IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 9 October 2023, accepted 13 October 2023, date of publication 23 October 2023, date of current version 2 November 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3326946

RESEARCH ARTICLE

Privacy and Transparency in Blockchain-Based Smart Grid Operations

PIERPAOLO LORETI[1], LORENZO BRACCIALE[1], EMANUELE RASO[1], GIUSEPPE BIANCHI[1], ELEONORA RIVA SANSEVERINO[2], AND PIERLUIGI GALLO[2]

[1]Department of Electronic Engineering, University of Rome Tor Vergata, 00133 Rome, Italy
[2]Department of Engineering, University of Palermo, 90128 Palermo, Italy

Corresponding author: Lorenzo Bracciale (lorenzo.bracciale@uniroma2.it)

This work was supported by the BLORIN Project funded by the Sicilian Region POFESR Azione 1.1.5. Grants under Grant CUP g79j18000680007 Cod. Prog. 08PA7112100263.

ABSTRACT In the past few years, blockchain technology has emerged in numerous smart grid applications, enabling the construction of systems without the need for a trusted third party. Blockchain offers transparency, traceability, and accountability, which lets various energy management system functionalities be executed through smart contracts, such as monitoring, consumption analysis, and intelligent energy adaptation. Nevertheless, revealing sensitive energy consumption information could render users vulnerable to digital and physical assaults. This paper presents a novel method for achieving a dual balance between privacy and transparency, as well as accountability and verifiability. This equilibrium requires the incorporation of cryptographic tools like Secure Multiparty Computation and Verifiable Secret Sharing within the distributed components of a multi-channel blockchain and its associated smart contracts. We corroborate the suggested architecture throughout the entire process of a Demand Response scenario, from the collection of energy data to the ultimate reward. To address our proposal's constraints, we present countermeasures against accidental crashes and Byzantine behavior while ensuring that the solution remains appropriate for low-performance IoT devices.

INDEX TERMS IoT, blockchain, privacy, accountability, verifiability, secure multiparty computation.

I. INTRODUCTION

To create a sustainable society, various renewable energy sources, such as wind power, photovoltaic (PV), etc., must be progressively included in the electrical grids. However, the unpredictability of these sources, compared to traditional ones, raised new challenges for grid operators that are becoming increasingly difficult to solve as the percentage of renewable energy in the grid increases. In this scenario, Smart Grids are playing a key role in managing this transition, as can be seen from the number of technological solutions that have been proposed and adopted in recent years. In fact, efficient management of the energy produced and consumed is only possible thanks to the timely analysis and control of the system achieved through Internet technologies [1].

The associate editor coordinating the review of this manuscript and approving it for publication was Fabio Mottola.

In fact, renewable energy sources, in particular, photovoltaic (PV), have allowed small communities or even individuals to generate their own electricity and potentially sell the surplus to other communities or to the network itself [2]. But the roles can be reversed and those who produce energy at some times can take it from the grid at other times. The volume of generated transactions is difficult to manage with traditional techniques and several works have proposed and successfully applied the blockchain to handle such complexity in a distributed way [3], [4]. In this scenario, blockchain technology has proven its applicability beyond digital currencies due to its inherent characteristics that allow the development of tamper-resistant, traceable, highly reliable, and decentralised systems [4]. The primary application of blockchain in smart grids has been to enable consumers and prosumers to trade electricity without the intervention of a third party. However, in a broader vision,

blockchain can be used *beyond energy trading*, allowing Grid Operators to implement balancing policies or optimisation strategies that can improve the sustainability of the network as a whole.

A. DISTRIBUTED GRID MANAGEMENT

Endeavors, exemplified in [5], [6], [7], [8], and [9], have been directed towards proposing decentralized grid management solutions employing Blockchain technology. However, these works have demonstrated complexity in execution and susceptibility to a range of security and privacy concerns. Consider, for example, the Demand Response (DR) technique proposed in [5], [6], and [8]: it is a popular solution which allows one to lower or postpone the demand/injection of energy in response to technical issues in the network. The process is in principle quite simple: the grid operator asks users to reduce or increase their load within a given time frame in the future; if they do that, they are rewarded. DR is particularly important for the integration of renewable energy in the electrical grid because it allows the operator to control the energy absorbed and cope with temporary shortages of energy produced in order to optimise energy production. To implement DR, the grid operator needs to determine how to divide the energy reduction/increase among end users, and this information depends on the history of consumption of each user, called *customer baseline* [8]. Specifically, the processes of monitoring consumption, deriving the consumption baseline of the customer, calculating the per-user energy demand and the reward based on actual consumption of the users [9] go far beyond basic energy trading but can be implemented on the blockchain using Smart Contracts as a Decentralised Application (dApp) [10]. Many functions within grid service provisioning exhibit comparable characteristics and challenges to those encountered in the field of Demand Response. Specifically, these functions require the gathering of measurements and data from both the network and users. This data is then used to identify needs, solicit the optimal grid service, and compensate end users accordingly.

B. SECURITY AND PRIVACY

The advantages inherent in such a decentralized approach, when compared with a centralized one, primarily encompass accountability, transparency, trust, and the system's capacity for thorough auditing. However, the primary drawback of this approach lies in the realm of user privacy, as highlighted for example in [11]. This concern gains significance due to the inherent sensitivity of prosumers' energy consumption data, a vital component that pertains to their personal patterns of energy utilization and production, as noted in the study by [12]. The potential exposure of such intricate details could not only lead to breaches of individual confidentiality but might also entail broader implications, ranging from security risks to the possibility of exploiting consumption habits for targeted marketing or even more malicious purposes. As a result, finding a delicate equilibrium between data-driven insights and preserving the privacy rights of users becomes an essential consideration in the continued development and implementation of this decentralized model.

Recently, to ensure both privacy and accountability in the blockchain, several works are proposing the use of Privacy Enhancing Technologies (PETs) such as Secure Multiparty Computation (SMC), which allows peers to perform a joint calculation of sensitive data without any privacy leakage [13], [14]. The foundational cryptographic methods for such systems include Homomorphic Encryption (HE), Secret Sharing (SS), and Zero-Knowledge Proof (ZKP) schemes. These techniques enable the creation of secure solutions adaptable to various scenarios, ensuring exceptional levels of security and privacy, as highlighted in [15]. The price to pay is the complexity of the system that sometimes limit its widespread applicability. Furthermore, the findings in [16] appear to indicate that incorporating privacy features into blockchain could potentially compromise accountability, a fundamental factor driving the adoption of this technology. Consequently, the system's ability to ensure transparency, fraud detection, identification, and other functionalities may be diminished. As a result, the previously perceived suitability of blockchain as an ideal solution for smart grid systems might be cast into doubt, prompting questions about the practical utility of this technology in such a context.

C. GOALS AND CONTRIBUTIONS

The primary objective of this study is to demonstrate the feasibility of utilizing blockchain for efficient execution of distributed management procedures within a smart grid, extending well beyond mere energy trading bookkeeping. In pursuit of this objective, we have devised a system framework that combines PETs with blockchain technology, thereby ensuring both security and privacy, while retaining all the advantageous features inherent to blockchain. Specifically the main contributions of the paper are:

- we devise a solution enabling blockchain smart contracts to utilize secure multiparty computation (SMC) for executing logical and mathematical operations on encrypted data;
- we emphasize the challenges that emerge when employing SMC in relation to reliability and transparency. Consequently, we present suitable cryptographic techniques that empower nodes to validate both the dependability and precise implementation of the procedure;
- we prove the effectiveness of the proposed system applying the solution to DR (Demand Response) and demonstrating its ability to protect users' privacy while retaining blockchain features (transparency, fraud detection, identification);
- we provide a comprehensive security analysis, considering all possible adversaries and investigating all possible threats to the various entities comprising the proposed solution;

- we experimentally evaluated the computational cost of privacy-preserving techniques integrated in the solution to assess its feasibility.

The paper is organised as follows: Section II presents the related work, Section III describes the reference scenario and the system model, Section IV describes the proposed security architecture and Section V presents the results of the experimentation. Finally conclusions are drawn.

II. RELATED WORK

The literature on blockchain privacy is vast (please refer to [30] for a general overview), so in this section we will focus on smart grid scenarios. In Table 1 we summarise the difference between the various approaches involving blockchain, privacy, and smart grids. The interested reader can find a more detailed survey in [31].

A. PRIVACY IN BLOCKCHAIN

In the context of smart grids, blockchain has been studied in the literature mainly with a focus on energy trading applications. Since blockchain identifiers are inherently anonymous by their own nature, such application already provides a certain degree of privacy to the users. However, in some cases, it may not be enough to protect users from linkability attacks. These attacks involve correlating blockchain data with external sources to discover the individual user associated with a blockchain identifier [17]. For this reason, additional techniques have been proposed such as address fuzzification, data/route hiding [6], or data perturbation to protect against malicious data miners [17].

