energies

MDPI

Article

Towards a Blockchain-Based Peer-to-Peer Energy Marketplace

Yeray Mezquita [1,*], Ana Belén Gil-González [1], Angel Martín del Rey [2], Javier Prieto [1] and Juan Manuel Corchado [1]

[1] BISITE Research Group, University of Salamanca, 37007 Salamanca, Spain; abg@usal.es (A.B.G.-G.); javierp@usal.es (J.P.); corchado@usal.es (J.M.C.)
[2] Department of Applied Mathematics, Institute of Fundamental Physics and Mathematics, University of Salamanca, 37008 Salamanca, Spain; delrey@usal.es
* Correspondence: yeraymm@usal.es

Abstract: Blockchain technology is used as a distributed ledger to store and secure data and perform transactions between entities in smart grids. This paper proposes a platform based on blockchain technology and the multi-agent system paradigm to allow for the creation of an automated peer-to-peer electricity market in micro-grids. The use of a permissioned blockchain network has multiple benefits as it reduces transaction costs and enables micro-transactions. Moreover, an improvement in security is obtained, eliminating the single point of failure in the control and management of the platform along with creating the possibility to trace back the actions of the participants and a mechanism of identification. Furthermore, it provides the opportunity to create a decentralized and democratic energy market while complying with the current legislation and regulations on user privacy and data protection by incorporating Zero-Knowledge Proof protocols and ring signatures.

Keywords: blockchain; energy market; multi-agent system; negotiation; distributed ledger technology

Citation: Mezquita, Y.; Gil-González, A.B.; Martín del Rey, A.; Prieto, J.; Corchado, J.M. Towards a Blockchain-Based Peer-to-Peer Energy Marketplace. *Energies* **2022**, *15*, 3046. https://doi.org/10.3390/en15093046

Academic Editor: Mohamed Benbouzid

Received: 3 March 2022
Accepted: 19 April 2022
Published: 21 April 2022

1. Introduction

The current traditional power grid is designed to transport energy over long distances. This characteristic of the traditional system implies that certain limitations exist, such as the maximum voltage capacity supported by the distribution lines [1]. When this capacity is exceeded, the heat generated by a line can cause it to sag or break, resulting in power supply instabilities such as phase and voltage fluctuations. Because the capacity of a line depends on its length and the transmission voltage, one solution is to create shorter lines and distribute the functionalities of the current power grid in smaller smart networks. These networks are called smart micro-grids, which are a type of discrete energy system that includes appropriated energy sources as well as power loads that provide power to residential, commercial, industrial, and governmental consumers. The main purpose of smart micro-grids is to provide affordable energy to areas independently of the main power supply network while optimizing the transmission of the energy.

In the current context of energy generation, thanks to renewable sources such as solar or wind, and together with the emergence of a new type of actor that consumes and produces energy within the system—the so-called prosumers—micro-grids have the potential to replace the traditional energy transmission system in the near future [2]. However, the rise of smart micro-grids comes with some challenges that must be faced. These challenges range from the vulnerability of platforms to DDOS attacks, to the emergence of intermediaries that do not contribute to energy distribution but end up making it more expensive [3].

In the past, some authors have proposed strategies for energy management on micro-grid platforms. For example, in [4], the excess or shortage of energy could be compensated by exchanging it with the utility grid or other external sources. However, that paper did not allow for direct energy exchange between individuals, nor did it allow for the automation

and distribution of the platform. Without the use of blockchain technology, democratized energy markets could not be created. A blockchain network acts as a reliable distributed ledger that is governed by the platform and where information of value is stored. The network can be utilized to distribute the control and governance of the smart grid, along with the communication that is carried out within it, thus avoiding the single point of failure and eliminating those intermediaries that do not give any value to the platform. Moreover, blockchain technology (BT) provides a mechanism for protecting the actors against identity theft by signing direct communications between peers [5].

After studying the literature on this topic, it was found that none of the works had been able to propose a truly decentralized platform that enables peer-to-peer energy trading, automatically, and with dynamic prices. For this reason, we propose a distributed Multi-Agent System (MAS) based on blockchain technology to enable decentralized control over a micro-grid platform that allows for an automated exchange of energy between its actors. In the proposed system, the MAS manages the workflow of the micro-grid, e.g., the negotiations between peers in the local market, or the correct balancing of the energy network. By using a blockchain network, the control of the platform is distributed between the agents while the resilience of the communication channel between them is improved. This allows for the deployment of a platform without a single point of failure. Moreover, existing research works do not take into consideration users' anonymity and privacy, something that we would also like to tackle with the proposed framework.

This paper shows a thorough study of the most important features of blockchain technology and smart micro-grids in Section 2. Section 3 studies how previous works in the literature tackle the challenges of using blockchain technology in smart micro-grids. Furthermore, the section studies how automated negotiation between machines could be achieved and its viability. Section 4 describes the proposed platform, which is a combination of a MAS and a blockchain network for improved decentralization, as well as the security of the platform, along with the viability of the creation of a local automated energy market that optimizes the payoffs for the micro-grid stakeholders. Finally, Section 5 draws up conclusions and some final remarks on the conducted research.

Contributions

This work is relevant for designers, developers, and practitioners alike who are working in the field of energy distribution and renewable energy adoption and who will get the most benefits from the proposed framework. The main contributions of this paper are as follows:

- The design of a framework that will help developers to create new platforms that allow for the appearance of automatic peer-to-peer energy markets with dynamic prices.
- The proposed framework also provides user flexibility in the negotiation algorithms used. They will be able to implement the algorithm they want depending on their needs, with the only prerequisite being that the communications between agents follow the same ontology.
- The framework designed also provides anonymity to their users, complying with the current data regulations.
- Following the proposed framework, the future platforms developed and deployed will be more democratic and decentralized, thus eliminating the single point of failure.

2. Conceptual Foundations of Micro-Grid Platforms and Blockchain Technology

Traditional power grids deliver energy from a few central generators to a large number of consumers. This creates a closed market in which energy prices are dictated in a monopolistic way. Sometimes, to avoid abusive pricing by companies towards consumers, states need to implement regulatory measures, with the European Union [6,7] being an example in this case.

In the face of this monopolistic behavior, the literature has proposed the distribution of the traditional main grid into smaller micro-grids [2]. These micro-grids are comprised of a set of loads and generators. The set of generators can be composed of individual houses with solar panels on the roof. The entry of more entities into the energy market reduces the risk of oligopolies and avoids the intervention of states by imposing the use of regularization measures. This way, the energy market is converted into a more democratic market in which the offer and demand of energy will be the only factors that can regulate the energy price.

Micro-grid platforms make use of a great number of Internet of Things (IoT) devices that exchange crucial information between them. The continuous communication between the devices allows for the distribution of the management and control of any IoT platform. This helps with the optimization of the workflow of the system, but not without some drawbacks [8].

- Heavy reliance on exchanged messages. Since each part of the system is controlled by an independent entity, the other entities have to trust the messages received to understand the system's global state. If a malicious entity could somehow modify the content of those messages, the proper functioning of the entire platform would be compromised.
- Reliance on the truthfulness of the transmitted data. Entities of the platform have to rely on the fact that the data transmitted have not been tampered with by the sender entity to make an unfair profit. In addition, it is a possibility that databases will be attacked in order to steal, modify, or delete sensitive information about the entities that are taking part in the system's workflow.

In the literature, the use of BT has been proposed to overcome the listed flaws of this kind of platform. BT consists of a peer-to-peer (P2P) network of nodes, governed by a consensus algorithm that dictates how the information is stored within the network. This technology allows for the creation of a distributed ledger where anything of value can be stored.

The use of a blockchain network within any IoT system makes it possible to distribute the process workflow while eliminating other centralized entities [8]. In addition, by eliminating the single point of failure factor of centralized platforms, protection against some traditional forms of cyberattacks is gained. In this way, the blockchain is used as a bulletin where important information about the system is stored. Furthermore, the data stored within the blockchain network are kept in the same state after their storage, which means that the information is tamper-proof [9].

Within a blockchain-based system, a cryptographic mechanism of pairs of asymmetric keys is used, which signs and encrypts the data transmitted. Hence, as long as the blockchain network is big enough, the consensus algorithm keeps the information in a consistent state [10], the keys are not compromised, and the information transmitted and stored is secure from any attack, thus maintaining its integrity and authorship [11]. If this mechanism is also used in the exchange of messages between individuals of the system, then the messages are protected from being read and modified by unauthorized third parties [12].

A user needs to generate a random private key to make use of a blockchain protocol. This key is usually part of a cryptography mechanism that uses a key pair mechanism: the random private key mentioned and a public one derived from that. This public-key cryptography mechanism is used, not only because they allow for an efficient management of the keys, but also because it is impossible for an attacker to obtain the private key even when knowing the public one.

To interact with a blockchain protocol, an individual needs to generate at least one wallet address as an identifier. It is a three-step process, which starts with the generation of a random private key that only the owner should know. Then, through a one-way algorithmic transformation, the public key is obtained, which is shared with the network and is used to verify the signatures made by the user with their private key. Finally, the

public key is hashed in order to obtain the wallet address to be used in the exchange of virtual assets between individuals within the blockchain protocol.

