrencies allow some degree of traceability [17] since all the transactions are anonymous yet publicly accessible, so the real degree of privacy is difficult to assess.

A similar proposal was made in [18] where energy offers and demands are matched by a transaction server. Payments are made through a blockchain-based e-coin system that includes a bank actor able to trace all the payments. The security analysis made by the authors focuses on data integrity and authentication, while the privacy of consumption patterns is not addressed.

The authors in [19] propose a system which makes use of a permissioned blockchain for managing energy allocation transactions. Privacy and security are enforced by means of an identity validation mechanism based on the use of group signatures together with a pseudonym-based node identification system. In spite of considering privacy, the proposal does not address energy payments. Consequently, it is not clear whether privacy could be preserved after the inclusion a billing procedure.

Another blockchain-based proposal is presented in [20]. The participants in energy trading protect their privacy by using pseudonyms. After an offer-demand matching, the supply user sends their account information to the acquiring user. The paper does not address the fact that account information is a quasi-identifier which can be used for reidentification.

A blockchain-oriented energy trading system focused on privacy is detailed in [21]. Privacy is enforced through an encryption method which limits the nodes able to access each piece of trading information. In our opinion, the proposal does not fit in with a microgrid trading scenario in which all the nodes are potentially interested in purchasing each energy offer, so it is not clear in which way you can limit the recipients of each piece of trading information. Apart from that, the proposal does not refer to the way in which bills are calculated.

A similar proposal is given in [22]. The authors propose a blockchain-based three-layer architecture for energy trading in an auction market. The described system makes use of advanced cryptography in order to preserve the privacy of the participants. As in other

proposals reviewed in this section, the authors do not address the way in which electricity is paid for.

An auction electricity market constructed over blockchain technology is also proposed in [23]. Privacy and security are achieved by means of data encryption and digital signatures. The proposal includes parties able to decrypt bidding messages and also a trusted party able to revoke the anonymity of participants. In a real deployment, this would arise concerns about possible collusion among them. Each transaction involves a payment from the buyer to the seller, but no details about the privacy required in this step are mentioned.

Another energy trading system addressing privacy concerns is presented in [24]. The authors propose a blockchain-based transaction scheme in which the privacy of participants is preserved by reducing the data stored on the public blockchain. The paper focuses on optimizing the transactions among market participants by defining a problem regarding electricity pricing. Nevertheless, the paper does not address the way in which electricity is actually paid for and the privacy leakage resulting from the data collected in order to manage these payments.

After reviewing existing relevant proposals, this section is concluded by stating the strong points of the new proposal presented in this paper with respect to existing work:

- The system allows electricity transactions among households (feature not provided in [10,14]).
- Meter consumption and production privacy is provided without the need to trust any third party (unlike [10,14,15,18,20]) and with no risk of reidentification arising from the use of blockchain pseudonyms (unlike [16]).
- The system enables the computation of bills without compromising privacy (unlike [19,21–24]).

3. System and Attacker Models

This section describes the scenario and assumptions considered during the design of the presented system.

3.1. System Model

Our system considers a community of households composing a microgrid. Some of them are prosumers (they consume but also produce energy) and some others are consumers. The following assumptions underpin the proposed design:

- The system has to prioritize the consumption of nearby generated energy. In this way, households will, first of all, consume the energy generated by themselves. When this is not enough, they will try to acquire energy produced by other prosumers in their microgrid. Finally, they will consume energy injected from the global grid by the DSO.
- The overall consumption of dwellings can be higher than their aggregated production capability. In this way, the local community depends on a connection to the global grid.
- Privacy is a fundamental aspect. At the end of a billing period, the only information the service provider should learn about an individual household is the difference between its consumed energy and the one it produced so that it can be charged or paid accordingly.
- The considered microgrid is composed of a substation, managed by the DSO, and a group of households each equipped with a smart meter.
- The price of energy remains constant during a billing period.

The previous assumption about price stability is made just to simplify the description of the proposal. Variable prices could easily be accommodated by allowing a dynamic adjustment of the time component of the "power–time" tuples traded in the system (see Section 5.3). More precisely, a decrease (increase) of electricity price could be compensated by setting a longer (shorter) time during which power is provided by the seller and consumed by the requester.

3.2. Communication Channel

All the actors communicate through a shared broadcast channel. The substation and the meters are continuously monitoring the transmitted data and process those messages which are of their concern. Figure 1 shows the channel modelled as a shared bus. It can be implemented using wired (Ethernet or PLC) or wireless technology.

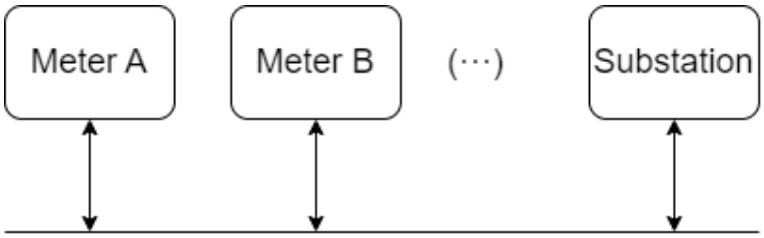

Figure 1. Microgrid communication channel model. The meters and the substation are assumed to communicate through a shared broadcast channel.

This channel allows both connection-oriented and connectionless communications. Connection-oriented communications are employed when authentication is needed for meters. That is the case for wallet loading (Section 5.4.1) and e-coin deposit at the end of a billing period (Section 5.4.4). Connectionless communications are used for the rest of communications in which meters act in an unidentified fashion.

In order to avoid external malicious interference, the messages sent through the channel are authenticated. All the meters and the substation share a secret key used for the HMAC authentication of messages at the data-link level. This mechanism prevents outsiders from disturbing the system by injecting fake data, while a shared-key mechanism authenticates the sender as a member of the microgrid without disclosing its identity. Store and reply attacks are prevented by appending a sequence number to messages. Throughout the paper, we do not refer to this underlying message authentication mechanism.