In [16], a system for decentralised energy trading using blockchain and anonymous messaging streams is presented. The authors adopted multi-signatures to ensure the authenticity of transactions, and anonymous messaging streams to protect the privacy of participants. Other works use modern encryption techniques to ensure user privacy. For example, in [19], a system for privacy-preserving data aggregation using homomorphic encryption is devised. Instead, in [20], the authors use attribute-based encryption (ABE) to protect the privacy of participants, and blockchain to ensure the security of transactions. In [21] Galois field are adopted to protect the privacy of data while [22] proposes asymmetric confidentiality to allow energy consumers to encrypt their energy consumption data before uploading it to the blockchain, so that only authorised entities can decrypt it.

Interesting solutions have been proposed in the context of blockchain-based measurement sharing using smart marketplaces: [23] proposes a system for sharing smart grid measurements while preserving the privacy of the data owners using differential privacy to allow data owners to share their data without revealing too much about themselves. In [24] a lightweight privacy-enabled message exchange mechanism is presented and in [25] the technique is extended using a protocol for anonymity and intractability of transaction data with cryptographic Proof-of-Authority, RSA and Chinese reminder threorem.

It is noteworthy that there are several existing solutions for centralized tamper-proof systems, such as LedgerDB [32], a centralized blockchain-like ledger database with tamper-evident and non-repudiation capabilities, and VeDB [33], a high-performance software- and hardware-enabled DBMS. While centralized systems have higher performance, we focus on distributed systems because they do not require a single credible central authority.

B. GRID MANAGEMENT PROCEDURES

Most of the application of blockchain in smart grid focus on energy trading, as also shown in table 1. In the last rows of the same table we summerize the works that use it for DR management. In [5] a blockchain-based system called Guardian for secure demand response management in smart grid systems is proposed. The system uses a smart contract to automate the demand response process and ensure that all participants are treated fairly. Guardian was implemented and evaluated in a real-world testbed, and the results showed that it can significantly improve the efficiency and security of demand response management. In [28], the authors propose a blockchain-based system for demand response that provides security and trust between the different participants in the system. The system uses a private blockchain to ensure that only authorised participants can access the data, and it uses a smart contract to automate the demand response process. The system was evaluated in a simulation study and the results have shown that it can improve the efficiency of demand response management. In [12], a system for energy transactions in demand response is presented. It uses a public blockchain to record energy transactions and zero-knowledge proofs to protect the privacy of participants. The work in [11] proposes a system for demand response that certifies the quality of demand response services. The system uses a smart contract to store the data about the demand response services and a reputation system to evaluate the quality of the services. The system was implemented and evaluated in a real-world testbed, and the results have shown that it can improve the transparency and reliability of demand response management. In [27] a framework for aggregation and remuneration in demand response is described. The framework uses a smart contract to aggregate the demand response bids from different participants, and it uses a payment channel to ensure that the participants are paid fairly. In [29] authors propose a privacy-preserving blockchain solution to support demand response in energy trading. The solution uses a homomorphic encryption scheme to encrypt the demand response data, and it uses a private blockchain to ensure that only authorised participants can access the data. The solution was evaluated in a simulation study, and the results have shown that it can preserve the privacy of the demand response data while still allowing for efficient and secure energy trading.

TABLE 1. Works addressing privacy in Blockchain-based Smart grid.

Ref	Smart Grid Application	PETs	Threat Model
[16]	Energy trading	Multi-signatures, anonymous messaging streams	Data forgeability, double spending, network takeover and wallet security attacks
[17]	Energy trading	Private key mechanism	Linking attacks by malicious miners
[18]	Energy trading	Group Signatures and covert channel authorization	Authorization attacks used to illegally distributing electricity
[19]	Energy trading	Homomorphic encryption and data aggregator	Honest but curious aggregator
[20]	Energy trading	Attribute-based encryption	Attack on user data confidentiality
[21]	Energy trading	Custom with permutation–substitution public key cryptosystem	Attack on user data confidentiality
[22]	Energy trading	Group signature	Attack on user data confidentiality
[23]	Measurement sharing	Differential Privacy	Attack on user data confidentiality
[24] [25]	Measurement sharing	Cryptographic Proof-of-Authority (PoA), RSA	Controlling communication channels, capturing session IDs, launching identity-related attacks and transactional data privacy attacks
[26]	Tariff decisions	Oblivious transfer; data transformation with distance-preserving embedding	Reveal other information than the minimum distance between the customers' load profile forecast and the template load profiles of the utility provider
[5]	DR management	Data minimization with miner selection	Invalid transactions stored in the BC
[11] [27]	DR management	ABAC and hyperledger channels for for data isolation	Attempts to break the confidentiality of user data
[12]	DR management	ABAC and hyperledger channels for for data isolation	Attempts to break the confidentiality of user data
[28]	DR management	Data minimization with intermediator (Virtual Nodes)	Not specific privacy threats; main concerns are about correct contracts execution
[29]	DR management	Trivial Secret Sharing	Malicious data miners, cheating users and infrastructure nodes

C. POSITIONING

Sometimes security and privacy push in apparently opposite directions: on the one hand, there is the need to make the trading system transparent to allow audits and all the stakeholders accountable for their trading; on the other hand, there is the need to protect prosumers' privacy. A key point is about the trust model: differently from cryptocurrencies, the electrical grid scenario involves a tangible asset (i.e., the electrical energy) that can be spoofed/faked at different levels, including the origin of the data (usually the smart meter), therefore invalidating any subsequent data processing. For this reason, our approach consists in designing an architecture that protects both the user and the grid operator or aggregator against cheating on the declaration of electricity demand/injection modulation.

To this aim, SMC techniques can come in handy. SMC has been proposed on the blockchain [14], together with Verifiable Secret Sharing (VSS), using the ledger and a game-theoretical approach to reward (or punish) the parties of the participants financially, encouraging everyone to play by the rules. Authors underline the need for SMC to be fair (either all parties get the output or none) and robust (a malicious adversary cannot easily mount a Denial of Service against the protocol) which also motivates our work.

Note that SMC and blockchain are philosophically antithetical technologies: in fact in blockchain by definition all nodes perform the same operations while in SMC techniques each node has to perform a part of the procedure. As will be described in detail, we use SMC to count encrypted data in a similar way to [29], but we guarantee the robustness of the procedure in a statistical way overcoming the reported denial of service problems.

III. SYSTEM MODEL

A. SMART GRID

First, we present the reference system model and the actors involved for the smart grid that is depicted in Figure 1. The physical level comprises users and *prosumers* equipped with PV installations that can be organised in energy communities. Usually, users are organized in associations, called energy communities and can be represented by an aggregator. We have also highlighted the so-called 'prevalent producers' according to the Italian transposition of the EU directive on Renewable Energy II (RED II): consumers who have a significant photovoltaic system and a legal entity that receives incentives for virtual or physical self-consumption. Figure 1 shows industries which normally consume a significant share of the grid's energy and, therefore, can play an important role in stabilising the grid as a whole. All prosumers are connected to the main grid powered by both renewable and fossil-based energy sources (i.e., non-renewable sources). The management of the high-voltage grid is entrusted to Transmission System Operators (TSOs) and while the distribution networks are managed by the Distribution System Operators (DSOs). In the following, for the sake of simplicity we will only consider refer to them as Grid Operators.

