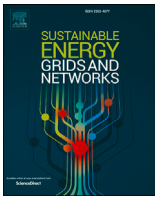
Sustainable Energy, Grids and Networks 43 (2025) 101796

Contents lists available at ScienceDirect

Sustainable Energy, Grids and Networks

journal homepage: www.elsevier.com/locate/segan



Blockchain-based energy trading with multi-factor trust: Ensuring fairness and security in peer-to-peer energy trading with blockchain technology

M. Zulfiqar[a], M.B. Rasheed[b,*], Daniel Rodriguez[c], Maria D. R-Moreno[b]

[a] Department of Telecommunication Systems, Bahauddin Zakariya University, Multan, Pakistan
[b] ISG Research Group, Universidad de Alcalá, Alcalá de Henares, 28802, Madrid, Spain
[c] Department of Computer Science, Universidad de Alcalá, Alcalá de Henares, 28802, Madrid, Spain

ARTICLE INFO

Keywords:
Blockchain
Proof-of-verifiability
Dynamic pricing
Cost reduction
Peer-to-peer networks

ABSTRACT

Contemporary power grid systems increasingly rely on sophisticated energy trading mechanisms to optimize resource allocation and operational performance. While prior studies have examined the coordination roles of energy intermediaries and utility operators, particularly through distributed ledger technologies that ensure data provenance and transaction verifiability in decentralized energy marketplaces, significant security vulnerabilities persist. Notably, fraudulent practices by energy suppliers characterized by payment collection without corresponding energy delivery pose substantial risks to market integrity and participant confidence. This research presents the Blockchain-based Energy Trading with Multi-Factor Trust Framework (BC-ET-MF), a novel architecture that addresses critical security deficiencies through advanced cryptographic protocols and consensus mechanisms. The framework utilizes anonymous credential systems to safeguard participant privacy while implementing time-locked commitment schemes that ensure transaction fairness and verifiability. The architecture incorporates granular access control mechanisms for secure service orchestration and establishes a consortium blockchain infrastructure among energy intermediaries to facilitate distributed transaction validation and immutable record-keeping. To mitigate computational overhead associated with conventional consensus algorithms, we introduce a Proof-of-Verifiability protocol that dynamically calibrates to real-time energy production and consumption patterns. This adaptive mechanism reduces system resource requirements while maintaining security guarantees. Experimental evaluation demonstrates that BC-ET-MF achieves substantial performance improvements: energy consumption reduction of 43.0 %, peak-to-average ratio optimization from 8.27 to 3.21 and 5.88 under 25 % and 50 % demand reduction scenarios respectively, and establishment of 92.5 % participant trust levels. The framework additionally yields 37.6 % transaction latency reduction while preserving user anonymity and enabling comprehensive audit capabilities, thus establishing a secure, efficient, and trustworthy energy trading ecosystem.

1. Introduction

The modern smart grid (SG) integrates electric vehicles (EVs) and distributed energy generators, reducing the need for expensive grid expansions [1]. However, this evolution presents operational challenges for network operators: increased EV adoption disrupts traditional load patterns, impacting voltage control and grid stability [2,3]. Existing energy management strategies, such as peak clipping, can balance loads but often do so at the expense of user comfort [4]. To effectively manage escalating electricity demand, it is crucial to integrate renewable energy sources with adaptable demand-side response models that prioritize user satisfaction while maintaining grid stability [5]. Energy trading (ET) within decentralized smart grids is gaining traction as a potential solution to improve operational efficiency and grid resilience. Conventional ET systems operating under centralized authority pose significant security and privacy risks, suffer from delayed responses, and lack local accountability. In contrast, local energy generation and trading—especially through peer-to-peer (P2P) mechanisms—offer the potential to empower communities and mitigate voltage fluctuations, despite facing regulatory constraints and price volatility [6,7]. At the

* Corresponding author.
Email addresses: zulfiqarchishti@gmail.com (M. Zulfiqar), muhammad.rasheed@uah.es (M.B. Rasheed), daniel.rodriguezg@uah.es (D. Rodriguez), malola.rmoreno@uah.es (M.D. R-Moreno).

https://doi.org/10.1016/j.segan.2025.101796
Received 1 March 2025; Received in revised form 29 May 2025; Accepted 4 July 2025
Available online 19 July 2025

Table 1
Abbreviations and Variables.