We also require the channel to be untraceable in the sense that it is not possible to determine the source of datagrams (unless some identifying data were included in them).

As for authenticated connection-oriented communications, an underlying secure protocol such as TLS is needed. It has to provide both sender and receiver authentication, data encryption and session hijacking avoidance.

Smart meters must include some sort of tamper-proof hardware preventing unauthorized access to the secret key material stored in them. The communication channel does not need to be connected to the global Internet. In this way, illegal access is much more difficult to achieve and limited in scope in case of success.

3.3. Attacker Model

Regarding the behaviour of the parties, our attacker model is based on the following two assumptions:

Assumption 1. *The substation is an honest-but-curious entity. It runs the protocols as specified but may try to analyse the data it has access to in order to infer individual information about the electricity consumption of households.*

Assumption 2. *Meters are semihonest entities. They do not disrupt the communication channel and consume and pour energy by following the protocol in a strict manner. Nevertheless, they may try to cheat in order to obtain free-of-charge e-coins.*

Regarding Assumption 1, an honest-but-curious substation is a reasonable assumption. Attempts to obtain private information by disturbing protocol execution may lead to deficiencies in the provided service with dire consequences for the company's reputation.

As to Assumption 2, in any electricity management system, the honesty of smart meters is mandatory. If they disrupted the communication channel, consumed energy in spite of not being allowed to, or they did not provide the energy they have agreed to supply, power shortages would occur. Such misbehaviours cannot be prevented by cryptographic means so they fall out of the scope of this paper.

3.4. Design Objectives

The presented system was designed in order to preserve the privacy of dwelling consumption patterns while providing an accurate billing. The objectives of the system are enumerated next:

Objectives 1. *Smart meters can offer and request energy in an anonymous and unlinkable manner.*

Objectives 2. *At the end of a billing period, the substation can determine the sum to be paid or charged to each household. No other private information about their consumption can be inferred.*

Note that Objective 2 implicitly requires the e-coin payment system to be secure. If e-coins could be forged or stolen, the quantities to be charged or paid could not be determined in an accurate way.

4. Cryptographic Background

This section briefly reviews the cryptographic primitives used by the proposed system. It also introduces the notation that is employed for its description.

4.1. Hash Functions

A hash function [25] is a deterministic procedure, denoted by $\mathcal{H}$, which receives an arbitrary bitstring as input (the message) and maps it into a fixed-length, usually between 160 and 256 bits, output (the digest). Let M be a message. We denote its digest as $\mathcal{H}(M)$. To be suitable for cryptographic purposes, a hash function must be both one-way and collision-free.

4.2. Public-Key Encryption

In public-key cryptography [26], each party possesses a key pair composed of a private key, which is kept secret, and a public key, which is made public.

Given a public key Pub, a message M can be encrypted into a ciphertext $\text{Enc}_{Pub}(M)$. Such a ciphertext can only be decrypted by a party possessing the corresponding private key.

4.3. Digital Signatures

In public-key cryptography, a party $\mathcal{P}$ possessing a key pair can compute digital signatures [27].

A digital signature of message M is usually computed over its hash digest, $\mathcal{H}(M)$, using the private key. The resulting signature, denoted as $\text{Sign}_{\mathcal{P}}(\mathcal{H}(\text{M}))$ is transmitted alongside message M and can be validated using the corresponding public key. Digital signatures provide integrity, authentication and nonrepudiation to M.

4.4. Blind Signatures

Blind signatures [11] are computed by running a protocol which involves two parties. One of them, Bob, possesses a key pair, while the other party, Alice, has a message M. After running the protocol, Alice obtains a digital signature from Bob over $\mathcal{H}(M)$, while Bob learns nothing about M nor the resulting signature $\text{Sign}_{Bob}(\mathcal{H}(M))$.

Such a protocol is run as follows. First of all, Alice takes $\mathcal{H}(M)$, blinds it using a random blinding factor and sends the blinded digest to Bob. Next, Bob signs the blinded digest and sends the result to Alice. Finally, Alice uses the blinding factor to transform the

data sent by Bob into a signature over $\mathcal{H}(M)$. This last step can only be performed by a person in possession of the blinding factor.

5. System Description

Our system fits in the "partly independent microgrid" model [1] in which prosumers are also connected to the main grid. In this setting, consumers and prosumers compose a community which builds a microgrid able to generate a portion of their energy requirements. This microgrid is connected to the central grid and asks for additional energy when the local production falls short.

In our proposal, as in [28], the meters and the substation (managed by the DSO) communicate among them through a broadcast channel.

5.1. Actors

The microgrid is composed of the following actors:

- Substation: This party is managed by the electricity provider (the DSO). It coordinates the trading system. It is in charge of matching electricity offers and demands. When required, it asks the global grid to pour additional electricity into the microgrid. In case of surplus, the excess of energy may be fed into the global grid. A microgrid includes just one substation.
- Smart meters: A dwelling is equipped with a smart meter which can both take or pour energy. It can also send and receive messages through the communication channel. When the individual production exceeds the individual demand, smart meters sell their surplus. Otherwise, they request and pay for additional energy.

5.2. Set Up

Before starting the system:

1. The substation generates a private–public key pair for some cryptosystem enabling the computation of blind signatures (RSA would be an option). This public key is certified in such a way that all the meters accept it as valid.
2. The substation generates a private–public key pair to be used for receiving encrypted data. The corresponding public key is also certified and made available to all the meters.
3. Each meter is provided a credential for identifying itself in connection-oriented communications. This may be a login–password pair or a public key certificate if TLS client authentication was used.

5.3. Basic Procedures

Electricity is traded in small pieces of energy specified as a "power–time" tuple. For instance, "10 W–10 min" (10 watts of energy for 10 min). There is only one type of piece whose content is set before the system starts to operate. Transactions in which an offered piece of energy is matched with an energy request are paid by means of an e-coin transaction. Each e-coin is worth the price of a piece of energy.

