Smart Contracts for a Secure and Privacy-Preserving Smart Grid

Joan Ferré-Queralt[1][0009−0002−0014−0065], Jordi Castellà-Roca[1][0000−0002−0037−9888], and Alexandre Viejo[1][0000−0003−2342−5100]

Universitat Rovira i Virgili
Departament d'Enginyeria Informàtica i Matemàtiques
UNESCO Chair in Data Privacy,
CYBERCAT-Center for Cybersecurity Research of Catalonia
Av. Països Catalans 26, E-43007 Tarragona, Catalonia, Spain
{joan.ferreq,jordi.castella,alexandre.viejo}@urv.cat

Abstract. The current energy landscape faces challenges such as escalating demand, rising prices, and the depletion of traditional energy sources. Existing electricity grids face significant limitations and vulnerabilities and the society would clearly benefit from the adoption of a new energy model that integrates locally-generated renewable energy. In order to achieve that, the use of the smart grid has been proposed as a way to modernize and optimize energy distribution. Generally, current works in the literature that study this area fail to effectively address the security and privacy threats that smart grids and their users may face while participating in the system. Moreover, those proposals that consider the privacy of the users do not prevent them from performing fraudulent actions while they hide in the anonymity. As a result of that, in this work, we propose a new smart grid system which uses blockchain technology and smart contracts as core components. The new scheme takes into account the privacy of the users and the availability and security of the system; while still offering measures to identify and take punitive actions against misbehaving users.

Keywords: Smart grid · Smart contracts · Security · Privacy

1 Introduction

In order to ensure the energy needs of a country, it is of paramount importance to find a balance between supply and demand. Traditionally, the energy supply has been carried out by the deployment of power plants that consume fossil fuels (i.e, coal, natural gas, etc.) or nuclear fuel. Those solutions have significant shortcomings such as the large expenses involved in the construction and maintenance of all the required infrastructure, the greenhouse gas emissions, pollution, nuclear waste, etc. Therefore, it might be beneficial to move towards another main source of energy. In recent years, the cost of renewable energy sources, such as wind and solar, has fallen significantly, making them more competitive and leading the European Union towards a more sustainable and decarbonized electricity

sector. However, the adoption of renewable energy has not been increasing at a sufficient pace[1]. This is due in part to the challenges of transitioning away from fossil fuels, as renewable sources may not be as reliable, available and efficient as traditional ones [20].

One way to potentially improving the availability and efficiency of the energy distribution system is to locate energy producers closer to consumers. This can help to reduce the cost and loss of distributing energy over long distances. The use of distributed renewable energy technologies, like solar panels, also opens up the possibility of local, decentralized production and consumption of electricity [8]. In this way, some households are currently using distributed energy resource (DER) systems, like solar panels, to generate and consume their own electricity. If these homes produce more energy than they need, they can sell the excess back to the main grid. However, the price at which this excess energy can be sold is often not attractive enough to sell due to certain impositions or taxes that may be applied by governments or electric utility companies.

In the light of the above, it can be concluded that the society would clearly benefit from the adoption of a new energy model that helps to meet the growing demand by incorporating decentralized and locally-generated renewable energy. In order to achieve that, the use of the *smart grid*, which has been proposed as a way to modernize and optimize energy distribution [6], can play a key role by properly encouraging those DER-equipped households to offer their surplus power to the main grid.

1.1 Related work

In the recent years, there have been lots of studies about different implementations of a smart grid system, each of those focusing on different aspects of it. In this work, we focus on those implementations that consider the trading of electricity between prosumers.

The first definition of a smart grid was made in [4], which made a first list of requirements that this new energy model should have. Later on, in [17], they discussed some different communication standards for the smart grid, all of which were focused on the traditional centralized structure of the main grid. However, a centralized structure in a smart grid is considered to have several security issues such as a Denial of Service attack, as explained in [3]. Some of those security concerns could be avoided using a distributed system, avoiding the single point of failure problem [14].

One of the first distributed-based solutions was introduced in [13]. The authors of this work proposed the use of an energy currency based on the blockchain technology proposed in [15]. This proposal paved the way for the use of the blockchain as the base for the new grid and the integration of smart contracts. In this way, numerous works have been conducted on this topic, including those proposed in [1, 2, 10, 12, 13], which present various blockchain architectures for implementing a smart grid.

[1] IEA: Wholesale energy costs made simple, https://www.edfenergy.com

At this point, it is important to note that all the aforementioned solutions employ a blockchain that uses the *Proof-of-Work* consensus mechanism. This method has been proved to be highly energy-intensive, as it requires substantial computing resources to verify transactions [5]. Such energy consumption is a major drawback that disqualifies them from being integrated in a real smart grid setting. It is, therefore, imperative to explore alternative consensus mechanisms that can minimize energy consumption while maintaining the integrity and security of the system.

