

Article

Decentralized Data Management Privacy-Aware Framework for Positive Energy Districts

Sidra Aslam ^{1,2,*}, Viktor Bukovszki ³ and Michael Mrissa ^{1,2}

¹ InnoRenew CoE, Livade 6, 6310 Izola, Slovenia; michael.mrissa@innorenew.eu

² Faculty of Mathematics, Natural Sciences and Information Technology, University of Primorska, Glagoljaška Ulica 8, 6000 Koper, Slovenia

³ Advanced Building and Urban Design Ltd., 1139 Budapest, Hungary; bukovszki.viktor@abud.hu

* Correspondence: sidra.aslam@innorenew.eu

Abstract: Energy Transition (ET) needs actors to perform independent actions on multiple levels of governance. These actors may need to write and read their data, and at the same time they want to protect their data from unauthorized access. This is particularly the case for positive energy districts (PED), a growing trend in the EU that requires actors to perform, write and read operations on a neighborhood scale where governance competences are typically absent. This paper presents a decentralized privacy-aware data management framework that enables actors to store, read, and modify data in PEDs. Our framework design integrates blockchain with a Distributed Hash Table (DHT), role-based access control, ring signature, and different encryption techniques. The proposed framework stores encrypted data on the DHT, and metadata and hash key are sent to the blockchain, which allows the data owner to keep track of their data. The proposed framework components handle multi-level data access in PEDs and enable data security at run-time. Moreover, we show security and privacy analysis and performance evaluation in time overhead. The results show that the proposed solution is effective, secure, and scalable.

Keywords: positive energy districts; access control; security; energy transition; decentralized framework; blockchain; security; privacy

Citation: Aslam, S.; Bukovszki, V.; Mrissa, M. Decentralized Data Management Privacy-Aware Framework for Positive Energy Districts. *Energies* **2021**, *14*, 7018. <https://doi.org/10.3390/en14217018>

Academic Editors: Joao Ferreira and Ali Elkamel

Received: 24 September 2021

Accepted: 21 October 2021

Published: 26 October 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Energy transition (ET)—the restructuring of energy systems to achieve carbon neutrality—increasingly relies on decentralized energy systems (DES) [1]. DES refers to the replacement of centralized, national, or regional energy production with either decentralized community-scale or distributed building-scale production, and a control framework to coordinate supply and demand [2]. In practice, they usually rely on small-scale hydro, cogeneration wind, solar photovoltaic, biomass, and biogas as energy sources [1]. DES are increasingly discussed in academia [3], and have been a strategic priority in the European Union to decentralize energy for the purpose of market diversification, decarbonization, and energy independence [4]. The main drivers behind DES are low-carbon, renewable energy production, more robust, secure grids, and decreased reliance on imports from a technical perspective [5,6], as well as a wider participation, both in terms of responsibility-sharing, and in terms of bonding in local communities from a social perspective [7], something that has been reinforced in a decade of community energy scholarship [8]. As such, DES represent not a purely technical, but a sociotechnical development, resulting in new organizations, with devolved competences and responsibilities, captured at hyperlocal scales and involving individual consumers and prosumers [9].

This sociotechnical dynamic of DES leads to increasing complexity in regards to managing and decreasing accountability to govern a basic resource—energy. Whereas a centralized energy system is managed by few, vertically integrated service providers, with

the regulatory oversight of democratic institutions, DES devolves energy provision to a multitude of scales that may include individual prosumers, and new organizations that may emerge from the scale of a multi-unit building complex to entire regions [10]. In the European context, while decentralization of energy is not necessarily followed by a decentralization of competences, governance models that deliver both are preferred [11,12]. EU-level legislation recognizes and promotes, for instance, self-governing energy communities and aggregators pooling individual consumers and producers [13]. While this drive empowers local actors or their networks, this does not ensure that their conduct is democratically legitimate [14], and it is significantly harder to provide oversight from existing institutions [15]. Yet, these new actors provide a basic resource, and are also instrumental in delivering ET while being less accountable. To ensure that the commonly, publicly declared requirements for energy provision are met, and to steer ET in a just, sustainable manner, it is crucial to address this accountability challenge of energy decentralization.

One promising avenue to govern decentralized energy is through digitalization. Information is crucial for strategic and operational decision-making regarding energy systems, a trait that is amplified with the increasing complexity of managing DESs [2]. Information and Communication Technologies (ICT) can, for example, support coordination along and between energy supply chains [16], increase the social scalability of cooperation in DES by enabling granular business models [17], disentangle complexity through remote sensing and analytics [18], and is instrumental in linking the scale of individual interactions to the aggregated, system-level management of energy [2]. In the context of energy governance, there is a growing prevalence of smart performance-based contracts that execute pre-agreed-upon rules and policies based on measurable, verifiable information [19]. For example, an aggregator service pooling several buildings may agree with the grid operator to delay heating/cooling in the morning to flatten peak demand in exchange for discounts. In this case, the heating control systems in each building sends data to the aggregator when they turn on, which is the performance-basis to credit the discount.

For such digitalized governance to work with a wide scope and minimal transaction costs, data must be stored and shared on a large scale, among a multitude of actors, with a large variety of different permissions and interactions. This data feeds into the functionalities described above—analytics to optimize individual actions on system-level and performance-based contracts to codify relations—which coordinate individual actions in energy production and distribution. Thus, these technologies perform governance roles as “institutional technologies” [20]. Data ownership, data access, and other permissions become crucial, since data feeds into institutional technologies. This means that in digitalized governance, it falls to the design of the ICT infrastructure to ensure legitimacy, privacy, security, and trust, all of which used to be in the domain of democratic institutions [21]. To ensure that this works, the system managing data and regulating actions must be able to efficiently leverage information and handle individual and system-level interests [22]. This pertains on the one hand balancing the autonomy of members with system-optimal performance, and on the other hand accessing, assimilating, and disseminating local knowledge. This means that efficient governance models will rely on data contributed by a multitude of actors. In energy governance, these actors have complex, often asymmetrical relationships spanning multiple scales, including large gatekeepers such as grid operators, small, but copious prosumers, such as households, various aggregating actors such as building managers, and public institutions enforcing strict regulatory constraints. The energy use-case adds another layer of complexity to the nascent field of data governance, a field where approaches to tackle the fluid nature of data access, ownership, and permission is a research challenge [23]. From a system architecture perspective, centralized digital platforms that are common brokers of data coming from many actors today alone have been shown incapable of providing legitimate data governance, prompting calls for regulatory oversight from existing institutions [24]. However, this still relies

on existing central institutions, which, while accountable, have less authority in a decentralized energy system. Efficient information assimilation and individual-system level optimization arguably requires some decentralization also on the side of the systems that enact digital governance [22]. The main driving need behind this research is providing a method for handling data ownership, access and permission in decentralized energy governance use-cases that provides accountability for them, should they rely on institutional technologies.

To overcome this challenge, there is great potential in applying technologies of decentralized data management. Nowadays, blockchain has been widely adopted because of its secure and decentralized database [25]. It replicates the transaction data over a set of nodes. Thus, it eliminates the need for a centralized system. As each technology has their own unique advantages, disadvantages, and uses, it is essential to develop and experiment with different combinations in various system designs for decentralized data management. It is expected that the richness of use-cases and their requirements in energy governance will trigger diverse system designs. With this article, our objective is to kick-start this development cycle, by developing and testing a generic prototype system for decentralized energy governance. This contribution explains, through a simple and common scenario, how some of the technologies in distributed data management could meet their challenges, what are their individual shortcomings, and how their combination can overcome these. More specifically, we demonstrate a system integrating access control, encryption, blockchain, distributed hash table, and ring signature, and argue for this architecture to be a generic framework for databases in future energy governance.

The contributions of our paper are as follows:

- We design decentralized data storage and access framework that combines blockchain and Distributed Hash Table (DHT) to enable data owners to update their data, and a fine-grained access control solution to handle multi-level data access in decentralized storage. We store metadata and hash key on the blockchain whereas actual encrypted data and encrypted symmetric key are sent to the DHT;
- Our second contribution is to provide an encryption design that enables actors to choose between different types of encryption methods while storing and querying data in a decentralized storage framework. The security design ensures data authenticity. Furthermore, our solution protects against Linking and modification attacks;
- We modify and extend the metadata structure discussed in [26]. Thus, our proposed metadata structure enables our framework to provide secure and privacy-aware data access. The data owner can easily track who wants to access his data and which part of the data are requested;
- We provide implementation details with performance evaluation to show the feasibility and scalability of our solution.

The rest of the paper is organized as follows. In Section 2, we present a review of most relevant work in the area and show how multi-scale energy management currently lacks privacy, security, data access management solutions. We present the motivation scenario that identifies the research problems in Section 3. We provide a detailed discussion of our proposed solution and its components in Section 4. In Section 5, framework evaluation, analysis, and results are presented. In Section 6, we summarize our work and discuss future work.

2. Related Work

This section presents the review of existing research on blockchain-based energy management and privacy-preserving energy management.

2.1. Decentralized Energy Management

The existing work focuses on energy data management using blockchain technology. In [27], the authors propose a blockchain-based Demand Response (DR) framework. The

proposed framework manages energy exchanges on a daily basis and handles electrical consumption in smart buildings. A smart contract is used to manage autonomous monitoring and billing. However, the proposed smart contract is unable to prevent the malicious nodes that can stop the algorithm execution. The authors in [28], present a blockchain-based framework to distribute daily energy data in a district-level energy system. A blockchain is used to enable energy producers to manage their pricing plans to increase profit. It allows consumers to charge minimum energy amount. However, more storage is required to make the process sustainable. However, their framework is not sustainable due to limited storage.