The process of exchanging assets is quite straightforward and shares the same steps as in every blockchain. Figure 1 illustrates how a user, Alice, wants to initiate a transaction with Bob with 2 coins. To do that, Alice signs the transaction (Tx) with her private key and broadcasts it in the network. Then, each node of the network verifies Alice's signature with her public key, and if the check is correct and the transaction is proven to have come from Alice, the network validates that she has the coins she wants to spend. If everything goes well, the transaction will be added to the blockchain.

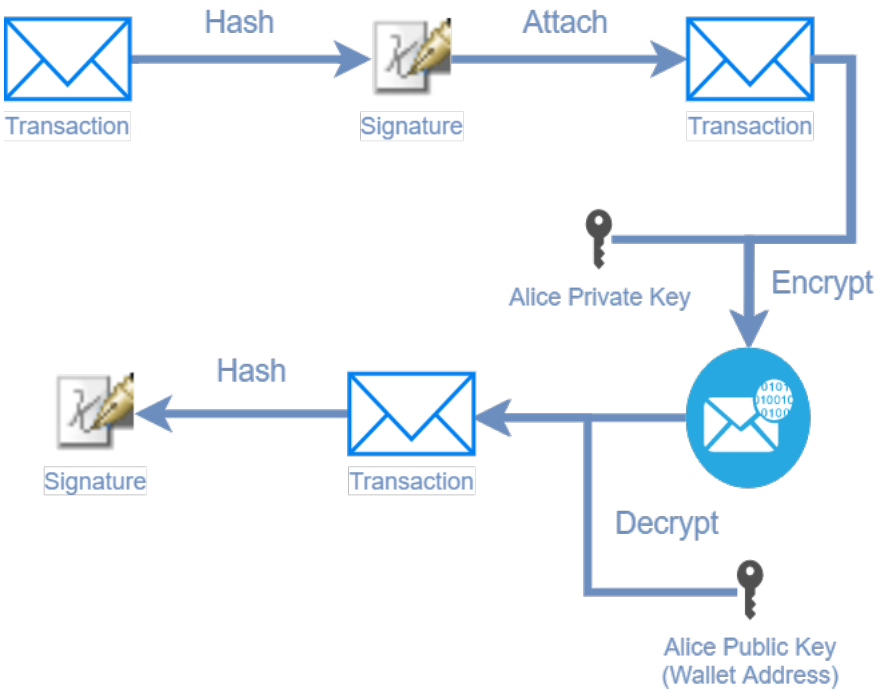

Figure 1. Example of the signature mechanism in a transaction.

2.1. Blockchain Consensus Algorithms

A consensus algorithm describes the mechanism that allows all agents in the system to coordinate in a distributed environment. It constitutes the only source of truth. Thanks to the consensus algorithm employed by the network of nodes, it is possible to keep the information stored and replicated in a consistent state. Among the functions of any consensus algorithm is ensuring that there is only one blockchain in the system, which can be an issue when a part of the network accepts a blockchain while the remaining nodes accept a different one (Fork). The consensus algorithm should enable the convergence of the chains into one as soon as possible. Moreover, it should offer resilience against attempts by malicious actors to take over the network and guarantee that there will not be any consensus failure when nodes try to add new blocks of data to the blockchain. Keeping the data stored in a blockchain makes it more difficult for attackers to take down the services of a system, and the attacker is forced to take down the majority of them to successfully hack the data [8].

There is a great variety of consensus algorithms, including the Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT) (see Table 1), or any of their variants that are the most widespread and have proven their effectiveness in practice [13].

Table 1. Comparison between consensus algorithms and their common usage.

Algorithm	Scalability	Consistency	Decentralization	Usage
PoW	No	Yes	Yes	Public blockchains
PoS	Yes	No	Yes	Public and permissioned blockchains
PBFT	Yes	Yes	No	Permissioned blockchains

PoW requires work to be performed by the miner and then verified by the network. The work required usually consists of the performance of a series of operations, algorithms, and mathematical calculations to be solved by the miners. These calculations vary and are different depending on the blockchain network they want to participate in. Each mathematical problem posed can only be solved by a very high computational calculation, which then encourages the nodes to behave in a certain way on the platform as compared with the simplicity of verifying the block mined. The greater problem of this algorithm is that a network using a consensus algorithm based on PoW wastes a massive amount of energy and is very slow. Therefore, it is not environmentally friendly and also not suitable for platforms that need to store information quickly [14].

PoS algorithms are based on the assumption that those who own more units of a PoS-based coin are especially interested in the survival and good functioning of the network that gives value to those coins. Therefore, they are the most suited to bearing the responsibility of protecting the system from possible attacks. That is why the protocol rewards them with lower difficulty in finding blocks (it is inversely proportional to the number of coins they prove to possess). The PoS algorithm has a theoretical vulnerability called the Nothing at Stake Theory, which has not been proven in practice. That theory states that forks in the blockchain network will occur more frequently [15].

In a PBFT consensus algorithm, all nodes communicate with each other, with the objective that honest nodes reach an agreement on the state of the system following the majority rule. Nodes not only have to verify that the message comes from a specific node, but they also have to verify that the message has not been tampered with. For the model to work, it is assumed that the number of simultaneous malicious nodes can never be equal to or greater than one-third of the total number of nodes. Therefore, the more nodes there are in the system, the more difficult it will be to reach that third. It is called practical in the sense that this proposal can work in asynchronous environments. This algorithm is used only in permissioned platforms and cannot be used in a public one, where nodes can access it freely [16].

In [17], the authors discussed the "blockchain trilemma", a term coined by Ethereum's founder Vitalik Butering to explain the problem of developing blockchain technology. According to this study, no blockchain satisfies the following three characteristics: scalability, consistency, and decentralization (see Table 1). For example, PoW solves the consistency and decentralization problems, but it lacks scalability. On the other hand, PoS can offer scalability and decentralization, but at the cost of consistency. Finally, PBFT-based algorithms can solve consistency problems while being scalable, but they centralize the process.

2.2. Blockchain Accessibility

The implementation of blockchain technology in the real world depends on the accessibility of the network underlying this kind of platform. If a player needs permission to be part of the blockchain network, it is said that it is a permissioned one. These kinds of networks are used in platforms where the actors are known, although they each have different interests. On the other hand, if anyone can be part of the network without requirements, the network is called a public blockchain.

A public blockchain, based on PoW, is less efficient in terms of reaching consensus and therefore managing transactions per second because it offers a truly decentralized ecosystem with proven security against attacks, with Bitcoin and Ethereum being their main representatives [10] (see Table 1). Public blockchains that make use of another consensus

algorithm, such as PoS or any of its variants, are far more efficient, although they lose some consistency. Blockchain networks that use PBFT-based consensus algorithms could only be used in permissioned environments because they lose decentralization in favor of scalability; to have consistency, it is required that the actors are known.

2.3. Smart Contracts

Another relevant aspect of some blockchain technologies is that they allow for the deployment and execution of coded scripts called smart contracts. Those scripts, due to the immutability feature of the blockchain technology, are considered self-enforcing and are used to automatize some processes, such as payments between entities within a platform that would otherwise need human intervention and/or that of third parties [18]. The code of smart contracts is transparent to the players that can make use of it, which means that they know the programmed clauses that rule it. Then, when those parties agree to use a smart contract, the workflow of the interactions between them is governed by the rules coded in the smart contract, all without the need for human hands to verify the process [19]. A smart contract ensures that the agreement will be carried out automatically when the conditions agreed upon are met [20].

3. Related Work on Micro-Grid Platforms Based on BT

Blockchain technology has been used to improve the performance of a broad range of platforms in today's industries. The state of the art encompasses, to enumerate a few examples, the pharmaceutical industry [21,22], the agri-food sector [23,24] as well as healthcare [8,25–27] and education services [28–30].

In this section, we will detail a small study on the state of the art related to the use of blockchain technology in the field of micro-grid platforms. Then, it will be followed by a study on the automatic negotiation algorithms that have been proposed in order to understand the requirements that need to be implemented in this type of platform.

3.1. Blockchain Technology and Micro-Grid Platforms

In the literature, we found some works that discussed the use of blockchain-based micro-grid platforms to create energy markets, focusing on specific characteristics such as the use of cryptocurrencies, decentralization, security, privacy, and state estimations [12,31–34].

Pichler et al. [35] studied real-world use cases of platforms based on blockchain technology and whose aim was to allow for the direct exchange of energy between its actors. The platforms studied have a general common aim: to create local markets based on renewable energy communities. However, they share the same cons: they do not try to create an autonomous market, and they do not offer real anonymity and privacy to their users (see Table 2).