Other works such as [9], [10], and [18] have explored the introduction of the blockchain technology into energy systems, but those proposals put little focus on the concealment of users' identities, which we consider as anonymity or their energy consumption patterns, which we consider as privacy. This situation, as a result, directly jeopardizes the privacy and anonymity of the users. It is essential to address these privacy concerns when designing blockchain-based energy systems to ensure that the data shared on the network is secure and not susceptible to malicious attacks. A lack of privacy measures can lead to various issues, such as unauthorized access to sensitive information or profiling of user behavior [21].

In response to that, other proposals such as [11], [7] and [19] have emerged recently. In this way, the solutions presented in [11] and [7] take into account the anonymity of the users, however they do not verify whether the production or consumption claimed by the users is truly the one being specified. As a result, a dishonest user could potentially submit a fake energy production record, which can mislead the system and other users, leading to undesirable outcomes. On the other hand, [19] uses a reputation system to punish those users who misbehave. However, in this scheme no one possesses the relationship between the smart grid accounts and real identity of the users and, hence, it is not capable of effectively applying coercing measures to the misbehaving user.

1.2 Contribution and plan of this paper

This work proposes a new energy trading system based on a smart grid that empowers users to both consume and produce electricity using distributed energy resources. The new system improves the current literature by taking into account the privacy of the users and the availability and security of the system; while still offering measures to identify and take punitive actions against misbehaving users. These features are achieved by means of the blockchain technology and the use of smart contracts.

Our smart grid system monitors the electricity consumption of every user, allowing for precise calculations of individual prosumers' total debts. Moreover, it facilitates seamless electricity trading among geographically proximate prosumers, providing the added flexibility of borrowing from or contributing to the main grid when necessary, whether due to a deficit or surplus.

The rest of the paper is organized as follows. Section 2 presents the system's architecture and offers an overview of how the new scheme works. Section 3 gives specific details about the system components and steps. Section 4 studies

how the new solution deals with security and privacy threats. Finally, Section 5 provides the conclusions and presents some lines of future work.

2 Architecture and system overview

2.1 General architecture

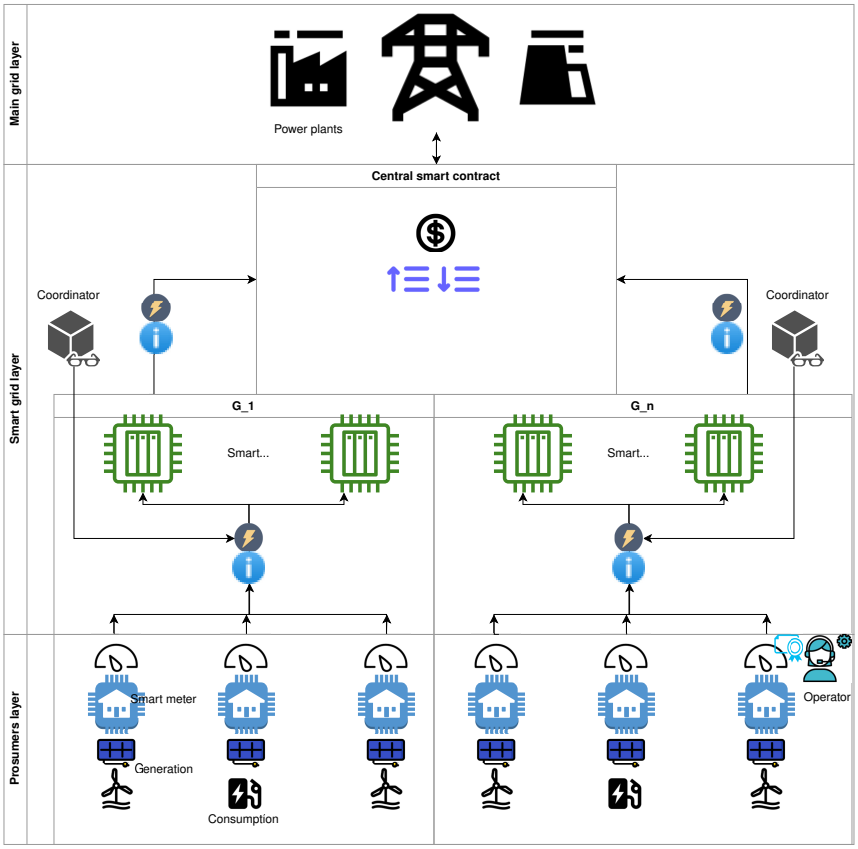


Fig. 1. Architecture scheme

The proposed architecture is depicted in Fig. 1. It consists of three main layers: *prosumers layer*, *smart grid layer*, and *main grid layer*. The following actors/components are involved:

– Smart meters (SM_i): devices who keep track of a prosumer's usage of energy (production and consumption).