In [29], the authors present a blockchain-based system to manage energy data. The proposed platform is used to handle energy activities between residential users. It allows users to interact with each other to trade energy. A blockchain-based optimization algorithm is designed to preserve user privacy and optimize the energy trading process. However, users' energy management information is collected by the centralized authorized coordinator. In [30], the authors discuss blockchain technology to solve the issue of centralized Internet of Energy (IoE) management systems. IoE uses sensors to collect, manage, and optimize energy data. Various consensus algorithms of blockchain in the context of IoE have been discussed. However, it is difficult to choose the best consensus algorithm because it depends on the problem requirements and available network resources.

In [31], the authors made a review of community energy storage with its role and challenges based on the energy system. In [32,33], the authors discuss a review of electrical energy storage, focusing on energy storage applications, technologies, and technical features such as capacity and efficiency.

In [34], the authors present a decentralized u-share framework for data sharing. The proposed framework enables users to control and trace the data they share with their family, friends, and others. A software client is used to share the private key with its circle members and ensures that the shared data are encrypted with the circle's public key. It maintains the record of shared keys and ensures that the shared data are encrypted with the circle's public key. However, private key sharing is subject to security issues. Additionally, this framework uses one type of encryption. In [35], the authors propose a permissionless blockchain-based framework that replicates all the transactions within the Distributed Hash Table (DHT) peers. Their solution allows every peer to access transactions using a skip graph. However, all the transactions are accessible which leads to data security issues.

2.2. Privacy-Preserving Energy Management

We explored the existing literature on privacy-preserving energy management using a rechargeable battery. Several approaches have been presented to ensure privacy for smart meter users such as anonymization [36], aggregation [37], homomorphic encryption [38], and obfuscation [39]. The authors in [40], present a technique to ensure the privacy of actors' everyday activities. However, the proposed approach modifies the user's data, which may not be acceptable for the data owner. Besides this, it requires high capacity and throughput for a rechargeable battery. The authors in [41,42], present a rechargeable battery-based privacy protection mechanism to ensure user's energy consumption data privacy. Their solution considers energy management rules based on a battery to achieve privacy and energy efficiency. However, higher battery capacity is required to minimize the information leakage rate.

In papers [36,43], a privacy-preserving energy management framework is presented.

This framework relies on a smart meter to collect information such as electricity consumption. A smart meter sends data directly to the energy supplier about how much electricity is used by a consumer. However, this data can be used by a malicious actor, which leads to privacy issues. To ensure smart meter data privacy, a rechargeable battery is used. The aim of a rechargeable battery is to store energy data and charge/discharge. It also minimizes the cost of the electricity bill. Hence, the proposed framework does not disclose

the details of electricity statistics as they are masked with battery usage. However, it relies on a rechargeable battery to preserve the privacy of electricity consumers.

The authors in [44], proposed an energy management framework based on blockchain technology. A smart contract is used to handle the energy utilization of each user. It ensures the privacy of users' private information. However, the proposed solution is dependent on hardware resources. The authors in [45], presented a smart contract-based a framework to trade energy data. A private blockchain is used to control the user's access to private data. Energy trading data are written on the smart contract and shared with other users. It helps to keep track of the energy data. However, the gas cost is high to run the smart contract.

In [46], the authors discuss electricity privacy issues (e.g., electricity privacy data leakage) in smart meters. Their solution is based on Monte Carlo simulations to optimize the electricity cost and to protect the electricity privacy for residential consumers. It ensures electricity privacy protection by using charge/discharge batteries within a fixed time. The authors in [47], made a review of approaches focusing on customer privacy protection and billing using smart meters. However, existing approaches depend on a centralized system to calculate the bills, which raises security and privacy issues.

There is also research into the application of artificial neurons for privacy protection in Internet-of-things IoT applications. In [48], the authors explore how multiple artificial neuron models can be used to generate chaotic time series from images. In the solution, the encrypted data are recovered when transmitted by synchronizing the neurons, which was tested in image transferring among Raspberry Pi devices using message-queuing-telemetry-transport protocol. However, the protocol itself relies on a message broker that routes data and as such presents a single point of failure risk.

In summary, existing energy management frameworks are dependent on centralized systems or hardware solutions such as rechargeable batteries to ensure data privacy in PEDs. Generally, a rechargeable battery needs a high capacity to store the energy data and throughput, thus motivating research towards decentralizing energy data storage, managing access to user's data, and ensuring data security and privacy without requiring storage devices such as a rechargeable battery.

3. Motivating Scenario and Research Problem

This section introduces a common, characteristic use-case for which distributed data management systems should be designed. Decentralized energy governance comes in multiple forms, including models of collective investment, such as renewable energy communities or community virtual storage, or models of peer-to-peer distribution, such as energy or flexibility markets [49]. The most well-established model in Europe is the renewable energy community, a governance network of autonomous, local actors collectively investing in renewable production [50], hence an investment-type model is chosen, with its key actors and activities summarized in Figure 1.

The scenario is based on an energy community, formed in an urban residential neighborhood with several housing estates. In each building, there are multiple households, and a household may consist of independent occupants, i.e., not necessarily members of the same family. The core activity of the energy community is to save housing costs by investing in the deep energy retrofitting of the neighborhood. Deep retrofitting means that the investment is systemic, involving several, mutually reinforcing interventions to minimize reliance on external energy input [51]. This usually includes building insulation, replacement of doors and windows, modernizing building systems, renewable energy production, smart metering, and smart building operation. The energy community members themselves can be households, or independent occupants within households, who make collective decisions on how to allocate their pooled resources, what exactly should be the deep retrofit mix. They are supported by technical representative actors on two levels: building managers, and community managers. Their role is executive, they carry out day-

to-day operations of either housing estates or the energy community, manage shared assets, provide decision-support for the investment and carry out and follow-up on the investment. Finally, two external actors engage in this activity: distribution service operators (DSO), and local governments. DSOs are involved because investment in energy production introduces new supply to the grid, which is their responsibility to balance. In this scenario, they make an agreement with the energy community to share this responsibility through demand-side response. The local government is involved as an investor via a performance-based contract. They subsidize investments granted they meet policy targets for on-site renewable energy production.







Member actors	Representative actors	Partnered actors
Occupant	Building manager	DSO
		
Invests resources in deep retrofit; Allocates resources on deep retrofit interventions.	Implements and monitors building-scale interventions; Allocates demand response to households; Reports to community.	Reports to partners; Provides external supply; Takes up excess energy; Enforces grid balance objectives.
Household	Community manager	Local government
		
Invests resources in deep retrofit; Allocates resources on deep retrofit interventions; Implements demand response.	Provides decision-support. Implements and monitors neighborhood interventions: Allocates demand response to buildings; Reports to partners.	Invests resources in deep retrofit; Enforces renewable production objectives.

Figure 1. Actor types and their core activities in the motivating scenario.

The role of data in this scenario is to regulate actions through performance-based contracts. The DSO, the local government, and members of the energy community have different interests in the investment, and each of these actors protects their interests by translating them to measurable performances to which rights and responsibilities are negotiated. For this scenario, the key performance indicator (KPI) for the members is operational expenditures, for the DSO is the supply cover factor, while for the local government is the annual renewable energy ratio. Real-life applications may involve more diverse and complex KPIs. The objective for distributed data management is thus to allow each actor

to access the data they need to calculate KPIs, ensure its validity, while at the same time ensuring privacy and security requirements of the data owners. Some of this data are scale-specific, meaning it is generated on the scale of a specific actor and is shared across scales as is. The window-to-wall ratio of buildings or the capacity of a community energy storage are scale-specific data. Some data on the other hand is multiscale, meaning for each scale, it is an aggregation of individual data points of the preceding scale. Energy consumption and GHG emissions are multiscale. Both types of data are expected to be shared, but an aggregation of multiscale data introduces a privacy-preserving measure by design that scale-specific data does not have (Figure 2).

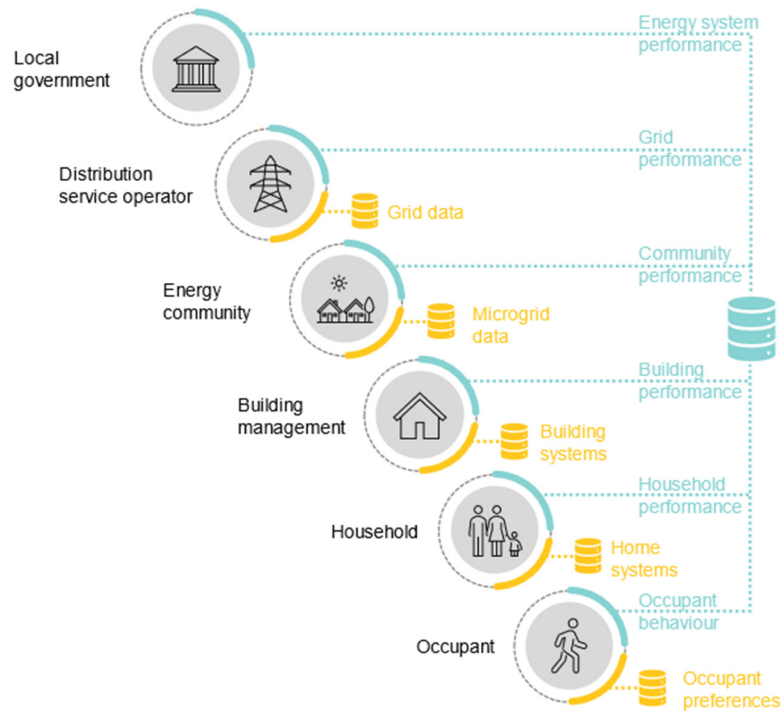


Figure 2. Multilevel data generation in the scenario. Gold indicates scale-specific, while blue indicates multiscale data.