The basic procedures composing the trading system can be divided into:

- Procedures for e-coin transactions, namely, "withdrawal", "payment" and "deposit";
- Procedures for energy trading, namely, "offer", "request" and "pairing and payment".

These procedures are next explained in detail:

1. E-coin withdrawal. Each meter manages a digital wallet which stores e-coins. An e-coin is withdrawn as follows:
   (a) The meter generates a random bitstring which is the payload of the e-coin to be minted. Let us denote it as $Payload$.
   (b) The meter asks the substation to engage in an execution of a blind signature protocol in which $\mathcal{H}(Payload)$ is provided as input. As a result, the meter gets the substation's signature $\mathrm{Sign}_{SubT}(\mathcal{H}(Payload))$, while the substation learns nothing about $Payload$ nor its resulting signature.

(c) The generated e-coin is the tuple

$$C = \{Payload, \text{Sign}_{SubT}(\mathcal{H}(Payload))\}$$

which is stored by the meter.

As is explained later, in some situations, the meter identifies itself before running the withdrawal protocol, while in some others, it runs it anonymously.

2. E-coin payment. An e-coin payment from a payer to a payee is performed as follows:
   (a) The payer takes an unspent e-coin C and transmits it to the payee.
   (b) Upon receiving C, the payee parses it as $C = \{Payload, Signature\}$ and checks whether $Signature$ is a correct signature of $\mathcal{H}(Payload)$ under the substation's public key or not.
   (c) Next, the payee sends C to the substation so as to verify that it has not been spent before. Then, C is recorded as an already spent e-coin by the substation.
   (d) If the previous checkings are both satisfied, the payee will be allowed to withdraw a new e-coin free of charge. This action can be carried out anonymously.
3. E-coin deposit. An unspent e-coin can be deposited to the substation. This procedure is as follows:
   (a) The meter identifies itself and sends an e-coin C to the substation.
   (b) The substation validates its digital signature and checks it has not been spent or deposited before. Then, C is recorded as an already deposited e-coin.
   (c) Finally, the substation pays or records the amount to be paid to the meter.
4. Energy offer. When a smart meter detects that its dwelling has available energy which can be poured into the microgrid, it partitions it into energy pieces and announces their availability by broadcasting offer messages. Each available piece of energy is announced anonymously as follows:
   (a) The meter generates a random serial number, i.
   (b) The meter generates a random private key, $Priv_i$, and the corresponding public one, Pub_i.
   (c) The meter checks its internal clock and records the current time. Let us denote it as $TimeStamp$.
   (d) The meter generates the following offer message:

$$\text{Offer}_i = \{\text{“Offer”}, i, TimeStamp, Pub_i\}$$

   (e) This message is sent anonymously through the communication channel. The substation records it.
5. Energy request. When the energy produced locally in a dwelling is not enough to satisfy its internal demand, its smart meter sends energy request messages through the broadcast communication channel. It sends as many requests as needed in order to satisfy its demand. Each request message asks for a piece of energy. A request message is generated and sent as follows:
   (a) The meter generates a random serial number, j.
   (b) The meter generates the following request message:

$$\text{Request}_j = \{\text{“Request”}, j\}$$

   (c) This message is sent anonymously through the communication channel. The substation processes it at its reception.
6. Pairing and payment. The substation monitors all the offer and request messages. When a request, with index j, is received, and an offer, with index i, is available:

(a) The substation broadcasts a message indicating the offer–request pairing:

$$\text{Pairing}_{i,j} = \{\text{“Pairing”}, i, j, Pub_i\}$$

with Pub_i being the public key included in the paired offer message.

(b) Upon receiving it, the requesting smart meter takes an unspent e-coin, denoted by *Coin*, from its wallet and generates a random bitstring denoted by *Receipt*.

(c) Then, the requesting meter generates and broadcasts the following message:

$$\text{Payment}_{i,j} = \{\text{“Payment”}, i, j, Enc_{Pub_i}(Coin, Receipt), \mathcal{H}(Receipt)\}$$

(d) The meter who post the *i*th offer decrypts the ciphertext included in the previous message, extracts *Coin* from the resulting plaintext and checks the digital signature embedded in it. It also asks the substation to check whether *Coin* has been spent before by sending a message encrypted under the substation's public key, which includes a one-time ephemeral public key generated by the meter.

(e) If the previous checks are satisfied, the meter is allowed to withdraw a new e-coin (the e-coin sent as a payment has been recorded as spent by the substation). The message requesting the withdrawal of this new e-coin has to include a digital signature verifiable under the ephemeral public key sent in the previous step.

(f) Next, the meter broadcasts the following message:

$$\text{Receipt}_{i,j} = \{\text{“Receipt”}, i, j, Receipt\}$$

(g) The substation checks that the hash digest of *Receipt* matches the value $\mathcal{H}(Receipt)$ included in the $\text{Payment}_{i,j}$ message. In such a case, the transaction is completed.

(h) Finally, the substation removes the Offer_i message from the pool of available offers.

Figure 2 depicts the messages transmitted during the trading process. The process begins with a meter sending an “offer” message and another one sending a “request”. When the substation has received them, it starts an execution of the “pairing and payment” process. As a result of this process, the offering meter will pour energy into the microgrid which is consumed by the requesting meter.

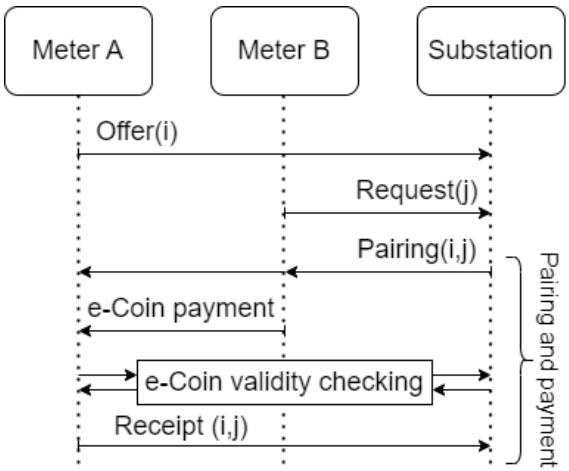

Figure 2. Messages exchanged during the trading process. The initial “offer” and “request” messages are paired by the substation. Next, an e-coin payment is made, and the validity of the coin is validated. Finally, the “receipt” message concludes a proper transaction.