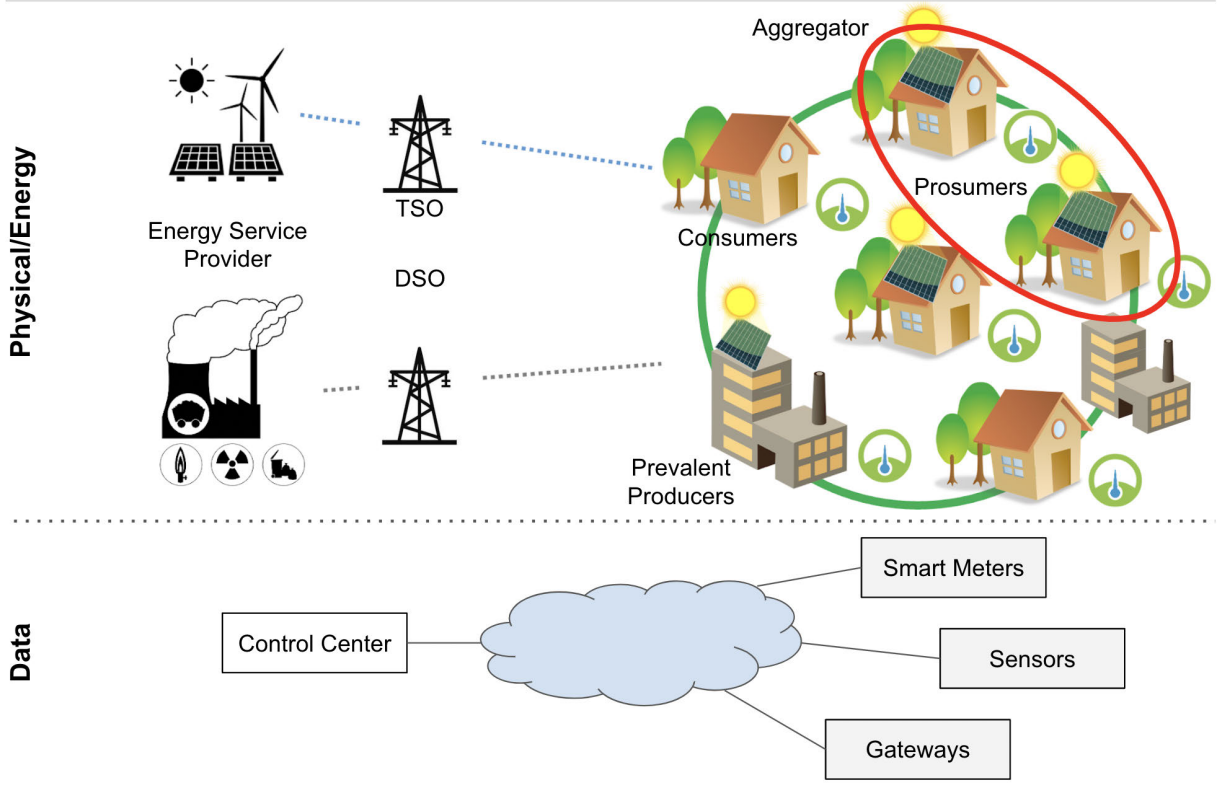

FIGURE 1. Smart Grid Reference System Scenario.

The lower part of Figure 1 shows the data level of the smart grid where IoT devices play a central role in controlling and monitoring all physical elements. The system includes the control center that is connected via the communication network to all IoT devices including the smart meters (SMs), sensors, gateways, etc. In fact, both residential and commercial buildings are equipped with devices that are able to control the local energy loads. Such loads can be classified according to their modulation capability in shiftable (e.g. pool pumps, dryer or washers), adjustable (e.g., heating, ventilation or air conditioning), or uninterruptible (e.g., lights or refrigerators) [34].

B. DEMAND RESPONSE

Load modulation is an important asset for modern smart grids that include renewable sources. In fact, traditional grid operators continuously adapt the output power according to the network load which, however, typically varies slowly over time. On the contrary, when renewable sources are considered the electricity production may vary dramatically, e.g. due to the weather, and thus users can help the operator in grid stabilisation by modulating their loads either to prevent consumption peaks, to cope with a weather-related energy shortage or to prevent congestions.

Over the time, numerous DR techniques have been designed, implemented and tested: using the smart grid data plane, the DSO asks prosumers to reduce their load in a given timeframe, emitting a DR request. Users may meet such requests and can be rewarded accordingly.

DR programs and supporting technologies can be extremely complex and a vast literature has been consolidated over the past 10 years. The generic workflow mentioned in [8] will be presented below and depicted in Figure 2. The DR procedure is enough complex to highlight the critical aspects that blockchain technology brings in these scenarios in terms of security and privacy, as well as all the features of the architecture of the proposed system.

The complete DR algorithm workflow is detailed in the following:

1 the grid operator publishes an energy reduction request, namely `Demand(timespan, amount)` where *timespan* is the duration of the reduction request and *amount* is how much energy reduction is required;
2 for each user, a baseline B^i is periodically computed calling the function `ComputeBaseline(user)`. The algorithms most commonly used to compute the DR baselines are in the "X of Y" family [35] that work as follows. Consider, for instance, a day divided into 96 time slots of 15 minutes each. With respect to a specific time slot (e.g., every day from 9:00 am to 9:15 am), a high X of Y baseline can be obtained by averaging the X highest values of consumption in the Y days preceding the DR event. For example, the average of the highest $X = 3$ energy values measured in the last

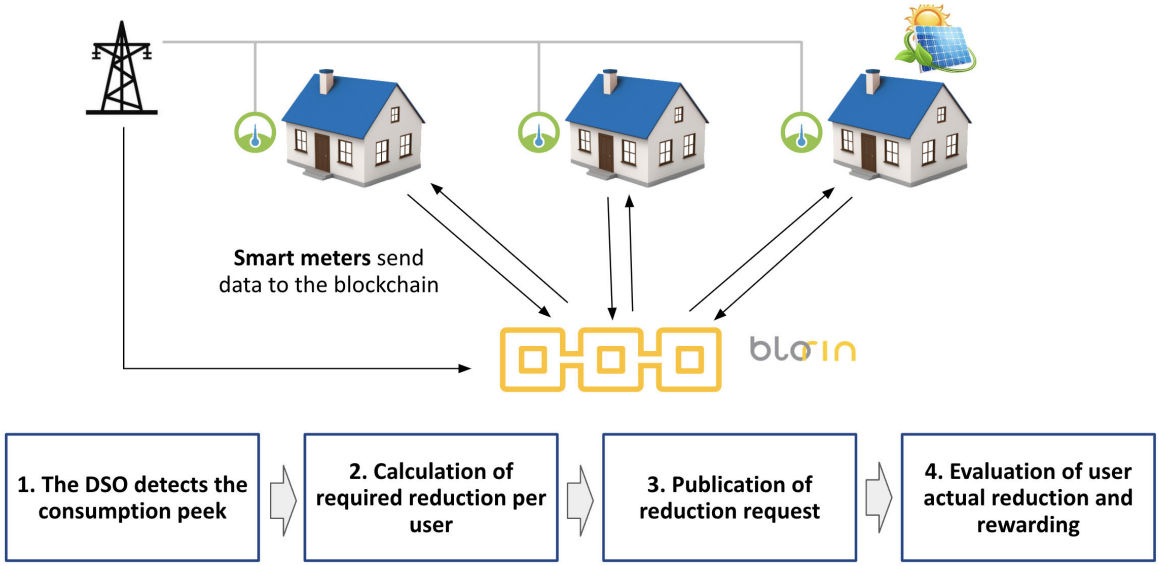

FIGURE 2. Demand Response workflow with a blockchain-based Energy Management System.

week ($Y = 7$) for a given slot (9:00 am to 9:15 am). This is repeated for all the time slots. The resulting baseline is thus a dynamic set of values, one for each specific time slot, that changes every day. In formulae, the baseline of the i-th user is equal to the vector:

$$B^i := [\bar{p}^i_{B,1}, \bar{p}^i_{B,2}, \ldots, \bar{p}^i_{B,h}, \ldots, \bar{p}^i_{B,96}]$$

with

$$\bar{p}^i_{B,h} := \frac{1}{X} \sum_{j \in High(X,Y)} p^i_{B,h,j} \quad \forall h \in \{1, \ldots, 96\}$$

where $p^i_{B,h,j}$ is the j-th highest comsumption value of the h-th time slot;

3 the reduction asked to each user is calculated using `ComputeRequestedReduction(user, user_baseline, amount, user_quality)`. For the sake of simplicity, we assume that the quota required to each user depends only on the ratio between the user's baseline and the aggregated baseline (sum of the baselines), namely $\frac{B^i}{B^{tot}}$. In more complex scenarios, this depends also on the user's rating, i.e., how the user contributed during past DR events;

4 finally, when the timespan of the DR event is over, the function `ComputeActualReduction(user, act_consumption, baseline)` computes the actual user reduction, given by the difference between the per-user request and its actual consumption and recognizes a remuneration for the user.

Steps 2, 3, 4 can be automated in the blockchain-based Energy Management System (EMS) using smart contracts that implement the functions indicated above, as described in [8] and [36].

C. BLOCKCHAIN ARCHITECTURE

We want to implement the described DR workflow using Blockchain with most of the operations performed automatically by smart contracts (SC). The considered scenario implies that at the users' premises an EMS device is installed. The device hosts a client application that is able to run a SC for reading/writing data on the blockchain. Measurement data can be acquired by the channel 2 of the Smart Meter used for registering energy consumption. Consumption data sent by the SM may be subject to audit by the DSO. This ensures that these data are considered reliable.

In the architecture, on one hand, we want to preserve the privacy of the user but, on the other, we want to make the user accountable (i.e., they must not cheat). For this reason, we propose an approach with multiple channels depicted in Figure 3: one channel that is available to all the involved actors (public) and several other channels that are visible only to subsets of actors (private).