Data are collected prior investment decisions to make accurate predictions on KPI, and after project completion to monitor agreed-upon responsibilities and the performance gap between predicted and actual KPI results. The full range of input data depends on the simulation engine used and can be inspected in various tool reviews, such as [52] or [53]. Some of the inputs, such as technical data on building systems or home appliances, are expected to be static, with occasional modifications, while others are expected to be broadcasted as a data stream at regular intervals. For the design of distributed data management, we can translate interactions with the data in the scenario as system requirements. These interactions are not comprehensive, but a representative for how users should be able to use the system:

- Occupants to write personal data, such as their occupancy schedule, which will be collected by building managers, who collect all occupancy schedules in that building only, without knowing which occupant they belong to;
- A household to update the energy efficiency data of their home appliances when they replace them;
- The energy community to report to both the DSO and the local government, but they disclose different data to different users: the DSO gets access to energy consumption data, the local government to renewable energy production;

- The DSO to make sure that energy consumption data they received is authentic and has not been tampered with;
- A building manager to write data on the energy efficiency of a new boiler, which is fully accessible for each household and occupant in their building, but not in other buildings.

Our multi-scale energy management scenario highlights the need for security, trust, decentralization, and privacy-aware data management in the energy management process. Existing solutions rely on the rechargeable battery to ensure privacy on energy data. Generally, a rechargeable battery acts as a centralized energy storage device which leads to a single point of failure. Furthermore, it also needs a high capacity to store the energy data and throughput (the energy must be charged/retrieved within a given time interval), thus motivating research towards decentralized energy management data without any storage device. A blockchain is a decentralized and distributed database that stores transactions on all nodes, which eliminates the risk of a single point of failure. A blockchain is a chain of blocks. Each block is linked to its previous block with a hash to avoid the modification of stored data [54], making it immutable [55]: once the data have been recorded, they cannot be modified.

However, actors require to write and read data are highlighted in our scenario. Therefore, it is required to design a solution that allows actors to delete and change their stored data to overcome the immutability feature of blockchain, while also protecting their privacy-sensitive data from an attacker. The proposed solution must enforce security on data and ensures multi-scale data access control depending on the data requester roles (e.g., data owner, partner, public user). According to the multi-scale energy management scenario discussed above, we highlight the following research problems:

Management of data modification: In our motivating scenario, actors want to make changes in their data (e.g., write data with pre-existing data) on the blockchain (e.g., comfort preference, consumption mix, etc.). However, due to the immutability feature of the blockchain, it is not possible to modify data after to record them in the chain. The challenge is to overcome this issue while respecting the original blockchain design.

Data security and fine-grained access control: The blockchain stores data publicly and anyone can view and access them. The difficulty is to design a decentralized solution that protects data from unauthorized access and manages data through an access control model.

To answer these issues, we design the following solution that combines relevant technologies in one framework. We describe the detail of the proposed framework and its modules as follows.

4. Proposed Framework

In our research, we present a new decentralized privacy-aware energy management framework that manages multi-scale energy management, data mutability and actor's anonymity. Our proposed framework would enable actors to have control over their data. The proposed framework is fully decentralized, highly scalable and secure. Our solution is not dependent on the hardware solutions (e.g., rechargeable batteries) to maintain data privacy in PEDs. We proposed a new metadata structure to enhance data privacy and actor's trust. We used REST API that allows actors to communicate with each other. We provide a REST implementation that demonstrates our solution applicability on the Web, with all the benefits that this architectural style brings. In the following subsections, we discuss the detail of each module as shown in Figure 3.

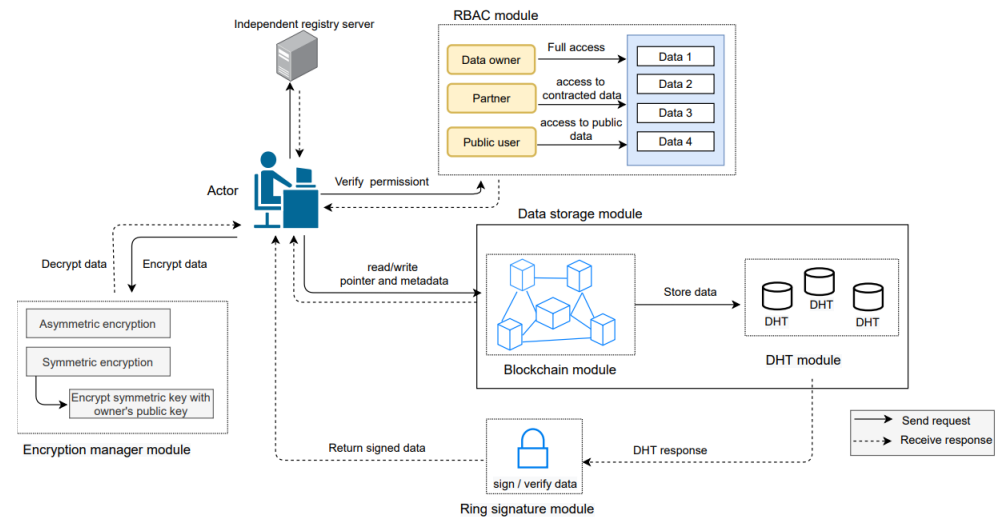


Figure 3. Overview of our peer framework.

4.1. Framework Overview

Our framework enables energy management actors to write and read data on request and interact with other actors using HTTP protocols. Figure 2 gives an overview of our framework and its modules. All actors are the framework's nodes (e.g., peers) and execute the *main* program which calls the *registry_server* module to register into the framework and retrieve the information of connected nodes.

To illustrate, we explain a scenario: a building occupant logs in to write the space heating value of this day. The occupant's program will provide its URL and public key to the other available nodes by calling the */peers* resource ('POST' method) of *registry_server*. After that, it will retrieve the list of connected nodes (*/peers* resource, method 'GET'). It will then call the */chain* resource with the 'GET' method to take the blockchain existing version (please note that some optimization is possible here, in which case only the last few blocks are provided, and the other can be accessible with a GET call with block numbers).

Upon request, the *RBAC_manager* is responsible to authenticate the actor's authorization for instance, the occupant is allowed to write and read data or not. We define all actor's rules and permissions in the *RBAC_manager* file.

The proposed framework enables the authenticated actor to select different encryption techniques to write the data. The *encryption_manager* is responsible to generate a public (Pu), private (Pr), or symmetric key (Sk) of all actors. To store the data the *encryption_manager* allows an actor to encrypt the data using their Pu or Sk according to the encryption technique chosen by the actor. This encrypted data will be sent to the *DHT_manager*, whereas corresponding hash key and metadata will be sent to the *blockchain_manager* component. Later, an authorized actor can modify, delete, and read their data through the hash key stored on the *blockchain_manager*.

Accordingly, an actor will call the */chain/<block_no>* resource ('POST' method) to generate a new block or modify it in the chain. Upon request to read the data, an authorized actor will call the */chain/<block_no>* resource with the 'GET' method.

The operation of our framework modules is detailed below.

4.2. Framework Modules

We present the details of our framework modules that support decentralized data management, permitted data access, enforce data security, and maintain actor's privacy by hiding its identity.

4.2.1. RBAC Manager Module

The Role-based Access Control (RBAC) model is used to handle multi-level data access. The RBAC users (such as actors) are involved in energy management. The role defines user identity to access the resource according to the assigned permission. Permission defines access to multiple levels of data in the same domain [21].

In the following, we proposed the users, roles, resources, and permissions for the data energy management use-case:

- **Users:** RBAC users are the actors defined in the energy management scenario. Thus, the following users are occupant, household, building manager, community manager, DSO, and government.
- **Roles:** A role contains permissions, and actors obtain permissions through the roles they have been assigned. Energy management users can perform different actions on the data based on the following roles:
 - **Data owner:** Each user can be a data owner except the end user that has only data read access. Our framework enables data owners to write and read their data. For instance, an occupant as a ‘data owner’ writes data (e.g., comfort preference: 10 a.m, 19–24 °C; schedule: 5 am and the person appears in the building, consumption mix: space heating, 0.5);
 - **Partner:** The partner role has access to some part of the data that are not available to everyone. Such as a DSO as a “partner” role has permission to read data e.g., (schedule: 5 am and a person appears in the building; consumption mix: space heating, 0.5);
 - **Public user:** The public user can read only public data. Such as household as a role “public user” is allowed to read data from the previous example (consumption mix: space heating, 0.5);
 - **Resources:** Our framework allows users to access a resource based on their roles and permissions. Each data unit stored at a specific location on the DHT is a resource and has a blockchain hash key pointing to it. For each data unit, we define the following data categories according to the requirements of our scenario: private, privacy-sensitive, and public data as discussed in Section 4.2.2. For instance, a building occupant has the role of “data owner” to write data. Table 1 gives examples of data that relate to our scenario.

Table 1. Dataset of energy management actors with example records.

Actor	Private Data	Privacy-Sensitive Data	Public Data
Occupant	Occupant location: Koper Comfort preference: 11:00 am, 10–21 °C	Schedule: 3:00 p.m., 0/1 0 indicates person is not in the building 1 indicates person is in the building.	Consumption mix: space heating: 0.3
Household	Performance data for appliances: fridge energy efficiency, 0.4	Energy consumption: 10:00 a.m., 20% (energy consumed by an actor)	Household size: 12
Building	Thermal transmittance of building envelope: 2, 0.4	Energy consumption: 12:17 p.m., 30%	Building location: Izola
Community	Performance data for power plant: 12, 0.7	energy production: 2:14 p.m., 0.5%	Share of renewables in energy production: 2.4% Carbon footprint: 3.7%
DSO	Distribution losses: 13, 1.4	Energy production: 10:45 a.m., 0.6%	Grid balance: 3:00 p.m., 0.8 net energy is a float value
Government	N/A	City scale energy Consumption: 4:35 a.m., 0.1	Grant amount: 400 euros

- **Rules:** It provides restriction criteria to access resources. we define the following rules in our framework to control access to private, privacy-sensitive, and public data;
 - **R1:** If the role is “data owner” then full (read and write) access is granted to the data resource including private, privacy-sensitive, and public data;
 - **R2:** If the role is “partner” then read-only access is only granted to privacy-sensitive and public data;
 - **R3:** Community can be a partner of DSO and government;
 - **R4:** Household can be a partner of building and community;
 - **R5:** occupant can be a partner of building, household, and community;
 - **R6:** If role is “public user” then read-only access is only granted to publicly available data.