5.4. System Operation

The following section describes how the previous basic procedures are run in order for the system to operate.

5.4.1. Wallet Loading

A short time before the beginning of a billing period, the meters have to load their wallets with e-coins. This is done as follows:

1. Each meter contacts the substation and requests a batch of e-coins by running the "e-coin withdrawal" procedure (Section 5.3, Procedure 1) as many times as needed. All the involved communications are carried out through an identified connection-oriented secure communication.
2. Each meter stores the acquired e-coins in its wallet.
3. The substation records the number of e-coins acquired by each meter.

The needed quantity of e-coins requested by a meter can be estimated from the previous billing period. If some meter runs out of e-coins before the end of the current billing period, it can request an additional batch.

5.4.2. Transmission and Management of Energy Offers

Energy offers are generated when a smart meter detects its household is generating more energy than consuming. In such case:

1. The smart meter partitions the available surplus into the established power–time pieces (for instance 10 W for 10 min) and each piece is announced through an offer message (Section 5.3, Procedure 4).
2. The substation records all the offer messages so that they can later be paired with energy requests. An offer message is valid during an established period of time (this is why offer messages are timestamped).
    - If that time elapses, and the offer has not been paired, it expires.
    - If its energy is still available, the offering meter generates and transmits a new offer message for it.

When an offer message is properly paired with a request (Section 5.3, Procedure 6):

1. The smart meter of the offering household has to put the established power into the grid during the established time.
2. When the supply time established as a result of a pairing is about to elapse:
    - If the supplied power is still available, the meter generates and sends a new offer.
    - Otherwise, when the supply time elapses, the meter stops pouring that energy into the grid.

The substation can establish a threshold so that when the number of available offers surpasses it, the substation generates and pairs energy requests by itself and then stores that energy or pours it into the global grid.

5.4.3. Transmission and Management of Energy Requests

When a smart meter detects its household needs more energy than it produces:

1. It generates and transmits as many energy requests (Section 5.3, Procedure 5) as required in order to meet its consumption needs.
2. Upon receiving a request, if there are available local offers, the substation pairs the request with an available offer.
    - During the pairing process, the requesting meter makes an e-coin payment for the acquired piece of energy.
    - After the pairing process has been completed, the requesting smart meter can take the acquired energy from the grid during the established time.

3. If there are no local offers in the microgrid, the substation generates an offer by itself and pairs it.
   - In such case, the energy is supplied from the global grid.
4. When the supply time established as a result of a pairing is about to elapse:
   - If the consuming meter expects to continue with that consumption of energy, it has to send a new request message.
   - Otherwise, when the supply time elapses, the meter has to stop consuming that energy from the grid.

5.4.4. Billing

At the end of a billing period:

1. The meters deposit all the unspent e-coins stored in their wallets (Section 5.3, Procedure 3).
   - All these deposits are carried out through identified connection-oriented secure communications.
   - The deposited e-coins can either be unspent coins acquired at the beginning or during the billing period, or coins received from paired energy offers.
2. For each meter, the substation computes the difference between the quantity of withdrawn e-coins and the number of deposited ones.
   - A positive difference determines the quantity to be charged on the next bill.
   - Meters with a negative difference are paid.

6. Privacy and Security Analysis

This section analyses the privacy and security of the proposal by means of a set of lemmas and theorems based on the properties provided by the employed cryptographic primitives (Section 4). Its validity is proven through verbal logic reasoning.

6.1. Privacy Analysis

The proposed system aims to prevent the substation from tracing the consumption habits of the households composing the microgrid. This is achieved by guaranteeing that the identity of the participants in each transaction remains unrevealed. The following lemmas and theorem prove it.

Lemma 1. *After an execution of the "e-coin withdrawal" protocol, the substation gets no information about the generated e-coin.*

Proof. When an e-coin is withdrawn, its payload is generated at random by the meter. Next, this payload is blindly signed by the substation. A blind signature protocol (Section 4.4) guarantees that the signer gets no information about the signed data nor about the resulting signature. Hence, the substation remains oblivious to the newly generated e-coin. □

Lemma 2. *An "offer" message cannot be related to the meter which transmitted it.*

Proof. An "offer" message just includes a random serial number, a timestamp, and a randomly created public key. None of these parameters can be related to the transmitting meter nor to previous offers generated by the same meter. □

Lemma 3. *A "request" message cannot be related to the meter which transmitted it.*

Proof. A "request" message only includes a random serial number which is unrelated to the transmitting meter. □

Theorem 1. *An execution of the "energy matching and payment" protocol does not reveal the identity of the involved meters.*

Proof. The mentioned protocol is run after the substation decides to pair an "offer" and a "request" message. As stated in Lemmas 2 and 3, none of these messages reveals the identity of the involved meters.

After the pairing has been announced by the substation, the requesting meter sends the "payment" message which includes an e-coin and a random piece of data (the "receipt"). From Lemma 1, we know that e-coins cannot be linked to the moment they were generated. Hence, this spent e-coin does not reveal the identity of the requesting meter. No additional action is performed by the requesting meter.

The offering meter checks the validity of the received coin against the substation by means of an anonymous message including the e-coin and an ephemeral public key generated at random. This way, the identity of the offering meter is not revealed as a result of this checking. Finally, the offering meter is allowed to withdraw a new e-coin. This operation is authenticated by including a digital signature verifiable under the previous ephemeral public key. Hence, its identity is not revealed at this step either.