- Prosumers: each system user that at a certain time can both produce and consume energy, depending on the balance between the production and consumption that prosumer can be: a *Consumer* (C_i) if she consumes more energy than produced; or a *Producer* (P_i) if she produces more energy than consumed. Each prosumer owns a smart meter and can have consumption, production facilities or both in their household.
- Main grid (MG): connects the main energy sources to the smart grid and is in charge of electricity distribution. Is the one in charge of energy consumption prediction and providing the extra electricity needed.
- Smart grid: keeps transactions between prosumers and between prosumers and the main grid. Also coordinates all payments.
- Coordinators (Co_i): responsible for verifying user's transactions, they own the smart meters used by the prosumers and, hence, they can verify that the prosumers are not lying about their consumption/production amounts. Also, if a prosumer fails to pay, the coordinator may take the necessary measures, although those are outside the scope of this proposal.
- Operators (O_i): are tasked with registering prosumers on the smart grid layer, connecting them, and giving them the authorization to send messages with the relevant trading information to their respective groups. They connect the prosumers to the smart grid physically (wiring) and digitally (giving them the necessary permissions).

The *prosumer layer* is composed of several groups of prosumers who are geographically close to each other. In these groups, they trade electricity among themselves to increase efficiency.

The *smart grid layer* is located between the prosumers layer and the main grid layer. This layer also has a coordinator for each group of prosumers, each coordinator verifies their group members transactions. This layer has the information of the energy usage of each group, which means that, in case a prosumer group needs more electricity or has a surplus, the smart grid layer communicates with the main grid level to buy or sell that electricity. In order to obtain that information, it records all transactions between prosumers in each group with the energy usage information.

Finally, the *main grid layer* is the system as we know of it today. It is composed of the main electrical companies with their bulk electricity generators and also control the distribution of energy.

2.2 Overview of the proposal

The four main steps of the envisaged system are: *Initialization*, *Price calculation*, *Energy trading*, and *Debt liquidation*.

In the *Initialization* step, prosumers (i.e., consumers and producers) should register to the operators and they must be authorized to interact with the smart grid infrastructure.

The *Price calculation* step starts the day before energy trading, with a prediction of energy usage, which is already in use in most energy markets and its

development is out of the scope of this work. That's when the main grid estimates the demand and communicates with the main electricity producers. The producers are ranked based on their prices, with the most expensive determining the trading price for electricity in each time slot. This is done in resemblance as in most parts of the EU [16]. In this proposal, the price is determined in different time slots of the day.

The *Energy trading* step consists of the communication between the prosumers' smart meters with the smart grid layer. In particular, the user's electricity usage and transactions is monitored by a smart meter located at their home. This device periodically stores the electricity production/consumption information to the smart grid layer via transactions on the blockchain, allowing to track the user's electricity usage so that the debt of the user can be calculated with the amount of energy produced/consumed and the price in each time slot. The smart grid infrastructure monitors the energy needs of each group and can request additional electricity from the main grid or sell any surplus energy back to it. To facilitate these transactions, the main grid is treated as an additional prosumer in the system. Prosumers' transactions are verified by the coordinators. These entities own the smart meters located at the prosumers' homes and they act as trusted third parties (TTPs).

Finally, in the *Debt liquidation* step, the smart grid collects all of user's transactions and assigns each of them a debt to be paid (to them if they're producers of from them if they're consumers). This debt is communicated to the consumers and, once it's paid, the corresponding amount is distributed to the producers. This way, there's no direct interaction between each consumer and producer.

3 The proposed system in detail

This section first explains the blockchain-based smart contracts which are the core components of the proposed solution. After that, it details the four main steps: *Initialization*, *Price calculation*, *Energy trading*, and *Debt liquidation*.

3.1 Main smart contract

The main smart contract (SC_{MG}) is the first component to be deployed. This contract acts as an intermediary between each prosumer group (G) and the main grid.

Its initial task is to obtain and store the necessary information about each main grid producer (MG_P) so they can communicate their energy production capacity and price of production. To achieve this, each MG_P creates a blockchain account and registers it with the main SC. The SC then verifies the provided information and stores the address of each MG_P. Using the information provided by each MG_P and the knowledge possessed by the main grid (MG), the SC_{MG} can calculate the price of electricity at any given time of the day. In addition

to that, the SC_{MG} needs the addresses of all the other SC so that they can communicate any missing or surplus energy in each group.

The MG_P keeps track of all transactions between each SC and the MG. Once a prosumer group needs energy from the MG or is willing to sell a surplus, the SC_{MG} registers the transaction with the quantity of energy and the price. This procedure is similar to the one followed between prosumers in each SC.