Rules give permission to perform actions on the data. The *verify permission (role, operation, resource)* method called by the *main* component verifies that if the “current role” has permission to make *read and write* actions on the “data” resource. We have defined the following the permissions according to the rules discussed above:

- According to R1, the data owner is allowed to perform write and read operations on the data;
- R2, R3, R4, and R5 allow a partner to just perform data read operations;
- R6 permits the public actor to read and access only the public data.

For instance, from the previous example, an occupant as a “data owner” and “is allowed” to write and read data, for instance, comfort preference: 10 a.m., 19–24 °C; schedule: 5 a.m. and the person appears in the building, consumption mix: space heating, 0.5. On the other hand, DSO as a role “partner” and “is allowed” to read data e.g., schedule: 5 a.m. and the person appears in the building.

Our framework ensures multi-level data access according to the role thus, an occupant as a “public reader” does not have permission to a perform write action on the data. We enforce security on the data by filtering illegal access to sensitive data according to the actor’s role. Our framework ensures that actors are only granted the necessary level of access to perform read/write operations on the data. It is flexible to add more data categories, actors, roles and rules depending on the scenario.

4.2.2. Blockchain Module

Our framework writes metadata (e.g., data entry date and time) and hash key of encrypted data on the *blockchain_manager*. In the following, we discuss the blockchain components including block transaction, consensus mechanism, and metadata extension.

Block and transactions: Each block is composed of a block header, consensus signature, previous block hash, validated metadata, and data hash key. Each block contains a unique hash value to ensure the blockchain integrity from the initial block called genesis to the last block in the network [22]. Our framework enables actors to download blockchain copy by calling method to *initialize (chain)* if other actors will be available, if not, genesis block will be created in the blockchain Each block in the blockchain may contain multiple transactions [22]. Every new transaction is broadcast to the network nodes to verify it. Miners validate the transaction using a consensus mechanism (e.g., proof of work (POW)) and then verified transaction is recorded in the block. Once adding metadata and hash key to the chain, the data owner receives the block number sends it by the proposed framework. Later, data owners can access their data from the blockchain using block numbers and perform, read, modify, and delete actions on their data.

Consensus algorithm: This is a key component of our *blockchain_manager* module as it enables peers to agree on the same data copy in the network. Furthermore, it prevents the malicious nodes from modification of the data in the network. Our *blockchain_manager* module is based on a POW mechanism to validate transactions and create a new block in the blockchain. Therefore, POW requires miners to solve complex mathematics that have

to be accepted by other miners on the network. Miners receive a new coin as a reward to validate a block. After validating block transactions by the miners, a validated block adds up to the chain. The POW algorithm restricts an attacker to take control of more than 51% hashing power of the blockchain. It is easy and fast to validate the proof. We have explained the proposed metadata structure in the following subsection:

Metadata structure: The authors in [26], writes metadata information on the blockchain. Our framework writes metadata for each new transaction to maintains the actor's trust. We propose a metadata extension inspired by the authors in [26], to manage privacy constraints on data. As detailed below, our *encryption_manager* module is responsible for encrypting the user's sensitive information such as location and we put this encrypted data on the *DHT_manager* module. The data stored on DHT contains comfort preference, actor's location, performance data for appliances, and energy consumption. Metadata structure on blockchain includes data hash key, date, and time to record the data as shown in Figure 4.

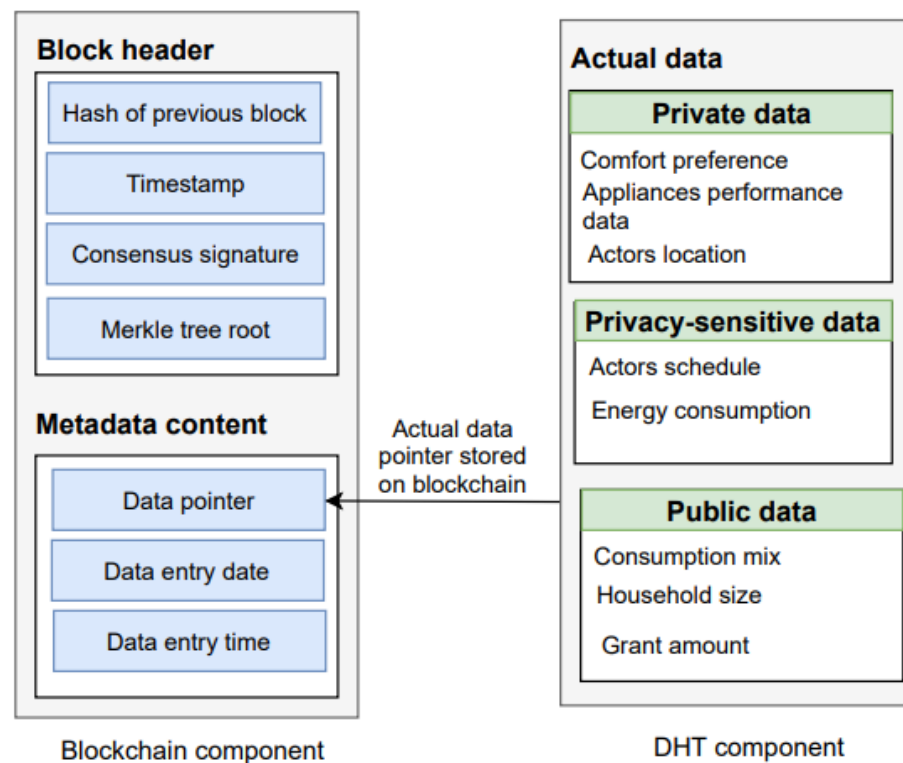


Figure 4. Metadata structure on blockchain.

As depicted in Figure 3, *e* the *RBAC_manager* module is used to manage data access and the *blockchain* module is responsible for recording metadata and hash key of the data while the corresponding data are sent to the *DHT_manager* module. Our framework uses REST APIs (*lchain*) to enable actors to download blockchain copy and to perform, write and read data operations. REST APIs are easy to maintain, provide better performance and enable HTTP client communication between nodes.

Data reading constraints: Table 1 presents the dataset of energy management actors. The data shown here do not intend to be a comprehensive account of all data that can appear as the motivating scenario, but examples that are common in the practice of energy modelling, and energy performance-based use-cases. This is deliberate, as real-life use-cases vary in terms of data content, and it is not in the scope of this study to cover them, rather it is to show how the framework functions. In the proposed framework, the data

owner enables requesters to read the data through (*chain/<block_no>, method "GET"*). To do so, we have explained the following encryption depending on data access constraints:

- Private data must not be shared with anyone. Therefore, our *encryption_manager* module will encrypt private data using the public key of the data owner. This way the data owner can decrypt their data using their private key;
- Privacy-sensitive data can only be shared with some actors. We used *encryption_manager* module to encrypt privacy-sensitive data with the requester's public key, so later, only authorized requesters can access or decrypt it, using their corresponding private key;
- Public data are available to everyone. Our framework allows the public reader to only read this data without modifying and delete it.

4.2.3. DHT Manager Module

A DHT is a decentralized storage system that allows actors to perform, write and read data operations. In our framework, we store encrypted data of all actors on the offline blockchain (key, value) known as *DHT_manager*. We use the Kademia library to implement the *DHT_manager* module of our framework. Actors' data are replicated on nodes of the network to avoid a single point of failure and data loss. Our solution records the date and time of every single transaction to maintain the track of energy data.

4.2.4. Encryption Manager Module

Our framework is flexible to select different encryption mechanisms to ensure data security. In the proposed framework, the *encryption_manager* module allows actors to choose between asymmetric or symmetric encryption techniques to write/read data. Asymmetric encryption mechanism comprises of separate public and private key pair. A public key is accessible to everyone to encrypt the data while the private key is kept by the authorized person to decrypt the data. In our motivating scenario, if an actor such as an occupant chooses asymmetric encryption, then the occupant's public key will be used to encrypt the energy data. After that, an occupant can decrypt this encrypted data using his private key. This encryption mechanism ensures that only the occupant can access his own data.

On the other hand, the symmetric key mechanism is comprised of one key for encryption and decryption. If an actor as a data owner chooses a symmetric key for encryption, then data would be encrypted using the symmetric key. Our *encryption_manager* is responsible for encrypting this symmetric key using the public key of the data owner to enhance the key security. Both encrypted data and encrypted symmetric key would be recorded in the *DHT_manager*. If an actor, such as household, requests to read the building-level, or community-level energy performance data, then the data owner will decrypt this key and will again be encrypted this key by using the data requester's public key. Later, only the data requester can access for a decryption.

4.2.5. Ring Signature Module

Our framework uses the ring signature to maintain the actor's anonymity within the group. Any actor can use a list of public keys to generate a signature. Therefore, there is no way to identify the identity of the data signer. For privacy-sensitive data, the data owner would use the ring signature to maintain his anonymity in the decentralized platform. The data requester is allowed to read the data and validate the signature. We provide an option here to sign the public data using a ring signature if some anonymity is required, or to encrypt it using the public key of the data owner to ensure who owns the data.