The concept of Blockchain channels is supported naively by several Blockchains such as Hyperledger Fabric or Multichain. However, it can also be implemented using multiple blockchain instances, instead of channels, jointly with an *Inter-Blockchain Communication* (*IBC*) protocol. In the remainder of the paper, for the sake of simplicity, we will only consider the case of a multi-channel blockchain. We assume that there is a private channel between each prosumer and the grid operator (or aggregator). Each private channel runs a Smart Contract SC^i that can read/write data on this channel and on the public one. The procedure is shown in Figure 4: users periodically publish their energy consumption $p^i_{B,h}$, while the smart contract is required to calculate the total baseline B^{tot}. The total energy demand D^{tot} is distributed to each user proportionally pro-quota (D^i), according to their contribution to the total customers baseline. Finally the

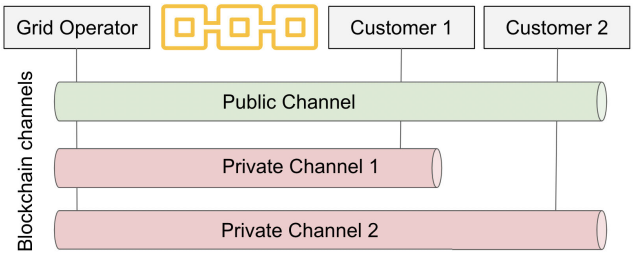

FIGURE 3. Architecture of the multi-channel blockchain solution supporting the EMS functions.

reward is calculated as a difference between the demanded energy consumption and the actual one as $|D^i - p^i_{B,h}|$.

IV. SECURE MULTIPARTY COMPUTATION ARCHITECTURE

A. THREAT MODEL

In traditional network systems, consumption data is private between the operator and the customer or the operator uses it for network management. When blockchain is introduced to operate distributed and transparent network management, the data of the various users must be made public. Thus, the following threats arise that we want to defend against:

1) users perform any kind of analysis on the data of other users, trying to extract, for example, their consumption profile; this is important because, by analysing the energy consumption of a user, an attacker could deduce his habits and use information about his presence or absence to commit theft or other criminal acts;
2) users can advertise bogus energy consumption; this misconduct could be used for personal gain or service disruption;
3) infrastructural elements can behave maliciously blocking network operations or producing output non-compliant with the expected processing.

Adversaries have free access to the BC's public channel, and can therefore read its entire contents. If the attacker is a malicious prosumer, it cannot alter the value acquired by the SM as it can be verified by the DSO, but can fake the values during the first phase of SMC; if it is an infrastructural node, the attacker can either not participate in the SMC process or fake the results. In the latter case, our solution allows us to handle a number of attackers depending on the threshold required by the cryptographic schemes used (more details on cryptographic schemes are described in Sections IV-B and IV-C).To be able to deal with the aforementioned threats, in the following we are going to introduce cryptographic techniques into our blockchain architecture that enable us to deal with the aforementioned threats.

B. PEDERSEN VERIFIABLE SECRET SHARING

Pedersen Verifiable Secret Sharing (VSS) [37] is a cryptographic technique that allows a secret to be shared in a secure way by splitting it into n shares and to reconstruct it just by using t ($\leq n$) of these. In addition, it allows the parties receiving the shares to verify that they are consistent, detecting malicious dealers and/or cheating parties. It is based on *Shamir Secret Sharing* [38] for the creation/distribution of shares and the threshold mechanism for the reconstruction of the secret, and makes use of *commitments* for the verifiability aspect. A more exhaustive description of this cryptographic scheme is detailed in Section IV-C, where the Elliptic Curve-based version is used.

We use VSS to protect against cheating prosumers and malicious privacy peers, as discussed in subsection IV-C.

C. RESILIENT SECURE MULTIPARTY SOLUTION

Building the consumption baseline of the users is one of the basic steps for DR programs to derive the individual reduction request (`ComputeRequestedReduction`). To this aim, DR algorithms need both the baseline of the single user (sensitive data) and the sum of the baselines of all the involved users (B^{tot}), that, in this context, can be considered a non-sensitive (aggregated) data.

To calculate B^{tot} without revealing the individual baseline to other users or a trusted central authority, we resort to a SMC algorithm running between prosumers and *privacy peers*, i.e. infrastructural elements selected at the beginning of the DR event to execute the private computation. Note that the *privacy peers* can be even the prosumers involved in the DR event.

The algorithm is explained by the simplified example shown in Figure 5 that reports the case with $N = 3$ prosumers, P_1, P_2 and P_3, $n = 3$ privacy peers, PP_1, PP_2 and PP_3, and $t = 2$. It can be divided into three steps: the first executed by *each* prosumer, the second by *at least* t privacy peers, and the last by *any* peer. Before the algorithm is executed, the following security parameters must be known to each participant (prosumers, privacy peers):

- the elliptic curve and the order q of its related finite field,
- two curve points G and H, such that $H = z * G$ with $z \in \mathbb{Z}^+$,
- the threshold values t and n.

In order to better and more effectively understand the operating process in the following, after the generic description of the operations to perform, the application of these to the example in Figure 5 is depicted.

1) PROSUMER'S OPERATIONS

During the first step, the i-th prosumer performs the following operations:

1) generates two (t-1)-degree random polynomials,

$$y_i(x) := s_i + a_{1,i}x + a_{2,i}x^2 + \ldots + a_{t-1,i}x^{t-1} \ mod \ q$$
$$z_i(x) := r_i + b_{1,i}x + b_{2,i}x^2 + \ldots + b_{t-1,i}x^{t-1} \ mod \ q$$

where $s_i := B^i$;
2) generates the share for the j-th privacy peer as a triple, $(x_j, y_{j,i}, z_{j,i})$, where $y_{j,i}$ and $z_{j,i}$ are $y_i(x_j)$ and $z_i(x_j)$ respectively;
3) *privately* sends the shares to the n privacy peers;

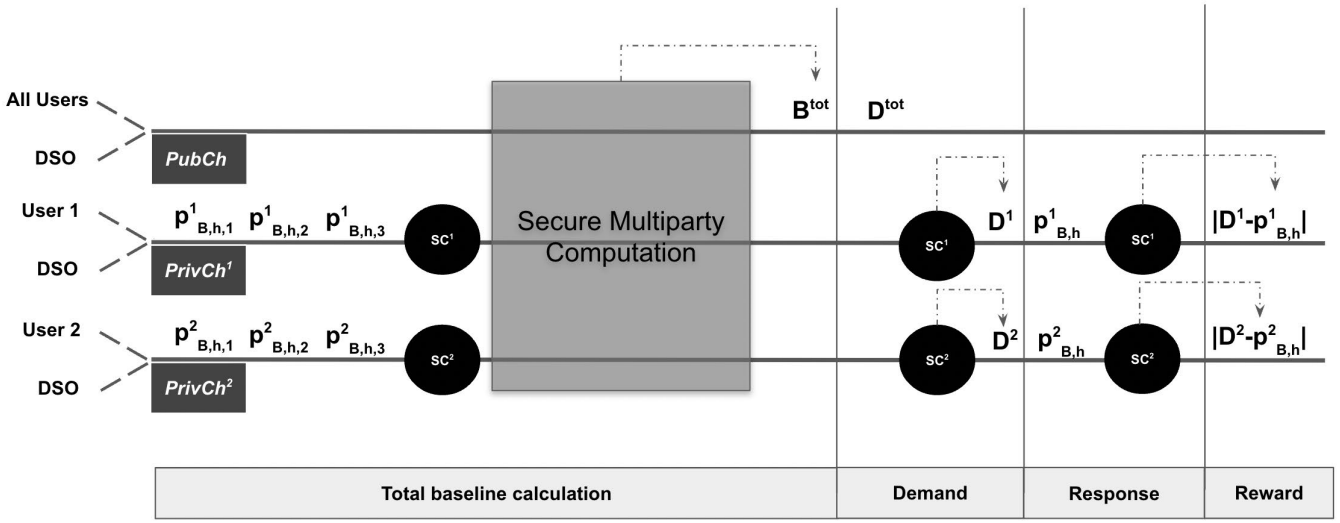

FIGURE 4. The proposed mechanism with two users: after the baseline calculation, DR takes place. The reward is then calculated on a per user basis as the difference between the user demand request D^i and the actual energy consumption $p^i_{B,h}$.

4) publishes the commitments:

$$\begin{aligned} C_{i,0} &:= s_i * G + r_i * H \\ C_{i,1} &:= a_{1,i} * G + b_{1,i} * H \\ C_{i,2} &:= a_{2,i} * G + b_{2,i} * H \\ &\dots \\ C_{i,t-1} &:= a_{t-1,i} * G + b_{t-1,i} * H \end{aligned}$$

With reference to the example in Figure 5, without loss of generality, consider peer P_1. Since $t = 2$ and $n = 3$, it generates two random polynomials of degree 1, $y_1(\cdot)$ and $z_1(\cdot)$, from which 3 shares are generated, $(x_1, y_{1,1}, z_{1,1})$, $(x_2, y_{2,1}, z_{2,1})$ and $(x_3, y_{3,1}, z_{3,1})$, and privately distributed to privacy peers PP_1, PP_2 and PP_3. Finally, the commitments $C_{1,0}$ and $C_{1,1}$ are published. Similarly, the same holds for the other two prosumers.