The SC_{MG} consists of a class which holds:

- *Date*: Date of the trading day of the SM_{MG}
- *Producer identities*: Public keys of MG_P which can interact with the SC_{MG} and sell electricity to the MG.
- *Coordinator identities*: Public keys of Co which can register SC into the SC_{MG}
- *Main Grid Authority*: Public key of the owner of the SC_{MG}.
- *Expected electricity consumption*: The predicted electricity consumption by the MG for the following day.
- *Production capacity*: List of the production capacity of the different MG_P and its price, divided by time slots.
- *Prices*: List of the price of electricity in each time slot.
- *Group smart contracts*: Addresses of all the SC that can interact with the SC_{MG} and sell or buy energy from the MG.
- *Transactions*: List of all transactions made between the MG and the SC. Each transaction contains the amount sold/bought and its price.
- *Debts*: List of all debts from each SC and the MG.
- *Time slot*: Number of the current time slot. -1 before the trading and 24 when it's over.
- *Trading flag*: Boolean which is "True" when the trading in the MG_{SC} is available.
- *Producers flag*: Boolean which is "True" when MG_P are able to be registered into the MG_{SC} and make an offer.
- *Smart Contracts flag*: Boolean which is "True" when the SC are able to be registered into the MG_{SC}.

When a new SC_{MG} is deployed, the MG must provide the following arguments: i) *Date of the trading day*; ii) *Expected energy consumption*. By default, *Trading flag* is set to "False" and *Producers flag* is set to "True", *Time slot* is set to -1.

Once the SC_{MG} is deployed, the different actors can interact with it with the following methods:

- *newProducer*() method can only be called by the MG authority when the *Producers flag* is set to "True". It introduces a new MG_P which will be able to sell electricity in the trading day. The producer is added to *identities*.
- *newSC*() method can only be called by the Co when *Smart Contracts Flag* is set to "True". It registers all SC that will be able to communicate the need or surplus of electricity of each group. The new SC is added to *Group Smart Contracts*.

- *addOffer*() method which can be called by MG_P when *Producers flag* is set to "True". It communicates the available production and its price at a certain time slot. The offer is added to *Production capacity*.
- *beginAuction*() method called by the MG which, once all MG_P have registered and added their offers or the time limit has come, it determines the electricity price for each time slot. It sets *Producers Flag* to "False".
- *beginTrading*() method called by the MG when the trading day starts. It sets *Smart Contracts Flag* to "False" and *Trading Flag* to "True". It also communicates all the SC that the trading begins.
- *changeTime*() method called by MG, it increases *Time slot* by 1.
- *buyElectricity*() and *sellElectricity*() methods are called by the SC during the trading day, when *Trading flag* is set to "True". SC communicate the needed electricity or the surplus that has to be bought/sold to the MG. Both the amount and the price is stored in *Transactions*.
- *calculateDebts*() method called by the MG once the trading has ended. From all the registered transactions, it calculates the debt each SC and the MG has. Every debt is stored in *Debts*. It sets *Trading Flag* to "False". It also calls the method *calculateDebts*() from each SC.
- *payElectricity*() method called by each SC which has a debt with the MG. The SC_{MG} distributes the funds to the corresponding sellers (MG_P or other SC).
- *getDebt*() method is called by any actor and, if it exists, it returns the debt that she has to pay.

3.2 Group smart contracts

After deploying the SC_{MG}, the next step is to deploy the SCs. Each prosumer group (G) has several SCs that are responsible for tracking the energy usage and price for each user (U) within the G. Each group has its own SC in order to incentivize first local electricity trading. Furthermore, each group has several SC in order to increase the privacy of the users by dividing their real electricity usage into different values.

To ensure that each U can send Tx to their respective SC, they must be registered in the SC. It possesses a table which contains the necessary information to authorize each user. Additionally, the SC must register with the SC_{MG} in order to receive information on the price at which electricity is sold during each time slot. It is worth mentioning that the authorization tables within each SC must be kept up to date. For example, if a new U joins the group or an existing U leaves, the table must be updated accordingly. This ensures that only authorized Tx are recorded and that the energy usage and billing remain accurate. Moreover, each SC must possess the identity of the coordinator (Co) of the group. The coordinator is the only authority that can verify the Tx from each U.

Once the SCs have been deployed and authorized, they can start collecting the Tx made by each U within the group. This data is important for ensuring fair and accurate billing according to the energy usage within the group.

*SC*s can communicate with the SC_{MG}. For example, if one group has a surplus of energy, they can communicate with the SC_{MG} which can communicate with another group that needs more energy and sell their surplus.