5. Results and Discussion

In this section, we present the results and discussion of the proposed decentralized data management and privacy-aware framework. The experimental setup and evaluation model are discussed in Section 5.1. The qualitative security and privacy analysis and quantitative performance evaluation are presented in Section 5.2. Section 5.3 discusses the reflection on decentralized energy governance.

Hash Key

5.1. Experimental Setup and Evaluation Model

We used Python 3 to perform all experimental processes because it is a scalable and dynamic language. Our prototype modules were created using the python language (<https://github.com/Sidra-Aslam/Registry-server-code-decentralized>, accessed on 20 Sep 2021). We implemented a blockchain component using the library [56]. We used the blockchain library to achieve consensus on a distributed network, create new transactions and blocks, mine them using a consensus mechanism (POW). For the DHT, we used Kademia [57] library, which is used to input and retrieve data associated with a given hash key/key on the peer-to-peer network. RBAC library is a python-based library that enabled us to control unauthorized access to the data. We define the actor's relationship (who is the partner of whom) and rules to manage authorized access to the privacy-sensitive data. We generate encryption/decryption keys and sign/verify signatures by using the cryptography RSA library.

Our framework evaluation is based on a Windows 10 operating system. The Central Processing Unit (CPU) architecture used in the 64-bit operating system was x64 Core i7 processor system with a clock cycle of 1.80 GHz. Our experimental specification included 16 GB of RAM. The experiments are conducted using data (see Table 2) taken by the energy actors involved in energy management.

Table 2. Overall results using symmetric encryption.

	Average Time	St Deviation	Min	Max
Write with no pre-existing data	2.3	0.12	2.1	2.6
Write with pre-existing data	0.01	0.08	0.05	0.11
Read data	0.17	0.01	0.13	0.21

The security and privacy evaluation of the proposed framework is based on security, attacks, and privacy. Moreover, in the performance evaluation, we calculated time consumption and provided a comparative analysis using a different number of actors

5.2. Security and Privacy Analysis

In the following, we discuss the security, privacy, and performance of our framework.

Security analysis: The following are the main security properties addressed by the proposed framework design: (1) confidentiality makes sure that data are available to the users who have the right to access it. We use asymmetric and symmetric encryption to achieve confidentiality, (2) integrity verifies that unauthorized actors may not be able to modify the data content. To achieve integrity, our framework encrypts data using the public key of the data owner, so later authorized data owner is allowed to read or modify their data using the corresponding private key, (3) availability means that data must be available to authorized actors when needed. We achieve availability using an access control model, (4) non-repudiation makes sure that no one can deny the data's existence once it has been added to the chain. To do so, we keep track of data by storing metadata in the chain. Our proposed metadata structure is comprised of date and time of data storage, so the data owner cannot deny storing data on the ledger.

Linking attack: To protect against this attack, our framework provides multiple types of encryption methods with ring signature, such as data owner's public key, symmetric key, and requester's public key depending on data requirements discussed above. The proposed *encryption_manager* component is responsible for generating public, private, and symmetric keys on runtime depending on an actor's encryption method selection. To ensure the security of the symmetric key, we encrypt the symmetric key using the public key of the data owner and sent it to the DHT. Later, only the data owner can use this symmetric key to access their data. This way adversary may not be able to connect various transactions to the same key, because data are encrypted using different encryption methods and keys [29,30].

Modification attack: Our solution enables data owners to use their public key for data encryption and record the corresponding hash key on the blockchain. We maintain the evidence of data storage date and time to identify the modification in the data. A malicious user would not be able to alter the data because data can only be decrypted with a corresponding private key that is only known to the data owner.

Privacy analysis: Our framework ensures that data owners own and control their data. Actors' private data will not be disclosed on the network. Before sharing privacy-sensitive data and public data with other actors, we encrypt the data using the requester's public key to ensure data protection from an adversary who might try to read or access the data during the data sharing process. Our solution achieves anonymity using ring signature. It ensures that adversary on the network may not be able to link data with their owner.

Performance evaluation: The proposed solution is scalable to handle many actors at the same time. We achieved a reasonable performance with 108 actors (we have 1 DSO, 1 government, and 1 energy community with 5 buildings, each with 5–10 households, each household with 1–4 occupants, which corresponds to a realistic proportion of actors in a typical energy community). The time consumption evaluation of our framework is based on the permission verification of an actor, data encryption, and decryption using the asymmetric or symmetric method, DHT access, blockchain access, and ring signature. We calculated the time consumption while performing a data write with no pre-existing data, write with pre-existing data, and read operations.

We calculated the time cost for asymmetric encryption as shown in Figures 5 and 6, respectively. We provide a comparative analysis between asymmetric encryption without ring signature and asymmetric encryption using ring signature as demonstrated in Figures 5 and 6. Overall data write time (with no pre-existing data) for asymmetric encryption without ring signature is higher than the overall time of asymmetric encryption using ring signature. The total time consumption to write data (with pre-existing data) for asymmetric encryption without a ring signature is greater than the overall asymmetric encryption time using ring signature. Total time to read data are not much affected for both Figures 5 and 6.

Figures 7 and 8 present the time cost for symmetric encryption without ring signature and symmetric encryption using ring signature. Blockchain access time for symmetric encryption without a ring signature is less as compared to the overall time of symmetric encryption using ring signature in case of data write (with no pre-existing data). The total time consumption to write data (with pre-existing data) of symmetric encryption using ring signature is greater compared to the total time of symmetric encryption without ring signature. For data read, the overall time consumption of symmetric encryption without a ring signature is smaller compared to the total time of symmetric encryption using ring signature.

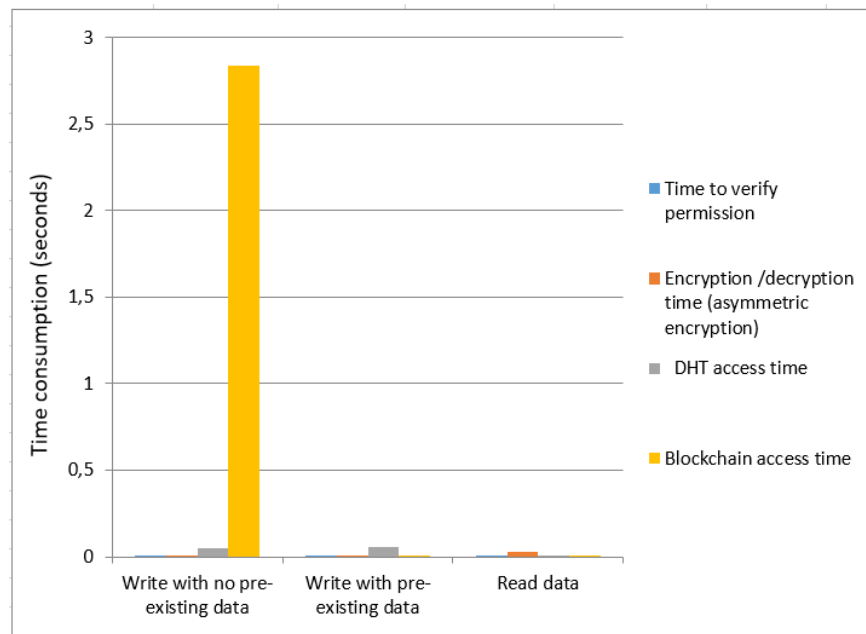


Figure 5. Asymmetric encryption time without ring signature.

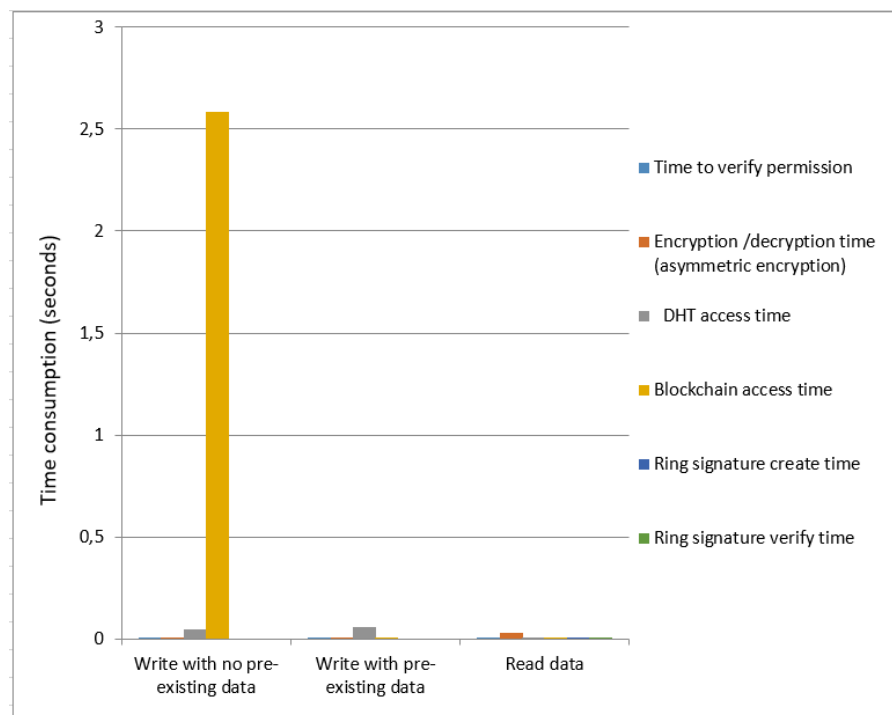


Figure 6. Asymmetric encryption time using ring signature.