The last message transmitted during the pairing procedure only includes the random *receipt* bitstring which keeps no relation with none of the involved meters. □

Lemmas 2 and 3 together with Theorem 1 ensure the fulfilment of Design Objective 1 (Section 3.4), which states that electricity should be traded in an anonymous and unlinkable manner.

Regarding Objective 2, when a meter loads its wallet, the meter is required to identify itself so that the substation can record the quantity of withdrawn e-coins. Also, at the end of a billing period, each meter identifies itself and deposits all the unspent e-coins available in its wallet. In this way, the substation can compute the amount to be charged or paid to each household from the difference between the withdrawn and deposited e-coins. For Objective 2 to be met, it has to be proven that the underlying e-coin system is secure in the sense that e-coins cannot be maliciously forged nor stolen among the meters. This security aspect is discussed next.

6.2. Security Analysis

Our system model assumes a message authentication mechanism preventing the injection of disturbing messages from outsiders. Regarding the parties composing the microgrid, the substation is assumed to be honest while meters may misbehave by trying to obtain free-of-charge e-coins. This section proves the security against this possibility by means of three lemmas and a conclusion theorem.

Lemma 4. *Illicit e-coins cannot be obtained while a wallet is being loaded.*

Proof. When the "withdrawal" procedure is being run as part of a wallet loading operation (Section 5.4.1), the procedure is run between a meter and the substation through an authenticated secure communication channel. Hence, no third party can gain any advantage from observing the encrypted communication.

Regarding the meter whose wallet is being loaded, it is required to authenticate itself, and the substation participates in the issuance of exactly as many blind signatures as the number of e-coins requested by the meter. That is the exact quantity of e-coins the requesting meter obtains. □

Lemma 5. *Illicit e-coins cannot be obtained while depositing e-coins.*

Proof. The "deposit" protocol, run at the end of a billing period (Section 5.4.4), is always executed through an authenticated secure channel. Hence, no third party can gain any advantage from observing the exchanged ciphertexts.

Each time an e-coin is deposited, that e-coin is recorded so that the substation rejects any attempt to deposit it again. Since e-coins cannot be forged, a meter can only deposit the exact quantity of e-coins it is in possession of. □

Lemma 6. *Illicit e-coins cannot be obtained from an execution of the "pairing and payment" procedure.*

Proof. During the execution of the "pairing and payment" procedure, the requesting meter transmits an e-coin to the offering one. That e-coin is then sent to the substation for checking. At that moment, the e-coin is recorded as already spent. In this way, the requesting meter cannot fraudulently use it as part of any other payment.

Next, the payee is allowed to anonymously withdraw a new e-coin. The payee meter is not required to identify itself, but the blind signature request has to include a digital signature verifiable under an ephemeral public key sent by the payee as part of the message asking for the verification of the e-coin received from the payer. This mechanism ensures that only the meter who checked the validity of the coin received as payment is able to withdraw a new e-coin.

Both the datagram in which the e-coin is transmitted from the payer to the payee and the datagram in which the e-coin is sent to the substation for validity checking are encrypted. In this way, third parties have no access to the e-coin and cannot try to use it for their own benefit. As for the newly minted e-coin, as stated before, only the payee can request it. The messages involved in this withdrawal operation do not need to be encrypted because the blinding factor (Section 4.4) required to obtain the digital signature over the new e-coin is only known to the payee. □

Theorem 2. *E-coins cannot be forged nor stolen among the meters.*

Proof. Lemmas 4–6 prove that e-coins cannot be fraudulently obtained while loading e-coins to a wallet, while depositing them, nor while making a payment as a result of a pairing between an energy offer and a request, respectively. These are the only procedures involving e-coins. □

7. Experimental Results

A simulator was implemented in order to test the correctness and feasibility of the system. It was developed in Sagemath 9.7 on Python 3.10 using its multiprocess features. The simulator was managed by a parent process which read the microgrid system configuration parameters (number of meters, production and consumption patterns, etc.) and then spawned a separate process for each smart meter as well as for the substation. The smart meters and the substation communicated asynchronously via a shared queue which simulated the communication channel. This queue was monitored in order to assess the performance of the communication system. For simplicity, we considered the communication channel allowed the transmission of a message every 30 ms independently of its length.

The consumption pattern for smart meters was taken from a data set containing real readings of electric power consumption in a household (https://www.kaggle.com/datasets/uciml/electric-power-consumption-data-set (accessed on 1 February 2024)). All the prosumers in the simulator followed the same consumption pattern. Regarding their production, we differentiated between type A (low producer) and type B (high producer). Diverse simulations were run by varying the number of type A (SM_A) and type B (SM_B) prosumers.

Figure 3 depicts the consumption and production patterns considered in our simulations. Production patterns were generated artificially in order to observe the system performance under different conditions. The simulated production patterns do not aim to consider real-world aspects like the absence of solar panel generation after sunset.

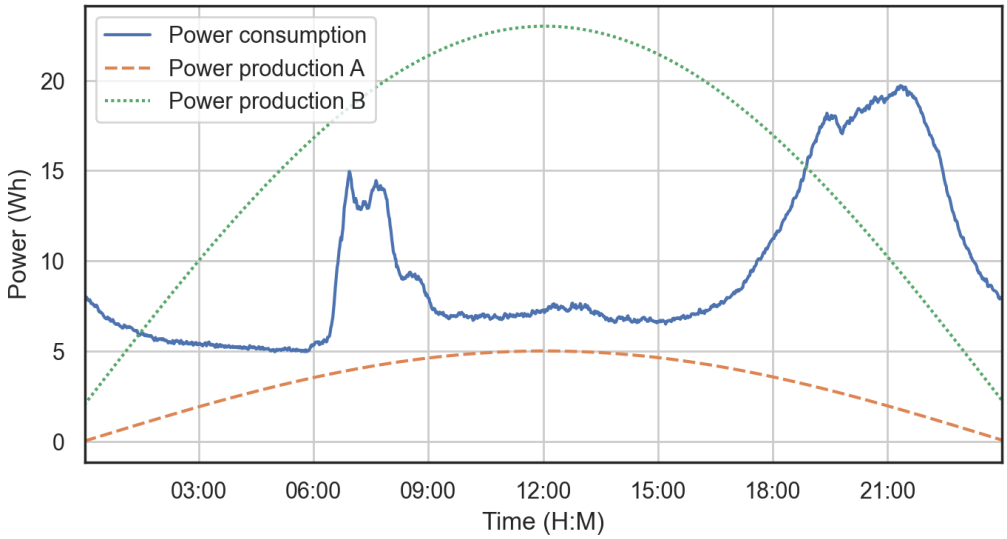

Figure 3. Consumption and production patterns for type A and B prosumers. Power consumption is assumed to be uniform across all smart meters.

