electronics

Article

A Blockchain-Based Lightweight Reputation-Aware Electricity Trading Service Recommendation System

Pingyan Mo [1], Kai Li [1], Yongjiao Yang [1], You Wen [1] and Jinwen Xi [2,*]

[1] Information Centre of Guangdong Power Grid Co., Ltd., 7-11/F, Southern Investment Building, No. 190 Pazhou Avenue, Haizhu District, Guangzhou 510600, China; mopingyan@xxzx.gd.csg.cn (P.M.); likai@gdxx.csg.cn (K.L.); yangyongjiao@xxzx.gd.csg.cn (Y.Y.); wenyou@xxzx.gd.csg.cn (Y.W.)
[2] School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China
* Correspondence: jwxi@bupt.cn

Abstract

With the continuous expansion of users, businesses, and services in electricity retail trading systems, the demand for personalized recommendations has grown significantly. To address the issue of reduced recommendation accuracy caused by insufficient data in standalone recommendation systems, the academic community has conducted in-depth research on distributed recommendation systems. However, this collaborative recommendation environment faces two critical challenges: first, how to effectively protect the privacy of data providers and power users during the recommendation process; second, how to handle the potential presence of malicious data providers who may supply false recommendation data, thereby compromising the system's reliability. To tackle these challenges, a blockchain-based lightweight reputation-aware electricity retail trading service recommendation (BLR-ERTS) system is proposed, tailored for electricity retail trading scenarios. The system innovatively introduces a recommendation method based on Locality-Sensitive Hashing (LSH) to enhance user privacy protection. Additionally, a reputation management mechanism is designed to identify and mitigate malicious data providers, ensuring the quality and trustworthiness of the recommendations. Through theoretical analysis, the security characteristics and privacy-preserving capabilities of the proposed system are explored. Experimental results show that BLR-ERTS achieves an MAE of 0.52, MSE of 0.275, and RMSE of 0.52 in recommendation accuracy. Compared with existing baseline methods, BLR-ERTS improves MAE, MSE, and RMSE by approximately 13%, 14%, and 13%, respectively. Moreover, the system exhibits 94% efficiency, outperforming comparable approaches by 4–24%, and maintains robustness with only a 30% attack success rate under adversarial conditions. The findings demonstrate that BLR-ERTS not only meets privacy protection requirements but also significantly improves recommendation accuracy and system robustness, making it a highly effective solution in a multi-party collaborative environment.

Keywords: electricity retail trading; personalized recommendation; blockchain; locality-sensitive hashing; privacy protection

Academic Editor: Dimitra I. Kaklamani

Received: 30 May 2025
Revised: 26 June 2025
Accepted: 27 June 2025
Published: 30 June 2025

Citation: Mo, P.; Li, K.; Yang, Y.; Wen, Y.; Xi, J. A Blockchain-Based Lightweight Reputation-Aware Electricity Trading Service Recommendation System. *Electronics* **2025**, *14*, 2640. https://doi.org/10.3390/electronics14132640

1. Introduction

With the continuous growth of energy demand and the ongoing optimization of the energy structure, the power trading system has become increasingly pivotal in the energy sector. By implementing a market-based trading model, the power trading system

effectively bridges the gap between power supply and demand, achieving the optimal allocation and efficient utilization of electricity resources. However, as user participation in power trading activities intensifies, the platform inevitably accumulates vast volumes of historical data. This data overload significantly undermines the efficiency of information utilization [1]. In this context, personalized recommendation technologies have emerged as a crucial approach to mitigating the challenge of information overload. By conducting an in-depth analysis of users' personal data and behavioral patterns, these technologies can provide precise and contextually relevant electricity retail transaction services. Furthermore, personalized services offer the potential to optimize electricity costs for users through dynamic pricing adjustments and real-time demand response strategies. These mechanisms not only facilitate the balance between electricity supply and demand, promoting rational price formation, but also enhance the overall efficiency of energy consumption and trading processes.

The importance of this research lies in addressing the dual challenges of privacy protection and recommendation accuracy, which are crucial for the effective operation of modern electricity trading platforms. As more users engage in electricity trading, ensuring the privacy of sensitive user data while maintaining the accuracy of personalized recommendations becomes vital. Despite the critical importance of these issues, research on retail electricity trading systems remains relatively sparse, with many questions still unaddressed. By proposing novel solutions to enhance privacy protection and recommendation accuracy, this study aims to fill these gaps and contribute to the development of more efficient, secure, and user-centric electricity trading systems.

To address the aforementioned challenges, an effective strategy involves integrating data resources from multiple platforms and deploying recommendation algorithms atop a unified data repository. However, in practice, achieving collaboration across platforms is often fraught with difficulty. This is primarily due to two factors: first, platforms are typically reluctant to share their data, driven by concerns about potential misuse, fraud, or loss of control [2]; second, ensuring that all data providers operate with integrity and trustworthiness during joint execution of recommendation algorithms is inherently challenging. These issues collectively constitute significant practical obstacles to implementing cross-platform data integration and recommendation systems.

Blockchain technology, as a tamper-evident distributed ledger system, is characterized by decentralization, collective maintenance, immutability, and inherent trustworthiness. In the design of our system, we leverage blockchain technology to enable data providers—who may not inherently trust one another—to collaborate securely and deliver accurate, personalized recommendations to users. Specifically, this work applies blockchain to the domain of personalized recommendation for electricity transactions, resulting in a blockchain-based recommendation framework tailored to electricity retail services. Within this framework, the reputation value of each recommender is treated as a key factor influencing the effectiveness of recommendations. To ensure both recommendation accuracy and user privacy, we propose an improved personalized recommendation algorithm based on Locality-Sensitive Hashing (LSH) and a distributed reputation management mechanism.

Contributions. The main contributions of this paper are as follows:

(1) We design a recommendation system for electricity retail trading services by incorporating distributed blockchain technology. This system leverages the inherent security properties of blockchain to protect the identity privacy of recommendation requesters and data providers, thereby mitigating the security vulnerabilities inherent in traditional centralized electricity trading platforms.

(2) To address the high computational demands and inadequate privacy protection of conventional distributed recommendation algorithms, we propose an enhanced LSH-based

recommendation algorithm. This approach enables data requesters to obtain recommendation results by disclosing only LSH hash signatures, while retaining full control over their original data. This not only significantly reduces computational complexity but also robustly preserves the privacy and security of user data.

(3) To improve data quality and detect malicious data providers, we introduce a global reputation management mechanism that substantially enhances recommendation accuracy in cross-organizational collaborations. By implementing a blockchain-based reputation scoring system, our mechanism ensures that the historical behavior of each data provider is transparently tracked and verified.

(4) Through rigorous theoretical analysis and extensive experimental validation, we demonstrate that the proposed approach achieves superior accuracy, with an MAE of 0.52, MSE of 0.275, and RMSE of 0.52 in the recommendation process. In addition, the system operates efficiently, with an average CPU load of 27 ms, a bandwidth usage of 265 Kbps, and energy consumption of 2480 millijoules. The efficiency of the proposed system is the highest among all compared methods, reaching 94%. Simultaneously, it preserves the privacy of both users and data providers, with an attack success rate as low as 30% when the number of hash tables is set to 10, demonstrating robust privacy protection under adversarial conditions.

The remainder of this paper is organized as follows. Section 2 reviews related work to provide context and identify research gaps. Section 3 introduces the necessary background, including LSH and personalized recommendation techniques. Section 4 presents the implementation details of the proposed BLR-ERTS method. Section 5 provides a theoretical analysis of the approach. Section 6 evaluates its performance through empirical experiments. Section 7 discusses the strengths, limitations, and broader implications of the method. Finally, Section 8 concludes the paper and outlines potential directions for future research.

2. Related Works

This section reviews related work on blockchain in electricity trading, personalized recommendation, privacy protection, and reputation mechanisms. We analyze the limitations of existing approaches, such as limited scalability and inadequate integration of trust and privacy. In contrast, our work offers a more comprehensive solution by combining blockchain-based trust management with privacy-preserving personalized recommendations, tailored to the needs of electricity trading systems.

2.1. Blockchain in Electricity Trading

With the rapid development of distributed energy systems and peer-to-peer (P2P) electricity trading, there has been a growing demand for both privacy protection and personalized service recommendations in the electricity market. Blockchain technology, characterized by decentralization, immutability, and transparency, offers novel technical approaches to addressing these challenges in power transactions. By enabling encrypted storage of user data and automatic transaction execution through smart contracts, blockchain not only establishes a robust foundation for privacy and security but also synergizes with reputation mechanisms and recommendation algorithms to enhance user experience and improve system operational efficiency. This integrative innovation has emerged as a critical research direction in privacy-preserving power transactions and personalized service recommendation, demonstrating significant application potential [3]. Furthermore, recent studies have highlighted the critical role of blockchain in enhancing authentication and privacy preservation in the Internet of Things (IoT).

Wang et al. [4] proposed a privacy-preserving power transaction framework that leverages blockchain technology to combine decentralized architectures with attribute-based encryption (ABE) schemes, thereby achieving fine-grained access control and protecting users' private information. However, the complexity inherent in such encryption techniques substantially impacts system usability and efficiency. To address privacy concerns in transaction information, Yang et al. [5] introduced a blockchain-based P2P energy trading model utilizing ciphertext-policy attribute-based encryption (CP-ABE). This model allows peer nodes—including buyers and sellers—to autonomously manage and validate transactions without reliance on third-party intermediaries. Nonetheless, the approach introduces considerable computational and communication overhead. To mitigate these burdens while maintaining security and privacy, Li et al. [6] designed a decentralized, secure, and privacy-preserving bidirectional electricity transaction scheme for interactions between trams and the grid, leveraging coalition chains. By incorporating an improved swarm optimization algorithm to determine optimal charging and discharging schedules for electric vehicles, this approach effectively reduces total load deviation while enhancing both the speed and accuracy of the model's solutions.

2.2. Recommendation in Electricity Trading

The core objective of applying recommendation systems in power trading lies in delivering accurate and personalized suggestions for power products and services based on users' consumption behaviors and preferences, thereby enhancing user satisfaction and improving market efficiency. Zhang et al. [7] employed collaborative filtering techniques to develop a power plan recommendation system that generates customized suggestions tailored to the unique consumption patterns of individual users. Similarly, Casino et al. [8] proposed a blockchain-based collaborative filtering framework that integrates the Interplanetary File System (IPFS) to minimize the volume of information stored and shared on the blockchain. He et al. [9] introduced a recommendation system designed to process extensive user characteristic data and personalized electricity demand information, enabling users to efficiently identify suitable retail tariff packages.

2.3. Privacy Protection and Reputation Mechanisms

To address the challenges of security, privacy, and reliability in the retail electricity trading process, extensive research has been conducted. Hassan et al. [10] introduced the innovative concept of the Virtual Power Plant (VPP), which facilitates intelligent and secure energy management among producers, sellers, buyers, and power stations. Furthermore, to enhance system security and privacy protection, their work incorporates differential privacy into the consensus mechanism and proposes a Private Consensus Model (PoEM).

In a related effort, Gaybullaev et al. [11] developed a novel bidding encoding algorithm using binary coding to reduce the computational burden of privacy-preserving cryptographic techniques, thereby improving the performance of power trading systems. To counter Sybil attacks, Baza et al. [12] proposed a prefix linkable anonymous authentication scheme for booking and offer submissions. Additionally, this study introduced an anonymous and efficient blockchain-based payment system designed to safeguard the privacy of transacting parties and prevent user identities from being linked to specific addresses.