A working example is the Pylon network [36], a Spanish startup that makes use of its permissioned blockchain-based Litecoin technology combined with a smart meter to certify energy flows and enable virtual transactions with the use of their own token. It makes use of a Proof of Cooperation (PoC) consensus algorithm, and its main aim is to create a neutral database, one that is not governed by the companies that sell the energy,in order to help the user decide how to optimize the energy costs. They made their platform open source to receive help from the community in case any kind of improvement is needed for their network. In Slovenia, SunContract [37] has created a market for peer-to-peer transactions of energy based on BT. They launched a crypto-asset within the Ethereum network in order to use it in the exchange of energy between the entities that are participating in the platform. On the other hand, there is Enosi [38], an Australian company whose aim is similar to that of SunContract: to create a community of peers transacting energy directly between them. By using smart metering, they trace, match, and settle energy production and consumption. Because of the platform, the producers can directly offer a price to the end consumer, with cheaper prices instead of the artificial ones that the power oligopolies have in the traditional energy market.

In the case of the Brooklyn micro-grid [39], LO3 developed the TransActive Grid elements (TAG-e), which allows for the exchange of energy between peers, the balancing of the grid, or the emergency management of the network. A TAG-e is composed of two elements: an electric meter and a computer. They are meant to read the information on the state of the grid and share it with other TAG-e in order to act upon the collected information. The market created with this platform allows for the trading of energy between peers with fixed prices; however, automatic negotiations within it are not permitted.

Table 2. Comparison of the studied startups.

Project	Description	Pros	Cons
Pylon Network [36]	The main aim is to create a neutral database. Makes use of its permissioned blockchain-based Litecoin technology. It makes use of a Proof of Cooperation (PoC) consensus algorithm. In addition, a smart meter (METRON) certifies energy flows and enables virtual transactions using their own token.	• Open source • Scalable • Latency • Improve prices	• Nothing about user's data privacy • It is not designed to create an autonomous market
SunContract [37]	The main aim is to create a marketplace that allows customers to trade energy without the need for intermediaries. They managed a market for P2P energy transactions based on BT for more than 2 years. They enable virtual energy transactions using their own token.	• Scalable • Latency • Improve prices	• Nothing about user's data privacy • It is not designed to create an autonomous market
Enosi [38]	Their main aim is to create a marketplace that allows the energy customers to trade energy without the need for intermediaries. They certify energy flows via smart metering.	• Scalable • Latency • Improve prices	• Nothing about user's data privacy • It is not designed to create an autonomous market
Brooklyn Micro-grid Network [39]	This project created a local energy marketplace in Brooklyn. Bacuase of it, prosumers can trade their energy surplus with their neighbors.	• Scalable • Latency • Improve prices	• Nothing about user's data privacy • It is not designed to create an autonomous market

3.2. Negotiation Algorithms on BT-Based Micro-Grid Platforms

Due to the increase in the production of renewable energy, grid consumers need to be flexible in adjusting their energy consumption. This adjustment occurs through different demand response mechanisms: either by reducing electricity consumption during hours where the global consumption is at its highest (peak hours) or by discouraging the consumption during those hours by affecting the prices with financial incentives. Regarding the last demand response mechanism, it is possible to implement it in a negotiation process based on the law of supply and demand. Then, peers of the network can trade energy directly through a local P2P network, thus allowing for the movement of local funds within the local economy [40] (see Figure 2).

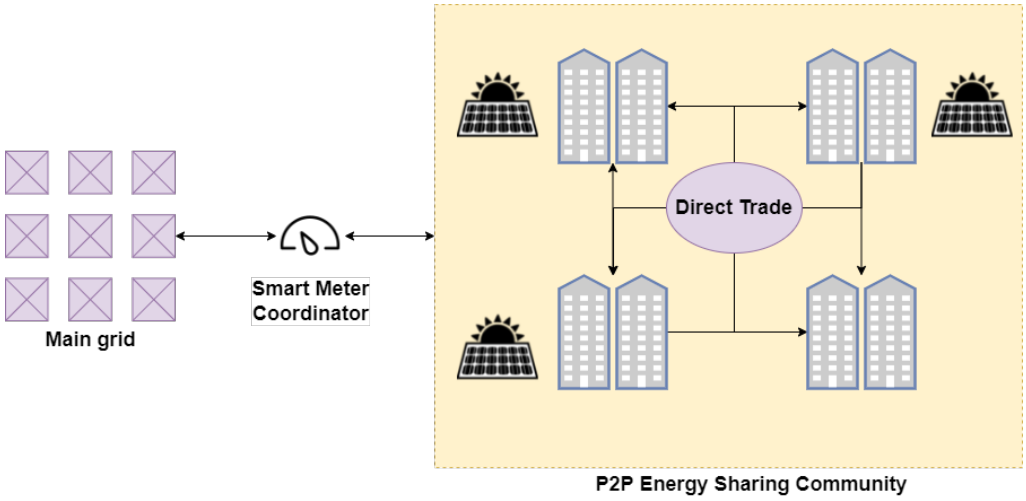

Figure 2. Basic diagram of a micro-grid architecture. The actors of the P2P network exchange energy locally and can potentially sell energy outside the community thanks to the existence of a smart meter coordinator.

In the study by Long et al. [41], in order to optimize the energy prizes for the players participating in the micro-grid community, they proposed a non-linear programming optimization algorithm with a rolling horizon of 30 min. The method proposed made use of a model based on the supply and demand proposed in [42]. In this model, the prices of energy fluctuate through the day, with a constraint that the price of the energy generated within the micro-grid should never be higher than the price of the energy bought from outside the grid. Moreover, the prize of the energy sold to the external grid must always be higher than that of the energy sold within the micro-grid. In this work, it was found that the smart meter coordinator was the most vulnerable part of the architecture proposed. The possibility of the smart meter being hacked was not considered, since BT was a mechanism that was required to avoid this kind of vulnerability while distributing the control of the activities and the negotiations carried out within the community.

Authors of [43] modeled a micro-grid scenario in which two variants appear, one based on cooperation between the different actors on the platform, and the other in which the actors play more selfishly in the market. This platform is only viable when all costs are equally shared between all households; therefore, there is no automated negotiation between the peers of the platform proposed. In this paper, it was also stated that a real scenario wherein all the actors collaborate is not feasible.

The companies studied in Section 3.1 allow for the trading of energy at a fixed price given by the producer. In other theoretical works such as that by Noor et al. [44], to allow for the exchange of energy with dynamic prizes, a game theory-based model was proposed. In this work, the blockchain network was used to distribute the control of the platform along with the exchange of information as a transparent energy market was created. Here, the actors that formed part of the platform negotiated the price of the energy in an automatic manner using a non-cooperative game-based algorithm to optimize their payoffs, based on the energy load of the entire grid. An important downside of this approach is that the system must know which specific appliances are connected throughout the entire network; this, along with the fact that no mechanism of encryption is used to store the data within the blockchain, creates a great privacy problem for the users.

3.3. Literature Review Conclusions and Manuscript Objectives

The present paper aims to create a transparent energy market with proven distributed security. Because of the nature of this kind of system, it will be impossible to use a public blockchain such as Ethereum due to its high fees and slow speed. A consortium of peers in the micro-grid will be needed to create a permissioned network that makes use of a

protocol such as PBFT, PoS, or dPOS, where it is assumed that all the network's participants are known and have the common goal of wanting the platform to work.

One of the features that the companies studied are lacking is the use of an automatic negotiation between the players of each platform. Our model makes use of a non-cooperative game between the consumers and producers that will regulate the energy market price in an autonomous way, thus allowing the stakeholders optimize their payoffs. Our model and its interactions with the blockchain are thoroughly explained to help startups and entrepreneurs to develop this kind of system. Furthermore, the scenario proposed in our work is based on a rolling horizon such as the one proposed by Long et al. [41], but with a time window of an hour to make the transactions more viable in the actual Ethereum network.

In the literature, compliance with the General Data Protection Regulation (GDPR) [45] has been found to be an important issue. Because of this, a careful selection of which data are to be collected and stored in the public ledger is needed, as well as which data must be encrypted and hidden from unauthorized peers. Moreover, ensuring the integrity and authenticity of the data is required by protecting it and the communication channels from unauthorized users [35]. Another issue of the proposed platform is its heavy dependence on the legislative framework of the country where it is to be installed. Laws that regulate the transaction of renewable energy between peers within communities are needed, such as in the case of Belgium, Greece, and Germany [35].

4. Proposed Architecture Design

In this section, we will describe the design of the proposed architecture, which aims to: (i) decentralize the energy market, (ii) automate, as much as possible, the energy market in small communities, (iii) and provide anonymity and privacy to its users. In the literature studied in the Section 3, there are working proposals that meet some of the above-mentioned requirements, although not all of them together.

The proposed architecture will follow the paradigm of distributed Multi-Agent Systems (MAS), which, in combination with blockchain technology, allows for the distribution of the processes and the control of the platform. The use of multi-agent systems was chosen because other works successfully achieved their main objective with the use of this paradigm, with the optimization and decentralization of platforms of any kind [46]. In the proposed architecture, features from different works studied in the literature have been put together, thus enabling decentralized control over the platform without a single point of failure and allowing for a negotiation process between the peers of the network as well as complying with the GDPR.