Variable	Meaning	Variable	Meaning
ET	Energy Trading	CA	Certificate Authority
EB	Energy Broker	EP	Energy Purchaser
ES	Energy Seller	CBC	Consortium Blockchain
AU	Attribute Universe	1^{λ}	Security Parameter
G	Group with prime order	q	Prime order of group G
g	Group Generator	H_1, H_2, H_3	Hash Functions
msk	Master Key	pak_a	Public Attribute Key
avk_a	Initial Attribute Version Key	ts	Time Slot
B_0	Genesis Block	$pubk^{EB}$	Public Key of Energy Broker
d^{ep}	Energy Demand of Energy Purchaser	pr^{ep}	Bid Price by Energy Purchaser
ct^{ep}	Encrypted Energy Request	r_0, r_1	Random Numbers
z^{ep}	Computed Hash Value	s^{ep}	Signature Component
t^{ep}	Transformed Signature Component	σ^{ep}	Signature of Energy Purchaser
tq^{eb}	Trading Qualification String	ik_i	Item Key
T	Access Structure	tk^{es}	Token of Energy Seller
Tx_{es}^{dep}	Deposit Transaction	rv^{ep}	Reputation Value of Energy Purchaser
BL^{eb}	Blacklist	tq_{pay}^{ep}	Payment Timestamp
Tx^{ep}	Payment Transaction	B	Energy Trading Bill
$Comm^{es}$	Commitment of Energy Seller	Tx_{es}^{Comm}	Commitment Transaction
usk'	Updated User Secret Key	ct_{ypd}	New Ciphertext
$F(p, b, h, \tau)$	Expected Progress Function	$C(p, \Delta)$	Catch-up Probability
$D(p, T, \Delta, \tau)$	Double Spending Probability	p	Processing Power
h	Block Height	τ	Time Interval
Δ	Initial Block Disadvantage	T	Confirmation Threshold

same time, fixed pricing mechanisms and complex market negotiations introduce further challenges in decentralized environments [8–10]. Blockchain technology emerges as a promising solution by ensuring data privacy, enhancing system integrity [11,12], and distributing control to strengthen resilience against cyberattacks. Its decentralized architecture can improve transparency and trust in ET systems, addressing vulnerabilities associated with centralized operations and market-based negotiation methods [13]. However, privacy concerns, particularly linking attacks, call for robust privacy-preserving mechanisms within blockchain frameworks [9]. Recent studies have explored various blockchain-based solutions for decentralized ET. Gurjar and Nikose [14] propose a fair, secure P2P ET model via smart contracts, yet it lacks protection against cheating attacks and provides limited privacy. Telagi and Pedapenki [15] provide a broad overview of P2P ET models, but lack practical implementation, identity management, and access control. Chabok et al. [16] offer a distributed trading framework but fall short in addressing privacy concerns and cheating prevention. Shen et al. [17] present a decentralized, privacy-conscious P2PET model, though its scalability and enforceability are limited. Shorya and Jagwani [18] address delay attacks using predictive analytics, but anonymity remains unsupported. Shang et al. [19] enhance extensibility via consensus-smart contract mechanisms but do not incorporate privacy or access control. Villa-Ávila et al. [20] emphasize decentralization and reliability, though implementation and fairness are not addressed. Joshi and Singh [21] propose a decentralized monitoring system, yet lack a trading focus and verified security. Varshith [22] introduces a fair auction model based on consortium blockchain but omits privacy and commitment safeguards. Moeini et al. [23] highlight secure blockchain-based trading frameworks, but further enhancements are necessary in authentication and transaction accountability.

1.1. Motivation and problem statement

The evolution of smart grids necessitates advanced energy management paradigms to accommodate bidirectional energy flow, EV integration, and distributed energy resource (DER) participation [1–3]. Peer-to-peer (P2P) ET, facilitated by decentralized architectures, emerges as a compelling solution for dynamic load balancing, local market participation, and improved energy utilization [6,7]. However, the lack of trust, verifiability, and privacy enforcement in existing decentralized platforms impedes their practical adoption [8–10]. Traditional ET frameworks rely on trusted third parties or centralized marketplaces, which introduce single points of failure, latency, and transparency concerns [11,12]. While blockchain technology addresses some of these limitations via immutability and decentralized consensus, it still faces performance bottlenecks and security vulnerabilities when applied to real-time, large-scale energy transactions [13]. Specifically, current systems struggle with ensuring fairness in trade execution, preventing seller-side non-compliance, and verifying buyer solvency without identity disclosure [14,16,18]. Moreover, conventional consensus algorithms such as Proof-of-Work (PoW) and Proof-of-Stake (PoS) are either computationally expensive or unsuitable for energy-constrained environments [19,20]. Privacy-preserving methods—though promising—often lack robustness against linking attacks or suffer from significant computational overhead [9,17,22]. These challenges necessitate a new architectural framework that holistically addresses security, scalability, verifiability, and privacy in P2P ET. Please note that, the mathematical symbols are defined in Table 1.