2.4. Research Discrepancies

Existing approaches exhibit several notable limitations in practical applications. First, most schemes do not provide additional safeguards for data stored on the blockchain, relying solely on the inherent security mechanisms of the blockchain for data management. Consequently, if the blockchain is compromised by a consensus attack, the integrity and security of on-chain data cannot be ensured. Second, while current encryption

techniques—such as homomorphic encryption—can provide a degree of data confidentiality, they suffer from inherent constraints, including limited computational depth and large key spaces, which hinder broader adoption. Third, user identities on the blockchain are tied to unique public key addresses, making it easier for privacy breaches to occur; moreover, if a user's private key is lost, the associated data resources become permanently inaccessible.

Therefore, ensuring the security of blockchain transaction information and data integrity remains a pressing research challenge. In the context of blockchain-based power transaction service recommendation, this paper proposes an innovative approach: adopting a LSH algorithm to efficiently match privacy requirements, thereby effectively preventing the disclosure of original data. Additionally, blockchain is leveraged to record the entire transaction process, ensuring data immutability and traceability. To further enhance recommendation efficiency and reliability, this paper integrates a reputation mechanism into the personalized recommendation process, thereby improving the precision of transaction matching. Finally, the proposed system employs smart contracts to automate execution, significantly reducing the need for human intervention and associated operational costs.

3. Preliminaries

This section outlines the key preliminaries of our approach, focusing on LSH for efficient similarity search and collaborative filtering techniques for personalized recommendation in electricity trading contexts.

3.1. Locality-Sensitive Hashing

LSH is a classical algorithm designed to efficiently solve the problem of nearest neighbor search in high-dimensional, large-scale datasets [13]. The fundamental principle of LSH is to project high-dimensional spatial data into a lower-dimensional space while preserving the similarity relationships among data points. In other words, after the hashing operation, two proximate data nodes in the original space are highly likely to remain proximate in the hashed space.

The following two conditions must be satisfied simultaneously:

(1) If $d(x, y) \leq d_1$, then $Pro(H(x) = H(y)) \geq p_1$);

(2) If $d(x, y) \geq d_1$, then $Pro(H(x) = H(y)) \leq p_2$).

Let $H(.)$ denote the LSH function, which is sensitive to the parameters (d_1, d_2, p_1, p_2). Here, x and y represent two points in the high-dimensional space, $d(x, y)$ denotes the distance between points x and y, and $Pro(A)$ represents the probability of event A occurring. Specifically, d_1 and d_2 denote distance thresholds, while p_1 and p_2 denote the corresponding probability thresholds.

3.2. Personalized Recommendation Algorithms Based on Collaborative Filtering

In recommendation systems, users interact with and rate various items through activities such as browsing, commenting, and posting. These items span diverse domains, including books, films, attractions, and restaurants. Formally, the rating of an item i by a user u is denoted as $r_{u,i}$, with $r_{u,i} = 0$ if the rating is missing [14]. Taking movie recommendation as an illustrative case, consider a target user U_{target} who seeks recommendation suggestions but has only provided ratings $r_{u,set_{movie}}$ for a subset of movies set_{movie}. The objective is to predict the user's potential rating for an unseen movie f, denoted as $Pre_{U_{target},f}$.

User rating information can typically be represented as vectors. When processing such data, service providers identify the top five users most similar to U_{target} to form a nearest neighbor set, which is then used to collaboratively generate recommendation results. Collaborative filtering (CF), a core methodology in recommendation systems, frequently

employs similarity measures such as cosine similarity and Pearson correlation to quantify user similarity [15]. In this work, cosine similarity is adopted to compute the degree of similarity between users. Specifically, the cosine similarity w_{u_1,u_2} between users u_1 and u_2 is defined as follows:

$$w_{u_1,u_2} = \frac{\vec{u_1} \cdot \vec{u_2}}{\|\vec{u_1}\| \cdot \|\vec{u_2}\|} \tag{1}$$

The user rating vectors maintained by the service provider are ranked in descending order of similarity to U_{target} and the top five user vectors are taken as the nearest neighbor set NB^k for U_{target}. The online prediction result $P_{u,f}$ for the target user U_{target} on the unseen item f can then be represented as follows:

$$P_{u,f} = \frac{\sum_{v \in Nei}(w_{u,v} \times r_{v,i})}{\sum_{v \in Nei}|w_{u,v}|} \tag{2}$$

Given the dynamic nature of user interests over time, the similarity between users is inherently variable. Consequently, in user-based collaborative filtering, the nearest neighbor set NB^k for U_{target} must be recalculated for each recommendation. The service provider then delivers personalized services to U_{target} based on the updated NB^k.

4. Implementation Details of BLR-ERTS

4.1. System Overview

To ensure the reliability of data service recommendations in a distributed environment, this paper proposes a blockchain-based recommendation system framework for electricity retail transaction services, as illustrated in Figure 1. Leveraging blockchain technology, the system achieves transparent and secure electricity transactions while integrating a reputation mechanism and personalized recommendation algorithms, combined with LSH to safeguard user data privacy. The framework encompasses multiple roles and their interaction processes, aiming to optimize data security, recommendation efficiency, and transaction reliability. The key roles in the system include the following:

(1) Requesters: Typically individual or enterprise electricity consumers, requesters submit transaction demands, such as preferences for green energy, price ranges, and service expectations. They initiate service queries within the system by requesting personalized electricity recommendations. To ensure the relevance of recommendations, they provide accurate demand parameters and pay a service fee. By participating, requesters receive high-quality, privacy-preserving electricity service recommendations that align with their preferences and needs.

(2) Data Providers: These are usually distributed energy generators (e.g., solar or wind power suppliers) or traditional electricity companies that maintain historical transaction data. They supply detailed electricity product profiles and historical user data needed for recommendation generation. Data providers ensure the availability, accuracy, and timeliness of service-related information, including capacity, energy type, and reputation. In return for sharing valuable data, they receive compensation from requesters and gain enhanced exposure of their services to potential buyers.

(3) Miners: Miners act as the core infrastructure of the blockchain network, typically possessing strong computation and storage capabilities. They validate and record transactions, execute smart contracts, and maintain system security through consensus algorithms (e.g., PoW or PoS). Miners are tasked with ensuring the correctness, immutability, and transparency of recorded data. They are incentivized through transaction fees or token rewards for their role in maintaining network integrity and executing recommendation-related smart contracts.

(4) Recommendation Service Module: Utilizing LSH technology, this module matches requester demands with data provider offerings and refines recommendation outcomes by incorporating reputation scores and historical transaction behavior.

(5) Smart Contracts: Automated scripts responsible for executing transaction matching, reputation updates, and payment settlements. These contracts embed rules governing reputation management, privacy protection, and recommendation logic.

(6) Blockchain Network: A distributed ledger that records transaction data and reputation scores, ensuring transparency and immutability of all operations. Each node could locally synchronize multiple blocks, with each block containing several transactions.

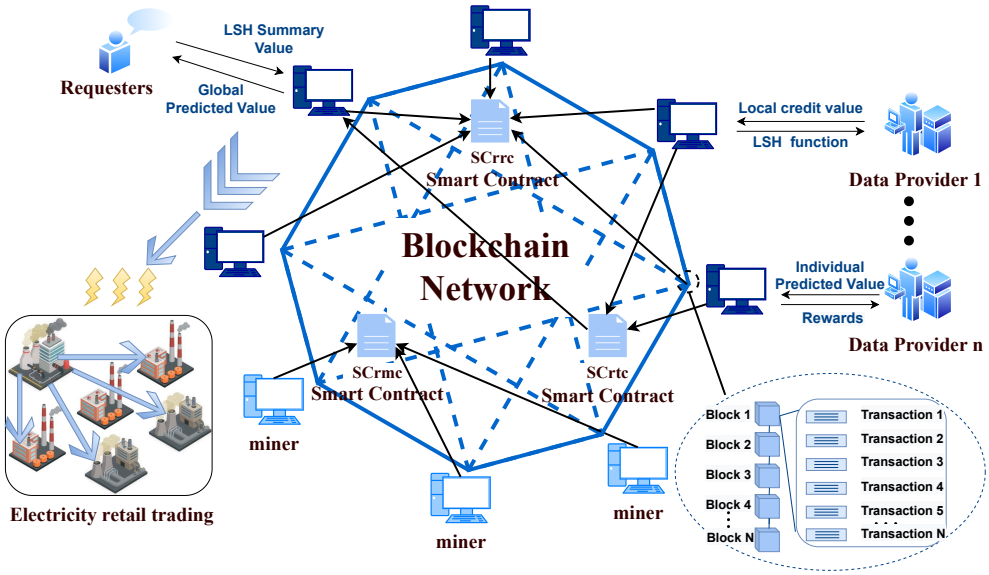


Figure 1. Overview of the blockchain-based electricity trading recommendation system.

The system workflow proceeds as follows: First, the requester submits electricity demand data (e.g., desired consumption volume, price preferences) via the client interface. The system then applies LSH hashing to the request data to generate privacy-preserving signatures. Based on these signatures, the recommendation module matches the request with data providers' offerings, and the smart contract verifies the match and identifies candidate data providers with higher reputation scores. Upon the requester's confirmation of the recommendation, the smart contract locks transaction parameters, and miner nodes verify and record the transaction on the blockchain. Finally, the smart contract executes payment settlements and updates participants' reputation scores in real-time, while the blockchain network securely records the transaction outcome.

4.2. Threat Model

In the reputation-aware electricity retail transaction service recommendation system proposed in this paper, miners are assumed to be non-malicious and trustworthy, while requesters and data providers may exhibit malicious behavior, posing threats to the recommendation system. This study therefore focuses on potential attacks from requesters and data providers, which can be categorized into three primary types:

(1) Data Manipulation by Malicious Data Providers: An attacker may provide falsified prediction values to disrupt system operation or copy prediction values from honest data providers to unfairly gain revenue—a strategy commonly referred to as the "free-rider" attack.

(2) Collusion and Inference Attacks: An attacker may collude with other data providers or requesters to infer sensitive service data from honest participants, compromising privacy and data integrity.

(3) Reputation Exploitation: Malicious data providers may manipulate predicted values to undermine the validity of recommendations. Given that data providers are incentivized by requester payments, adversaries may intentionally submit falsified predictions to maximize their own gains.

In practice, these attacks can result in privacy breaches, degradation of recommendation quality, and financial losses for honest data providers.

4.3. Workflow of BLR-ERTS

The interaction process proposed in this paper comprises five main phases: demand submission, recommendation matching, transaction signing, payment and settlement, and reputation updating, as illustrated in Figure 2. The detailed descriptions of each phase are as follows:

(1) Demand Submission Phase: The requester (either a household or an enterprise) submits its electricity demand to the system, including details such as type of electricity consumption, consumption volume, time period, and price preference. The system processes this demand data using a LSH algorithm to generate a hash signature, thereby preventing direct exposure of raw data. The generated hash signatures and associated metadata (e.g., submission time, demand ID) are subsequently recorded on the blockchain via smart contracts to ensure immutability and transparency.

(2) Recommendation Matching Phase: The system matches the requester's demand hash with the data provider's power supply information to generate a personalized recommendation list. Data providers upload their power supply information—including types of power, maximum capacity, time period, dynamic price range, and other relevant details—and generate corresponding hash signatures using LSH. The recommendation module computes the hash distances between demand and supply hashes, and integrates these distances with reputation scores to derive weighted recommendation scores. These scores are then sorted to produce a ranked recommendation list, which is returned to the requester via smart contracts.