- Through the MAS, the control and management of the micro-grid platform is achieved, along with the negotiation between peers for energy in the market. However, to achieve full decentralization of the platform, the use of a blockchain platform is required, in which the smart contracts deployed will be used by the agents in the workflow of the platform. Thanks to this approach: (i) we will achieve a decentralized platform without a single point of failure; (ii) we will provide confidence to platform users and agents that agreements would be enforced, and in case they are not, encourage trust that the platform will compensate those who behave while punishing those agents who do not; and (iii) we will allow for the optimization of the prices of the energy transacted within the platform, balancing them while maximizing the payoffs of each kind of actor involved.
- The smart meters read the energy consumed and/or produced by each household. They are connected to each independent house, representing a peer in the micro-grid network. Each smart meter is connected to the internet and interacts with the blockchain on behalf of the household. Moreover, the agent who negotiates with their peers to buy or sell energy should be deployed here or in a device connected to the smart meter.
- The use of a blockchain network allows for the distribution of the communication and the interactions between the agents of the platform. The network is used not only as a

historical log in that each agent stores their activity on the platform, but it is also used as a validation and tamper-proof system that will help them to trust the platform and the activities of the actors involved. In addition, the smart contracts deployed in the network help in the control of the workflow of the platform.

- The information stored in the blockchain is encrypted, maintaining the data hidden from others. It is possible to maintain a verified and encrypted log in the blockchain by using Zero-Knowledge Proof (ZKP) protocols. Furthermore, by using ring signatures, the identity of the entities that store information within the blockchain is kept secret.

4.1. Blockchain Technology and Smart Contracts

The design of the proposed platform is based on the negotiation, payment, and exchange of energy. In time windows of one hour, agents negotiate the energy prices based on the amount they wish to transact during the following hour. The platform will use a permissioned blockchain, governed in a consortium way between the market actors. A permissioned blockchain network, as seen in the background section, allows for a high transaction output but with a very low cost.

The use of a permissioned network is proposed because it achieves two things that cannot be achieved using a permissionless network [47]: (i) transaction speed, since there are only known nodes within the network, it is possible to make use of faster consensus algorithms at the cost of a certain level of security; (ii) system scalability, because of the above-mentioned characteristics, by not requiring a large computational capacity to reach consensus, the system is scalable; (iii) the network protocols can be adapted to the system requirements during development, e.g., with the addition of ZKP protocols and ring signatures that are not available in any permissionless blockchain that allows for the deployment of smart contracts.

In a consortium blockchain, only verifiable actors are allowed to take part in the proposed platform. If new actors, e.g., new households, want to take part in the created market within the micro-grid, they have to make a proposition to the platform; here, in a consortium and not in an automated way, the actors of the micro-grid will vote if they will let them enter or not. If the actors suspect that the new actor trying to enter the platform has no good intentions or has intentions that are not aligned with the well-being of the platform, they will not be allowed to enter. On the other hand, if it is a typical household that wants to benefit from the good use of the platform, they will allow it to enter. To summarize, the consortium blockchain proposed in this framework should be governed equally by all the nodes of the blockchain; they all have equal voting rights.

Due to the characteristics of the blockchain network used, the platform will need a margin to store the agreements carried out by the agents. In the proposed platform, the margin is 5 min, enough time for the network to validate the information of the platform [48]. In that time window of 5 min, agents cannot continue their negotiations. Then, after 55 min, the agents will only sign the agreements that best benefit them after the negotiation period. In this way, the energy prices are fixed by each batch of energy independently negotiated, dependent only on the supply and demand, and each buyer and seller will make their own decisions based on their situation and the payoffs they want.

On the platform, smart contracts are used to generate tokens that represent the amount (in KWh) of energy available for exchange in the batteries. The virtualization of this energy is achieved by using Ethereum's fungible token standard: ERC20. Making use of standards is important for future system extensions as well as for the improvement of interoperability.

In the proposed platform, a smart contract is used to control the workflow of the platform (see Figure 3). The usual sequence of steps followed by the platform is described below:

1. Through the function *PublishInfo()*, agents can identify themselves on the platform. They can store data in relation to how other agents can initiate negotiations with them, the household they belong to, etc. With that information, it is possible for authorized actors to carry out auditory processes as well as to track their activity on the platform. This step should be performed the first time an agent is deployed in the system.

2. To publish any energy offer on the platform, authors should call the function *MakeOffer()*. Agents can calculate the forecasted energy surplus that could be sold to the network and create an offer with the predicted amount of energy for the next time window.
3. When an agent predicts a need to buy energy for the next time window, it will need to call the function GetOffers(). This function will return all the information related to the offers published for the next time window. Then, the agent will start the negotiation process directly with all the publishers of offers.
4. During the negotiation process, the agents try to reach an equilibrium on the price of the energy and the amount that must be bought. The price of the energy sold has an upper constraint, which is the price of the energy bought from outside the grid. It also has a lower constraint, which is the minimum price needed to produce the energy. Between those thresholds, agents have the autonomy to decide; they could use whatever negotiation algorithm they find more comfortable with as long as it exchanges messages following the ontology defined by the platform communications. The agents negotiate on the basis of different parameters such as the energy needed to buy or sell, the time left to finish the negotiation, the number of buyers or sellers, the amount of energy to be expected to generate or consume in the next time window, etc. When the last minutes of the negotiation are reached, each seller agent will start agreeing to sell the energy to those that offer the higher prices until the energy is all sold out. The buyer agents will do the opposite—they will buy at the lower prices given by the sellers during their negotiation. Because of the constraints, it is ensured that all the energy will be sold out; no buyer will buy from the main grid while energy is still available within the system. Therefore, each agent should have a time out to get answers from an offer. If they do not receive an answer during that time out, they will have to drop the offer and try to reach an agreement with the next best offer on their list. This will ensure an equilibrium point while avoiding getting stuck in infinite waiting periods.
5. After negotiating the price and the amount of energy to sell and to whom, the seller can publish on the blockchain to whom, how much, and for how much they are selling the energy with the function *AllowTransaction()*.
6. Finally, when the corresponding smart meters have detected the flow of energy to and from a house, automatic payments can be made by calling the function *MakeTransaction()*.

For the platform to function optimally, the amount of energy available to exchange within the market must be auditable. A guarantee is needed that this energy exists on the platform, so the smart meters in charge of reading this energy from the batteries and virtualizing it into tokens for sale undergo periodic auditing processes to ensure its proper functioning [47]. In addition, the smart meters are in charge of reading the energy flow in and out of the houses, another critical element for the proper functioning of the platform. In this sense, we call smart meters oracles, since they are in charge of virtualizing real-world data in smart contracts, a critical point of any platform based on blockchain and of which it is necessary to be very cautious [49].

Each agent of the platform interacting in one way or another with the blockchain network needs to make use of a wallet. Some agents, such as those in charge of using virtual money in exchanges, need to obtain that money beforehand. For example, if a household consumes more energy than it produces, it will need to put fiat money on the platform; hence, a consortium of human agents and/or machines will be needed to virtualize the money introduced and mint more tokens that represent it. In addition, they must allow the withdrawal of real money when a user decides to take out part of the virtual money for use outside the platform.