2) PRIVACY PEER'S OPERATIONS

During the second step, the j-th privacy peer performs the following operations:

1) for each received share, $(x_j, y_{j,i}, z_{j,i})$, checks its validity by verifying the following equality

$$\begin{aligned} &C_{i,0} + x_j * C_{i,1} + x_j^2 * C_{i,2} + \ldots + x_j^{t-1} * C_{i,t-1} \\ &\quad \stackrel{?}{=} y_{j,i} * G + z_{j,i} * H \end{aligned}$$

2) if all the shares are valid, publishes the sum of the received shares

$$(x_j, \sum_{i \in prosumers} y_{j,i}, \sum_{i \in prosumers} z_{j,i}).$$

With reference to the example in Figure 5, without loss of generality, consider PP_1. Since $t = 2$ and $n = 3$, it can check the validity of each of the 3 shares received, $(x_1, y_{1,1}, z_{1,1})$, $(x_1, y_{1,2}, z_{1,2})$ and $(x_1, y_{1,3}, z_{1,3})$, simply by verifying that

$$\begin{aligned} C_{1,0} + x_1 * C_{1,1} &\stackrel{?}{=} y_{1,1} * G + z_{1,1} * H \\ C_{2,0} + x_1 * C_{2,1} &\stackrel{?}{=} y_{1,2} * G + z_{1,2} * H \\ C_{3,0} + x_1 * C_{3,1} &\stackrel{?}{=} y_{1,3} * G + z_{1,3} * H \end{aligned}$$

Finally, if all 3 shares are valid, their sum, $(x_1, y_{1,1} + y_{1,2} + y_{1,3}, z_{1,1} + z_{1,2} + z_{1,3})$, is published. Similarly, the same applies to the other two privacy peers.

3) COMPUTATION OF THE SUM OF THE BASELINES

Finally, using any t of the sums published, B^{tot} can be calculated simply by applying the *Lagrange Interpolation* on the points $(x_j, y_{j,i})$ of the polynomial $y_i(\cdot)$. Being an aggregation, this value is far less privacy-sensitive with respect to individual user energy consumption and, in some cases, may be publicly disclosed for transparency.

D. SECURITY ANALYSIS

To be effective against the threats described in Section IV-A, our solution requires that private channels are present, that the consumption measurements acquired by the SM are trusted, and that the number of malicious prosumers does not exceed the threshold t chosen for the Pedersen algorithm to run. By making use of private channels and Pedersen VSS in public channels, it is possible to efficiently prevent one user from "spying" on the data of others without affecting the operational performance of the system. In fact, it is easy to demonstrate that the only way to retrieve any data about a specific user is by collusion of *at least t* users who received a share of those specific data. Table 2 summarises the protection provided by our solution against several threats.

TABLE 2. Protection against privacy and security threats.

Threat	Protection Strategy
Attacks against the privacy of prosumer's metering data	Blockchain private channels
Attacks against the privacy of prosumer's baseline	Shamir Secret Sharing and Blockchain private channels
Cheating prosumer (fake shares)	Pedersen Commitments
Cheating prosumer (fake secret)	Pedersen Commitments with DSO's ground truth verification
Privacy Peer failure	Shamir Secret Sharing
Malicious Privacy Peer	Pedersen Commitments

1) PROTECTION AGAINST MALICIOUS PROSUMERS

Consider two scenarios: i) a prosumer providing wrong shares to some privacy peers, ii) a prosumer lying about the real baseline. In the first scenario, the prosumer P_i has generated a proper polynomial $y_i(\cdot)$, using the actual baseline, and provides incorrect shares using fake points of the curve. To do so, she has to provide points out of curve. Thanks to the commitments $C_{i,0}, \ldots, C_{i,t-1}$, privacy peers can verify the validity of these points and detect the malicious prosumer. In the second scenario, the prosumer P_i has generated a *fake* polynomial $y_i(\cdot)$ and provides correct shares using the points of the curve. This time, privacy peers have no way to detect the malicious prosumer, since the verification is successful. However, the DSO can ask the prosumer for the random value r_i used for the polynomial $z_i(\cdot)$ and, since it also knows G, H and her baseline B^i, it can verify

$$B^i * G + r_i * H \stackrel{?}{=} C_{i,0} \tag{1}$$

and detect the malicious prosumer.

2) PROTECTION AGAINST CHEATING PRIVACY PEERS

Suppose that a privacy peer PP_j provides an incorrect sum of shares, $(x_j, y_{j,1} + y_{j,2} + y_{j,3}, z_{j,1} + z_{j,2} + z_{j,3})$. Again, thanks to the commitments, each participant can verify the validity of the sum and detect the cheating privacy peer. It is only necessary to verify $C_{1,0} + C_{2,0} + C_{3,0} + x_j^1 * C_{1,1} + x_j^1 * C_{2,1} + x_j^1 * C_{3,1} + \ldots + x_j^{t-1} * C_{1,t-1} + x_j^{t-1} * C_{2,t-1} + x_j^{t-1} * C_{3,t-1} \stackrel{?}{=} (y_{j,1} + y_{j,2} + y_{j,3}) * G + (z_{j,1} + z_{j,2} + z_{j,3}) * H$.

V. PERFORMANCE EVALUATION

In this section, we evaluate the robustness of the system in terms of the resistance to node or message failure, and the computation complexity required by the adopted cryptographic algorithms.

A. RESISTANCE TO FAILURE

The possible failure can happen due to node failure or errors during message transmission. The first case is simpler to analyse: if a prosumer fails (e.g., its hardware is broken), it will simply not be accounted for in the overall baseline. On the contrary, if a privacy peer would fail, the system will be resistant if at least t out of n continue to work because of the properties of Shamir Secret Sharing. The second case, transmission failure, requires a bit more calculations. Indeed, because of the security construction, it only needs that *a single message* from a prosumer to a privacy peer is lost to invalidate all the data acquired by this privacy peer that, therefore, must be excluded from the computation of the sum. To help the correct sizing of the system, we want to express the reliability of the system R_{sys} in relation to the probability of error of the message. Considering that each of the n privacy peers must receive a message from each of the N prosumers and indicating with p the probability that this message will be correctly received (assumed i.i.d.), we can easily calculate the probability that a privacy peer will receive the right set of data as

$$Prob_{PP} = p^N$$

On average, we can readily say that if $n \times Prob_{PP} \geq t$, the system will work most of the time. In general terms, the reliability of the system works is given by

$$R_{sys} = 1 - F(t-1; n, Prob_{PP})$$

where $F(a; b, p)$ is the binomial cumulative distribution function for a successes over b trials with success probability p. Then, using the Hoeffding inequality, we can limit the total resiliency of the system as:

$$R_{sys} \geq 1 - e^{-2n\left(p^N - \frac{t-1}{n}\right)^2}$$

Figure 6 shows the reliability of the system R_{sys} for $N = 100$ prosumers, $n = 10$ privacy peers and varying the number of required privacy peers t and the probability p of having a message delivered. As we can see, the system performs well with a probability of error of the order of 10^{-3}, which is fairly acceptable in many data networks.

B. SCALABILITY

Figure 7 shows the number of messages exchanged in a network with N peers and n privacy peers. As expected, doubling the number of privacy peers results in the same effect on the number of messages exchanged.

C. COMPUTATIONAL EFFICIENCY

Now we wonder whether the computational complexity is compatible with the commodity hardware used in an Energy Management System. To answer this fundamental question, we run a set of tests using a Raspberry Pi 3 model B+ (SoC Broadcom BCM2835 single-core ARM11 and 512MB of RAM). We used the Elliptic Curve Cryptography (ECC) module of *pycryptodome*,[1] one of the most popular cryptographic library in Python, and the curve *P-256*, a NIST-recommended elliptic curve on a finite field $\mathbb{F}_q$. The pycryptodome ECC python module overrides the arithmetic