Each *SC* consists of a class which holds:

- *Main smart contract*: Address of the SC_{MG} in which the *SC* is registered.
- *Date*: Date of the trading day of the *SC*.
- *Coordinator*: Public key of the *SC*'s *Co*.
- *User Identities*: Public keys of all *U* of *SC*'s *G*. Those users are able to sell/buy electricity.
- *Operator Identities*: Public key of operators who can register new *U* into the *SC*.
- *Prices*: List of the price of electricity in each time slot.
- *Transactions*: List of all transactions made between *U*. Each transaction contains the amount sold/bought and its price.
- *Debts*: List of all debts from each *U*.
- *Time slot*: Number of the current time slot. -1 before the trading and 24 when it's over.
- *Trading flag*: Boolean which is "True" when the trading in the *SC* is available.

When the *SC* is deployed, the *Co* must provide the following arguments: i) *Date of the trading day*; ii) *Main smart contract address*. By default, *Trading flag* is set to "False", *Time slot* is set to -1.

Once the *SC* is deployed, the different actors can interact with it with the following methods:

- *newOperator*() method called by the *Co* which adds a new *O* public key which will be able to register *U*.
- *newUser*() method called by the *O* which adds a new *U* which will be able to sell/buy electricity.
- *beginTrading*() method called by the SC_{MG} which sets the *Trading flag* to "True" and also communicates all prices.
- *buyElectricity*() and *sellElectricity*() methods are called by *U* during the trading day once every time slot, only when *Trading flag* is set to "True". *U* communicates the consumed or produced electricity to be bought/sold to others *U*. Both the amount and the price of the time slot is stored in *Transactions*.
- *verifyTransaction*() method is called by *Co* when, at the end of each time slot, the *Co* verifies each *U* transaction.
- *calculateDebts*() method is called by the SC_{MG} once the trading day has ended. From all the registered transactions, it calculates the debt each *U* has.
- *payElectricity*() method called by each *U* which has a debt with the *G*. The *SC* distributes the funds to the corresponding sellers (SC_{MG} or other *U*).
- *changeTime*() method called by *Co*, it increases *Time slot* by 1. It also calculates the surplus energy or the needed energy that the *G* has had in the previous time slot and communicates it to the SC_{MG}.

– *getDebt*() method is called by any actor and, if it exists, it returns the debt that she has to pay.

3.3 Initialization

During the initialization stage some tasks must be performed by the Main Grid (MG), Operators (O), Coordinators (Co), and Users (U). These tasks for each entity are next detailed:

– The MG authority performs the following steps:
  1. Deploys the SC_{MG}, with the corresponding arguments explained in the previous section.
  2. Communicates the SC_{MG} address to the Co and MG_P.
  3. Registers MG_P to the SC_{MG} using *newProducer()*.
– The Co of each group performs the following steps:
  1. Deploys each SC, with the corresponding arguments explained in the previous section.
  2. Communicates each SC address to the SC_{MG} using *newSC*().
  3. Registers O to the SC using *newOperator*().
– Each O performs the following steps:
  1. Installs a sealed smart meter SM_k at U_k's domicile.
  2. Connects SM_k to U_k generation and consumption's electricity line in order for SM_k to read U_k's electricity usage information.
  3. Connects SM_k to Co_k in order for Co_k to validate SM_k information.
– Each U registers to the system by following the next steps:
  1. U is given a blockchain account and a private key and uses a Key Derivation Function to create n key pairs/addresses. The private keys are stored in a secure storage in which only U has access.
  2. U communicates every public key to the O, as well as their identification via a secure and private communication system.
  3. O registers U into each SC using the*newUser*() function and a group signature scheme.
  4. O communicates U information to Co in order for the Co to be able to identify the U.
  5. O sends U each SC address.

Users of the smart grid need to have a wallet address to interact with the smart grid It also serves as a form of identification and verification, allowing other users and smart contracts to confirm the user's identity.

The user registration process is a crucial aspect of any smart grid system, as it ensures that only authorized individuals are able to access and perform transactions within the network. In this particular smart grid system, the registration of users is managed by the operators through the use of smart contracts. These contracts provide a secure and reliable mechanism for verifying the identity of users and controlling their access to the network. During the registration process, users are required to provide certain information such as their name,

contact information, and other relevant details. This information is then stored by the coordinator, and it's linked to the user's blockchain address in a private storage. Once a user is registered, the smart contract assigns them a unique identifier or address, which is used to track their transactions within the network. This address is also used to authorize their access to the network, ensuring that only authorized users are able to perform transactions.