(3) Transaction Signing Phase: Upon selection of a suitable transaction option from the recommendation list, the smart contract locks the transaction parameters and generates an electronic contract. This contract includes key details such as transaction IDs of the requester and data provider, type of electricity traded, time period, price, total cost, and performance conditions. The contract is verified by miner nodes and recorded on the blockchain to ensure openness, transparency, and immutability.

(4) Payment and Settlement Phase: Following contract execution, the smart contract automatically handles payment and settlement. Prior to settlement, the system verifies whether the data provider fulfilled contractual obligations (i.e., delivering the agreed electricity supply) and whether the requester's consumption data has been accurately uploaded via smart meters or IoT devices. If obligations are met, the smart contract deducts the agreed amount from the requester's account and transfers it to the data provider. If the power supply fails or conditions are unmet, the smart contract triggers a compensation mechanism, such as refunding payments or imposing penalties.

(5) Reputation Update Phase: Based on the transaction outcome and user evaluations, the system updates the reputation scores of both parties. Evaluation criteria for requesters include transaction timeliness and payment reliability, while criteria for data providers include performance quality, response speed, and price fairness. Updated reputation scores

are securely recorded on the blockchain via smart contracts to ensure transparency and tamper-resistance.

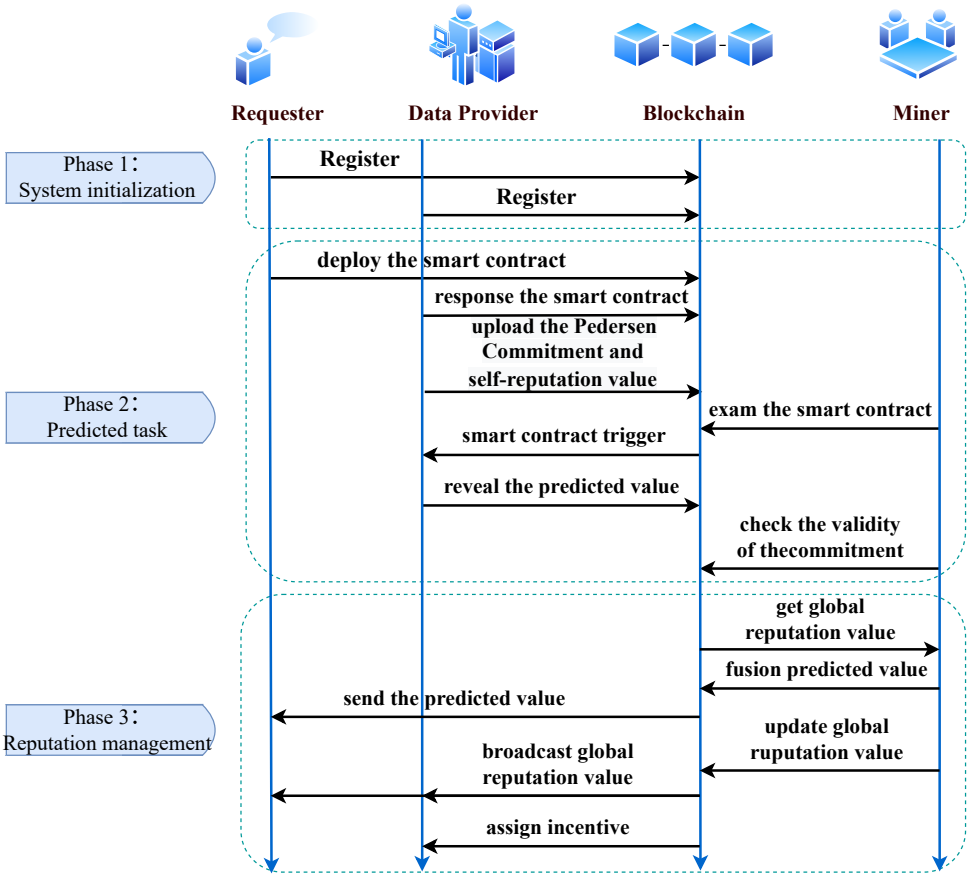


Figure 2. Workflow of BLR-ERTS system.

4.4. Design of Smart Contracts

This section presents the design of a distributed recommendation system based on blockchain, focusing on three primary types of smart contracts: role registration contracts, reputation management contracts, and recommendation task contracts.

(1) Role registration contract (SC_{rrc}): Requesters can engage with the system anonymously after registration, without disclosing real identity information. In contrast, data providers are required to register with verifiable identity credentials, certified by a trusted authority. The certification authority is responsible for issuing public–private key pairs and generating blockchain addresses derived from public key hashes. For brevity, the detailed certification process is omitted here.

(2) Reputation management contract (SC_{rmc}): This contract is primarily responsible for calculating and maintaining reputation scores of data providers. Deployed on the blockchain by miners, reputation serves as a core system parameter reflecting a data provider's historical performance in recommendation tasks. Reputation scores are initialized with default values and dynamically updated as recommendation activities progress. Notably, the reputation score directly influences the final recommendation outcomes.

(3) Recommendation task contract (SC_{rtc}): Requesters initiate recommendation requests through this smart contract. The contract governs key operations including task submission, commitment submission, commitment verification, and joint prediction. During the task submission phase, the requester must provide an LSH signature, specify the

minimum acceptable reputation threshold for potential data providers, and set a task response deadline.

When a data provider responds to SC_{rtc}, a security deposit is required. If the prediction result is valid and the commitment verification succeeds, the deposit is refunded. Conversely, if the prediction result is deemed invalid, the deposit is forfeited.

4.5. Improved Distributed LSH Recommendation Algorithm

This section introduces a distributed recommendation algorithm for electricity trading services based on LSH. The notations and their corresponding descriptions used throughout this algorithm are summarized in Table 1.

Table 1. Symbols and description.

No.	Symbols	Description
1	$H(.)$	Hash value
2	$DP_1, \cdots, DP_k$	Data provider
3	$h_1(.), \cdots, h_r(.)$	Hash function
4	$\vec{U}_1^k, \cdots, \vec{U}_m^k$	Rating vector of users
5	$\vec{u}_{q,1}^k, \cdots, \vec{u}_{q,d}^k$	User rating
6	$Table_1^k, \cdots, Table_t^k$	Data provider hash table
7	$Table_{fin}^k$	Final hash table
8	map_q^k	Hash value-user vector mapping
9	NB^k	Nearest neighbor set of service provider

It is assumed that users in the system have evaluated each electricity service assessed by active users, with each user providing only one evaluation per service.

Step 1: A generic LSH function family $H_{ij}(.)(i \in [1,t], j \in [1,r])$ is randomly selected from the blockchain. The selection of the LSH function family is based on the type of distance metric employed for user similarity calculation. Specifically, the LSH functions corresponding to the Pearson Correlation Coefficient (PCC) are utilized to construct user metrics.

According to LSH theory, the hash value $\vec{R}$ is calculated using the LSH function applied to the requester's rating vector for data provider DP_k. The computation of the LSH value $h_i(.)(i \in [1,r])$ is expressed in Equation (3), where $\vec{H}_{ij} = (ran_{ij1}, \cdots, ran_{ijd})$, and $ran_{ij}(j \in [1,d]))$ represents random numbers uniformly drawn from the interval $[-1, 1]$, with d denoting the dimensionality of the user rating vector.

$$h_{ij}(\vec{R}) = \begin{cases} 0, & \text{if } \vec{H}_{ij} \cdot \vec{R} \leq 0 \\ 1, & \text{if } \vec{H}_{ij} \cdot \vec{R} > 0 \end{cases} \tag{3}$$

The LSH value $\vec{U}_q^k$ is computed, where $H(\vec{U}_q^k) = (h_1(\vec{U}_q^k), \cdots, h_r(\vec{U}_q^k)) = \{0,1\}^r$. Here, the data provider $DP_k(k \in [1,n])$ maintains m user rating vectors $(\vec{U}_1^k, \cdots, \vec{U}_m^k)$, with each vector $\vec{U}_q^k = (\vec{u}_{q,1}^k, \cdots, \vec{U}_{q,d}^k)$ representing user q's ratings of d electricity services. Once all $\vec{U}_q^k$ vectors in DP_k are processed, a hash table is constructed, mapping each vector to its corresponding hash value. The requester rating vector is similarly processed to compute its LSH values, ordered according to $H_{ij}(.)$ in Equation (3), yielding $h_{ij}(R_r) = (\{0,1\}_1^r, \cdots, \{0,1\}_t^r)$.

Furthermore, the requester deploys a smart contract SC_{rtc} that contains its hash value $h_{ij}(R_r)$ transaction fee details, credit limits, time constraints, and quantitative requirements for data providers. The requester retrieves relevant parameters stored on the blockchain and utilizes the LSH algorithm to compute the corresponding hash buckets for its rating

vector. Upon deployment of the smart contract, the data providers can detect the requester participation and immediately respond by invoking the contract. Once the number of rating vectors satisfies a predefined threshold, the selected service provider for U_{target} and its blockchain address are notified via SC_{rtc}.

Step 2: In Step 1, the hash table is generated by DP_k. However, since LSH is a probabilistic nearest neighbor search algorithm, predictions based on a single hash function may be unstable or imprecise. To enhance stability, Step 1 is iteratively repeated until t hash tables $(Table_1^k, \cdots, Table_t^k)$ are generated. These tables are then merged into a final hash table $Table_{fin}^k$, where each hash value aggregates all rating vectors that appeared in any of the t tables, ranking in descending order of occurrence frequency. The top k vectors with the highest frequencies are selected as the nearest neighbor set corresponding to each hash value in $Table_{fin}^k$. As $Table_{fin}^k$ is maintained offline by DP_k, this approach significantly reduces computational overhead.

The fusion process is illustrated in Figure 3. Let V_{max} denote the maximum number of neutrosophic vectors and V_{act}^k denote the actual number of neutrosophic vectors in $Table_{fin}^k$, as used in this example. To satisfy the recommendation request of a specific requester, this paper introduces a local reputation value to evaluate the recommendation capability of each data provider. The local reputation value R_i^l is defined as the data provider's estimated accuracy P_i, where a higher R_i^l indicates greater confidence in its recommendation accuracy, and vice versa. Let U_i represent the historical user records stored in DP_i, $S_{request}$ denote the set of power services requested by the requester, and $S_{U_j}^i$ denote the set of services rated by user U_j in DP_i.

$$R_i^l = \frac{V_{act}^k}{V_{\max}} * \frac{\sum_{u_q^k \in NB^k} \mathrm{map}_q^k}{t * \left|NB^k\right|} \tag{4}$$

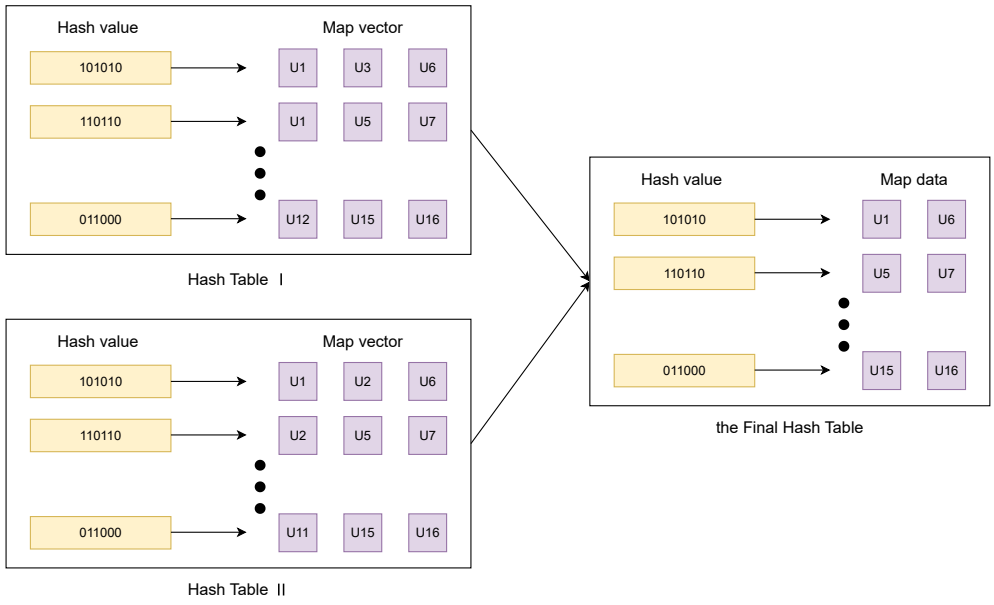


Figure 3. Hash table fusion $V_{max} = 2$.