[1] https://pycryptodome.readthedocs.io/

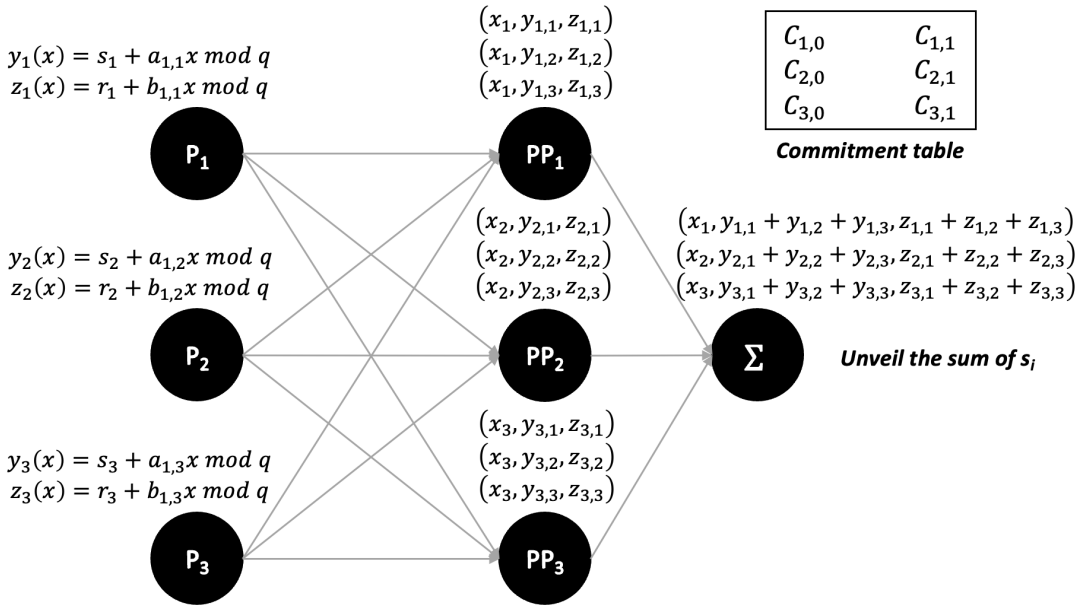

FIGURE 5. Example of the SMC algorithm to compute the aggregated baseline without disclosing the individual ones with 3 users and a 2-out-of-3 threshold.

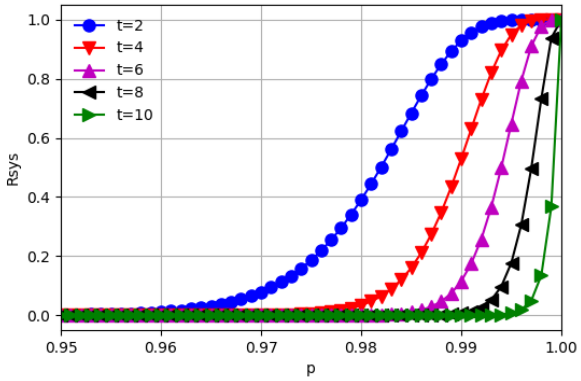

FIGURE 6. Reliability of the system for $N = 100$ prosumers, $n = 10$ privacy peers and varying the number of required privacy peers t and the probability p of having a message delivered.

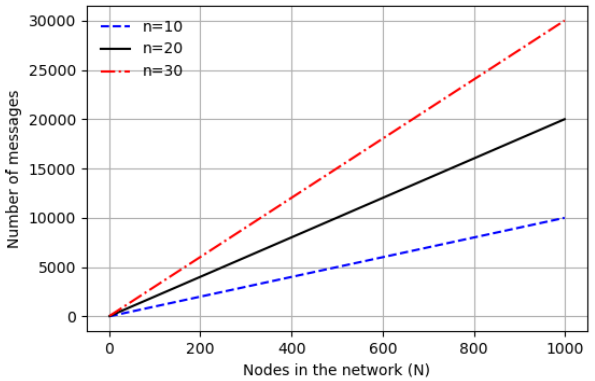

FIGURE 7. Number of messages exchanged in a network with N peers and n privacy peers.

operands, making it straightforward to implement from scratch all the operations described in Section IV-C, and run the tests with a growing number of privacy peers ($n = 10, 30, 50, 70, 100$) and varying the ratio of required peers t/n. For example, if we have $n = 100$ privacy peers and $t/n = 0.5$, only 50 out of 100 privacy peers are needed to reconstruct the secret. Figure 8 shows the computational time required to create the polynomials (Prosumer's operations step 1), while Figure 9 shows the time needed to create a single share (Prosumer's operations step 2). In both cases, the time is perfectly compatible with the hardware and the scenario; also in the extreme case of $n = 100$ privacy peers and the threshold $t = 90$, it requires less than 3 *ms* to execute the operations.

Verification operations are conversely far more computational intensive. Figures 10 and 11 show, respectively, the time required to create the commitments (Prosumer's operations step 4) and to use them to validate a share (Privacy Peer's operations step 1). Especially, the creation of the commitments (in charge of the prosumer) is computationally very demanding because of multiple operations on the points of the elliptic curve. However, if one considers a single multiplication of the points of the elliptic curve, the time required is around 6 *ms*, not particularly significant.

Figure 11 shows the time required by a privacy peer to verify a share coming from one single peer. Therefore, it is important to note that this time has to be multiplied by N, the number of peers involved in the DR event.

The performance evaluated so far describes only the operation needed to check the validity of the shares, that is, verify if the shares belong to the curve declared with the commits. However, as described in Section IV, we also considered some other threats. To protect against a prosumer

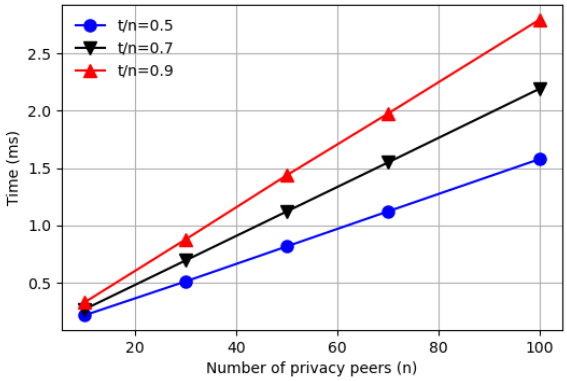

FIGURE 8. Computational time to create the polynomials.

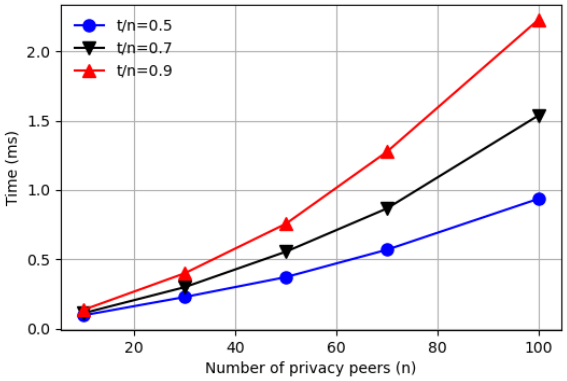

FIGURE 9. Computational time to create a share.

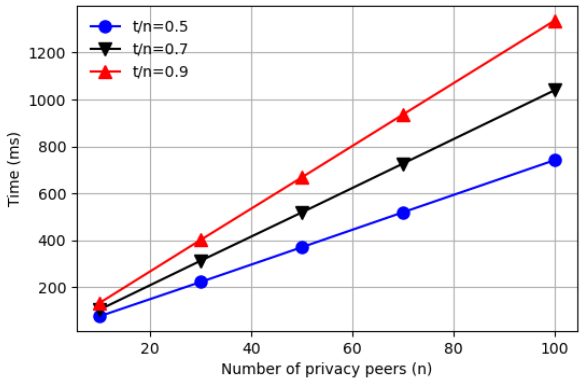

FIGURE 10. Computational time to create the commitments.

that lies about her baseline, the grid operator can compute the check described in equation 1 at the price of two multiplications and a sum of the points of the elliptic curve. Thus, the computation time is similar to the one reported in Figure 10 divided by t.

Finally, the time to verify the honest behaviour of a privacy peer is equal to the computational time to verify a share (Figure 11), multiplied by the number of received shares.

VI. RESULT DISCUSSION

On one hand, the performance evaluation highlights the feasibility of building a system on commodity hardware

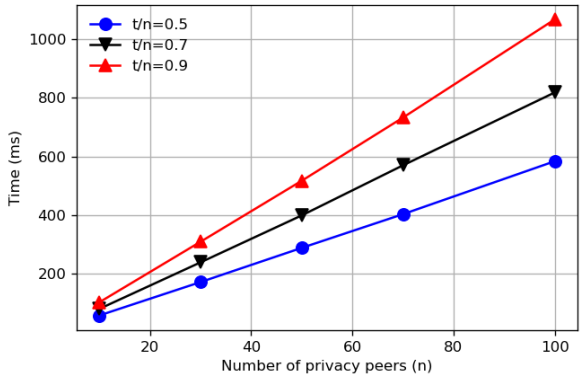

FIGURE 11. Computational time to validate a share.

to achieve privacy and resilience. On the other hand, the verification part shows several issues that can be critical when scaling t or N. According to the targeted sustainable delay, the timing can be improved using concurrency or by upgrading the computational capacity of the nodes. Notably, verification of the shares can also be done offline or on-demand in case of anomalies. Hence a large number of prosumers could not represent a critical issues for the timing of the operations.

Similarly to [11] and [27], we use blockchain channels, such as those available with Hyperledger Fabric, which natively partition the individuals who can access the published information, e.g., establishing one channel for each grid operator-market operator-customer group, and another general channel to which all the customers of the network take part. However, such an approach suffers from the impossibility of deriving a network-wide calculation such as the sum of all the prosumers' baselines, which, if computed naively, involves the disclosure of the baselines of all the users to a central trusted authority.