3.4 Price calculation

1. All available P send their offer to the SC_{MG} using *addOffer*().
2. When the deadline comes, MG authority ends the bidding time using *beginAuction*().
3. SC_{MG} does the following:
   (a) In each time slot, it sorts the offers from the cheapest to the most expensive one.
   (b) Selects the n cheapest MG_P in each time slot so that the expected electricity consumption meets with the production.
   (c) The price in that time slot is the one from the most expensive MG_P offer from the n selected.

3.5 Energy trading

1. The MG authority sends the method *beginTrading*() to the SC_{MG} when the trading day starts.
2. When the SC_{MG} receives the order, it also sends the method to all the SC.
3. In order for a U/SM to communicate the consumption/production of energy in order to sell or buy it, they have to go through the following steps:
   (a) Every n amount of time, at least once in every time slot, SM checks if the electricity usage is positive or negative. Depending on the result, it will use the method *sellEnergy*() or *buyEnergy*(), but the procedure is the same.
   (b) The energy usage is divided into m transactions.
   (c) From k SC the G possesses, m SC are selected to receive each, one of the m transactions.
   (d) Each SC, when it receives the transaction, it adds it to the *Transactions* list with the current price of electricity. However, it's still marked as unverified.
4. Before the end of the time slot, Co must verify U's transactions in order for them to be traded successfully. To do so, it follows the next steps:
   (a) During the time slot, it stores the energy usage information from each U of the G.
   (b) It checks the *Transactions* list and for each transaction it's able to verify, it sends the method *verifyTransaction*() with the transaction ID to the SC_{MG}.
   (c) SC_{MG} marks the transaction as verified.

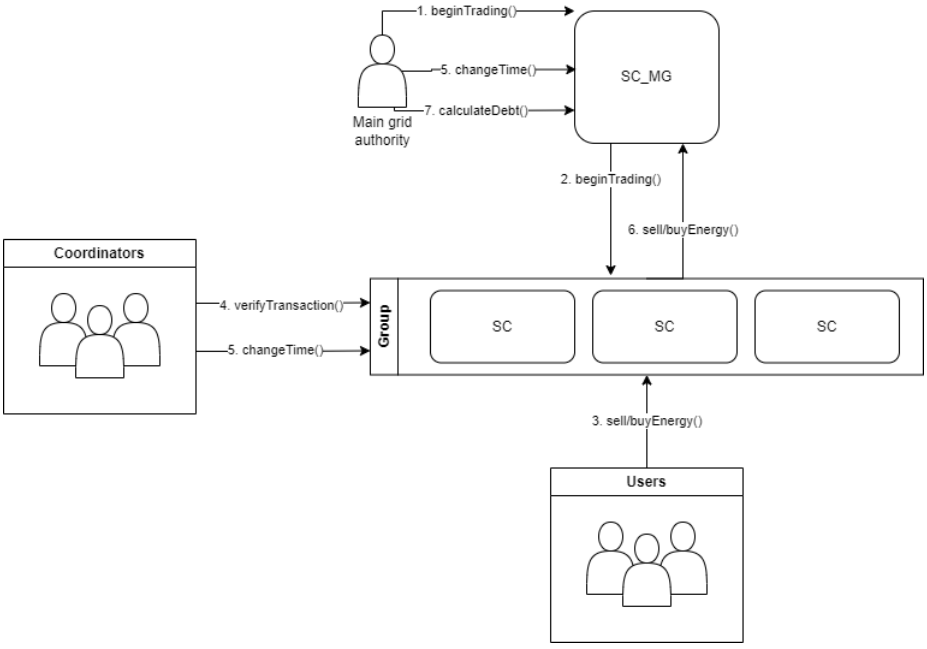


Fig. 2. Energy trading

5. *Co* now communicates the end of the current time slot to the *SC*. *MG* authority does the same with the SC_{MG}. They both use the method *changeTime*().
   (a) *SC* calculate the difference between the total electricity produced and consumed by *G*.
6. *SC* depending on the result of the difference, will call the methods *sellEnergy*() or *buyEnergy*() in the SC_{MG} with the total electricity produced or consumed.
   (a) If it's not the last time slot, the procedure returns to the point 3.
7. At the end of the trading day, the *MG* authority calls the method *calculateDebt()* which ends the trading phase.

3.6 Debt liquidation

1. The stage starts when the *MG* authority calls the method *calculateDebt()* in the SC_{MG}.
2. SC_{MG} calls the method *calculateDebt()* of each *SC*.
3. Each *U* who has consumed more than produced during the trading day, calls the method *getDebt()* from their *G* *SC*s.
4. Once each *C* has their debt, they must pay it to each *SC* with the method *payElectricity()*.