1.2. Research gaps and challenges

Despite growing interest in decentralized ET, several critical challenges remain unaddressed. Current systems lack robust mechanisms to prevent seller-side cheating and fraudulent behaviors in peer-to-peer (P2P) transactions, undermining trust and transactional fairness. Additionally, most platforms do not offer fine-grained access control or effective identity protection, exposing participants to privacy risks. Existing privacy-preserving solutions often fail to guarantee anonymity or impose significant computational overhead, making them impractical for large-scale deployment. Furthermore, scalable consensus mechanisms tailored for consortium-based or community-scale ET are largely absent, limiting the adaptability and real-world applicability of proposed frameworks.

1.3. Research questions

- *RQ1: How can seller-side cheating be effectively prevented in blockchain-based P2P ET?*
- *RQ2: What privacy-preserving authentication schemes can ensure anonymity without compromising performance?*
- *RQ3: Can a scalable consensus algorithm be designed to support fairness and resilience in consortium ET?*

1.4. Contributions and novelty

To address the identified research challenges, this paper proposes BC-ET-MF—a decentralized and privacy-preserving blockchain-enabled framework designed to ensure fairness, trust, and security in peer-to-peer (P2P) ET ecosystems. The primary contributions and novelties of this work are summarized as follows:

1. A comprehensive problem formulation that identifies unresolved issues in decentralized ET, including transaction-level security, bid manipulation, inadequate privacy safeguards, absence of pricing fairness, and limited trust among participating agents.
2. Design of a verifiable fairness model that integrates cryptographic commitment schemes and traceable transaction records to deter fraudulent behaviors, such as seller-side reneging and buyer-side double-spending attacks.
3. Integration of blockchain infrastructure with privacy-enhancing technologies—such as anonymous authentication and zero-knowledge verification—to achieve traceability, accountability, and non-repudiation, while preserving participant confidentiality and enabling fine-grained access control.
4. Development of a lightweight, energy-aware *Proof-of-Verifiability (PoV)* consensus mechanism that links block validation to actual energy generation and consumption metrics. This reduces reliance on resource-intensive mining, thereby enhancing scalability, reducing carbon footprint, and incentivizing active stakeholder participation.

While the proposed architecture achieves decentralization at the operational layer, it incorporates a minimally trusted Certificate Authority (CA) for initial identity registration and key issuance. Furthermore, the PoV mechanism requires parameter tuning for optimal deployment under heterogeneous demand profiles. Nonetheless, BC-ET-MF advances the state of the art by offering a scalable, secure, and privacy-compliant solution tailored for community-scale ET in future smart grids. The paper is organized as follows. Section 2 reviews current works and trends in blockchain-based ET. Section 3 details the key components of the proposed ET framework, followed by Section 4, which describes the methodologies and algorithms developed for BC-ET-MF. Section 5 analyzes the security of our trading scheme, while Section 6 empirically validates its performance. Section 7 evaluates the system's security and privacy mechanisms. Finally, Section 8 summarizes the findings of the study.

2. State of the art

This literature review analyzes recent blockchain-based energy trading developments from three perspectives: architectural designs that enable peer-to-peer transactions, security and privacy enhancement mechanisms, and a comparative evaluation of 2025 research contributions to demonstrate the distinctive advantages of our framework.