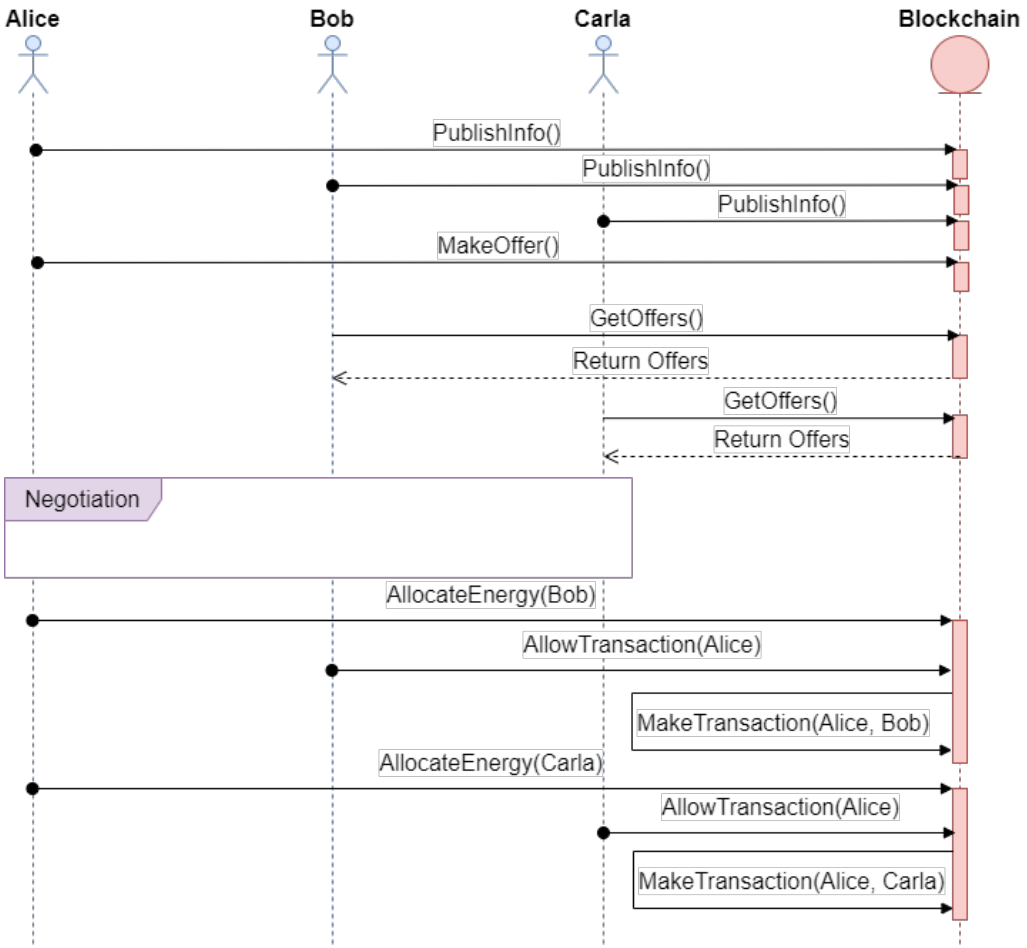

Figure 3. UML diagram of a sample workflow of the proposed platform.

4.2. Privacy Preservation Protocols

One of the problems that arise in state-of-the-art literature is that of user privacy and data protection, which are needed to comply with the GDPR. In this regard, the proposed model has been designed using protocols based on ZKPs used by the Monero cryptocurrency and described in [50]. Thanks to the use of these protocols, it is possible to hide the users who perform transactions within a blockchain as well as the related information [51].

For example, in [52], the authors proposed a framework that allows people who have been in close contact with infectious disease patients to be traced. Moreover, the authors proposed the use of ZKP to protect patient information based on bulletproofs [53].

The ring signatures protocol is used to allow actors to call smart contracts anonymously. This protocol requires what is called a Key Image [51], obtained from a list of randomly selected public keys (see Figure 4). The public key of the actor performing the transaction is also required since the transaction must be signed. Given that all the selected keys have the same probability of performing the transaction, it is not possible to associate the transaction with the real user. In addition, these groups of actors are improvised randomly from the pool of transactions.

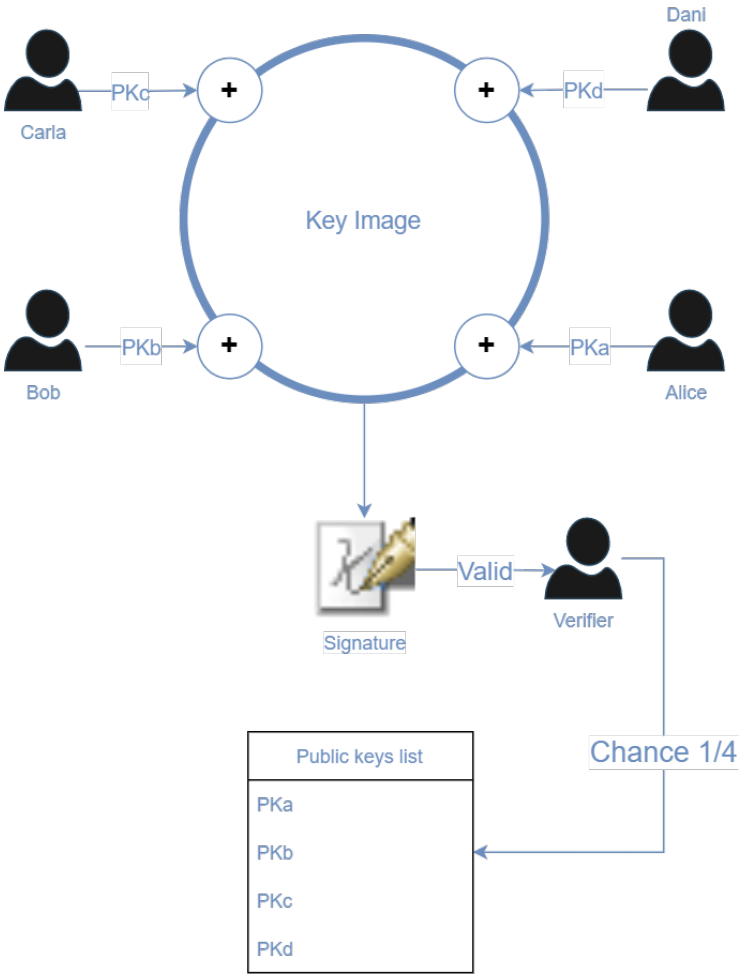

Figure 4. Key image, created from a list of the signatures of the users Bob, Alice, Carla, and Dani.

To complement the ring transaction signing process and ensure the anonymity of the actors within the system, stealth addresses are used in the smart contracts to identify actors. It is impossible to link these addresses to a user; however, a user can identify the stealth addresses that belongs to it. Taking advantage of the properties of elliptic curves [51], a stealth address (P) is defined by Equation (1):

$$P = F + S \tag{1}$$

where F is defined in (2), and S is the public key of the recipient of the transaction.

$$F = Hash(rS) * G \tag{2}$$

where r is a random private key generated by the actor that emits the transaction, and G is the base point of the elliptic curve.

To identify which stealth address belongs to a user, thanks to the properties of Equation (3), the actor can hash the product of the address public key (R) and its private key (s), then the public key (S) has to be added, and the final result is the stealth address. For a user to prove that a stealth address belongs to them, they need to recover the one-time private key generated for that transaction. By hashing the product of the stealth-address public key (R) and the user private key (s), and then adding the private key s to the obtained hash, it is possible to recover the one-time private key of the address (r). Then, it is necessary to sign the transactions from that address with that key to prove the ownership.

$$rS = rsG = rGs = Rs \tag{3}$$

where R is the public key of the randomly generated private key, and s is the private key of the transaction recipient.

The use of these protocols increases the need for the computational power of each actor that makes use of them. In Figure 3, it is possible to study the number of times each agent must write to the blockchain, thus making use of these protocols, within a system based on the proposed framework. The agents only need to write the information in the following cases:

1. When they are registered within the system and store information related to them. In the whole life cycle of the platform, this occurs once for each agent.
2. At the end of each hour, every agent writes in the blockchain the agreement reached during the negotiation process. For example, if Alice reaches an agreement with Bob and Carla, then Alice will need to create two transactions. On the other hand, according to the example, Bob and Carla only need to create one each.

This step will depend on the number of agents involved, but with the time limits proposed—from 5 to 10 min—in a permissioned blockchain, it is enough time to not overcharge the agents and their computational resources. Therefore, the performance will not be affected when the system escalates.

4.3. Security Model

This section details the security assumptions made by the framework and how the data generated within the platform are treated. The implementation of blockchain technology in this platform ensures the application of a secure identification protocol between the actors. Furthermore, the information stored is tamper-proof, and the smart contracts deployed allow for the decentralized control of the platform, ensuring that there will not be a single point of failure that will be prone to attacks.

Regarding the storage of the generated data, which will be used to create the predictive models that will help with the proper functioning of the system, each actor will be responsible for them. We assume that each actor is responsible for providing an access point to their data so that they can control to whom they give access to the data. For each hour, a batch can be created with the generated data, storing in the blockchain a hash of such data that will help to verify that it has not been modified afterwards. The use of auditability systems allows for the generation of data that can be trusted. Otherwise, it would be impossible to know that the generated data has not been modified before the storage of its hash in the blockchain [47].

As for the proposed privacy protocols, they ensure that the information stored in the blockchain cannot be read by third parties without permission, nor will it be possible to identify or track user activity. This information that is stored is, for example, the energy bids posted, the money paid for energy transactions, or the amount of energy transacted. The only vulnerability of this platform is when an attacker steals the keys of a user. However, this is not possible just by using the platform; it can only happen if the user is not careful enough with the passwords used or with where the keys are stored.

In this work, we have made security assumptions that the network of blockchain nodes is large enough so that it is not easy to throw it from a typical Distributed Denial of Services (DDOS) attack. It has also been assumed that the actors that are part of the platform benefit more from its proper functioning than from trying to sabotage it. Different actors could collude with each other to achieve a greater benefit, but this scenario is not realistic based on the study conducted by [43]. Having in mind the previous assumptions, we can thus say that the actors of the platform will benefit from the creation of this platform and the competition between them rather than in trying to sabotage the negotiation process and the well-being of the platform.