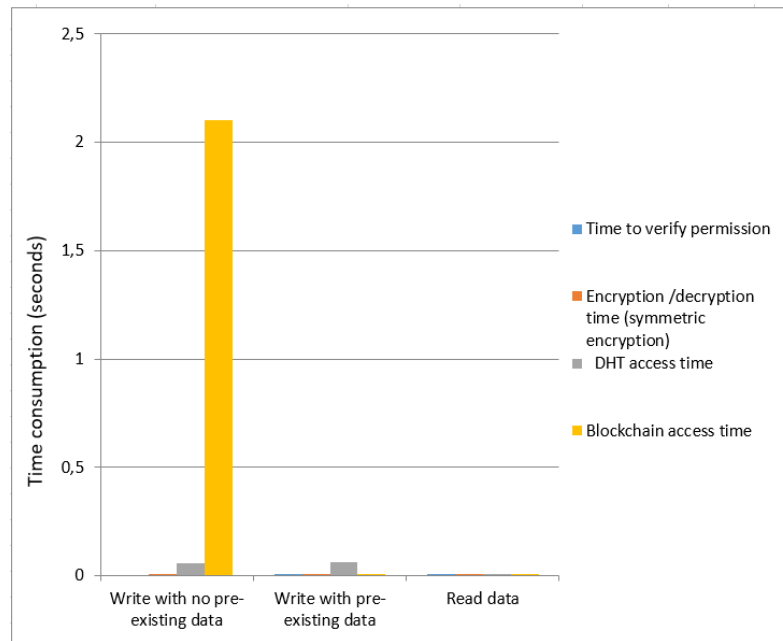


Figure 7. Symmetric encryption time without ring signature.

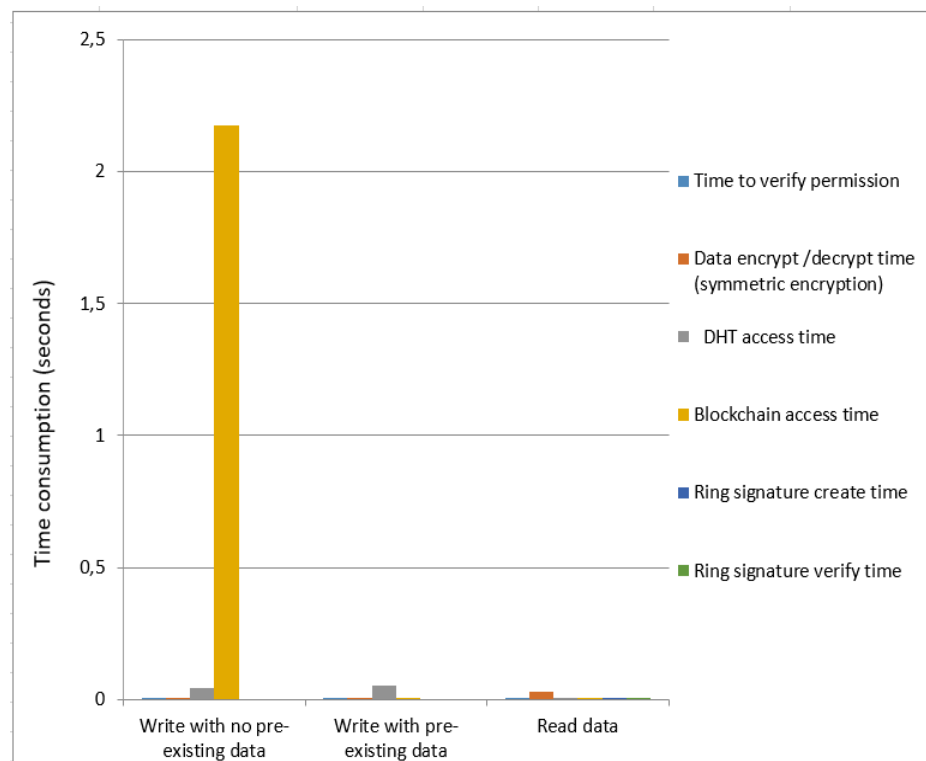


Figure 8. Symmetric encryption time with ring signature.

Moreover, we tested our prototype 100 times for each data write (without pre-existing data and with pre-existing data) and read operation using asymmetric and symmetric encryption methods and then calculated the average time (in seconds), Standard Deviation (SD), min, and max values for accurate results of operations. We presented detailed results for symmetric encryption and asymmetric encryption in Tables 2 and 3. The results

demonstrate that symmetric encryption gives a SDof 0.12 s and asymmetric encryption has an SD of 4.12 s for the data write (with no pre-existing data) operation. To read data, symmetric encryption gives average of 0.17 s and asymmetric encryption provides 0.15 s. To read data, symmetric encryption gives a max value of 0.21 s and asymmetric encryption provides 0.19 s. To write data (with pre-existing data), symmetric encryption gives a min value of 0.05 s and asymmetric encryption has a 0.03 s min value.

Table 3. Overall results using asymmetric encryption.

	Average Time	St Deviation	Min	Max
Write with no pre-existing data	3.62	4.12	2.73	3.5
Write with pre-existing data	0.07	0.01	0.03	0.09
Read data	0.15	0.01	0.11	0.19

We tested our prototype scalability with 58, 87, and 108 actors as depicted in Table 4 and show the graphical representation in Figure 9. In the case of 58 actors, write with no pre-existing data gives an average of 1.4 s, and write with pre-existing data has an average of 0.03 s. In the case of 87 actors, write with no pre-existing data has average time consumption of 1.5 s, and write with pre-existing data gives an average of 0.06 s. Similarly, In the case of 108 actors, write with no pre-existing data gives an average of 1.5 s that is similar to the case of 87 actors, and write with no pre-existing data gives an average of 0.02 s which is less than the case of 58 actors and case of 87 actors. The Average time to read data are not much affected for all three cases and gives an average of 0.1 s. After a detailed performance evaluation, we can see that our framework provides a promising result and is scalable to handle a large number of actors. Experimental results demonstrate that our solution has a low overhead.

Table 4. Detailed results of average time consumption for different cases.

	Case 1	Case 2	Case 3
Number of actors	58	87	108
Write with no pre-existing data	1.43	1.52	1.53
Write with pre-existing data	0.03	0.06	0.02
Read data	0.12	0.10	0.12

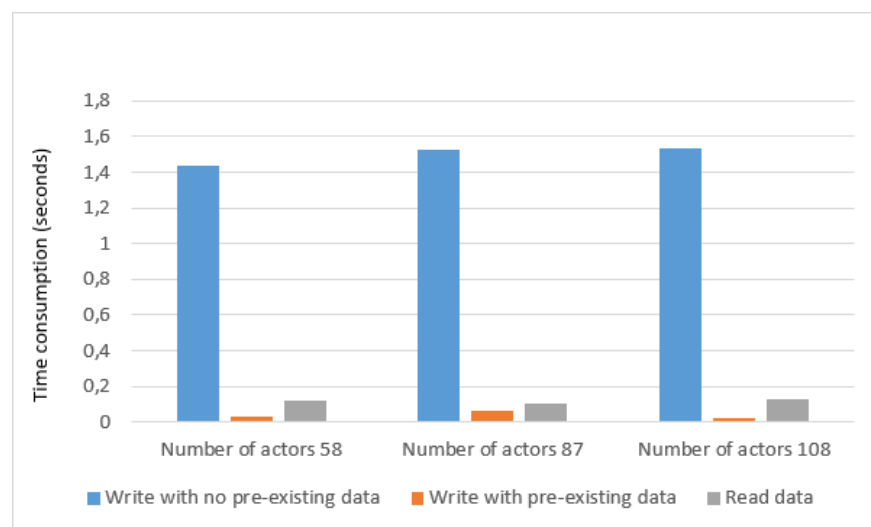


Figure 9. Average time consumption comparison by increasing number of actors.

5.3. Reflection on Decentralized Energy Governance

As stated in the scenario, the objective for distributed data management is to allow each actor to access the data they need to calculate KPIs and ensure its validity, while at the same time ensuring privacy and security requirements of the data owners. To judge whether the system achieves these requirements, we reflect on the five user-data interaction requirements stated in Section 3.

The first interaction referred to collecting personal occupancy data on the building level by building managers. In this case, the occupant, as a data owner may share data with the building manager as a partner, using symmetric encryption. It is the ring signature feature that ensures anonymity when validating occupancy data, as there is no way of telling which actor signed the data.

The second interaction is updating an energy efficiency record for a home appliance on the household level. This is expected to occur each time an appliance is changed; thus, the interaction conflicts with the immutability blockchain provides. In our framework, only the data hash key is stored on the blockchain, and data owners are authorized to do write actions to modify data on the DHT without changing this hash key.

The third and fifth interactions refer to fine-grained access control: an energy community reporting consumption data to a local DSO, and renewable production data to the local government, and a building manager writing data that is fully accessible for households. The third interaction reflects a typical performance-based contract scenario, where the distribution of consumption throughout the day is the basis of a flexibility trading scheme with the DSO, while renewable production is a condition for a public subsidy. The RBAC allows the energy community to allow specific data they own to be read by specific partners, using (a) symmetric encryption to secure the disclosed data. Furthermore, as timestamped consumption/production data are stored on the blockchain, its immutability allows the performance-based contract to be partially disintermediated, meaning there is a reduced role for third parties to provide assurances for the contracts. This corresponds to the requirement for tamper-proof data in the fourth interaction. In real world cases, building management systems, automation systems, or the sensors themselves can register the data, and the data pipeline beyond this point is tamper-proof. However, it is still possible to tamper with the data source itself, or to intervene in the conditions the sensors are measuring, which leaves room for at least third-party calibration and control of the equipment and is a limitation to the proposed framework.