Here, map_q^k denotes the number of times the LSH value corresponding to vector u_q^k matches the LSH value of the requester's vector. A higher frequency of successful LSH value matches indicates a greater similarity between the data provider's rating and the requester's rating, consistent with the probabilistic characteristics of the LSH algorithm. The local reputation value R_i^l and the commitment P_i are encapsulated into a transaction and recorded on SC_{rtc}.

Step 3: According to the principles of LSH, if two users share the same hash value, it is highly probable that they are similar. The hash value $H(req)$ for the requester is generated in the same manner as in Step 1. The vectors corresponding to the $H(req)$ identified from $Table^k_{fin}$ in Step 2 form the nearest neighbor set NB^k. The system employs personalized recommendation strategies within NB^k to predict the requester's rating for the service in dimension q.

$$P_i = \frac{1}{\left|NB^k\right| * \sum_{u^k_q \in NB^k} \mathrm{map}^k_q} * \sum_{u^k_q \in NB^k} \text{it. } g^k_q * \mathrm{map}^k_q \tag{5}$$

Here, map^k_q denotes the number of successful matches (not exceeding t) between the hash value of u^k_q and that of the requester. To protect the predicted value P_i (where $P < 0.05$)) against potential plagiarism by malicious data providers, this work adopts the Pedersen commitment scheme [16], a cryptographic primitive designed to ensure data confidentiality and integrity. The Pedersen commitment operates as a two-phase interaction protocol involving a committing party (the data provider) and the receiving party (the blockchain ledger).

When the trigger condition of SC_{rtc} is satisfied, such as when a predefined deadline is reached or the data provider submits a sufficient number of commitments, no additional participation requests from data providers are accepted. At this point, each data provider DP_i reveals their committed value, which is then recorded by SC_{rtc} on the blockchain.

4.6. Joint Recommendation Based on Distributed Reputation

To integrate prediction results from multiple data providers, this paper introduces a reputation aggregation algorithm based on the k-means clustering algorithm, which calculates the global reputation value by aggregating local reputation value scores. This approach enables joint recommendation, where the final recommendation result depends not only on the predicted values provided by data providers but also on their global reputations.

Step 1 (Final Predicted Value Calculation): The final predicted value P^{fin} is computed by miners on the blockchain. Specifically, a weighted average of all local predicted values P_i is calculated, where weights are determined by the local and global reputation scores of each data provider. Data providers are rewarded proportionally to their respective reputation value.

To further enhance prediction accuracy, the k-means algorithm is applied to the local prediction values P_i, and the cluster center is selected as the final prediction value P^{fin}. The prediction accuracy is then evaluated by computing the Euclidean distance between each local prediction value and the cluster center. Let P^{fin} denote the cluster center, the Euclidean distance between a local predicted value and the center is calculated as follows:

$$d_i = \mathrm{dist}^2\left(P^{fin}, P_i\right) = \left(P^{fin} - P_i\right)^2 \tag{6}$$

The target clustering center P^{fin} is defined as the point P_i that minimizes the total sum of Euclidean distances to all valid local predicted values, expressed as

$$P^{fin} = \mathrm{argmin}\, S\left(P^{fin}\right) \tag{7}$$

where the function $S(.)$ is calculated as follows:

$$S\left(P^{fin}\right) = \sum_{i=1}^{n}\left(\mathrm{dist}^2\left(P^{fin}, P_i\right) * q_i\right) \tag{8}$$

where q_i denotes the accuracy score of the predicted value provided by data provider DP_i. Higher local and global reputation values correspond to higher prediction quality. The initialization of q_i is given by $q_i := R_i$, where R_i represents the combined reputation value, comprising both the global reputation R_i^g and the local reputation R_i^l:

$$R_i = \sqrt{\frac{R_i^{l^2} + R_i^{g^2}}{2}} \tag{9}$$

The initial value of P^{fin} is obtained by taking the partial derivative of P^{fin}:

$$\sum_{i=1}^{\mathrm{n}} \left(2 * \left(P^{fin} - P_i\right) * q_i\right) = 0 \tag{10}$$

$$P_{ini}^{fin} = \frac{\sum_{\mathrm{i}=1}^{\mathrm{n}} P_i * q_i}{\sum_{\mathrm{i}=1}^{\mathrm{n}} q_i} \tag{11}$$

Based on the initial values P^{fin}, recalculate d_i and update the accuracy scores q_i:

$$q_i = \left(1 / \left(\frac{d_i}{\lambda} + \varepsilon\right)\right) / \left(\sum_{i=1}^{\mathrm{n}} \left(1 / \left(\frac{d_i}{\lambda} + \varepsilon\right)\right)\right) \tag{12}$$

where ε denotes a very small positive constant that ensures the equation remains well-defined when $d_i = 0$. The parameter λ represents the total Euclidean distance between each P_i and the cluster center P^{fin}. The computation is iteratively performed using Equations (6)–(8) and (12), updating P^{fin} until convergence. convergence is achieved when the difference between the updated $P^{fin'}$ and the previous P^{fin} is less than or equal to a threshold Δ. In this paper, Δ is set to 0.001.

Step 2 (Global Reputation Updating): Once the final predicted value has been determined, the global reputation score is updated based on the quality of the recommendation result. Specifically, if the recommendation quality is high, the reputation score is incremented by a small amount; conversely, if the prediction is inaccurate, the reputation score is significantly reduced. To model this behavior, the Gompertz function [17,18] is employed, which exhibits slow growth at both extremes and rapid growth in the middle. The Gompertz function is defined as

$$G(x) = e^{-e^{-\lambda x}} \tag{13}$$

where λ denotes the growth rate parameter, which controls the speed of reputation convergence. The updated global reputation value for DP_i is denoted as $R_i^{g'}$, and is calculated as follows:

$$R_i^{g'} = G\left(G^{-1}\left(R_i^g\right) + R_i^l \cdot q_i'\right) \tag{14}$$

where q_i' is the input parameter to the Gompertz function, determined according to the following rule:

$$q_i' = \begin{cases} (1 - q_i)\left(q_i - \frac{1}{n}\right), & \text{if } q_i \leq \frac{1}{n} \\ q_i\left(q_i - \frac{1}{n}\right), & \text{if } q_i > \frac{1}{n} \end{cases} \tag{15}$$

The global reputation value directly influences both the revenue earned by data providers and their contribution weight in subsequent prediction tasks. Miners reward data providers who generate high-quality results, with the reward amount calculated as

$$\text{Reward}_i = \begin{cases} R_i^l \cdot q_i' / \sum_{q_i'>0} R_i^l \cdot q_i', & \text{if } q_i' > 0 \\ 0, & \text{if } q_i' \leq 0 \end{cases} \tag{16}$$

5. Theoretical Analysis

To demonstrate the security advantages of the proposed scheme, this section provides an in-depth analysis of the potential attacks outlined in Section 4.2 and details the corresponding defensive measures. Each defense mechanism is grounded in established cryptographic principles and security theories.

(1) Malicious Data Providers: The threat of malicious data providers attempting to steal prediction values from others is a serious concern in collaborative recommendation systems. To counter this threat, our scheme adopts the Pedersen commitment scheme, a well-established cryptographic method that ensures that each data provider submits their prediction values and local reputation scores independently. This commitment prevents providers from altering their data after submission, enhancing accountability. Furthermore, we introduce a reputation management mechanism, based on a weighted average approach, which identifies inaccurate predictions by monitoring the deviation of predictions from the consensus. If discrepancies are found, the reputation of the malicious provider is penalized, reducing their influence on the final prediction results. This approach is backed by reputation-based security theories, which suggest that decentralized trust can mitigate the impact of malicious nodes by isolating their influence on the system. These defense mechanisms effectively mitigate or eliminate the impact of malicious data providers.

(2) Privacy Leakage: Privacy preservation is one of the critical components in a decentralized system, particularly when dealing with sensitive user data. To ensure the protection of user privacy, all computations involving sensitive user data are performed locally on the user's device, and no raw data is ever transmitted. The LSH algorithm, which has been proven to work well for privacy-preserving applications, is employed to desensitize the user's data before publishing it on the blockchain. The hashes of the data and the prediction values are the only information that is shared, rendering it computationally infeasible for adversaries to reverse-engineer the original data. The security of LSH in preserving privacy is supported by cryptographic theory, which asserts that with the proper choice of hash functions, LSH can ensure that data is obfuscated in such a way that only approximate similarities can be computed without revealing sensitive information. This method guarantees the computational infeasibility of reconstructing the original data, thus ensuring user privacy.

(3) Sybil Attacks: Sybil attacks, where attackers create multiple fake identities to manipulate the system, are a significant threat to decentralized networks. To mitigate this, we introduce a security deposit mechanism that requires all data providers responding to smart contracts deployed by the requester to make a financial commitment. If a data provider fails to validate their prediction during the reveal phase, they forfeit their security deposit. This mechanism is based on game theory, where the cost of failure (i.e., losing the deposit) outweighs the potential gain from attacking the system. The economic deterrent imposed by the security deposit significantly reduces the incentives for Sybil attackers. This mechanism is akin to Proof-of-Stake principles, where stakeholders are incentivized to act honestly to avoid losing their investment. The combination of financial cost and reputational penalties effectively combats Sybil attacks in the proposed framework.

6. Performance Evaluation

This section presents the implementation details and performance evaluation of the proposed BLR-ERTS system. The effectiveness of the system is closely linked to the underlying device configuration. As illustrated in Figure 4, the BLR-ERTS was tested on eight devices, including Raspberry Pi 4 Model B (Raspberry Pi Foundation, Cambridge, UK), which primarily served for consensus processing. To comprehensively evaluate system performance, up to 100 independent nodes were deployed using server-based virtual machines (VMs). In this configuration, each Raspberry Pi node and VM node was interconnected with other nodes to facilitate retail electricity transactions.

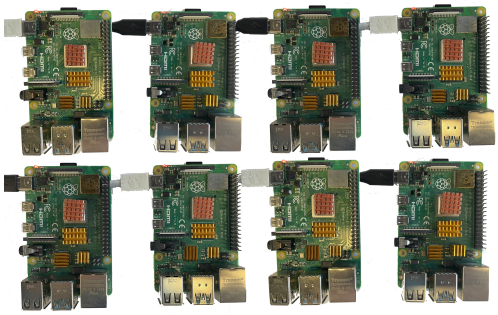


Figure 4. Testbed setup (Raspberry Pi 4 Model B).