2.1. Blockchain-based architectures for energy trading

Foundational research in blockchain-enabled energy trading focuses on decentralized market mechanisms and security protocols. Key studies investigate smart contract implementations, efficient consensus algorithms, and frameworks addressing fairness, transparency, and system scalability challenges. Notable examples include: Nizamuddin et al. [24] develop a blockchain framework securing digital asset royalties through Ethereum smart contracts, achieving transparent distribution and robust transaction security. While targeting digital markets, their approach shares conceptual similarities with the transparency requirements in energy trading. Hassija et al. [25] introduce an efficient blockchain protocol for vehicle-to-grid networks, enabling low-cost microtransactions through reduced computational overhead, while prioritising scalability and economic viability. Inayat et al. [26] and Han et al. [27] discuss the utilization of blockchain for decentralized ET and management. They emphasize the role of blockchain in achieving load balancing and enhancing P2P ET through secure, automated platforms. These studies are directly comparable to our research where we aim to improve upon these frameworks by integrating advanced privacy protection and equitable access in ET. Zulfiqar et al. [28] introduce a blockchain-driven trust-aware framework that utilizes game theory for managing ET in smart grids. They propose a unique consensus mechanism to foster collaboration among agents. This corresponds with the focus of our study, which also explores multi-agent coordination, emphasizing decentralization and security, similar to the approach taken by the authors. Guan et al. [29] address the scalability and security issues inherent in centralized ET models by introducing a two-level blockchain-based ET Scheme (BC-ETS) that enhances security and system availability for IIoT environments. Their approach introduces a credibility-based equity-proof mechanism tailored for devices with lower computing power, an area where our BC-ET-MF builds upon by introducing a dual PoV protocol that further enhances both energy generation and consumption efficiency, thereby addressing intermittency and dynamic demand challenges not fully tackled by the authors.

2.2. Security, privacy, and fairness mechanisms in ET models

Research on trust, privacy, and fairness mechanisms in peer-to-peer energy trading encompasses homomorphic encryption, anonymous verification systems, noise-based privacy techniques, and game-theoretic collaboration models. Samuel et al. [9] combine additive homomorphic encryption with consortium blockchain architecture, implementing dynamic pricing and dispute resolution while minimizing computational costs. Building upon this foundation, our approach incorporates enhanced privacy protocols and optimized consensus mechanisms that further reduce processing overhead. Li et al. [30] introduce the "energy blockchain" consortium framework, which addresses security challenges in Industrial IoT energy trading through credit-based payment systems, enabling rapid transactions. Our framework extends this work by integrating advanced cryptographic verification, ensuring equitable energy distribution alongside transaction efficiency. Meng Li et al. [31] developed FeneChain, emphasizing fairness through anonymous authentication and timed commitment protocols for secure energy trading management. While they focus on the integrity and transparency of transactions, our BC-ET-MF further innovates by integrating a PoV consensus that leverages real-time data for more adaptive and responsive ET, significantly building on the foundations laid by Meng Li et al. Lin et al. [32] introduce a blockchain-based system, BSeIn, for secure mutual authentication with fine-grained access control within Industry 4.0. They address multiple security concerns relevant to smart factories and Industry 4.0. In contrast, our BC-ET-MF applies similar blockchain security advancements to the energy sector, ensuring not only secure transactions but also equitable access to energy resources, thereby expanding the applicability of Lin et al.'s security-focused innovations to broader industrial contexts. Gai et al. [33] focus on privacy-preserving mechanisms in ET using a consortium blockchain to protect against data mining attacks. Their approach to privacy is foundational, yet our work introduces additional layers of security and operational efficiency by implementing noise-based privacy-preserving mechanisms that are robust against more sophisticated adversarial tactics, enhancing the privacy framework established by Gai et al. Aitzhan et al. [34] provide a solution for decentralized ET that enhances transaction security using multi-signatures and anonymous messaging streams. Our BC-ET-MF extends these security features by incorporating state-of-the-art cryptographic techniques that ensure not only the security of transactions but also their irreversibility and resistance to collusion and other security threats, addressing some of the limitations noted in Aitzhan et al.'s approach. Kang et al. [35] design a localized P2P electricity trading system for PHEVs using a consortium blockchain. They improve the transaction security and pricing mechanisms to maximize social welfare. Our system

Table 2
Comprehensive Comparison of BC-ET-MF with Recent Models..

Model	Seller Cheating	Privacy	Identity	Fairness	Access Control	Consensus	Auction	Scalable	Drawbacks
Gurjar and Nikose [14]	✗	✗	✗	✓	✗	✓	✗	✗	No privacy or cheating prevention
Telagi and Pedapenki [15]	✗	✗	✗	✗	✗	✗	✓	✗	Lack of transaction verification and privacy guarantees
Chabok et al. [16]	✗	✓	✗	✓	✗	✓	✓	✗	Partial fairness; lacks identity management
Shen et al. [17]	✗	✓	✗	✓	✗	✓	✓	✗	No seller verification or ID protection
Shorya and Jagwani [18]	✗	✓	✗	✓	✗	✗	✗	✗	No consensus and seller validation
Shang et al. [19]	✗	✗	✗	✓	✗	✓	✗	✗	Basic P2P logic, lacks control and ID security
Villa-Ávila et al. [20]	✗	✓	✗	✓	✗	✗	✗	✗	Unaddressed seller/identity threats
Joshi and Singh [21]	✗	✓	✗	✓	✗	✗	✗	✗	Limited control, identity anonymity not ensured
Varshith [22]	✗	✓	✗	✓	✗	✓	✓	✗	No full-scale ID validation or access control
Moeini et al. [23]	✗	✓	✗	✓	✗	✓	✗	✗	Cooperation lacks proper identity/security tools
Proposed BC-ET-MF	✓	✓	✓	✓	✓	✓	✓	✓	Minor reliance on CA and overhead from PoV tuning

builds on Kang et al.'s localized trading model by optimizing the load balancing and integrating renewable energy sources more effectively, which makes their solution more suitable for modern smart grids with high renewable penetration.