Further research could investigate ways to ensure immutability closer to and beyond the edge, for example through designing energy community databases with multiple cross-validation options. A further limitation of the framework is the handling of representative actors—building managers and energy community managers—as described in the fifth interaction. The interaction describes a situation where the data itself was written by an actor, and then other actors—households—ought to become data owners. Representative actors are not independent actors, but a representation of the pooled competences of constituent actors, meaning that any data registered on the level of buildings and communities should be owned by every member. In the proposed framework, each data has one data owner, in this case, the building manager, who may decide to allow households to read this data. Naturally, they ought to be contractually bound to do so with the households in the building and nobody else, but it still gives these actors more of an intermediary, rather than a representational role, which goes against the principles of the framework. This is a shortcoming subjected to further research.

Reflecting on the interactions show a picture of the framework could work for decentralized energy governance. Table 5 describes how each component enables this scenario. In short, it affords the digitalization of relationship management among the actors involved in energy, meaning it offers a practical way to take objective, real-time, measurable data the basis of enforcing contracts, rules, policies in a peer-to-peer, rather than in an intermediated way. The framework also provides a safe transition to decentralization, as existing institutions, such as local governments and DSOs could have—depending on the

contracts designed—more options to oversee what happens in the energy community and assert their interests and competences.

Table 5. Advantages of our framework components in energy governance.

Our Framework	Benefits in Energy Governance
RBAC manager component	Allows DSOs, energy community members and local governments to enforce their contractual rights through granular data access to relevant metrics, such as on-site energy production.
Encryption manager component	Allows protection of non-disclosed data (asymmetric encryption), such as custom set-points of households and secure disclosure of data between partner actors (symmetric encryption), such as occupancy schedules.
Blockchain manager component	Ensures the authenticity and immutability of data in performance-based contracts, such as energy consumption.
DHT manager component	Adds necessary scalability to handle the stream of energy-related data, as well as to manage the scaling of the energy community itself.
Ring signature manager component	Allows a privacy-sensitive disclosure of data, in particular multiscale data aggregated by building managers and energy community managers.

6. Conclusions and Future Work

We proposed a decentralized data storage and management framework that ensures data security, data update, and user privacy in multi-scale energy management scenario. Our solution combines the blockchain with, role-based access control, DHT, ring signature, and various types of encryption methods. The proposed framework enables authorized actors to write and read the data without revealing their private data (e.g., identity) on a public ledger. We discussed the advantages and limitations of existing literature to highlight the research gap. The limitation of existing work is a trusted third party to manage the data.

We used REST APIs and design modules in such a way that can easily expand, reuse, and act as a platform to build other applications and use-cases. We discussed results in terms of security, privacy, and performance evaluation regarding its operation on a decentralized ledger. The results present that the proposed solution attains an acceptable overhead.

Our prototype was tested on exemplary data samples and for realistic models of energy communities in terms of user composition and size, but not in an actual, real-life environment. The study is a mere simulation of how the system works. It is still necessary to test the system in an operational environment and for it to be validated by the intended users before wider application. Our prototype is more widely applicable for any use-case that relies on data to digitalize decentralized governance and management, because the prototype manages the data privacy problems that arise without sacrificing scalability. These use-cases entail trust-free supply chains (e.g., in medical or industrial applications) or common pool resource management (e.g., energy, agriculture, infrastructure).

Our framework is the first work that combines multiple technologies with PEDs and ensures decentralized data management, data security, and access control without requiring the involvement of a trusted third party. As future work, we will test our solution over a large number of peers, check the performance for large-scale networks, and increase the number of actors with different data. We also have a plan to investigate blockchain attacks and to propose a solution for mitigating our scenario. Further work can be extended to compare different access control models e.g., attribute-based access control model, rule-based access control model, mandatory-access control model in terms of their advantages, limitations, and performance.

Author Contributions: Conceptualization, S.A., V.B. and M.M.; methodology, S.A., V.B. and M.M.; software, S.A. and M.M.; validation, S.A., V.B. and M.M.; formal analysis, S.A., V.B. and M.M.; investigation S.A., V.B. and M.M.; resources, S.A., V.B. and M.M.; data curation, S.A., V.B. and M.M.; writing—original draft preparation, S.A., V.B. and M.M.; writing—review and editing, S.A., V.B. and M.M.; visualization, S.A., V.B. and M.M.; supervision, M.M.; project administration, M.M.; funding acquisition, M.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research was co-funded by the InnoRenew project (Grant Agreement #739574) under the Horizon2020 Widespread-Teaming program and the Republic of Slovenia (Investment funding of the Republic of Slovenia and the European Regional Development Fund). It was also co-funded by the Slovenian Research Agency ARRS through the project J2-2504.

Acknowledgments: The authors gratefully acknowledge the European Commission for funding the InnoRenew project (Grant Agreement \#739574) under the Horizon2020 Widespread-Teaming program and the Republic of Slovenia (Investment funding of the Republic of Slovenia and the European Regional Development Fund). They also acknowledge the Slovenian Research Agency ARRS for funding the project J2-2504. This work is based on Cooperation in Science and Technology activities carried out by the authors as part of the COST Action CA19126—Positive Energy Districts European Network (PED-EUNET), supported by COST (European Cooperation in Science and Technology).

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

References

- Javid, I.; Chauhan, A.; Thappa, S.; Verma, S.K.; Anand, Y.; Sawhney, A.; Tyagi, V.V.; Anand, S. Futuristic decentralized clean energy networks in view of inclusive-economic growth and sustainable society. *J. Clean. Prod.* **2021**, *309*, 127304.
- Alstone, P.; Gershenson, D.; Kammen, D.M. Decentralized energy systems for clean electricity access. *Nat. Clim. Chang.* **2015**, *5*, 305–314.
- Weinand, J.M.; Scheller, F.; McKenna, R. Reviewing energy system modelling of decentralized energy autonomy. *Energy* **2020**, *203*, 117817.
- Leal-Arcas, R.; Alemany Rios, J.; Akondo, N. Energy Decentralization in the European Union. *Georget. Environ. Law Rev.* **2019**, *32*, 1–58.
- Chiradeja, P.; Ramakumar, R. An approach to quantify the technical benefits of distributed generation. *IEEE Trans. Energy Convers.* **2004**, *19*, 764–773, doi:10.1109/TEC.2004.827704.
- Akorede, M.F.; Hizam, H.; Pouresmaeil, E. Distributed energy resources and benefits to the environment. *Renew. Sustain. Energy Rev.* **2010**, *14*, 724–734.
- Walker, G.; Devine-Wright, P. Community renewable energy: What should it mean? *Energy Policy* **2008**, *36*, 497–500, doi:10.1016/j.enpol.2007.10.019.
- Creamer, E.; Taylor Aiken, G.; van Veelen, B.; Walker, G.; Devine-Wright, P. Community renewable energy: What does it do? Walker and Devine-Wright (2008) ten years on. *Energy Res. Soc. Sci.* **2019**, *57*, 101223, doi:10.1016/j.erss.2019.101223.
- Adil, A.M.; Ko, Y. Socio-technical evolution of Decentralized Energy Systems: A critical review and implications for urban planning and policy. *Renew. Sustain. Energy Rev.* **2016**, *57*, 1025–1037.
- Brisbois, M.C. Decentralised energy, decentralised accountability? Lessons on how to govern decentralised electricity transitions from multi-level natural resource governance. *Glob. Transit.* **2020**, *2*, 16–25, doi:10.1016/j.glt.2020.01.001.
- European Parliament Directives. Directive (eu) 2018/2001 of the European Parliament and of the Council of 11 December 2018 on the Promotion of the Use of Energy from Renewable Sources. 2018. Available online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L2001> (accessed on 11 December 2018).
- European Parliament. Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on Common Rules for the Internal Market for Electricity and Amending Directive 2012/27/EU. 2019. Available online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L0944> (accessed on 5 June 2019).
- Gollner, C.; Hinterberger, R.; Bossi, S.; Theierling, S.; Noll, M.; Meyer, S.; Schwarz, H.-G. Europe towards Positive Energy Districts—A Compilation of Projects towards Sustainable Urbanization and the Energy Transition. 2020. Available online: https://jpi-urbaneurope.eu/wp-content/uploads/2020/06/PED-Booklet-Update-Feb-2020_2.pdf (accessed on 1 February 2020).
- Skelcher, C.; Torfing, J. Improving democratic governance through institutional design: Civic participation and democratic ownership in Europe. *Regul. Gov.* **2010**, *4*, 71–91, doi:10.1111/j.1748-5991.2010.01072.x.
- Van Kersbergen, K.; Van Waarden, F. “Governance” as a bridge between disciplines: Cross-disciplinary inspiration regarding shifts in governance and problems of governability, accountability and legitimacy. *Eur. J. Polit. Res.* **2004**, *43*, 143–171, doi:10.1111/j.1475-6765.2004.00149.x.