A. COMPARISON WITH OTHER DR MANAGEMENT SOLUTIONS

The presented solution from the computational point of view results in a performance degradation compared to solutions that do not provide the same level of privacy. For this reason, we performed a comparison with feature-based literature solutions that we present in Table 3.

Some of the works presented in Section II were employed in the comparison, along with three additional works that, despite not utilizing blockchain, prioritize the security and privacy of the system as their requirement. All solutions provide privacy protection for measurement data. Specifically, authors in [28] use a private blockchain to ensure that only authorised participants can access the data and smart contracts to automate the demand response process. The solution proposed in [12] uses off-chain storage to save measurement data, zero-knowledge proofs to protect the privacy between aggregators and prosumers, and a public blockchain to record measurements fingerprints and energy transactions. Both solutions involve aggregators, and, due

TABLE 3. Comparison of the DR management solutions.

	[28]	[12]	[29]	[39]	[40]	[41]	Proposed Solution
Components and Techniques	Private Blockchain, Aggregator	Blockchain, Aggregator, ZK-Proof	Blockchain and Secret Sharing	Federated Learning	Pseudonyms, Aggregator	Homomorphic (Paillier), Aggregator	Blockchain and SMC
Blockchain	Yes	Yes	Yes	No	No	No	Yes
Privacy of prosumer's measurement data	Yes	Yes	Yes	Yes	Yes (weak)	Yes	Yes
Privacy of user's baseline	N/D	Yes	Yes	Yes	Yes (weak)	Yes	Yes
Protection against cheating prosumer	N/D	Yes	Yes	No	No	No	Yes
Baseline calculation	N/D	Difference	Average	AI	Average	Average	Average
Fault tolerance	N/D	N/D	No	No	No	No	Yes
Protection against malicious internal node	N/D	N/D	No	No	No	No	Yes

to architectural decisions, issues such as privacy of the baselines and reliability of any components needed are not taken into account. Reference [39] is based on federated learning to estimate user baselines: where data is processed locally and the aggregator nodes perform the inference to ensure privacy-preserving baseline computation. In [40], the authors transmit the consumption profile using pseudonyms along with public and private keys. The demand/response provider carries out the counts without knowledge of the sender's identity. However, the achieved privacy in this case is weak as it does not guarantee unlinkability (see [17]). Finally, [41] ensures privacy through the employment of homomorphic transformations and Paillier-based techniques. Instead, in [29] and in the proposed solution, due to the choice of using baselines as the basic building blocks of the demand response scheme and the absence of aggregators, these problems arise automatically. In particular, trivial secret sharing in [29] allows the baseline privacy and the detection of cheating prosumers, but not the fault tolerance and the detection of malicious nodes within the architecture. On the other hand, using more advanced Secure Multiparty Computation schemes, such as Pedersen Verifiable Secret Sharing, makes it possible to guarantee the latter two properties as well.

Analysing the solutions shown in Table 3, starting from the leftmost one and moving to the right, each successive solution introduces a certain computational and performance overhead compared to the previous one.

VII. CONCLUSION

In this paper, we presented a multi-channel blockchain architecture for Smart Grids, that integrates privacy-preserving technologies to guarantee prosumers' privacy while allowing the grid operator to implement network-wide optimisation policies, such as Demand Response, that require sensitive user data. The use of private channels allows the user's privacy to be guaranteed, while smart contracts by means of Shamir Secret Sharing and Pedersen Commitments allow the user to operate on certified and non-repudiable data in an oblivious manner. In addition, the proposed system also guarantees the user about the reliability and security of the infrastructure. We show how the parameters can be adjusted to target a trade-off between the system's resistance to data loss (robustness) and the privacy introduced by encryption. Furthermore, we tested the proposed cryptographic techniques on devices to assess the sustainability of the proposed architecture in the IoT domain.

REFERENCES

[1] K. Mahmud, B. Khan, J. Ravishankar, A. Ahmadi, and P. Siano, "An Internet of Energy framework with distributed energy resources, prosumers and small-scale virtual power plants: An overview," *Renew. Sustain. Energy Rev.*, vol. 127, Jul. 2020, Art. no. 109840.

[2] R. Zafar, A. Mahmood, S. Razzaq, W. Ali, U. Naeem, and K. Shehzad, "Prosumer based energy management and sharing in smart grid," *Renew. Sustain. Energy Rev.*, vol. 82, pp. 1675–1684, Feb. 2018.

[3] M. B. Mollah, J. Zhao, D. Niyato, K.-Y. Lam, X. Zhang, A. M. Y. M. Ghias, L. H. Koh, and L. Yang, "Blockchain for future smart grid: A comprehensive survey," *IEEE Internet Things J.*, vol. 8, no. 1, pp. 18–43, Jan. 2021.

[4] N. Ul Hassan, C. Yuen, and D. Niyato, "Blockchain technologies for smart energy systems: Fundamentals, challenges, and solutions," *IEEE Ind. Electron. Mag.*, vol. 13, no. 4, pp. 106–118, Dec. 2019.

[5] A. Jindal, G. S. Aujla, N. Kumar, and M. Villari, "GUARDIAN: Blockchain-based secure demand response management in smart grid system," *IEEE Trans. Services Comput.*, vol. 13, no. 4, pp. 613–624, Jul. 2020.

[6] A. Kumari, R. Gupta, S. Tanwar, S. Tyagi, and N. Kumar, "When blockchain meets smart grid: Secure energy trading in demand response management," *IEEE Netw.*, vol. 34, no. 5, pp. 299–305, Sep. 2020.

[7] S. A. Chaudhry, H. Alhakami, A. Baz, and F. Al-Turjman, "Securing demand response management: A certificate-based access control in smart grid edge computing infrastructure," *IEEE Access*, vol. 8, pp. 101235–101243, 2020.

[8] P. Gallo, E. R. Sanseverino, G. L. Restifo, G. Sciumè, and G. Zizzo, "Demand response for integrating photovoltaic plants in Lampedusa island," in *Proc. IEEE Int. Conf. Environ. Electr. Eng. IEEE Ind. Commercial Power Syst. Eur.*, Sep. 2021, pp. 1–6.

[9] D. Mariano-Hernández, L. Hernández-Callejo, A. Zorita-Lamadrid, O. Duque-Pérez, and F. Santos García, "A review of strategies for building energy management system: Model predictive control, demand side management, optimization, and fault detect & diagnosis," *J. Building Eng.*, vol. 33, Jan. 2021, Art. no. 101692.

[10] A. M. Antonopoulos and G. Wood, *Mastering Ethereum: Building Smart Contracts and Dapps*. Sebastopol, CA, USA: O'Reilly Media, 2018.

[11] G. Sciumè, E. J. Palacios-García, P. Gallo, E. R. Sanseverino, J. C. Vasquez, and J. M. Guerrero, "Demand response service certification and customer baseline evaluation using blockchain technology," *IEEE Access*, vol. 8, pp. 139313–139331, 2020.

[12] C. D. Pop, M. Antal, T. Cioara, I. Anghel, and I. Salomie, "Blockchain and demand response: Zero-knowledge proofs for energy transactions privacy," *Sensors*, vol. 20, no. 19, p. 5678, Oct. 2020.