Throughout the simulation, type A prosumers kept a low production profile with a varying consumption. As for type B prosumers, their behaviour was divided into five episodes:

- From 00:00 h to 06:00 h: low and stable consumption with a linearly growing production.
- From 06:00 to 09:00 h: consumption peak with a high and increasing production.
- From 09:00 h to 18:00 h: moderate and stable consumption with a high and stable production.
- From 18:00 h to 21:00 h: increasing consumption with a decreasing production.
- From 21:00 h to 00:00 h: decreasing production and consumption.

Figure 4 depicts the number of offers generated by the substation and the smart meters. It shows the way in which the system reacts to varying conditions. As expected, in periods in which the production of meters could not meet their overall demand, the substation generated offers for the electricity supplied from the global grid. It can also be observed that meters only transmitted offers during the simulation period in which their production was high.

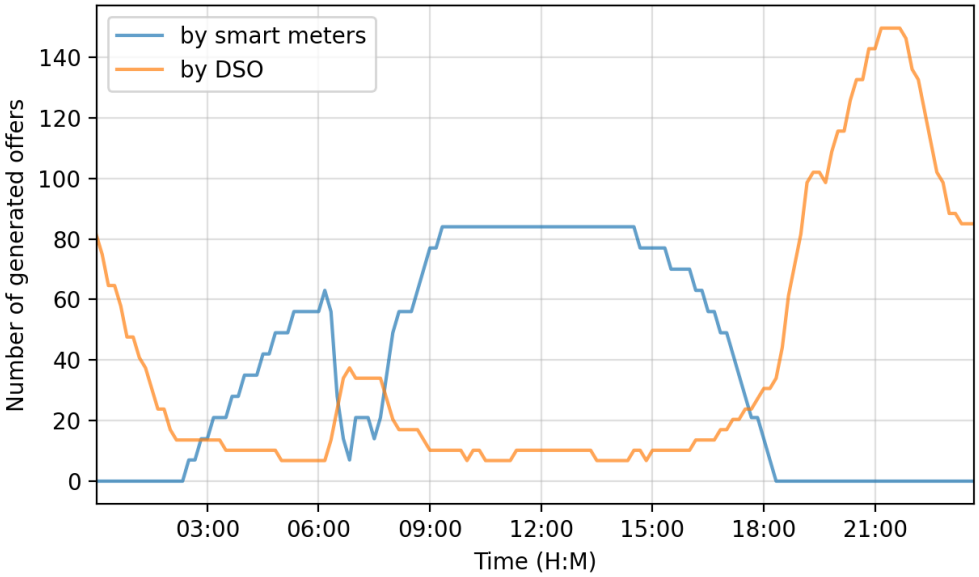

Figure 4. Number of offers generated by the smart meters and the substation in a simulated microgrid with parameters $SM_A = 6$ and $SM_B = 4$.

Our experiments also tracked the usage of the shared-bus communication channel. More specifically, the number of messages waiting to be sent was monitored. The simulator stored the messages to be sent in a queue whose size was monitored throughout the simulation. The size of that queue is depicted in Figure 5. As expected, the number of pending messages increased with the number of transactions, which was highly correlated with the number of offer messages. Figure 6 shows the average time between the transmission of a request message and the conclusion of the pairing process. As expected, this delay time was higher when the number of meters in the microgrid increased.

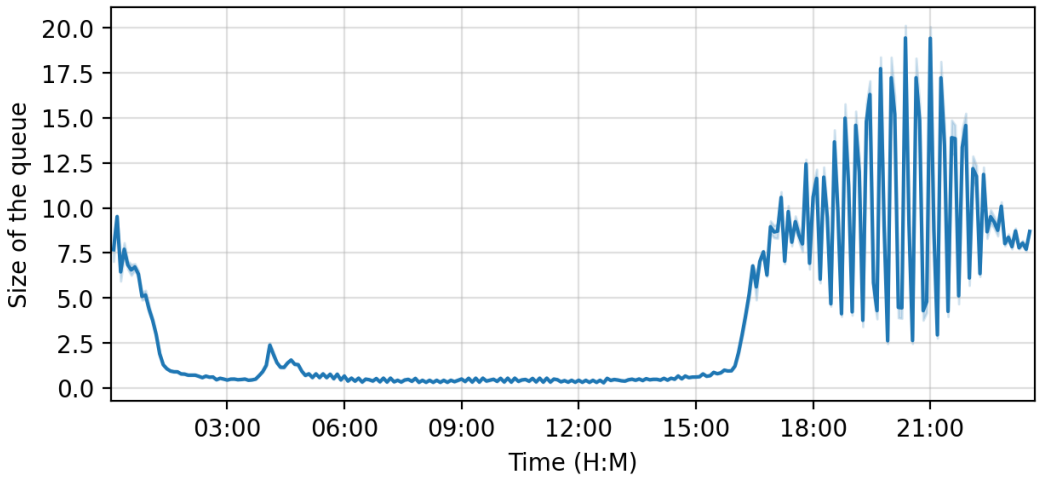

Figure 5. Evolution of the size of the simulator message queue in a simulated microgrid ($SM_A = 4$, $SM_B = 8$). A longer queue results in a higher message transmission delay.