2.3. Comparative analysis with recent works

Recent research addresses various energy trading challenges with mixed success. Telagi and Pedapenki [15] provide comprehensive P2P trading analysis but lack concrete security implementation frameworks. Chabok et al. [16] develop blockchain-based transactive systems emphasizing fairness while omitting privacy protection measures. Shen et al. [17] advocate sustainable decentralized markets through blockchain but face scalability limitations. Shorya and Jagwani [18] integrate predictive analytics with blockchain for attack mitigation, whereas Shang et al. combine consensus protocols with smart contracts yet provide insufficient identity safeguards. Villa-Ávila et al. [20] Joshi and Singh, and Varshith examine decentralization, monitoring, and auction mechanisms respectively, though their approaches lack comprehensive privacy validation and fraud prevention capabilities. Our BC-ET-MF framework addresses these limitations through timed commitment protocols and anonymous authentication, providing verifiable protection against fraudulent seller behavior. It introduces a novel PoV consensus and employs a consortium blockchain to ensure scalability and governance, supported by energy validators and authorized energy broadcasters (EBs). Table 2 compares the BC-ET-MF model with recent ET models from 2025. Gurjar and Nikose [14] focus on fairness and secure automation but lack cheating prevention and privacy. Telagi and Pedapenki [15] provide an overview without implementation and miss access control. Chabok et al. [16] offer fairness but lack privacy and cheating resistance. Shen et al. [17] present a decentralized model, though scalability concerns exist. Shorya and Jagwani [18] mitigate delay attacks but lack anonymity support. Shang et al. [19] emphasize extensibility but lack privacy and access control. Villa-Ávila et al. [20] stress decentralization but lack implementation and fairness. Joshi and Singh [21] focus on energy monitoring but miss key trading features. Varshith [22] introduces a fair auction but lacks privacy. The proposed BC-ET-MF model, as shown in Table 2, addresses seller cheating, privacy, and access control, with fine-grained scalability and PoV consensus. However, it introduces minor centralization and calibration overhead.

3. Proposed system model and methodology

The described system, depicted in Fig. 1, is centred around a microgrid ecosystem comprising energy prosumers, a consortium blockchain, smart meters, a power plant, a local energy aggregator, and a certificate authority. In this setup, prosumers are key actors, generating and storing excess energy and engaging in transactions such as buying, selling, or retaining energy reserves based on their current energy status. The integrity of the system is reinforced by secure smart meters, which meticulously record consumption and trading data, guaranteeing the secure logging of these transactions on the blockchain. A local energy manager oversees transactions via smart contracts, while an aggregator verifies and facilitates monetary deposits, issuing refunds if no disputes arise. To sell energy, users must:

1. Register with the central authority.
2. Meet their local energy demands before trading.

Within this framework, energy suppliers undergo attribute validation through automated contract protocols. Trading operations utilize distributed blockchain validation where participating nodes collectively ensure ledger integrity. High-credibility validators mitigate aggregator misconduct through decentralized verification processes. Communication channels between system components implement public-key cryptography for data integrity and confidentiality. Successfully verified transactions receive immutable storage within blockchain structures, while invalid data is immediately eliminated. New block creation maintains cryptographic linkage with previous entries, utilizing customized Proof-of-Verifiability algorithms explicitly designed for energy market dynamics.

4. Proposed scheme

This section introduces our blockchain-based energy trading architecture designed to address security vulnerabilities and market fairness challenges. The framework integrates several core modules: initial system setup, participant enrollment protocols, energy supply-demand matching, equitable transaction processing, conflict arbitration mechanisms, and dynamic membership management. Additionally, we examine prevention strategies for fraudulent spending attempts, specialized consensus algorithms optimized for energy markets, adaptive pricing methodologies, and reputation-based trust evaluation systems.