6.1. Dataset

Firstly, we prepared the data for building our proposed model. Apart from traditional data processing techniques, we also applied the data partitioning approach to split the data into training and testing energy consumption datasets. We used an 8:2 train–test split and averaged results over multiple runs to ensure evaluation stability, without applying k-fold cross-validation: 80% of the energy consumption data is used for training, and 20% data is used for testing purposes. This paper utilizes the Electricity Market Dataset, which comprises over 500,000 transaction records, detailing user consumption patterns, pricing models, energy types (e.g., renewable, non-renewable), and tariff structures (e.g., peak, off-peak rates). This dataset provides a comprehensive collection of electricity market data, focusing on long-term forecasting and strategic planning in the energy sector. The data is derived from real-world electricity market records and policy reports from Germany, specifically the Frankfurt region, a major European energy hub. It includes hourly observations spanning from 1 January 2018 to 31 December 2024, covering key economic, environmental, and operational factors that influence electricity market dynamics.

6.2. Experimental Environment Setting

The experimental environment consisted of a workstation running Windows 10, equipped with a 12th Gen Intel Core i7-12700 processor, NVIDIA GeForce RTX 3050 (8 GB) graphics card, and 128 GB RAM (3200 MT/s). The software environment included Spyder 4.1.5 Python IDE and Flask 0.12.2 on Anaconda Navigator, while the blockchain network was implemented using Python 3.12.7.

6.3. Comparison Baselines

To comprehensively evaluate the performance of the proposed blockchain- and reputation-based service recommendation system in electricity retail transaction scenarios, two representative baseline recommendation systems are selected for comparison: the traditional collaborative filtering recommendation system (CF-ERTS) [7] and the blockchain-based collaborative filtering recommendation system (BCF-ERTS) [8]. These two schemes are widely adopted and theoretically mature in the recommendation domain, providing

a comprehensive baseline for comparison from multiple perspectives. By contrasting the proposed system with these baselines, we demonstrate its unique advantages in terms of recommendation accuracy, privacy protection, system performance, and reputation management, thereby verifying its effectiveness and feasibility in electricity retail transactions.

Additionally, to assess the effectiveness of the proposed reputation-aware lightweight consensus mechanism, several representative consensus mechanisms are selected for comparison, including Practical Byzantine Fault Tolerance (PBFT) [18], Proof of Stake (PoS) [19], Proof of Authority (PoA) [20,21], and reputation-based consensus mechanisms [22–24].

(1) PBFT: Yao et al. [18] proposed an efficient and secure PBFT consensus algorithm designed to handle large-scale microgrid electricity transactions. PBFT offers high fault tolerance and reliability, making it suitable for electricity retail scenarios that require secure and dependable transactions.

(2) PoS: Yang et al. [19] presented a peer-to-peer energy trading scheme based on PoS, where miners compensate for power loss by sacrificing part of their equity and reducing price disparities in traditional producer-to-grid transactions. PoS is widely adopted for its rapid transaction confirmation and low energy consumption.

(3) PoA: Traditional centralized databases are prone to data tampering. Grigoryan et al. and Khan et al. [20,21] proposed a PoA-based blockchain electricity retail transaction scheme to address these issues. By leveraging blockchain to store data and using PoA consensus for verification, this scheme achieves faster transaction processing and higher trustworthiness, aligning well with electricity retail scenarios.

(4) Reputation-based Consensus Mechanism: Zhang et al. [22] proposed the STEM system, integrating multiple rounds of double auctions and energy transmission algorithms with a reputation mechanism to enhance robustness and defend against malicious attacks. Zhao et al. [23] introduced the DPoR mechanism, a reputation-based distributed energy trading method designed to address inefficiencies and scalability limitations in existing blockchain systems. Lv et al. [24] developed the RMCT model, a real-time peer-to-peer electricity transaction framework incorporating user behavior-based reputation management, effectively mitigating malicious activities and improving transaction compliance. The RMCT's feasibility and innovation have been validated through extensive experimental results and comparative analysis.

6.4. Evaluation Metrics

In this section, we evaluate the performance of the energy consumption prediction models in terms of a regression performance measure, such as (1) Mean Absolute Error (MAE), (2) Mean Square Error (MSE), and (3) Root Mean Square Error (RMSE) [1]. First, we explain these measures in detail.

(1) **Mean Absolute Error** is used for evaluating the performance of the regression model, and determines the deviation among the actual and predicted values. The formulation of MAE is given as follows:

$$MAE = \frac{1}{n}\sum_{i=1}^{n}|P_{u,i} - r_{u,i}| \tag{17}$$

(2) **Mean Square Error** is used for eliminating the below zero values and determining the average among the predicted and the actual values. The formulation of MSE is given as follows:

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(P_{u,i} - r_{u,i})^2 \tag{18}$$

(3) **Root Mean Square Error** is used for the regression model, and determines the deviation among the actual and predicted values. The formulation of Mean Absolute Error is given as follows:

$$RMSE = \sqrt{\frac{1}{n}\sum_{i=1}^{n}|(P_{u,i} - r_{u,i})|^2} \tag{19}$$

where $P_{u,i}$ denotes the predicted rating of service i by user u and $r_{u,i}$ represents the corresponding actual rating.

In the experimental setup, we simulate transaction recommendations across 50 data providers and equally distribute the dataset among honest data providers. For each experiment evaluating metric, 10 independent trials are conducted, and the average value is reported as the final result. The experimental parameters are configured as follows: $t = 10$, $r = 10$, and all initial values of R_i^g are set to 0.5.

To compare the performance of the proposed BLR-ERTS system with state-of-the-art (SoTA) consensus mechanisms, the following evaluation metrics are used: CPU workload (W_{CPU}), network bandwidth usage ($U_{Bandwidth}$), energy consumption (C_{Energy}), and number of pending transactions per block ($T_{pending}$).

Referencing [25], a multidimensional efficiency evaluation formula is introduced to comprehensively assess the efficiency of blockchain consensus mechanisms in electricity retail transaction scenarios. This formula captures the subtle performance differences among various mechanisms and is expressed as

$$\text{Efficiency } = \alpha \cdot W_{CPU} + \beta \cdot U_{Bandwidth} + \gamma \cdot C_{Energy} + \delta \cdot T_{Pending} \tag{20}$$

In this context, the CPU index (α), bandwidth index (β), energy index (γ), and pending transaction index (δ) represent key parameters encapsulating the respective dimensions of performance. The terms W_{CPU}, $U_{Bandwidth}$, C_{Energy}, and $T_{Pending}$ denote the normalized values of CPU workload, network bandwidth usage, energy consumption, and the number of pending transactions per block, respectively. Determining these coefficients is essential for quantifying the overall efficiency of blockchain consensus mechanisms in electricity retail transaction scenarios.

To further evaluate the execution efficiency of consensus mechanisms, we evaluate the number of pending transactions per block. This metric reflects the volume of unconfirmed transactions awaiting inclusion in the next block and is a critical indicator of processing efficiency across nodes, particularly within dynamic electricity retail trading environments.

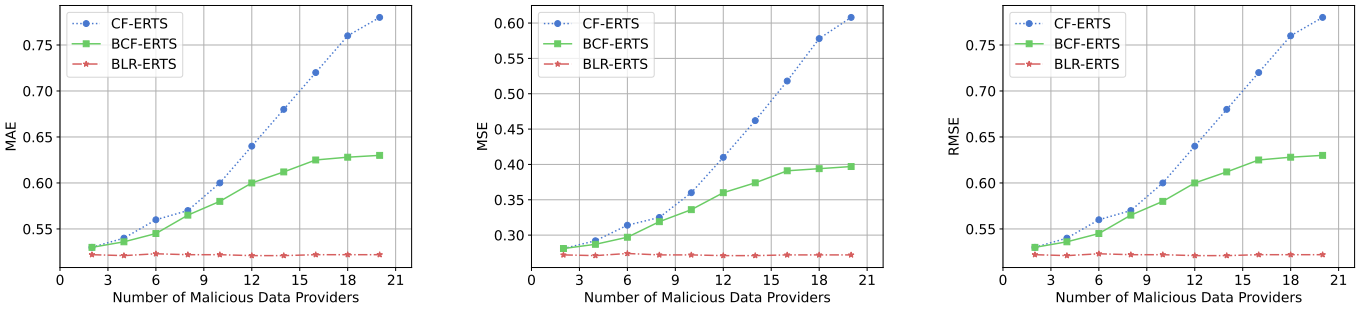
6.5. Experimental Results and Analysis

6.5.1. Performance Analysis of Recommendation Systems

The performance of different recommendation systems in the presence of malicious nodes was analyzed experimentally. The experimental results, illustrated in Figure 5, show that as the number of malicious nodes increases, the MAE, MSE, and RMSE values of all three recommendation systems exhibit an upward trend. However, there is a considerable performance difference between the systems.

Specifically, the proposed BLR-ERTS system consistently exhibits lower MAE, MSE, and RMSE values throughout the experiment, indicating a clear advantage in recommendation accuracy. In comparison, the BCF-ERTS [8] system shows slightly higher MAE, MSE, and RMSE values than BLR-ERTS but outperforms the traditional collaborative filtering system CF-ERTS [7]. Notably, the MAE, MSE, and RMSE values of CF-ERTS [7] increase sharply with the number of malicious nodes, highlighting its vulnerability to malicious data. Both BCF-ERTS [8] and BLR-ERTS leverage blockchain technology; however, BLR-ERTS incorporates a lightweight consensus mechanism and an enhanced LSH algorithm. These

features enable BLR-ERTS to more effectively identify and filter malicious nodes, thereby maintaining lower MAE, MSE, and RMSE values even in adversarial scenarios. Furthermore, the improved LSH facilitates efficient similarity searches without compromising user privacy, not only enhancing recommendation accuracy but also preventing malicious nodes from tampering with or misusing user data. This dual protection mechanism contributes to the further reduction of MAE, MSE, and RMSE values in BLR-ERTS.



(**a**) Comparison of MAE. (**b**) Comparison of MSE. (**c**) Comparison of RMSE.

Figure 5. Accuracy of recommendations when malicious data.

6.5.2. Performance Analysis of Lightweight Consensus Mechanisms

In this section, the performance of various consensus mechanisms is compared to evaluate their suitability in a blockchain-based electricity retail transaction recommendation system. The experiments are conducted in two groups: Group 1 includes PBFT [18], PoS [19], PoA [20,21], and the proposed BLR-ERTS; Group 2 consists of reputation-based consensus mechanisms, including STEM [22], DPoR [23], RMCT [24], and the proposed BLR-ERTS. The experimental results for all schemes are summarized in Table 2.

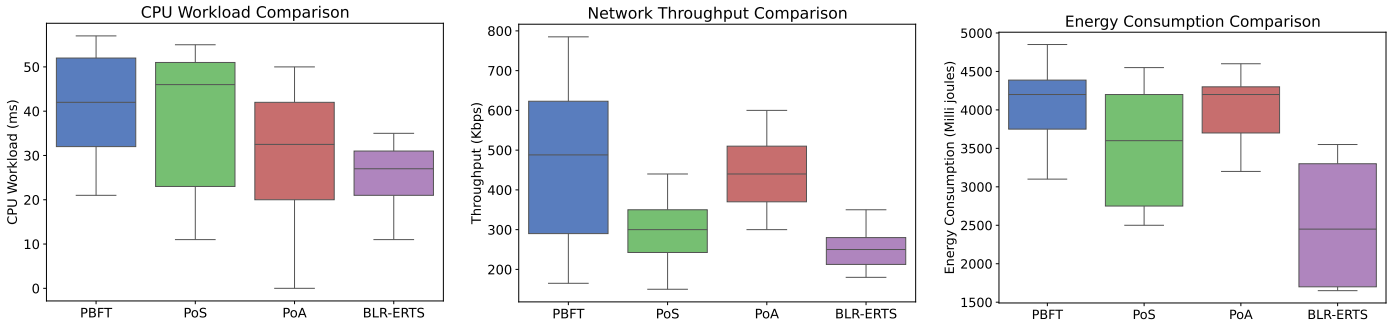
Table 2. Performance comparisons of BLR-ERTS with state-of-the-art schemes (all data are arithmetic means, '↑' indicates an increase, '↓' indicates a decrease).