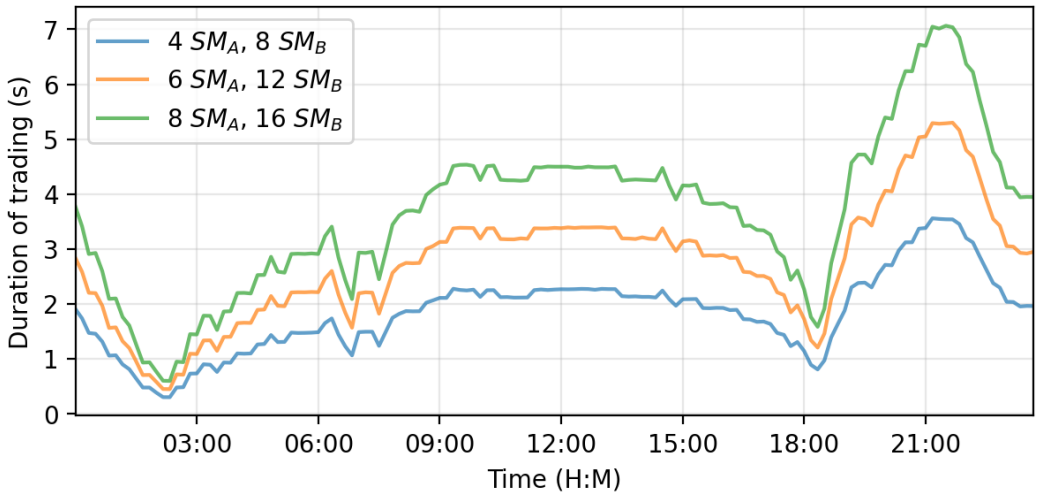

Figure 6. Evolution of transaction time in three different scenarios ($SM_A = 4$, $SM_B = 8$), ($SM_A = 6$, $SM_B = 12$) and ($SM_A = 8, SM_B = 16$).

Finally, we compared the difference between the time taken to conclude a transaction when the offer comes from a smart meter and when the offer comes from the substation. The average times are shown in Table 1. It can be observed that transactions were a bit faster (an average of 16.7% in all scenarios) when the substation was involved. This is due to the fact that the substation does not need to request the withdrawal of a new e-coin when it receives a payment, so the matching and payment process is faster.

We conclude that the results obtained from our simulator demonstrate the viability of the system. One of the critical factors contributing to its viability is its reduced transaction delay. Unlike blockchain systems, which often introduce substantial delays due to block

confirmation processes, our system achieves near-instantaneous transactions. Short processing times are crucial for real-time electricity trading, where efficiency and immediacy are of great importance.

Table 1. Average pairing time (in seconds) obtained from different simulations. The table differentiates between pairings involving the substation (offers by DSO) and pairings between two meters (offers by SMs).

SM_A	SM_B	Offers by *DSO*	Offers by *SMs*
2	4	0.639616	0.744040
4	8	1.251317	1.462731
6	12	1.869893	2.176571
8	16	2.475705	2.884149
10	20	3.092991	3.618586

The scalability of our proposal mainly depends on the capacity of the communication channel to transmit the data with short delay. Nowadays, a deployment using wired technology can accommodate gigabit data transmission rates ensuring a proper performance for quite a big microgrid.

We have not included a comparison with other existing proposals due to several reasons. First of all, because of the lack of availability of prototype implementations for them. Apart from that, other proposals focus on different objectives and make assumptions which would not allow a fair comparison. The contribution of our proposal comes from the provided features in terms of privacy and security. The experiments just aimed to prove its feasibility.

8. Conclusions

This paper presented a system enabling the management of electricity in a microgrid in which households can act as consumers as well as small-scale producers. By using cryptography, the proposal guaranteed the anonymity of the participants involved in each transaction in such a way that the service provider, at the end of a billing period, could compute the exact quantity to be charged or paid to each household while being unable to obtain information about its consumption habits.

The privacy and security of the system were proven. Its proper performance and accuracy were tested through simulations.

Author Contributions: Conceptualization, O.A. and F.S.; system design, F.S.; software, O.A.; formal analysis, F.S.; data curation, O.A.; writing—original draft preparation, F.S.; writing—review and editing, O.A.; funding acquisition, F.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Spanish Ministry of Science and Innovation (grant number PID2021-124613OB-I00).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The consumption pattern for smart meters was taken from a data set containing real readings of electric power consumption in a household available at https://www.kaggle.com/datasets/uciml/electric-power-consumption-data-set (accessed on 1 February 2024).

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

References

1. Raffaele, D.; Bolwerk, V.; ten Boske, L.; Tjallingii, I. Peer to Peer Energy Trading. Available online: https://www2.deloitte.com/nl/nl/pages/energy-resources-industrials/articles/peer-to-peer-energy-trading.html (accessed on 1 February 2024).
2. Long, C.; Wu, J.; Zhang, C.; Cheng, M.; Al-Wakeel, A. Feasibility of Peer-to-Peer Energy Trading in Low Voltage Electrical Distribution Networks. *Energy Procedia* **2017**, *105*, 2227–2232. [CrossRef]