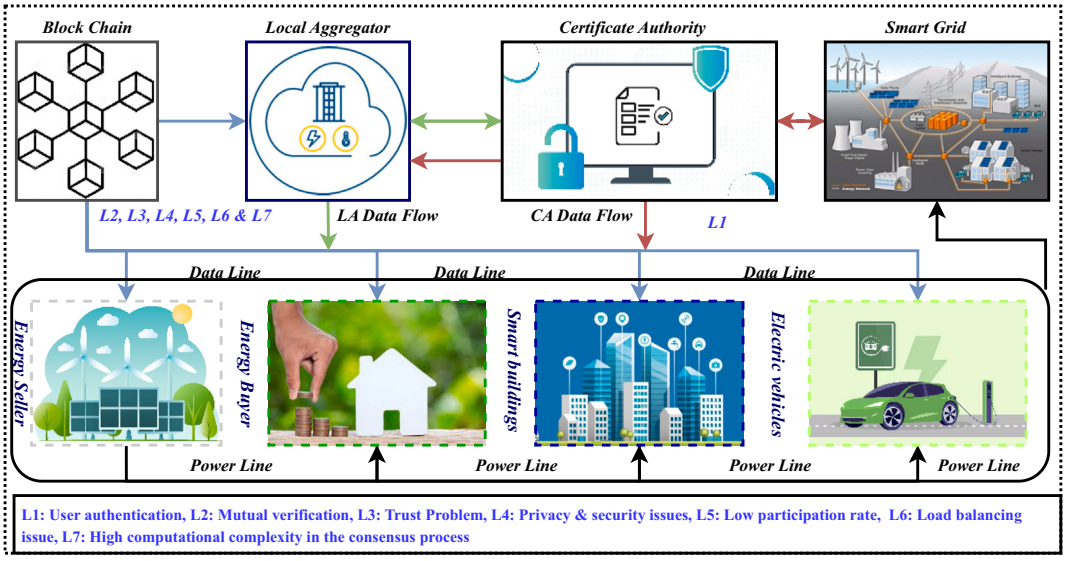


Fig. 1. Line flow of the proposed blockchain-based energy trading system.

Following sections provide comprehensive analysis of each architectural component.

4.1. System setup and initialization

The certificate authority establishes system parameters by selecting a security threshold 1^{λ} and constructing a cyclic group G of prime order q with λ-bit length. The authority designates a base generator g and defines cryptographic hash mappings H_1 and H_2. Subsequently, it initializes multiplicative group structures G_1 and G_2 of order p, establishes a bilinear mapping e, selects generator element $\tilde{g}$, and specifies hash function H_3. For master key generation, the CA randomly samples elements $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ from the integer field $\mathbb{Z}_p$ to form the master secret key (msk). The public parameters are computed as the tuple $(\tilde{g}^{\alpha_1}, \tilde{g}^{1/\alpha_2}, \tilde{g}^{\alpha_2}, e(\tilde{g}, \tilde{g})^{\alpha_4})$. After consulting with EB, the CA defines an attribute universe $AU = \{a_i\}$. For each attribute a, it selects a random number v_a as the initial attribute version key avk_a and computes a public attribute key pak_a. Finally, the CA sets up a consortium blockchain (CBC) with the EBs, dividing time into slots $\{ts_1, ts_2, \ldots\}$. Each EB_i creates a ledger CBC_i, starting with the genesis block B_0, which includes an empty block header, EBs' identities and public keys, a timestamp, and signatures.

4.2. Entity registration

Each EB broadcasts its public keys $pubk^{EB}$ in its coverage area. When an EP wants to purchase energy, it creates an energy request ER^{eb} as follows:

First, they determine the amount of energy d^{ep} and bid price pr^{ep}. These are encrypted with $pubk^{EB}$ to form the ciphertext as in Eq. (1):

$$ct^{ep} = \left(g^{r_0}, (d^{ep} \parallel pr^{ep}) \cdot (pubk^{EB})^{r_0}\right) \tag{1}$$

where $r_0 \in \mathbb{Z}_q^*$ is a random number. They then calculate z^{ep} and s^{ep} as follows in Eqs. (2) and (3):

$$z^{ep} = H1(h^{ep1}, h^{ep2}) \tag{2}$$

$$s_{ep} = g^{z_{ep} \cdot y_{ep}} \tag{3}$$

Choosing $r_1 \in \mathbb{Z}_q^*$, they compute t^{ep} in Eq. (4):

$$t^{ep} = (s^{ep})^{r_1} = (g^{z^{ep} \cdot y^{ep}})^{r_1} \tag{4}$$

They generate a signature $\sigma^{ep} = (\sigma^{ep1}, \sigma^{ep2})$:

$$\sigma^{ep1} = H2(ct^{ep}, h^{ep1}, h^{ep2}, t^{ep}) \tag{5}$$

$$\sigma^{ep2} = r_1 - x^{ep} \cdot \sigma^{ep1} \mod q \tag{6}$$

Finally, the energy request $ER^{ep} = (pubk^{ep}, ct^{ep}, \sigma^{ep})$ is sent to the EB.