4.4. Multi-Agent System

This section will describe the MAS structure in detail. It is divided into four different subsystems, in which the agents are grouped according to their function within the platform

(see Figure 5). The following is a detailed description of the different subsystems and the agents that comprise them:

- Device Driver System (DDS). This system groups all the agents in charge of the management and control of the different smart devices of the platform (e.g., batteries, smart meters, PV panels). These agents are allowed to interact with the blockchain network, so they also have an assigned wallet to identify and track their activity within the platform, thus helping in the auditing process. The agents in charge of monitoring the state of the PV panels (e.g., their energy production, the provided voltage and current, and their active and reactive powers) are the PV agents (PVA). They store those data in the blockchain, which helps their owners to monitor them while also owning that information which they could sell in the future. The batteries are monitored by agents called Battery State Agents (BSA). They store in the blockchain data related to the state of a battery, its charge and discharge capability, and its current state of charge. The agent that stores the data related to the flow of current from or to a household is the Smart Meter Agent (SMA).
- Micro-grid Operator System (MGOS). In this system, all those agents that are responsible for monitoring, controlling, and managing the status and good credit of the micro-grid are grouped together. These agents are also connected to the blockchain, storing the relevant information that favors the traceability of the micro-grid monitoring, flows of power to and from the utility network, the balance of the micro-grid power, and the voltage level (Micro-grid Operator agent or MGO), or the energy transactions made from the grid to the micro-grid and vice versa (External Market Interactor Agent or EMI). In addition, this system owns a series of batteries that improve the balance of the grid load, governed by the State Of Charge agents (SOC). This part of the platform is economically maintained by the penalties of users who do not fulfill their part of the contracts and by the exchange of energy between the external grid and the micro-grid.
- Data Analytic System (DAS). This system is crucial for the platform as it is in charge of grouping all those agents that are in charge of the data market and the creation of predictive models, which are required by the rest of the agents of the system to be able to infer the amount of energy they expect to obtain in the next hour, that which they could sell, and that which they will need to buy based on their past consumption. The agents in charge of reading the data provided by the other subsystems of the platform on the blockchain and merging it with data coming from other external data sources are called Data Reader Agents (DRA). The agents that create and update new behavioral models on demand are the Knowledge Extractor Agents (KEA). The agents that make predictions based on these models and the information extracted from the environment are the Forecasting Agents (FA). This subsystem benefits from the data market created with the addition of blockchain technology to the platform. As it has been found in other works in the literature, it is also possible to improve the creation of the models with the use of blockchain technology by applying a federated learning framework similar to the one proposed in [54].
- Transaction Manager System (TMS). In this subsystem, all those agents that are responsible for the negotiation and exchange of energy within the micro-grid are grouped. These agents make use of the blockchain network to publish and search for energy offers as well as register the agreements that take place. The agents in charge of publishing the offers are the Seller Agents (SA), while those who search for them in order to buy are the Buyer Agents (BA). The agents in this system negotiate with each other directly and make use of the DAS to estimate the energy they will need to buy and/or sell. As a way to improve the search process in the blockchain, a middleware layer could be used to optimize the search for information (offers in this case) within the blockchain, such as the one proposed in [55].

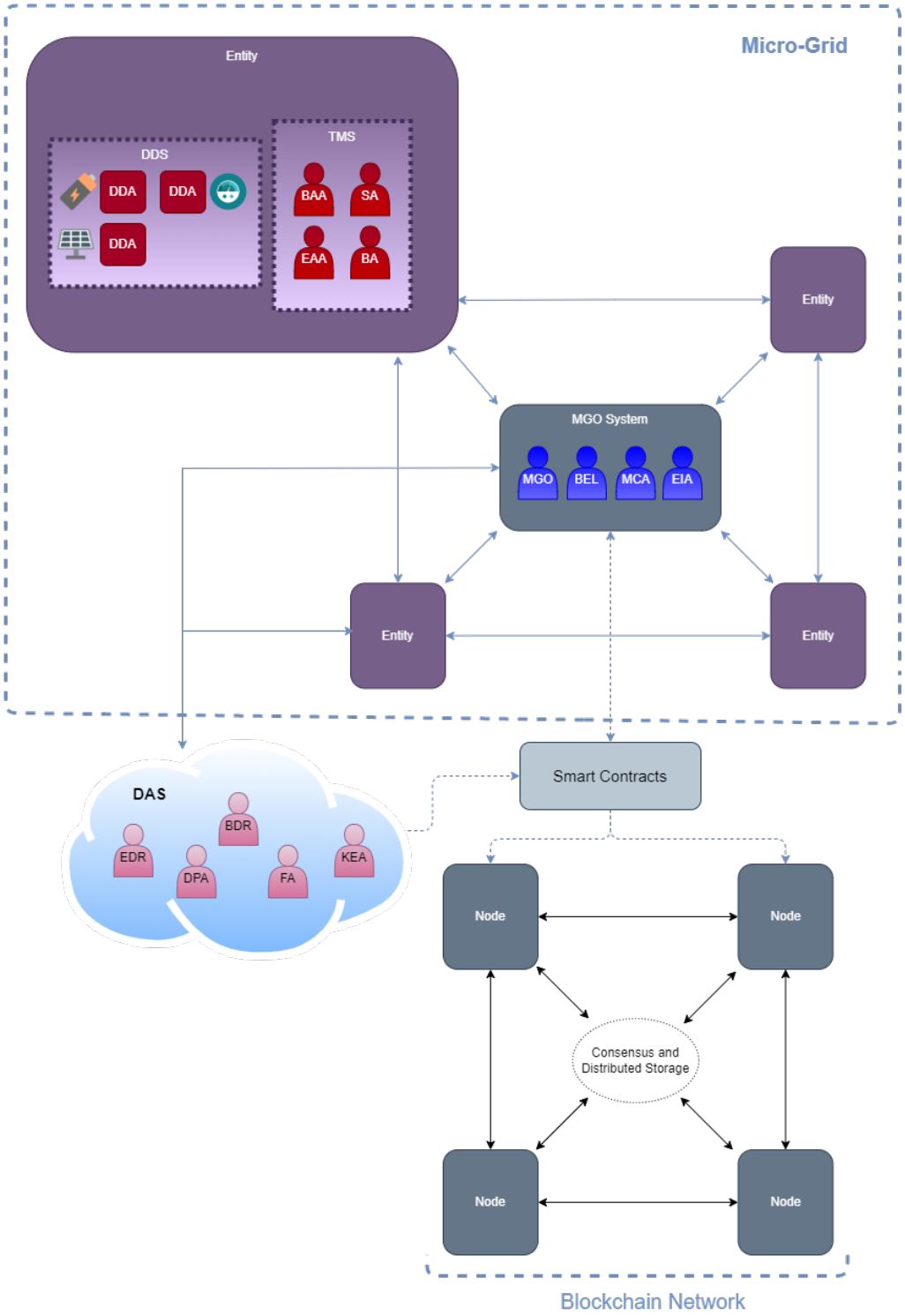

Figure 5. Proposed platform architecture.

4.5. Deployment of the Platform

In the proposed platform, there are three types of actors: consumers who receive energy that they buy from the grid, PV panels as producers that produce the energy and dump it into batteries, and batteries as prosumers who store and distribute the energy (e.g., consumed by their owners, or, if leftover, dumped into the micro-grid to make a profit). There are also actors who are in charge of the good credit of the micro-grid and who additionally make a profit by connecting it to the external grid. Finally, there are other

players who help the platform to function properly, such as those in charge of exchanging fiat money for digital money and vice versa.

As shown in Figure 6, the interconnections between the parts of the platform are made through the Internet, in the creation of cloud services. The platform agents in charge of knowledge extraction with regard to the platform data needs large computational power; hence, the infrastructure is outsourced to a provider (e.g., Amazon Web Services, Google Cloud, or Azure). The blockchain network, controlled by the platform actors, is accessible to the parties and does not need high computational power; only one computer per participant is required to be always on. The agents in charge of controlling the smart devices will need to be deployed in them or in a system such as a Raspberry Pi that has direct access to them. The rest of the agents only need to be deployed in computers that always have access to the Internet and do not have any special requirements.