Schemes	CPU Workload (ms)	Bandwidth Usage (Kbps)	Energy Consumption (Milli Joules)	Variation Range of CPU Workload	Variation Range of Bandwidth Usage	Variation Range of Energy Consumption
PBFT [18]	41.0	490	4230	34.15% ↓	48.98% ↓	41.37% ↓
PoS [19]	36.0	300	3600	25.00% ↓	16.67% ↓	31.11% ↓
PoA [20,21]	33.0	440	4200	18.18% ↓	43.18% ↓	40.95% ↓
STEM [22]	35.5	275	3230	23.94% ↓	9.09% ↓	23.22% ↓
DPoR [23]	33.0	297	2680	18.18% ↓	15.82% ↓	7.46% ↓
RMCT [24]	**26.0**	253	3870	3.85% ↑	1.19% ↓	35.92% ↓
This work	27.0	**250**	**2480**	n.a.	n.a.	n.a.

CPU Workload Comparison: As shown in Figures 6a and 7a, consensus mechanisms that scale more efficiently can accommodate increasing network participants by reducing CPU workload. This scalability allows the network to process more transactions and support additional users without sacrificing performance. Specifically, BLR-ERTS achieves a reduction in CPU workload by 34.15%, 25%, 18.18%, 23.94%, and 18.18% compared to PBFT [18], PoS [19], PoA [20,21], STEM [22], and DPoR [23], respectively. However, due to the introduction of the enhanced LSH and global reputation update algorithm, BLR-ERTS exhibits a 3.85% increase in CPU workload compared to RMCT [24].

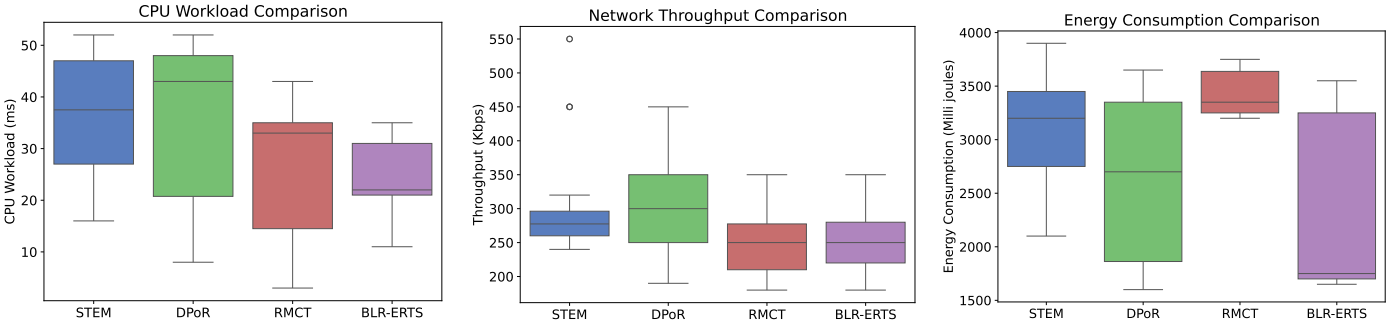
Network Bandwidth Usage Comparison: Reducing bandwidth usage is critical for minimizing latency in communication between nodes, thereby improving responsiveness and reducing operational costs. BLR-ERTS utilizes lower bandwidth by leveraging compact message sizes optimized for retail electricity transactions. As shown in Figures 6b and 7b,

BLR-ERTS achieves a reduction of 48.98%, 16.67%, 43.18%, 9.09%, 15.82%, and 1.19% compared to PBFT, PoS, PoA, STEM, DPoR, and RMCT.



(**a**) Comparison of CPU workload. (**b**) Comparison of network throughput. (**c**) Comparison of energy consumption.

Figure 6. Performance benchmarking: BLR-ERTS vs. traditional SoTA schemes.



(**a**) Comparison of CPU workload. (**b**) Comparison of network throughput. (**c**) Comparison of energy consumption.

Figure 7. Performance benchmarking: BLR-ERTS vs. reputation-based SoTA schemes.

Energy Consumption Comparison: Lower energy consumption enhances consensus efficiency by reducing operational costs and resource usage. BLR-ERTS introduces a reputation mechanism, allowing only nodes with global reputation scores above a certain threshold to participate in consensus, thereby reducing energy consumption. As shown in Figures 6c and 7c, BLR-ERTS achieves energy saving of 41.37%, 31.11%, 40.95%, 23.22%, 7.46%, and 35.92% relative to PBFT, PoS, PoA, STEM, DPoR, and RMCT, respectively.

Pending Transactions Comparison: The efficiency of pending transactions per block was evaluated across various consensus mechanisms, as shown in Figures 8 and 9. PBFT demonstrated the least efficiency, averaging 75 pending transactions per block. PoS followed with 46 pending transactions, while PoA showed 35. STEM and DPoR exhibited similar performance with 35 and 38 pending transactions per block, respectively. RMCT performed better with an average of 28 pending transactions per block. Notably, BLR-ERTS achieved the best performance, maintaining only 11 pending transactions per block. This result highlights BLR-ERTS's superior processing efficiency and suitability for dynamic, real-time electricity retail transactions.

Overall Efficiency: To quantitatively assess the efficiency of each consensus mechanism, we adopt a multidimensional efficiency formula incorporating CPU workload α, bandwidth usage β, energy consumption γ, and pending transactions δ. Based on [25], the coefficients are set as $\alpha = 0.3$, $\beta = 0.2$, $\gamma = 0.3$, and $\delta = 0.2$. Using these weights, as shown in Table 3, we calculate the overall efficiency for each consensus mechanism. Furthermore, Figures 10 and 11 depict the system's performance with adjusted CPU workload and energy consumption to optimize efficiency.

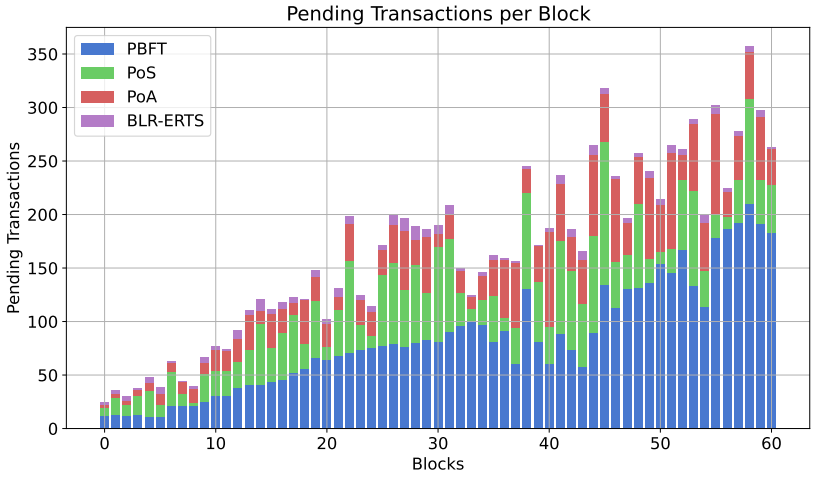


Figure 8. Pending transactions per block (BLR-ERTS vs. traditional SoTA schemes).

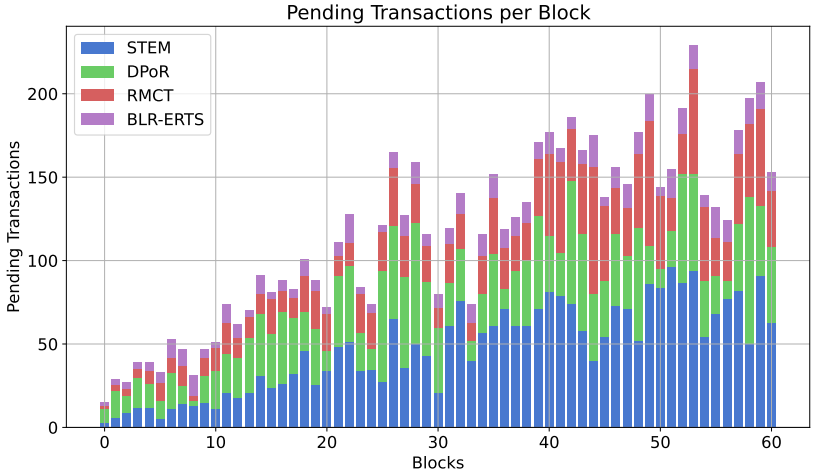
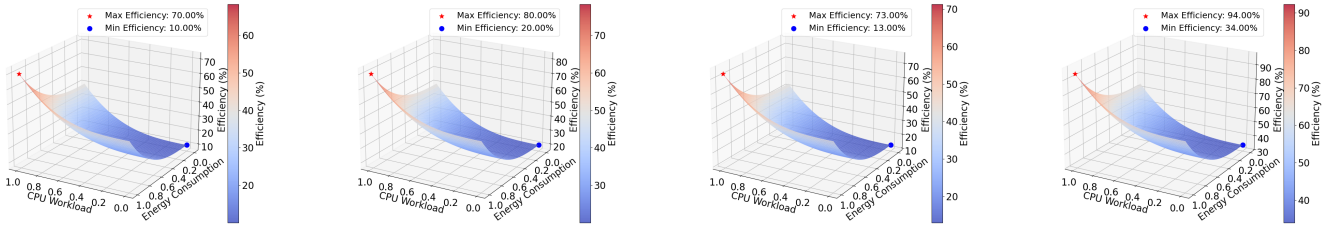
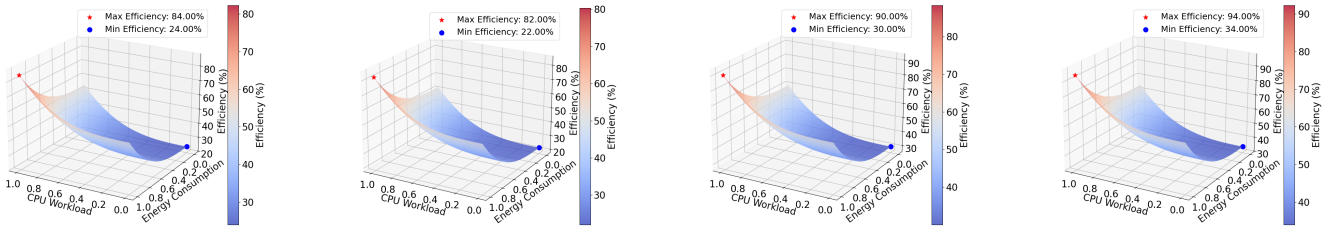


Figure 9. Pending transactions per block (BLR-ERTS vs. reputation-based SoTA schemes).



(**a**) PBFT (**b**) PoS (**c**) PoA (**d**) BLR-ERTS

Figure 10. Efficiency values (BLR-ERTS vs. traditional SoTA schemes).



(**a**) STEM (**b**) DPoR (**c**) RMCT (**d**) BLR-ERTS

Figure 11. Efficiency values (BLR-ERTS vs. reputation-based SoTA schemes).