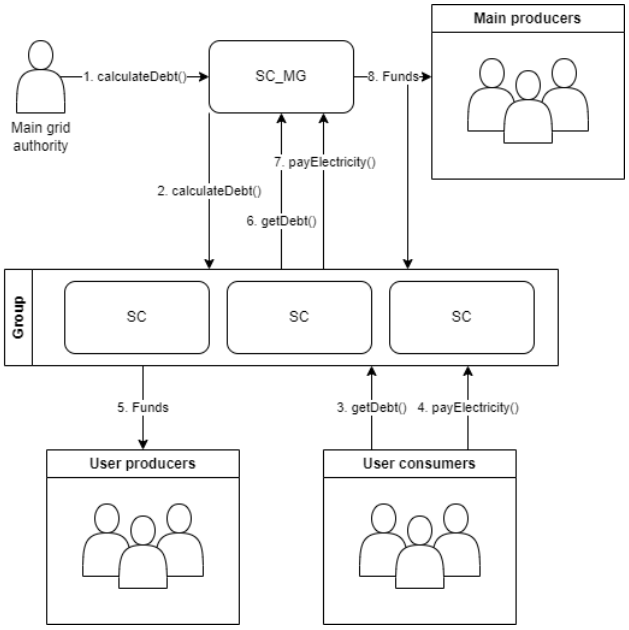


Fig. 3. Debt liquidation

5. SC pays each U who produced more than consumed and has to be compensated.
6. Each SC checks if G consumed more than produced by calling the method *getDebt()* in the SC_{MG}.
7. If SC owes funds to the SC_{MG}, it calls the method *payElectricity()* to pay the MG for the extra electricity the G needed.
8. Finally, SC_{MG} pays every MG_P for the energy produced, ending the third and final stage.

4 Dealing with security and privacy threats

This section studies the set of security and privacy claims that the new scheme fulfills.

Claim 1 *The system can detect unauthorized modifications or tampering of data.*

Proof. The immutability of transactions within a blockchain ensures the integrity and authenticity of each transaction, eliminating the possibility of double-spending. Given a secure and functioning blockchain, modifications or tampering of the ledger are not possible.

Claim 2 *Modified messages from producers and the smart grid layer are prevented from participating in the system.*

Proof. The system is secure due to the use of blockchain, which ensures that only legitimate transactions are allowed. This is due to the digital signature that each transaction possesses, if someone tried to modify a sent message to the smart contract, the signature would no longer be valid.

Claim 3 *The proposed system maintains high availability and is able to function without interruption.*

Proof. The proposed system provides high availability by leveraging the use of a blockchain with enough working nodes. The decentralized nature of the blockchain provides availability, providing constant and reliable access to data.

Claim 4 *The proposed system effectively restrict access to only authorized users preventing unauthorized individuals from performing protected actions and accessing protected resources and functions.*

Proof. The smart contract verifies the identity of users who sign every transaction. Then, it authorizes transactions only for registered users, maintaining the authorization requisites in the smart grid system.

Claim 5 *Users cannot deny having performed a particular action or Tx.*

Proof. The blockchain technology and the use of smart contracts ensure that transactions are traceable and tamper-proof, providing non-repudiation.

Claim 6 *Energy usage patterns cannot be derived from the Tx of the SC, even when having access to some of the Tx.*

Proof. Users are registered in multiple smart contracts in the group using a unique address in each one. In this way, only partial information about each user is available in each contract and those addresses cannot be linked by an external observer.

Claim 7 *The identity of a user and other personal information is not visible within the system.*

Proof. The link between each U's address and their true identity is only known by the Co which is assumed to be a TTP. Blockchain transactions do not uniquely identify users and they do not contain any personal information, only the partial energy usage. The link between the users and the operators that registered them is hidden behind the use of group signatures for operators. Operators use this method to generate a digital signature on behalf of the group of operators, hence, hiding the specific signing operator within the group and still validating the signature. Moreover, to further enhance user anonymity, users should periodically update their addresses.

Claim 8 *The proposed system uses coordinators to verify the messages sent by prosumers and to identify the misbehaving ones.*

Proof. Coordinators verify each prosumer's message to ensure that all transactions are free from any fraudulent activity such as double spending. Moreover, they can see all the transactions made by a certain U and evaluate whether they are fraudulent or not. Then, they can identify that U.

5 Conclusions and future work

This work has proposed a new energy trading system that serves as a bridge between the traditional grid and a smart grid, addressing the challenges associated with increasing demand, rising prices, and the limited availability of renewable energy sources.

The new scheme empowers users to both consume and produce electricity using distributed energy resources and it improves the current literature by taking into account the privacy of the users and the availability and security of the system; while still offering measures to identify and take punitive actions against misbehaving users.

As future work, we plan to implement this solution in lightweight devices (as real smart meters are assumed to be) and perform a deep study of its functionality, deployability (i.e., the economical and energetic cost of using smart contracts should be reasonable), and resiliency against security attacks.