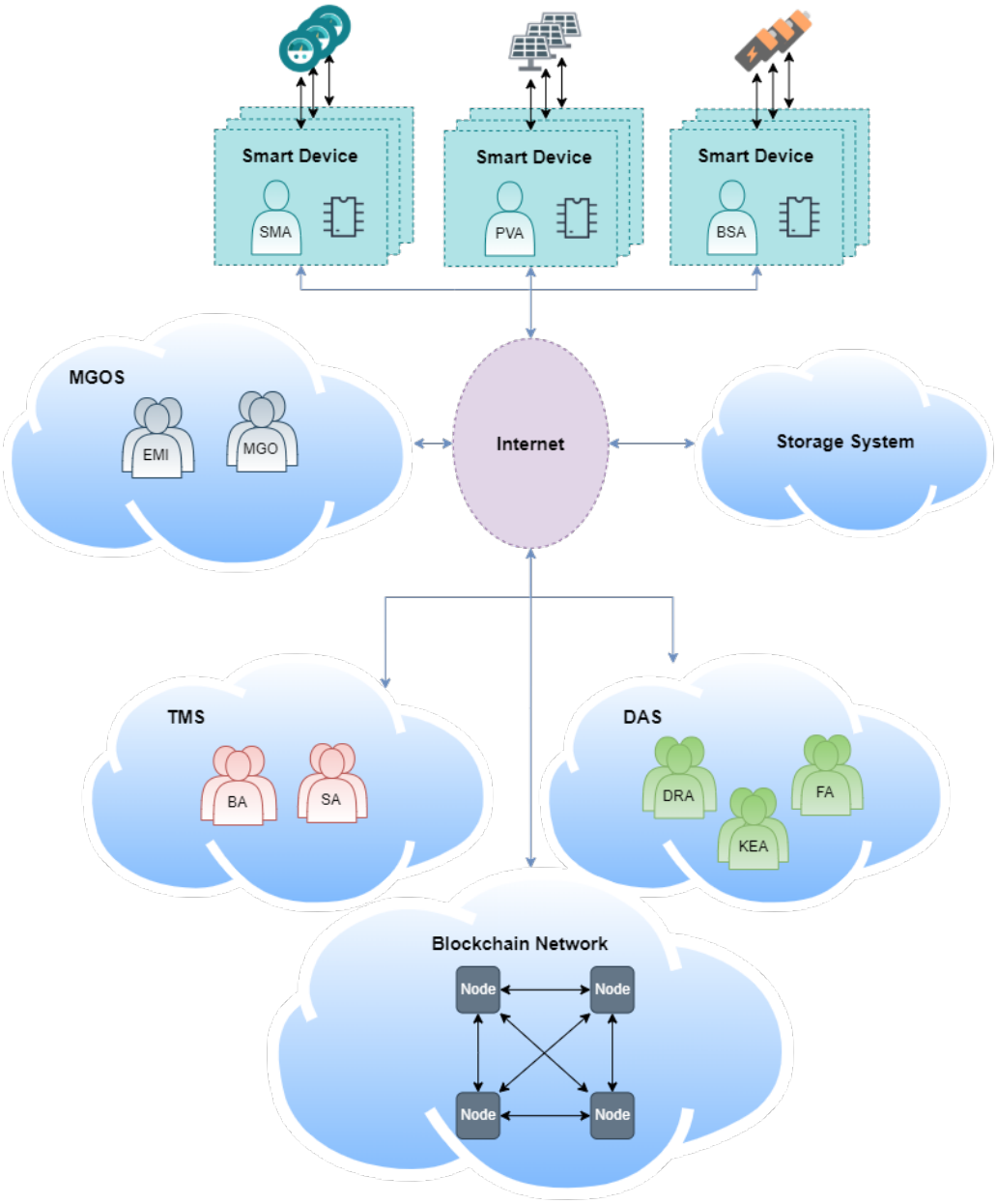

Figure 6. Platform deployment diagram.

5. Conclusions and Future Work

This manuscript highlights and discusses concepts and technologies such as blockchain, smart micro-grids, and negotiation algorithms that have been applied to the energy market. Furthermore, this work elaborates on the proposal of an innovative high-technology-based architecture of a fully distributed and autonomous smart micro-grid to support new forms of business in the smart energy market. With independent and dynamic pricing between the transactors in the network, the proposal presented makes it possible to create a Local Energy Market (LEM) in order to achieve efficiency in the transmission and distribution of energy as compared to the traditional distribution model.

In the mentioned context, this paper has studied the implementation and development of smart micro-grids that would allow for the entrance of more entities, whose aim is self-consumption and making money with the excess energy generated, as competitors in the energy market. If it is possible to introduce more actors into the power market that can compete for revenue in the energy market, the regularization of prices is no longer necessary. Because the energy transactions between entities of a micro-grid that are closer to each other are cheaper and better than those made between distant entities, the market law of supply and demand would work, thus making their current regularization unnecessary. Finally, the use of ring signatures and ZKP protocols has been proposed to ensure the privacy of the users and the protection of the data stored within the platform, thus complying with the GDPR.

In general terms, for future work, the designed proposal should be implemented as a pilot project. This will allow for the design of ad hoc consensus algorithms for the energy market. In this way, it will be possible to validate the proposed framework as a standard guideline for similar platforms. This will help to reduce development costs and encourage the adoption of the system by companies and individuals.

Author Contributions: Funding acquisition, J.P. and J.M.C.; Investigation, Y.M.; Methodology, Y.M. and A.B.G.-G.; Project administration, Y.M.; Supervision, A.B.G.-G., A.M.d.R., J.P. and J.M.C.; Writing—original draft, Y.M. and A.B.G.-G.; Writing—review & editing, Y.M., A.B.G.-G. and A.M.d.R. All authors have read and agreed to the published version of the manuscript.

Funding: The research of Yeray Mezquita is supported by the pre-doctoral fellowship from the University of Salamanca and co-funded by Banco Santander. Besides this work has been partially supported by the Institute for Business Competitiveness of Castilla y León, and the European Regional Development Fund under grant CCTT3/20/SA/0002 (AIR-SCity project).

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.

References

1. Hirst, E.; Kirby, B. *Transmission Planning for a Restructuring US Electricity Industry*; Consulting in Electric-Industry Restructuring: Washington, DC, USA, 2001.
2. Fang, X.; Misra, S.; Xue, G.; Yang, D. Smart grid—The new and improved power grid: A survey. *IEEE Commun. Surv. Tutor.* **2011**, *14*, 944–980. [CrossRef]
3. Memon, A.A.; Kauhaniemi, K. A critical review of AC Microgrid protection issues and available solutions. *Electr. Power Syst. Res.* **2015**, *129*, 23–31. [CrossRef]
4. Bui, V.H.; Hussain, A.; Kim, H.M. A multiagent-based hierarchical energy management strategy for multi-microgrids considering adjustable power and demand response. *IEEE Trans. Smart Grid* **2016**, *9*, 1323–1333. [CrossRef]
5. Tosh, D.K.; Shetty, S.; Liang, X.; Kamhoua, C.; Njilla, L. Consensus protocols for blockchain-based data provenance: Challenges and opportunities. In Proceedings of the 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), New York, NY, USA, 19–21 October 2017; pp. 469–474.
6. Cameron, P.D.; Brothwood, M. *Competition in Energy Markets: Law and Regulation in the European Union*; Oxford University Press: Oxford, UK, 2002.
7. Von Danwitz, T. Regulation and Liberalization of the European Electricity Market-A German View. *Energy* **2006**, *27*, 423.