3. Soto, E.A.; Bosman, L.B.; Wollega, E.; Leon-Salas, W.D. Peer-to-peer energy trading: A review of the literature. *Appl. Energy* **2021**, *283*, 116268. [CrossRef]
4. Mollah, M.B.; Zhao, J.; Niyato, D.; Lam, K.Y.; Zhang, X.; Ghias, A.M.Y.M.; Koh, L.H.; Yang, L. Blockchain for Future Smart Grid: A Comprehensive Survey. *IEEE Internet Things J.* **2021**, *8*, 18–43. [CrossRef]
5. Cao, Y.N.; Wang, Y.; Ding, Y.; Guo, Z.; Wu, Q.; Liang, H. Blockchain-empowered security and privacy protection technologies for smart grid. *Comput. Stand. Interfaces* **2023**, *85*, 103708. [CrossRef]
6. Kumar, P.; Lin, Y.; Bai, G.; Paverd, A.; Dong, J.S.; Martin, A. Smart Grid Metering Networks: A Survey on Security, Privacy and Open Research Issues. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2886–2927. [CrossRef]
7. Rekeraho, A.; Cotfas, D.T.; Cotfas, P.A.; Bălan, T.C.; Tuyishime, E.; Acheampong, R. Cybersecurity challenges in IoT-based smart renewable energy. *Int. J. Inf. Secur.* **2024**, *23*, 101–117. [CrossRef]
8. Rubio, J.E.; Alcaraz, C.; Lopez, J. Recommender System for Privacy-Preserving Solutions in Smart Metering. *Pervasive Mob. Comput.* **2017**, *41*, 205–218. [CrossRef]
9. Devlin, M.; Hayes, B.P. Non-Intrusive Load Monitoring using Electricity Smart Meter Data: A Deep Learning Approach. In Proceedings of the 2019 IEEE Power Energy Society General Meeting (PESGM), Atlanta, GA, USA, 4–8 August 2019; pp. 1–5. [CrossRef]
10. Dimitriou, T.; Karame, G. Privacy-Friendly Tasking and Trading of Energy in Smart Grids. In Proceedings of the 28th Annual ACM Symposium on Applied Computing (SAC '13), New York, NY, USA, 18–22 March 2013; pp. 652–659. [CrossRef]
11. Chaum, D. Blind Signatures for Untraceable Payments. In Proceedings of the Advances in Cryptology, Santa Barbara, CA, USA, 21–24 August 1983; Chaum, D., Rivest, R.L., Sherman, A.T., Eds.; Plenum Press: New York, NY, USA, 1983; pp. 199–203.
12. Karopoulos, G.; Ntantogian, C.; Xenakis, C. MASKER: Masking for privacy-preserving aggregation in the smart grid ecosystem. *Comput. Secur.* **2018**, *73*, 307–325. [CrossRef]
13. Samy, A.; Yu, H.; Zhang, H.; Zhang, G. SPETS: Secure and Privacy-Preserving Energy Trading System in Microgrid. *Sensors* **2021**, *21*, 8121. [CrossRef] [PubMed]
14. Fan, C.I.; Tseng, Y.F.; Huang, J.J.; Chen, Y.H.; Kuo, H.N. Verifiable Privacy-Preserving Payment Mechanism for Smart Grids. In Proceedings of the Internet and Distributed Computing Systems, Tokyo, Japan, 11–13 October 2018; Xiang, Y., Sun, J., Fortino, G., Guerrieri, A., Jung, J.J., Eds.; Springer: Cham, Switzerland, 2018; pp. 52–63.
15. Kvaternik, K.; Laszka, A.; Walker, M.; Schmidt, D.; Sturm, M.; Lehofer, M.; Dubey, A. Privacy-preserving platform for transactive energy systems. *arXiv* **2017**, arXiv:1709.09597.
16. 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.* **2018**, *15*, 840–852. [CrossRef]
17. Perlroth, N.; Griffith, E.; Benner, K. Pipeline Investigation Upends Idea That Bitcoin Is Untraceable. *The New York Times*, 2021. Available online: https://www.nytimes.com/2021/06/09/technology/bitcoin-untraceable-pipeline-ransomware.html (accessed on 10 June 2021).
18. Li, Z.; Kang, J.; Yu, R.; Ye, D.; Deng, Q.; Zhang, Y. Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things. *IEEE Trans. Ind. Inform.* **2018**, *14*, 3690–3700. [CrossRef]
19. 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]
20. Zhang, S.; Pu, M.; Wang, B.; Dong, B. A Privacy Protection Scheme of Microgrid Direct Electricity Transaction Based on Consortium Blockchain and Continuous Double Auction. *IEEE Access* **2019**, *7*, 151746–151753. [CrossRef]
21. Guan, Z.; Lu, X.; Yang, W.; Wu, L.; Wang, N.; Zhang, Z. Achieving efficient and Privacy-preserving energy trading based on blockchain and ABE in smart grid. *J. Parallel Distrib. Comput.* **2021**, *147*, 34–45. [CrossRef]
22. Wang, B.; Xu, L.; Wang, J. A privacy-preserving trading strategy for blockchain-based P2P electricity transactions. *Appl. Energy* **2023**, *335*, 120664. [CrossRef]
23. Zhang, S.; Guo, Y.; Wang, B. A Privacy Protection Scheme for Bidding Users of Peer-to-Peer Electricity Call Auction Trading in Microgrids. *IEEE Syst. J.* **2023**, *17*, 3316–3327. [CrossRef]
24. Wang, B.; Zhao, S.; Li, Y.; Wu, C.; Tan, J.; Li, H.; Yukita, K. Design of a privacy-preserving decentralized energy trading scheme in blockchain network environment. *Int. J. Electr. Power Energy Syst.* **2021**, *125*, 106465. [CrossRef]
25. Naor, M.; Yung, M. Universal One-Way Hash Functions and Their Cryptographic Applications. In Proceedings of the Twenty-First Annual ACM Symposium on Theory of Computing (STOC '89), Seattle, WA, USA, 14–17 May 1989; pp. 33–43. [CrossRef]
26. Katz, J.; Lindell, Y. *Introduction to Modern Cryptography*; CRC Press: Boca Raton, FL, USA, 2007.
27. Brazell, L. *Electronic Signatures and Identities: Law and Regulation*; Sweet & Maxwell: London, UK, 2018.
28. Sherman, A.T.; Phatak, D.; Sonawane, B.; Relan, V.G. Location authentication through Power Line Communication: Design, protocol, and analysis of a new out-of-band strategy. In Proceedings of the ISPLC2010, Rio de Janeiro, Brazil, 28–31 March 2010; pp. 279–284. [CrossRef]