[13] J. Zhou, Y. Feng, Z. Wang, and D. Guo, "Using secure multi-party computation to protect privacy on a permissioned blockchain," *Sensors*, vol. 21, no. 4, p. 1540, Feb. 2021.
[14] H. Gao, Z. Ma, S. Luo, and Z. Wang, "BFR-MPC: A blockchain-based fair and robust multi-party computation scheme," *IEEE Access*, vol. 7, pp. 110439–110450, 2019.
[15] S. Wu, J. Li, F. Duan, Y. Lu, X. Zhang, and J. Gan, "The survey on the development of secure multi-party computing in the blockchain," in *Proc. IEEE 6th Int. Conf. Data Sci. Cyberspace*, Oct. 2021, pp. 1–7.
[16] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 5, pp. 840–852, Sep. 2018.
[17] K. Gai, Y. Wu, L. Zhu, M. Qiu, and M. Shen, "Privacy-preserving energy trading using consortium blockchain in smart grid," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3548–3558, Jun. 2019.
[18] K. Gai, Y. Wu, L. Zhu, L. Xu, and Y. Zhang, "Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7992–8004, Oct. 2019.
[19] P. Singh, M. Masud, M. S. Hossain, and A. Kaur, "Blockchain and homomorphic encryption-based privacy-preserving data aggregation model in smart grid," *Comput. Electr. Eng.*, vol. 93, Jul. 2021, Art. no. 107209.
[20] Z. Guan, X. Lu, W. Yang, L. Wu, N. Wang, and Z. Zhang, "Achieving efficient and privacy-preserving energy trading based on blockchain and ABE in smart grid," *J. Parallel Distrib. Comput.*, vol. 147, pp. 34–45, Jan. 2021.
[21] B. Banerjee, A. Jani, and N. Shah, "Asymmetric confidentiality in blockchain embedded smart grids in Galois field," *Frontiers Blockchain*, vol. 4, Dec. 2021, Art. no. 770074.
[22] X. Chen, J. Shen, Z. Cao, and X. Dong, "A blockchain-based privacy-preserving scheme for smart grids," in *Proc. 2nd Int. Conf. Blockchain Technol.*, Mar. 2020, pp. 120–124.
[23] N. Fotiou, I. Pittaras, V. A. Siris, G. C. Polyzos, and P. Anton, "A privacy-preserving statistics marketplace using local differential privacy and blockchain: An application to smart-grid measurements sharing," *Blockchain, Res. Appl.*, vol. 2, no. 1, Mar. 2021, Art. no. 100022.
[24] B. M. Yakubu, M. I. Khan, N. Javaid, and A. Khan, "Blockchain-based secure multi-resource trading model for smart marketplace," *Computing*, vol. 103, no. 3, pp. 379–400, Mar. 2021.
[25] B. M. Yakubu, M. I. Khan, A. Khan, A. Anjum, M. H. Syed, and S. Rehman, "A privacy-enabled, blockchain-based smart marketplace," *Appl. Sci.*, vol. 13, no. 5, p. 2914, Feb. 2023.
[26] F. Knirsch, A. Unterweger, G. Eibl, and D. Engel, *Privacy-Preserving Smart Grid Tariff Decisions with Blockchain-Based Smart Contracts*. Cham, Switzerland: Springer, 2018, pp. 85–116.
[27] M. L. Di Silvestre, P. Gallo, E. R. Sanseverino, G. Sciumè, and G. Zizzo, "Aggregation and remuneration in demand response with a blockchain-based framework," *IEEE Trans. Ind. Appl.*, vol. 56, no. 4, pp. 4248–4257, Jul. 2020.
[28] A. C. Tsolakis, I. Moschos, K. Votis, D. Ioannidis, T. Dimitrios, P. Pandey, S. Katsikas, E. Kotsakis, and R. García-Castro, "A secured and trusted demand response system based on blockchain technologies," in *Proc. Innov. Intell. Syst. Appl. (INISTA)*, Jul. 2018, pp. 1–6.
[29] L. Bracciale, P. Loreti, E. Raso, G. Bianchi, P. Gallo, and E. R. Sanseverino, "A privacy-preserving blockchain solution to support demand response in energy trading," in *Proc. IEEE 21st Medit. Electrotech. Conf.*, Jun. 2022, pp. 677–682.
[30] J. Bernal Bernabe, J. L. Canovas, J. L. Hernandez-Ramos, R. T. Moreno, and A. Skarmeta, "Privacy-preserving solutions for blockchain: Review and challenges," *IEEE Access*, vol. 7, pp. 164908–164940, 2019.
[31] L. Bracciale, E. Raso, P. Gallo, E. R. Sanseverino, G. Bianchi, and P. Loreti, "Privacy in blockchain-based smart grids," in *Proc. Workshop Blockchain Renewables Integr. (BLORIN)*, Sep. 2022, pp. 37–41.
[32] X. Yang, Y. Zhang, S. Wang, B. Yu, F. Li, Y. Li, and W. Yan, "LedgerDB: A centralized ledger database for universal audit and verification," *Proc. VLDB Endowment*, vol. 13, no. 12, pp. 3138–3151, Aug. 2020.
[33] X. Yang, R. Zhang, C. Yue, Y. Liu, B. C. Ooi, Q. Gao, Y. Zhang, and H. Yang, "VeDB: A software and hardware enabled trusted relational database," *Proc. ACM Manage. Data*, vol. 1, no. 2, pp. 1–27, Jun. 2023.
[34] S. Lee and D.-H. Choi, "Energy management of smart home with home appliances, energy storage system and electric vehicle: A hierarchical deep reinforcement learning approach," *Sensors*, vol. 20, no. 7, p. 2157, Apr. 2020.
[35] M. S. Martinez and R. Hamilton, "Role of demand response baselines in estimating participant impacts," in *Proc. EUEC*, 2013, pp. 1–30.
[36] A. Augello, P. Gallo, E. R. Sanseverino, G. Sciabica, and G. Sciumè, "Tracing battery usage for second life market with a blockchain-based framework," in *Proc. IEEE Int. Conf. Environ. Electr. Eng. IEEE Ind. Commercial Power Syst. Eur.*, Sep. 2021, pp. 1–6.
[37] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in *Proc. Annu. Int. Cryptol. Conf.* Cham, Switzerland: Springer, 1991, pp. 129–140.
[38] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.
[39] Y. Chen, C. Chen, X. Zhang, M. Cui, F. Li, X. Wang, and S. Yin, "Privacy-preserving baseline load reconstruction for residential demand response considering distributed energy resources," *IEEE Trans. Ind. Informat.*, vol. 18, no. 5, pp. 3541–3550, May 2022.
[40] Y. Gong, Y. Cai, Y. Guo, and Y. Fang, "A privacy-preserving scheme for incentive-based demand response in the smart grid," *IEEE Trans. Smart Grid*, vol. 7, no. 3, pp. 1304–1313, May 2016.
[41] H. Yu, J. Zhang, J. Ma, C. Chen, G. Geng, and Q. Jiang, "Privacy-preserving demand response of aggregated residential load," *Appl. Energy*, vol. 339, Jun. 2023, Art. no. 121018.

PIERPAOLO LORETI has been a Professor in telecommunications and a Research Fellow with the University of Rome Tor Vergata, since 2021 and since 2006, respectively. Throughout his career, he has collaborated with various public and private research consortiums and companies, participating in numerous European and national projects in both research and coordination roles. To date, he has authored over 80 peer-reviewed articles published in reputable journals and presented at international conferences. His expertise encompasses a range of topics, including wireless and mobile networks, the IoT systems and platforms, framework design, analytic modeling, and performance evaluation through simulation and test-bedding.

LORENZO BRACCIALE is currently an Assistant Professor with the Department of Electronic Engineering, University of Rome Tor Vergata. His primary research interests include distributed systems, with a focus on machine learning and data privacy, which includes distributed programmable networks, eHealth systems, and the application of privacy enhancing technologies.

EMANUELE RASO received the M.S. degree in computer science engineering from the University of Rome Tor Vergata, in 2019, where he is currently pursuing the Ph.D. degree with the Department of Civil Engineering and Computer Science Engineering. His research interests include cybersecurity, particularly on applied cryptography, data privacy, and confidentiality. He was a Researcher for the EU H2020 BRP4GDPR Project.

GIUSEPPE BIANCHI has been a Full Professor in networking with the University of Roma Tor Vergata, since January 2007. His research interests include IP networking, wireless LANs, privacy and security, traffic monitoring, and is documented in about 180 peer-reviewed international journals and conference paper, accounting for more than 11.500 citations and a H-index of 29 (Scholar Google). He is the co-inventor in seven filed patents. He is an Editor of IEEE/ACM TRANSACTIONS ON NETWORKING, an Area Editor of IEEE TRANSACTIONS ON WIRELESS COMMUNICATION, and an Editor of *Computer Communication* (Elsevier).

ELEONORA RIVA SANSEVERINO received the master's and Ph.D. degrees in electrical engineering from the University of Palermo, Palermo, Italy, in 1995 and 2000, respectively. She is currently a Full Professor in power systems with the University of Palermo. She is also a scientific coordinator of various industrial research projects with research organizations and companies. She is also responsible of many research and teaching cooperation agreements with foreign institutions. These include European institutions, such as Aalborg University, Aalborg, Denmark, and Chalmers University, Gothenburg, Sweden, and non-European institutions, such as Electric Power University and the Institute of Energy Science, Hanoi, Vietnam. She has authored more than 250 papers on international journals and conference proceedings and edited books and book chapters. She is the Editor-in-Chief of the *UNIPA Springer Series*.

PIERLUIGI GALLO received the M.S. degree in electronic engineering and the Ph.D. degree in electrical, electronic, and telecommunication engineering, mathematics, and automation from the University of Palermo, Palermo, Italy, in 2002 and 2015, respectively. He has been an Assistant Professor with the University of Palermo, since November 2010. He has participated to national and international research projects, as a work package or a technical leader. He coordinates the Security, Network Applications and Positioning Laboratory, University of Palermo. He is also the CEO and the Founder of SEEDS srl, an academic spinoff on agri-food traceability with blockchain. His research interests include wireless medium access control layer, indoor localization, cybersecurity, blockchain, and their applications in several fields, including smart grids and agri-food traceability.

Open Access funding provided by 'Università degli Studi di Roma "Tor Vergata"' within the CRUI CARE Agreement