4.3. Energy responding

The local EB conducts the following verification and broadcast process upon receiving an energy request ER^{ep} from an EP: It begins by computing $z = H1(h^{ep_1}, h^{ep_2})$ and $t' = (g^z y^{ep})^{\sigma^{ep_2}} (h^{ep_1})^z (h^{ep_2})^{\sigma^{ep_1}}$. If $\sigma_1 \neq H2(ct^{ep}, h^{ep_1}, h^{ep_2}, t')$, the request is dropped; otherwise, the operations continue. The decryption process for ct^{ep} using the private key $prik^{EB}$ is elaborated. A trading qualification string tq^{eb} is generated, partitioned as $tq^{eb} = (I_1, \ldots, I_4)$, and encrypted using different item keys ik_i via AES encryption. Each ik_i is encrypted under an access structure T over the attribute universe AU. The ciphertext of tq^{eb} is formed as ct^{eb}. Upon receiving the energy requests, an ES responds by computing c' and verifying the shares of c based on T. The tq^{eb} is decrypted, and ct^{es} is generated by encrypting tq^{eb} with $pubk^{eb}$. A signature σ^{es} is created, and tokens tk^{es} are deposited on the blockchain through a deposit transaction Tx_{es}^{dep} (Eq. 9). The deposit serves as a safeguard against qualified-but-malicious energy sellers for blockchain integration). EB verifies ES's identity and attributes and confirms membership for ET, broadcasting $pubk^{es}$ as an available energy source upon successful verification.

4.4. Fair energy trading

Upon receiving the identifier $pubk^{es}$, EP initiates a payment transaction to transfer a portion of the bid price (tk^{ep}) to ES, as depicted in Eq. (7):

$$Tx^{ep} = (\text{Payment}, pubk^{es}, tq_{pay}^{ep}, tk^{ep}, pubk^{ep}, h^{ep1}, \tau^{ep}) \tag{7}$$

Here, tq_{pay}^{ep} represents a timestamp, and τ^{ep} denotes a digital signature generated using x^{ep}. Subsequently, ES delivers the corresponding energy to EP via $pubk^{ep}$ and generates an ET bill B. This bill, crafted by ES's smart meter, encapsulates crucial details such as the energy account of EP, the energy account of ES, the quantity of energy transferred, and the transfer time. Following this, ES generates a commitment

$Comm^{es} = H_1(B)$ and commits it to the blockchain through a commitment transaction to EB, as outlined in Eq. (8):

$$Tx_{es}^{Comm} = (\text{Commitment}, pubk^{es}, tq^{es^{com}}, Comm^{es}, \tau^{es}) \tag{8}$$

Here, $t_q^{es^{Com}}$ denotes a timestamp, and τ^{es} signifies a digital signature generated using x^{es}. All transactions are processed by EBs, who maintain the blockchain network through a practical Byzantine fault tolerance (PBFT) consensus mechanism. Upon expiration of T, if no complaints are raised against ES, the system formally acknowledges the ET between EP and ES.

4.5. Dispute arbitration

If an EP files a complaint against an ES before the expiration of a predefined time T, the ES is required to disclose their commitment $Comm^{es}$ by presenting the Energy Transaction bill B to the EB. Failure to provide B indicates prior misconduct by the ES. Consequently, the ES is placed on the blacklist BL^{eb}, resulting in a decrease in their reputation value rv^{ep}. The EB then broadcasts the updated blacklist, accompanied by its signature sig_{EB}. The duration of an ES's presence on BL^{eb} varies depending on the application, typically ranging from one hour to one month. Additionally, certain attributes A^{es}_{revoked} of the ES may be revoked as detailed in the subsequent section. The flowchart in Fig. 2 depicts the procedure when an EP files a complaint against an ES before the expiration time T. If the complaint is filed after this period, no action is taken. Upon a timely complaint, the ES must disclose its commitment $Comm^{es}$ by submitting the Energy Transaction bill B to the EB. If the ES provides B, the EB verifies it and the complaint is resolved fairly. If B is not provided, the ES is marked as malicious, added to the blacklist BL^{eb}, and its reputation value rv^{ep} is penalized. The updated blacklist, signed by the EB, is broadcast to all network nodes. The ES remains on the blacklist for a duration $\tau_{\text{blacklist}}$, typically ranging from one hour to one month, and certain attributes may be revoked according to application policies. Therefore, Fig. 2 illustrates the ET process in two scenarios: normal ET and abnormal ET with fair arbitration. In the normal ET scenario, an honest energy seller and purchaser participate in the standard trading process where the seller receives payment and the purchaser receives energy without any dispute. In contrast, the abnormal ET scenario involves a dishonest energy seller and purchaser, where the seller's deceit is detected and addressed through the arbitration mechanism during the trading process.