16. Ilavarasan, P.V.; Levy, M.R. ICTs and Urban Microenterprises: Identifying and Maximizing Opportunities for Economic Development. 2010. Available online: <https://www.unapcict.org/sites/default/files/2019-01/871.%20ICTs%20and%20Urban%20Microenterprises.pdf> (accessed on 1 July 2010).
17. Soto, D.; Basinger, M.; Rodriguez-Sanchez, S.; Adkins, E.; Menon, R.; Owczarek, N.; Willig, I.; Modi, V. A prepaid architecture for solar electricity delivery in rural areas. In *ACM International Conference Proceeding Series*; Association for Computing Machinery: New York, NY, USA, 2012; pp. 130–138.
18. Rosa, J.; Madduri, P.A.; Soto, D. Efficient microgrid management system for electricity distribution in emerging regions. In Proceedings of the 2012 IEEE Global Humanitarian Technology Conference, Seattle, WA, USA, 21–24 October 2012; pp. 23–26.
19. Costanzo, E.; Martino, A.; Varalda, G.M.; Antinucci, M.; Federici, A. EPBD Implementation in Italy. 2016. Available online: <https://www.epbd-ca.eu/wp-content/uploads/2018/08/CA-EPBD-IV-Italy-2018.pdf> (accessed on 1 December 2016).
20. Davidson, S.; Filippi, P.D.; Potts, J. Blockchains and the economic institutions of capitalism. *J. Inst. Econ.* **2018**, *14*, 639–658, doi:10.1017/S1744137417000200.
21. Cohen, J.E. Law for the Platform Economy. 2017. Available online: https://lawreview.law.ucdavis.edu/issues/51/1/Symposium/51-1_Cohen.pdf (accessed on 1 July 2017).
22. Chen, Y.; Pereira, I.; Patel, P.C. Decentralized Governance of Digital Platforms. *J. Manag.* **2020**, *47*, 1305–1337, doi:10.1177/0149206320916755.
23. Abraham, R.; Schneider, J.; vom Brocke, J. Data governance: A conceptual framework, structured review, and research agenda. *Int. J. Inf. Manag.* **2019**, *49*, 424–438, doi:10.1016/j.IJINFORMGT.2019.07.008.
24. van Hoboken, J.; Fathaigh, R. Smartphone platforms as privacy regulators. *Comput. Law Secur. Rev.* **2021**, *41*, 105557, doi:10.1016/j.CLSR.2021.105557.
25. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In Proceedings of the 2017 IEEE 6th International Congress Big Data, BigData Congress, Honolulu, HI, USA, 25–30 June 2017; pp. 557–564, doi:10.1109/BIGDATAACONGRESS.2017.85.
26. Ali, S.; Wang, G.; White, B.; Cottrell, R.L. A Blockchain-Based Decentralized Data Storage and Access Framework for PingER. In Proceedings of the 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; pp. 1303–1308, doi:10.1109/TRUSTCOM/BIGDATASE.2018.00179.
27. Van Cutsem, O.; Ho Dac, D.; Boudou, P.; Kayal, M. Cooperative energy management of a community of smart-buildings: A Blockchain approach. *Int. J. Electr. Power Energy Syst.* **2020**, *117*, 105643, doi:10.1016/j.ijepes.2019.105643.
28. Yu, Q.; Meeuw, A.; Wortmann, F. Design and implementation of a blockchain multi-energy system. *Energy Inform.* **2018**, *1*, 311–318, doi:10.1186/S42162-018-0040-4.
29. Yang, Q.; Wang, H.; Wang, T.; Zhang, S.; Wu, X.; Wang, H. Blockchain-based decentralized energy management platform for residential distributed energy resources in a virtual power plant. *Appl. Energy* **2021**, *294*, 117026, doi:10.1016/J.APENERGY.2021.117026.
30. Miglani, A.; Kumar, N.; Chamola, V.; Zeadally, S. Blockchain for Internet of Energy management: Review, solutions, and challenges. *Comput. Commun.* **2020**, *151*, 395–418, doi:10.1016/J.COMCOM.2020.01.014.
31. Parra, D.; Swierczynski, M.; Stroe, D.I.; Norman, S.A.; Abdon, A.; Worlitschek, J.; O’Doherty, T.; Rodrigues, L.; Gillott, M.; Zhang, X.; et al. An interdisciplinary review of energy storage for communities: Challenges and perspectives. *Renew. Sustain. Energy Rev.* **2017**, *79*, 730–749, doi:10.1016/j.rser.2017.05.003.
32. Chen, H.; Cong, T.N.; Yang, W.; Tan, C.; Li, Y.; Ding, Y. Progress in electrical energy storage system: A critical review. *Prog. Nat. Sci.* **2009**, *19*, 291–312, doi:10.1016/J.PNSC.2008.07.014.
33. Huggins, R.A. *Energy Storage*; Springer US: Berlin/Heidelberg, Germany, 2010.
34. Chakravorty, A.; Rong, C. Ushare: User controlled social media based on blockchain. In Proceedings of the IMCOM '17: 11th International Conference on Ubiquitous Information Management and Communication, Beppu, Japan, 5–7 January 2017; doi:10.1145/3022227.3022325.
35. Hassanzadeh-Nazarabadi, Y.; Küpçü, A.; Özkasap, Ö. LightChain: A DHT-based Blockchain for Resource Constrained Environments. *arXiv* **2019**, arXiv:1904.00375v3.
36. Yang, L.; Chen, X.; Zhang, J.; Poor, H.V. Optimal privacy-preserving energy management for smart meters. In Proceedings of the IEEE INFOCOM, Toronto, ON, Canada, 27 April–2 May 2014; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2014; pp. 513–521.
37. Efthymiou, C.; Kalogridis, G. Smart Grid Privacy via Anonymization of Smart Metering Data. In Proceedings of the IEEE International Conference on Smart Grid Communications (SmartGridComm), Gaithersburg, MD, USA, 4–6 October 2010; Institute of Electrical and Electronics Engineers (IEEE): Piscataway, NJ, USA, 2010; pp. 238–243.
38. Bohli, J.M.; Sorge, C.; Ugus, O. A privacy model for smart metering. In Proceedings of the 2010 IEEE International Conference on Communications Workshops, ICC 2010, Cape Town, South Africa, 23–27 May 2010.
39. Garcia, F.D.; Jacobs, B. Privacy-friendly energy-metering via homomorphic encryption. In *Lecture Notes in Computer Science*; Springer: Berlin/Heidelberg, Germany, 2011; Volume 6710, pp. 226–238.
40. Kim, Y.; Ngai, E.C.H.; Srivastava, M.B. Cooperative state estimation for preserving privacy of user behaviors in smart grid. In Proceedings of the 2011 IEEE International Conference on Smart Grid Communications, SmartGridComm 2011, Brussels, Belgium, 17 October 2011; pp. 178–183.

41. Koo, J.; Lin, X.; Bagchi, S. PRIVATUS: Wallet-friendly privacy protection for smart meters. In *Lecture Notes in Computer Science*; Springer: Berlin/Heidelberg, Germany, 2012; Volume 7459, pp. 343–360.
42. Tan, O.; Gunduz, D.; Poor, H.V. Increasing smart meter privacy through energy harvesting and storage devices. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 1331–1341, doi:10.1109/JSAC.2013.130715.
43. Yang, L.; Chen, X.; Zhang, J.; Poor, H.V. Cost-effective and privacy-preserving energy management for smart meters. *IEEE Trans. Smart Grid* **2015**, *6*, 486–495, doi:10.1109/TSG.2014.2343611.
44. Yang, Q.; Wang, H. Privacy-Preserving Transactive Energy Management for IoT-aided Smart Homes via Blockchain. *IEEE Internet Things J.* **2021**, *8*, 11463–11475.
45. Wang, B.; Zhao, S.; Li, Y.; Wu, C.; Tan, J.; Li, H.; Yukita, K. Design of a privacy-preserving decentralized energy trading scheme in blockchain network environment. *Int. J. Electr. Power Energy Syst.* **2021**, *125*, 106465, doi:10.1016/j.ijepes.2020.106465.
46. Chen, Z.; Wu, L. Residential appliance DR energy management with electric privacy protection by online stochastic optimization. *IEEE Trans. Smart Grid* **2013**, *4*, 1861–1869, doi:10.1109/TSG.2013.2256803.
47. Finster, S.; Baumgart, I. Privacy-aware smart metering: A survey. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 1088–1101, doi:10.1109/COMST.2015.2425958.
48. González-Zapata, A.M.; Tlelo-Cuautle, E.; Cruz-Vega, I.; León-Salas, W.D. Synchronization of chaotic artificial neurons and its application to secure image transmission under MQTT for IoT protocol. *Nonlinear Dyn.* **2021**, *104*, 4581–4600, doi:10.1007/S11071-021-06532-X.
49. Bukovszki, V.; Magyari, Á.; Braun, M.K.; Párdi, K.; Reith, A. Energy Modelling as a Trigger for Energy Communities: A Joint Socio-Technical Perspective. *Energies* **2020**, *13*, 2274, doi:10.3390/en13092274.
50. Lowitzsch, J.; Hoicka, C.E.; van Tulder, F.J. Renewable energy communities under the 2019 European Clean Energy Package—Governance model for the energy clusters of the future? *Renew. Sustain. Energy Rev.* **2020**, *122*, 109489, doi:10.1016/j.rser.2019.109489.
51. Lohse, R.; Zhivov, A. *Deep Energy Retrofit Guide for Public Buildings*; SpringerBriefs in Applied Sciences and Technology; Springer International Publishing: Cham, Switzerland, 2019; ISBN 978-3-030-14921-5.
52. Allegrini, J.; Orehounig, K.; Mavromatidis, G.; Ruesch, F.; Dorer, V.; Evins, R. A review of modelling approaches and tools for the simulation of district-scale energy systems. *Renew. Sustain. Energy Rev.* **2015**, *52*, 1391–1404, doi:10.1016/j.rser.2015.07.123.
53. Sola, A.; Corchero, C.; Salom, J.; Sanmarti, M. Multi-domain urban-scale energy modelling tools: A review. *Sustain. Cities Soc.* **2019**, *54*, 101872, doi:10.1016/j.scs.2019.101872.
54. Bertino, E. RBAC models—Concepts and trends. *Comput. Secur.* **2003**, *22*, 511–514, doi:10.1016/S0167-4048(03)00609-6.
55. Nofer, M.; Gomber, P.; Hinz, O.; Schiereck, D. Blockchain. *Bus. Inf. Syst. Eng.* **2017**, *59*, 183–187, doi:10.1007/S12599-017-0467-3.
56. Kansal, S. Python Blockchain app 2020. Available online: <https://lagnypontcarrecyclisme.com/yee/blockchain-in-python-github> (accessed on 15 September 2021).
57. Muller, B. Kademia Library 2021. Available online: <https://github.com/bmuller/kademia> (accessed on 15 September 2021).