8. Mezquita, Y.; Casado-Vara, R.; González Briones, A.; Prieto, J.; Corchado, J.M. Blockchain-based architecture for the control of logistics activities: Pharmaceutical utilities case study. *Log. J. IGPL* **2021**, *29*, 974–985. [CrossRef]
9. Liang, X.; Shetty, S.; Tosh, D.; Kamhoua, C.; Kwiat, K.; Njilla, L. Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. In Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, Madrid, Spain, 14–17 May 2017; pp. 468–477.
10. Buterin, V. Ethereum: Platform Review. In *Opportunities and Challenges for Private and Consortium Blockchains*; Available online: http://www.smallake.kr/wp-content/uploads/2016/06/314477721-Ethereum-Platform-Review-Opportunities-and-Challenges-for-Private-and-Consortium-Blockchains.pdf (accessed on 19 April 2022).
11. Huh, S.; Cho, S.; Kim, S. Managing IoT devices using blockchain platform. In Proceedings of the 2017 19th International Conference on Advanced Communication Technology (ICACT), Pyeongchang, Korea, 19–22 February 2017; pp. 464–467.
12. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA, 13–17 March 2017; pp. 618–623.
13. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An overview of blockchain technology: Architecture, consensus, and future trends. In Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 25–30 June 2017; pp. 557–564.
14. Beikverdi, A.; Song, J. Trend of centralization in Bitcoin's distributed network. In Proceedings of the 2015 IEEE/ACIS 16th International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), Takamatsu, Japan, 1–3 June 2015; pp. 1–6.
15. Martinez, J. Understanding Proof of Stake: The Nothing at Stake Theory. 2018. Available online: https://medium.com/coinmonks/understanding-proof-of-stake-the-nothing-at-stake-theory-1f0d71bc027 (accessed on 9 October 2019).
16. Witherspoon, Z. A Hitchhiker's Guide to Consensus Algorithms. 2017. Available online: https://hackernoon.com/a-hitchhikers-guide-to-consensus-algorithms-d81aae3eb0e3 (accessed on 9 October 2019).
17. Abadi, J.; Brunnermeier, M. *Blockchain Economics*; Technical Report; National Bureau of Economic Research: Cambridge, MA, USA, 2018.
18. Sikorski, J.J.; Haughton, J.; Kraft, M. Blockchain technology in the chemical industry: Machine-to-machine electricity market. *Appl. Energy* **2017**, *195*, 234–246. [CrossRef]
19. Weber, I.; Xu, X.; Riveret, R.; Governatori, G.; Ponomarev, A.; Mendling, J. Untrusted business process monitoring and execution using blockchain. In *International Conference on Business Process Management*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 329–347.
20. Khaqqi, K.N.; Sikorski, J.J.; Hadinoto, K.; Kraft, M. Incorporating seller/buyer reputation-based system in blockchain-enabled emission trading application. *Appl. Energy* **2018**, *209*, 8–19. [CrossRef]
21. Schöner, M.M.; Kourouklis, D.; Sandner, P.; Gonzalez, E.; Förster, J. *Blockchain Technology in the Pharmaceutical Industry*; Frankfurt School Blockchain Center: Frankfurt, Germany, 2017.
22. Sylim, P.; Liu, F.; Marcelo, A.; Fontelo, P. Blockchain technology for detecting falsified and substandard drugs in distribution: Pharmaceutical supply chain intervention. *JMIR Res. Protoc.* **2018**, *7*, e10163. [CrossRef]
23. Galvez, J.F.; Mejuto, J.; Simal-Gandara, J. Future challenges on the use of blockchain for food traceability analysis. *TrAC Trends Anal. Chem.* **2018**, *107*, 222–232. [CrossRef]
24. Kamath, R. Food traceability on blockchain: Walmart's pork and mango pilots with IBM. *J. Br. Blockchain Assoc.* **2018**, *1*, 3712. [CrossRef]
25. Yue, X.; Wang, H.; Jin, D.; Li, M.; Jiang, W. Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. *J. Med. Syst.* **2016**, *40*, 218. [CrossRef]
26. Mettler, M. Blockchain technology in healthcare: The revolution starts here. In Proceedings of the 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), Munich, Germany, 14–17 September 2016; pp. 1–3.
27. Ekblaw, A.; Azaria, A.; Halamka, J.D.; Lippman, A. A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data. In Proceedings of the IEEE Open & Big Data Conference, Vienna, Austria, 22–24 August 2016; Volume 13, p. 13.
28. Turkanović, M.; Hölbl, M.; Košič, K.; Heričko, M.; Kamišalić, A. EduCTX: A blockchain-based higher education credit platform. *IEEE Access* **2018**, *6*, 5112–5127. [CrossRef]
29. Grech, A.; Camilleri, A.F. Blockchain in Education. 2017. Available online: https://www.pedocs.de/volltexte/2018/15013/pdf/Grech_Camilleri_2017_Blockchain_in_Education.pdf (accessed on 19 April 2022).
30. Funk, E.; Riddell, J.; Ankel, F.; Cabrera, D. Blockchain technology: A data framework to improve validity, trust, and accountability of information exchange in health professions education. *Acad. Med.* **2018**, *93*, 1791–1794. [CrossRef]
31. Pop, C.; Cioara, T.; Antal, M.; Anghel, I.; Salomie, I.; Bertoncini, M. Blockchain based decentralized management of demand response programs in smart energy grids. *Sensors* **2018**, *18*, 162. [CrossRef]
32. Imbault, F.; Swiatek, M.; De Beaufort, R.; Plana, R. The green blockchain: Managing decentralized energy production and consumption. In Proceedings of the 2017 IEEE International Conference on Environment and Electrical Engineering and 2017 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe), Milan, Italy, 6 June 2017; pp. 1–5.

33. 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]
34. Mengelkamp, E.; Gärttner, J.; Rock, K.; Kessler, S.; Orsini, L.; Weinhardt, C. Designing microgrid energy markets: A case study: The Brooklyn Microgrid. *Appl. Energy* **2018**, *210*, 870–880. [CrossRef]
35. Pichler, M.; Meisel, M.; Goranovic, A.; Leonhartsberger, K.; Lettner, G.; Chasparis, G.; Vallant, H.; Marksteiner, S.; Bieser, H. Decentralized Energy Networks Based on Blockchain: Background, Overview and Concept Discussion. In Proceedings of the International Conference on Business Information Systems, Colorado Springs, CO, USA, 8–10 June 2018; Springer: Berlin/Heidelberg, Germany, 2018; pp. 244–257.
36. Pylon Network Team. Pylon Network Whitepaper. The Energy Blockchain Platform. 2018. Available online: https://pylon-network.org/wp-content/uploads/2019/02/WhitePaper_PYLON_v2_ENGLISH-1.pdf (accessed on 6 November 2019).
37. Suncontract. Suncontract Whitepaper. An Energy Trading Platform that Utilises Blockchain Technology to Create A New Disruptive Model for Buying and Selling Electricity. 2017. Available online: https://suncontract.org/wp-content/uploads/2020/12/whitepaper.pdf (accessed on 6 November 2019).
38. Aliyev, N.; Brooks, S.; Hale, M.; Hoy, S. Enosi Green Paper 2018. Available online: https://github.com/enosi/green-paper/blob/master/enosi-green-paper.pdf (accessed on 19 April 2022).
39. Goranović, A.; Meisel, M.; Fotiadis, L.; Wilker, S.; Treytl, A.; Sauter, T. Blockchain applications in microgrids an overview of current projects and concepts. In Proceedings of the IECON 2017-43rd Annual Conference of the IEEE Industrial Electronics Society, Beijing, China, 28 October–1 November 2017; pp. 6153–6158.
40. Koirala, B.P.; Koliou, E.; Friege, J.; Hakvoort, R.A.; Herder, P.M. Energetic communities for community energy: A review of key issues and trends shaping integrated community energy systems. *Renew. Sustain. Energy Rev.* **2016**, *56*, 722–744. [CrossRef]
41. Long, C.; Wu, J.; Zhou, Y.; Jenkins, N. Peer-to-peer energy sharing through a two-stage aggregated battery control in a community Microgrid. *Appl. Energy* **2018**, *226*, 261–276. [CrossRef]
42. Liu, N.; Yu, X.; Wang, C.; Li, C.; Ma, L.; Lei, J. Energy-sharing model with price-based demand response for microgrids of peer-to-peer prosumers. *IEEE Trans. Power Syst.* **2017**, *32*, 3569–3583. [CrossRef]
43. van Leeuwen, G.; AlSkaif, T.; Gibescu, M.; van Sark, W. An integrated blockchain-based energy management platform with bilateral trading for microgrid communities. *Appl. Energy* **2020**, *263*, 114613. [CrossRef]
44. Noor, S.; Yang, W.; Guo, M.; van Dam, K.H.; Wang, X. Energy Demand Side Management within micro-grid networks enhanced by blockchain. *Appl. Energy* **2018**, *228*, 1385–1398. [CrossRef]
45. European Parliament and Council: Regulation on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (Data Protection Directive). 2016. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN (accessed on 9 December 2021).
46. Francisco, M.; Mezquita, Y.; Revollar, S.; Vega, P.; De Paz, J. Multi-agent distributed model predictive control with fuzzy negotiation. *Expert Syst. Appl.* **2019**, *129*, 68–83. [CrossRef]
47. Mezquita, Y.; Casado, R.; Gonzalez-Briones, A.; Prieto, J.; Corchado, J.M.; AETiC, A. Blockchain technology in IoT systems: Review of the challenges. *Ann. Emerg. Technol. Comput.* **2019**, *3*, 17–24. [CrossRef]
48. Combi, C. What Are Blockchain Confirmations and Why Do They Matter? 2017. Available online: https://coincentral.com/blockchain-confirmations/ (accessed on 19 April 2022).
49. Gatteschi, V.; Lamberti, F.; Demartini, C.; Pranteda, C.; Santamaría, V. Blockchain and smart contracts for insurance: Is the technology mature enough? *Future Internet* **2018**, *10*, 20. [CrossRef]
50. Van Saberhagen, N. CryptoNote v 2.0. 2013. Available online: https://www.getmonero.org/ru/resources/research-lab/pubs/whitepaper_annotated.pdf (accessed on 19 April 2022).
51. Roy Walker. The Battle for Blockchain Privacy: Monero. 2018. Available online: https://medium.com/all-things-venture-capital/privacy-protocol-analysis-monero-c116d7c2106f (accessed on 19 April 2022).
52. Peng, Z.; Xu, C.; Wang, H.; Huang, J.; Xu, J.; Chu, X. P2b-trace: Privacy-preserving blockchain-based contact tracing to combat pandemics. In Proceedings of the 2021 International Conference on Management of Data, Xi'an, China, 20–25 June 2021; pp. 2389–2393.
53. Bünz, B.; Bootle, J.; Boneh, D.; Poelstra, A.; Wuille, P.; Maxwell, G. Bulletproofs: Short proofs for confidential transactions and more. In Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 21–23 May 2018; pp. 315–334.
54. Peng, Z.; Xu, J.; Chu, X.; Gao, S.; Yao, Y.; Gu, R.; Tang, Y. VFChain: Enabling verifiable and auditable federated learning via blockchain systems. *IEEE Trans. Netw. Sci. Eng.* **2021**, *9*, 173–186. [CrossRef]
55. Wu, H.; Peng, Z.; Guo, S.; Yang, Y.; Xiao, B. VQL: Efficient and Verifiable Cloud Query Services for Blockchain Systems. *IEEE Trans. Parallel Distrib. Syst.* **2021**, *33*, 1393–1406. [CrossRef]