Table 3. Efficiency comparisons of BLR-ERTS with state-of-the-art schemes.

Schemes	α	β	γ	δ	Efficiency
PBFT [18]	0.3	0.2	0.3	0.2	70%
PoS [19]	0.3	0.2	0.3	0.2	80%
PoA [20,21]	0.3	0.2	0.3	0.2	73%
STEM [22]	0.3	0.2	0.3	0.2	84%
DPoR [23]	0.3	0.2	0.3	0.2	82%
RMCT [24]	0.3	0.2	0.3	0.2	90%
This work	0.3	0.2	0.3	0.2	**94%**

6.5.3. Ablation Experimental Results and Analysis

As shown in Figure 12, the evolution of node reputation values during the transaction process is illustrated. Each line represents a node, and the changes in its reputation reflect its behavior in participating in consensus and transaction validation. The x-axis denotes the transaction rounds, while the y-axis shows the corresponding reputation scores. To clearly depict the changes in global reputation, experimental data with five data providers are considered, with one data provider (DP_5) replaced by a malicious node. The malicious data provider supplies the system with randomly generated predictions P_{mal} uniformly distributed within [0, 5]. As shown in Figure 13, the global reputation value of the malicious data provider converges towards zero after the sixth prediction, indicating rapid convergence of the system. The low global reputation value effectively minimizes the influence of the malicious data provider's predictions on the final recommendation outcomes.

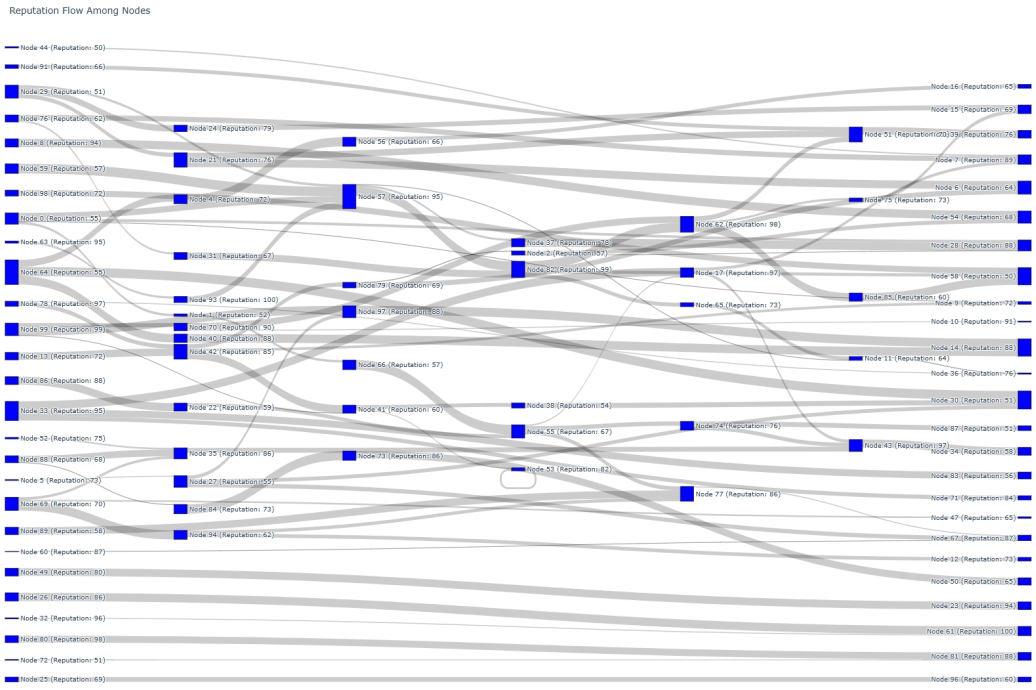


Figure 12. Change curve of node reputation with the progress of transactions. The horizontal layout reflects transaction progression, and the vertical variation shows reputation changes.

Despite the high error associated with the randomly generated predictions resulting in higher MAE for DP_5, the overall prediction error (P_{fin}) depends predominantly on the accuracy of predictions from other honest data providers, as shown in Figure 14.

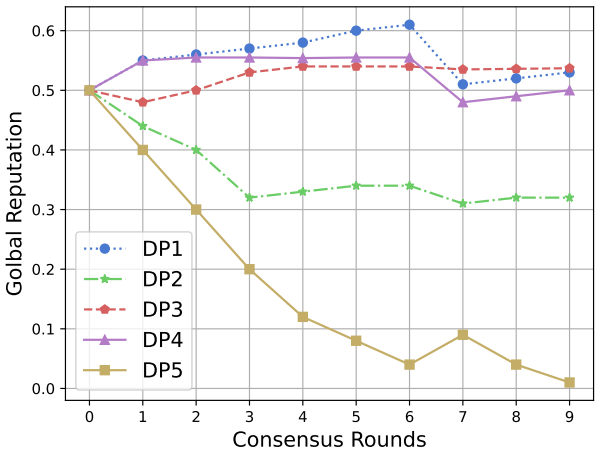


Figure 13. Global reputation value changes.

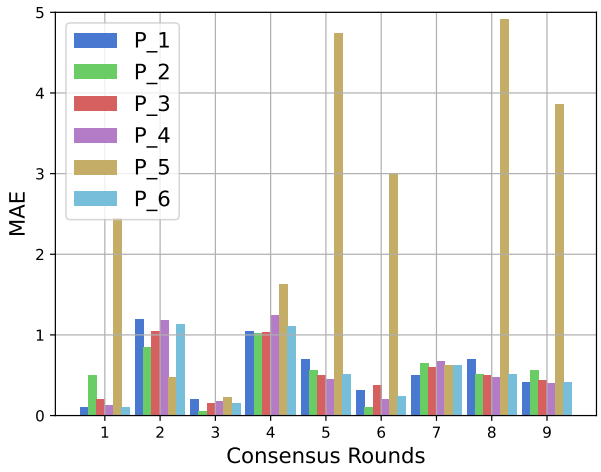


Figure 14. MAE of the five data provider predicted values and the final predicted values.

Furthermore, the user-supplied dataset was distributed among all honest data providers, comprising 30 honest nodes and 20 malicious nodes, with each provider receiving ratings from approximately 201 users. The parameters of the LSH function (r and t) play a critical role in determining the nearest neighbor set, directly influencing recommendation accuracy. Experiments were conducted to evaluate the effect of varying r from 6 to 12 and t from 6 to 12 on accuracy, with initial global reputation values set to 0.5, $\lambda = 10$, and $\varepsilon = 0.01$. The results are summarized in Figure 15.

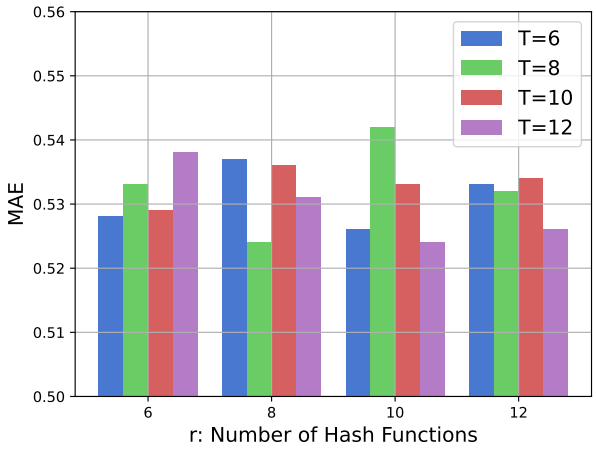


Figure 15. Impact of r and t on recommendation accuracy.

Subsequently, the variation in the average size of the nearest neighbor set with respect to r and t was examined. Experimental parameters were set to 6 to 12 for r and 6 to 12 for t. As shown in Figure 16, the size of the nearest neighbor set increases with larger r, as higher r values imply stricter selection criteria. For a fixed r, increasing t results in more nearest neighbors, as a larger t introduces more hash tables, thereby capturing more users with at least one hash match.

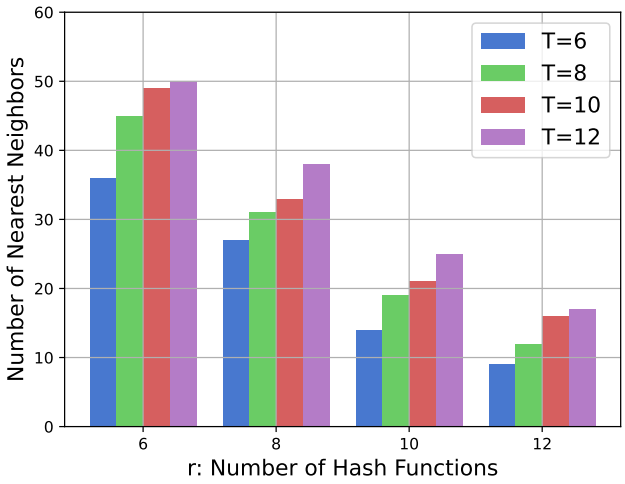


Figure 16. Impact of r and t on selected nearest neighbors.

To evaluate the impact of LSH parameters on privacy protection and the system's resilience to complex attacks, we conducted experiments varying the number of hash tables (L) and hash functions (k). The results in Table 4 indicate that increasing L and k enhances privacy by reducing the similarity between users in the same hash bucket, thereby decreasing the attack success rate. However, this improvement comes with increased computational overhead. These findings underscore the importance of optimizing LSH parameters to balance privacy protection and system performance.

Table 4. Impact of LSH parameters on privacy protection.

Number of Hash Tables (L)	Number of Hash Functions (k)	Privacy Metric (Lower Is Better)	Attack Success Rate (%)
1	10	0.85	75%
3	15	0.70	60%
5	20	0.60	50%
7	25	0.55	40%
10	30	0.50	30%

Finally, to disclose the execution time and gas consumption of key smart contract operations, we deployed three smart contracts—role registration contract, reputation management contract, and recommendation task contract—in the Ethereum testnet. By invoking the functions of each contract, we measured the execution time and gas usage during typical interactions. Based on the experimental results in Table 5, we observed a clear performance distinction between the different smart contract operations. Specifically, the role registration contract's *registerRole* function exhibited an average execution time of 120 ms and consumed 40,000 gas, while the *getRole* function executed in 60 ms and consumed 20,000 gas. The reputation management contract's *updateReputation* function took 140 ms to execute and consumed 45,000 gas, with the *getReputation* function taking 70 ms and consuming 18,000 gas. Lastly, the recommendation task contract's *assignRecommendation*

function showed a slightly higher execution time of 160 ms and gas usage of 50,000, while *getRecommendation* required 75 ms and 22,000 gas.

Table 5. Execution time and gas usage of proposed smart contracts.

Smart Contract	Key Operations	Execution Time (ms)	Gas Usage (Gas Units)
Role Registration Contract	*registerRole*	120	40,000
	getRole	60	20,000
Reputation Management Contract	*updateReputation*	140	45,000
	getReputation	70	18,000
Recommendation Task Contract	*assignRecommendation*	160	50,000
	getRecommendation	75	22,000

These results reflect the trade-off between computational efficiency and the functionality provided by each contract; while all operations exhibit relatively low execution times and reasonable gas consumption, the *assignRecommendation* function in the recommendation task contract showed the highest cost in both time and gas, which may be attributed to the complexity of the data processing involved. These measurements are critical for understanding the practical limitations of deploying such smart contracts on the blockchain, especially in a production environment with high transaction volumes.