Acknowledgments and disclaimer

This research is supported by the European Union Regional Development Fund within the framework of the ERDF Operational Program of Catalonia 2014-2020 with a grant of 50% of the total cost eligible, under the "FEM-IOT" project [001-P-001682]; by the EU's European Regional Development Fund (ERDF), through the "ERDF Catalonia Operational Programme 2014-2020, investment priority for the creation of jobs and sustainable growth", under the Territorial Specialisation and Competitiveness Project (PECT) "Cuidem el que ens uneix - Sensòrica" project [PR15-020174]; and projects RTI2018-095094-B-C21 "Consent" and PID2021-125962OB-C32 "SECURING/DATA" funded by MCIN/AEI /10.13039/501100011033/ FEDER, UE. HERMES project co-funded by INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA (INCIBE) and "European Union NextGenerationEU / PRTR".

References

1. Agung, A.A.G., Handayani, R.: Blockchain for smart grid. Journal of King Saud University - Computer and Information Sciences **34**(3), 666–675 (2022)
2. Aitzhan, N.Z., Svetinovic, D.: Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. IEEE Transactions on Dependable and Secure Computing **15**(5), 840–852 (2018)
3. Bhat, K., Sundarraj, V., Sinha, S., Kaul, A.: Ieee cyber security for the smart grid. IEEE Cyber Security for the Smart Grid pp. 1–122 (2013)

4. Congress, U.: Energy independence and security act of 2007. Public law **2**, 110–140 (2007)
5. de Vries, A.: Bitcoin's energy consumption is underestimated: A market dynamics approach. Energy Research & Social Science **70**, 101721 (2020)
6. Fang, X., Misra, S., Xue, G., Yang, D.: Smart grid — the new and improved power grid: A survey. IEEE Communications Surveys & Tutorials **14**(4), 944–980 (2012)
7. Guan, Z., Si, G., Zhang, X., Wu, L., Guizani, N., Du, X., Ma, Y.: Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities. IEEE Communications Magazine **56**(7), 82–88 (2018)
8. Hoffacker, M.K., Hernandez, R.R.: Local energy: Spatial proximity of energy providers to their power resources. Frontiers in Sustainability **1** (2020)
9. Hou, J., Wang, H., Liu, P.: Applying the blockchain technology to promote the development of distributed photovoltaic in china. International Journal of Energy Research **42**(6), 2050–2069 (2018)
10. Kang, J., Yu, R., Huang, X., Maharjan, S., Zhang, Y., Hossain, E.: Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains. IEEE Transactions on Industrial Informatics **13**(6), 3154–3164 (2017)
11. Khalid, R., Javaid, N., Almogren, A., Javed, M.U., Javaid, S., Zuair, M.: A blockchain-based load balancing in decentralized hybrid p2p energy trading market in smart grid. IEEE Access **8**, 47047–47062 (2020)
12. Mengelkamp, E., Notheisen, B., Beer, C., Dauer, D., Weinhardt, C.: A blockchain-based smart grid: towards sustainable local energy markets. Computer Science-Research and Development **33**, 207–214 (2018)
13. Mihaylov, M., Jurado, S., Avellana, N., Van Moffaert, K., de Abril, I.M., Nowé, A.: Nrgcoin: Virtual currency for trading of renewable energy in smart grids. In: 11th International Conference on the European Energy Market (EEM14). pp. 1–6 (2014)
14. 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 of Things Journal **8**(1), 18–43 (2021)
15. Nakamoto, S.: Bitcoin whitepaper. URL: https://bitcoin. org/bitcoin. pdf-(: 17.07. 2019) (2008)
16. PETCU, I.: How are eu electricity prices formed and why have they soared? . (2022), https://www.eurelectric.org/in-detail/electricity_prices_explained/
17. Reddy, K., Kumar, M., Mallick, T., Sharon, H., Lokeswaran, S.: A review of integration, control, communication and metering (iccm) of renewable energy based smart grid. Renewable and Sustainable Energy Reviews **38**, 180–192 (2014)
18. Samuel, O., Javaid, N.: A secure blockchain-based demurrage mechanism for energy trading in smart communities. International Journal of Energy Research **45**(1), 297–315 (2021)
19. Samuel, O., Javaid, N.: Garlichain: A privacy preserving system for smart grid consumers using blockchain. International Journal of Energy Research **46**(15), 21643–21659 (2022)
20. Stram, B.N.: Key challenges to expanding renewable energy. Energy Policy **96**, 728–734 (2016)
21. Zhuang, P., Zamir, T., Liang, H.: Blockchain for cybersecurity in smart grid: A comprehensive survey. IEEE Transactions on Industrial Informatics **17**(1), 3–19 (2021)