7. Discussion

Privacy Protection Enhancement: Although LSH is introduced to safeguard data privacy, LSH along does not offer absolute security. Attackers may infer user data by analyzing the distribution and frequency of hash values, particularly when certain services or user groups exhibit distinctive patterns. Moreover, in scenarios with a large number of malicious nodes, coordinated analysis of hash information may increase the risk of privacy leakage. To further strengthen privacy protection, additional privacy-preserving techniques such as homomorphic encryption and zero-knowledge proofs could be integrated with LSH. However, achieving an optimal balance between enhanced privacy and system performance remains an open challenge.

System Performance and Scalability Limitations: While the incorporation of a lightweight consensus mechanism enhances system performance, practical deployments may encounter scalability bottlenecks as the volume of electricity retail transactions and the number of users increase. Specifically, under high concurrency, the consensus mechanism may face issues such as elevated transaction latency and reduced throughput. To address these challenges, further optimization of the consensus algorithm, including streamlined communication protocols, reduction in redundant message exchanges, and minimization of computational overhead, could be pursued. Additionally, adopting advanced distributed storage solutions (e.g., sharding, data compression) can alleviate storage burdens on nodes and enhance system scalability.

Data Quality and Accuracy Challenges: Despite the system's data processing and screening mechanisms, challenges associated with data quality and accuracy persist, particularly given the complexity and heterogeneity of electricity retail trading data. User-provided data may contain inaccuracies, incompleteness, or outdated information, adversely impacting the system's recommendation performance and reliability. To mitigate these issues, a robust data validation and cleaning framework should be established to verify and cross-check user-submitted data. Moreover, data fusion techniques can be

employed to integrate information from multiple sources, enhancing data reliability and accuracy through mutual verification and complementation.

Diversity and Dynamics of User Demand: The highly diverse and dynamic nature of user demand in the retail electricity market presents additional challenges. Users' preferences and requirements for electricity services vary with time, location, and context; while the recommendation system provides personalized recommendations based on historical data, capturing and adapting to rapid shifts in user demand remains difficult. To better address these dynamics, the recommendation algorithm could incorporate real-time data processing and adaptive learning mechanisms, enabling the system to perceive evolving user needs and adjust recommendation strategies promptly based on the latest behavioral data and feedback. This would result in more accurate and personalized recommendation services.

8. Conclusions and Future Direction

With the continuous growth of energy demand and the optimization of energy structure, electricity retail transactions are rapidly evolving. Ensuring users' acceptance of transaction service recommendations while safeguarding data privacy has become increasingly challenging. To address this, this paper proposes a blockchain-based, lightweight, reputation-aware electricity retail transaction service recommendation system. By introducing an LSH-based recommendation method, the system effectively enhances user privacy security. Furthermore, the proposed reputation management mechanism enables the detection and prevention of malicious data providers, thereby ensuring the quality and credibility of recommendations. Extensive experiments conducted on public datasets demonstrate that the proposed method outperforms existing benchmark approaches in terms of recommendation accuracy, system performance, consensus efficiency, and lightweight implementation. This research offers practical implications for electricity service providers and consumers aiming to enhance trust and personalization in decentralized markets. It also provides methodological insights for scholars and engineers working on privacy-aware recommendation systems and blockchain-based service infrastructures. Future research will focus on exploring more efficient lightweight blockchain consensus mechanisms to further enhance system performance. Additionally, plans are in place to apply the proposed approach to more diverse datasets to improve its generalization capability.

Author Contributions: Conceptualization, P.M. and K.L.; methodology, P.M., Y.Y. and J.X.; software, Y.W.; validation, P.M., K.L. and Y.Y.; formal analysis, Y.Y.; investigation, K.L.; resources, P.M.; data curation, P.M.; writing—original draft preparation, P.M. and J.X.; writing—review and editing, K.L., Y.Y. and J.X.; visualization, K.L.; supervision, Y.W.; project administration, P.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study. Written informed consent was obtained from the patient(s) to publish this paper.

Data Availability Statement: The original data presented in the study is openly available in UCI Machine Learning Repository at https://www.kaggle.com/datasets/datasetengineer/electricity-market-dataset, accessed on 26 June 2025.

Conflicts of Interest: Authors Pingyan Mo, Kai Li, Yongjiao Yang and You Wen were employed by the company Information Centre of Guangdong Power Grid Co., Ltd. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

Abbreviations

The following abbreviations are used in this manuscript:

LSH	Locality-Sensitive Hashing
P2P	Peer-to-peer
ABE	Attribute-based encryption
CP-ABE	Ciphertext-policy attribute-based encryption
IPFS	Interplanetary File System
VPP	Virtual Power Plant
CF	Collaborative filtering
PoW	Proof of Work
PoS	Proof of Stake
PBFT	Practical Byzantine Fault Tolerance
PoA	Proof of Authority
SC	Smart contract
PCC	Pearson Correlation Coefficient
VMs	Virtual machines
BLR-ERTS	Blockchain-based lightweight reputation-aware electricity retail trading service
CF-ERTS	Collaborative filtering recommendation system
BCF-ERTS	Blockchain-based collaborative filtering recommendation system
MAE	Mean Absolute Error
MSE	Mean Square Error
RMSE	Root Mean Square Error
SoTA	State-of-the-art

References

1. Gao, T.; Duan, L.; Feng, L.; Ni, W.; Sheng, Q.Z. A novel blockchain-based responsible recommendation system for service process creation and recommendation. *ACM Trans. Intell. Syst. Technol.* **2024**, *15*, 1–24. [CrossRef]
2. Albshaier, L.; Almarri, S.; Hafizur Rahman, M. A review of blockchain's role in E-Commerce transactions: Open challenges, and future research directions. *Computers* **2024**, *13*, 27. [CrossRef]
3. Asthana, S.; Im, J.; Chen, Z.; Banovic, N. "I know even if you do not tell me": Understanding Users' Privacy Preferences Regarding AI-based Inferences of Sensitive Information for Personalization. In Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems, Honolulu, HI, USA, 11–16 May 2024; pp. 1–21.
4. Wang, B.; Xu, L.; Wang, J. A privacy-preserving trading strategy for blockchain-based P2P electricity transactions. *Appl. Energy* **2023**, *335*, 120664. [CrossRef]
5. Yang, W.; Guan, Z.; Wu, L.; Du, X.; Lv, Z.; Guizani, M. Autonomous and privacy-preserving energy trading based on redactable blockchain in smart grid. In Proceedings of the GLOBECOM 2020-2020 IEEE Global Communications Conference, Taipei, Taiwan, 7–11 December 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1–6.
6. Li, Y.; Hu, B. A consortium blockchain-enabled secure and privacy-preserving optimized charging and discharging trading scheme for electric vehicles. *IEEE Trans. Ind. Informatics* **2020**, *17*, 1968–1977. [CrossRef]
7. Zhang, Y.; Meng, K.; Kong, W.; Dong, Z.Y. Collaborative filtering-based electricity plan recommender system. *IEEE Trans. Ind. Informatics* **2018**, *15*, 1393–1404. [CrossRef]
8. Casino, F.; Patsakis, C. An efficient blockchain-based privacy-preserving collaborative filtering architecture. *IEEE Trans. Eng. Manag.* **2019**, *67*, 1501–1513. [CrossRef]
9. He, Y.; Wang, M.; Yu, J.; He, Q.; Sun, H.; Su, F. Research on the hybrid recommendation method of retail electricity price package based on power user characteristics and multi-attribute utility in China. *Energies* **2020**, *13*, 2693. [CrossRef]
10. Hassan, M.U.; Rehmani, M.H.; Chen, J. Vpt: Privacy preserving energy trading and block mining mechanism for blockchain based virtual power plants. *arXiv* **2021**, arXiv:2102.01480.
11. Gaybullaev, T.; Kwon, H.Y.; Kim, T.; Lee, M.K. Efficient and privacy-preserving energy trading on blockchain using dual binary encoding for inner product encryption. *Sensors* **2021**, *21*, 2024. [CrossRef] [PubMed]
12. Baza, M.; Sherif, A.; Mahmoud, M.M.; Bakiras, S.; Alasmary, W.; Abdallah, M.; Lin, X. Privacy-preserving blockchain-based energy trading schemes for electric vehicles. *IEEE Trans. Veh. Technol.* **2021**, *70*, 9369–9384. [CrossRef]
13. Yan, C.; Cui, X.; Qi, L.; Xu, X.; Zhang, X. Privacy-aware data publishing and integration for collaborative service recommendation. *IEEE Access* **2018**, *6*, 43021–43028. [CrossRef]

14. Li, D.; Lv, Q.; Shang, L.; Gu, N. Efficient privacy-preserving content recommendation for online social communities. *Neurocomputing* **2017**, *219*, 440–454. [CrossRef]
15. Cacheda, F.; Carneiro, V.; Fernández, D.; Formoso, V. Comparison of collaborative filtering algorithms: Limitations of current techniques and proposals for scalable, high-performance recommender systems. *ACM Trans. Web* **2011**, *5*, 1–33. [CrossRef]
16. Pedersen, T.P. Non-interactive and information-theoretic secure verifiable secret sharing. In *Proceedings of the Annual International Cryptology Conference*; Springer: Berlin/Heidelberg, Germany, 1991; pp. 129–140.
17. Ioannidis, Y.; Kotidis, Y.; Mailis, T.; Möller, R.; Neuenstadt, C.; Ozçep, O.L.; Svingos, C. Data Mining and Query Log Analysis for Scalable Temporal and Continuous Query Answering. 2015. Available online: http://www.optique-project.eu/ (accessed on 26 June 2025).
18. Yao, Z.; Fang, Y.; Pan, H.; Wang, X.; Si, X. A secure and highly efficient blockchain PBFT consensus algorithm for microgrid power trading. *Sci. Rep.* **2024**, *14*, 8300. [CrossRef] [PubMed]
19. Yang, J. Blockchain Applications for Peer-to-Peer Energy Trading. Ph.D. Thesis, Nanyang Technological University, Singapore, 2022.
20. Grigoryan, H. Cost-Effective Integration of Blockchain Technologies Into P2P Energy Trading Systems. In Proceedings of the 2024 IEEE International Conference on Omni-layer Intelligent Systems (COINS), London, UK, 29–31 July 2024; IEEE: Piscataway, NJ, USA, 2024; pp. 1–5.
21. Khan, M.T.; Dowla, M.N.U.; Niloy, F.A. A blockchain-based efficient data storage and sharing scheme for renewable energy trading in smart grid. *Int. J. Blockchains Cryptocurrencies* **2022**, *3*, 222–234. [CrossRef]
22. Zhang, P.; Wu, P.; Liu, Y.; Chen, Y.; Li, Y.; Yan, J.; Ghafouri, M. Toward a Blockchain-Based, Reputation-Aware Secure Transactive Energy Market. *Blockchains* **2024**, *2*, 61–78. [CrossRef]
23. Zhao, C.; Han, D.; Li, C.; Wang, H. A blockchain consensus mechanism to optimize reputation-based distributed energy trading in urban energy system. *IEEE Access* **2024**, *12*, 53698–53712. [CrossRef]
24. Lv, S.; Zhang, X.; Wang, J.; Xiong, W.; Yang, L. RMCT: Distributed electricity transaction based on reputation mechanism and multi-chain technology in blockchain environment. *Electr. Power Syst. Res.* **2025**, *243*, 111516. [CrossRef]
25. Kumar, A.; Mondal, K.K.; Vishwakarma, L.; Das, D. RBCET: A Reputation based Blockchain Consensus Mechanism for Fast and Secured Energy Trading in Internet of Electric Vehicles (IoEV). *IEEE Trans. Consum. Electron.* **2025**. [CrossRef]