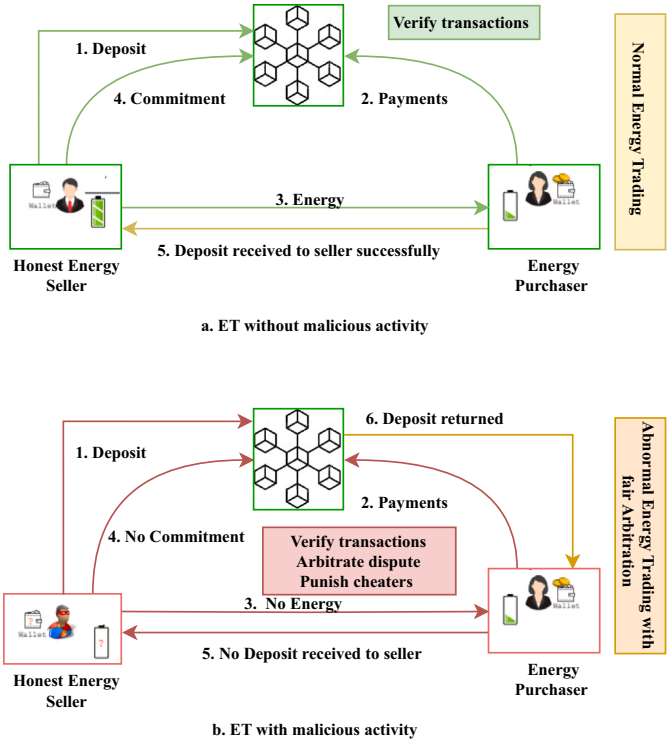


Fig. 2. Iterative Transaction Resolution (ITR) process in energy trading, showing normal and abnormal conditions with complaint handling and penalties.

4.6. Membership updating

In case of misconduct within the ET framework, specific attributes undergo revocation. For instance, if Alice engages in deceptive ET, her attribute y is revoked to halt further transactions. The CA selects a fresh random number v'_y as the new attribute version key, computes an update key uk^y, renews the public attribute key pak^y, and disseminates the update. Each non-revoked seller forwards L and S_y to the CA, which calculates a new value S'_y using Eq. (9):

$$S'_y = \left(\frac{S_y}{L^{\gamma_2^2}}\right)^{uk_1^y} \cdot L^{\gamma_2^2} \tag{9}$$

The seller's user secret key usk' is updated accordingly. Finally, the EB adjusts the ciphertext associated with y and generates a new ciphertext ct_{ypd}.

4.7. Double spending attack

The attacker model described in this study, inspired by Pinzon et al. [36], involves three primary parameters:

1. Expected Progress Function $F(p, b, h, \tau)$: This function estimates the attacker's expected branch length using parameters such as processing power p, block height h, and time interval τ.
2. Overtaking Probability $C(p, \Delta)$: This metric evaluates the likelihood of fraudulent spending attacks, accounting for the malicious actor's initial blockchain lag Δ relative to legitimate network participants.
3. Fraudulent Transaction Probability $D(p, T, \Delta, \tau)$: Constructed from parameters (C) and (F), this measure determines the probability of successful double-payment execution by adversaries, where (T) represents the confirmation requirement threshold.

Key metrics for evaluating fraudulent spending behaviors encompass:

- $C(p, \Delta)$: The probability that malicious nodes can overtake legitimate chain growth given their initial deficit of Δ blocks.
- $F(p, b, h, \tau)$: The chance that an adversarial entity can append (b) additional blocks during time period τ, considering computational capacity (p) and current chain height (h).
- $D(p, T, \Delta, \tau)$: The probability of successful fraudulent payment execution by adversarial nodes possessing enhanced computational resources.

Consider the function $F(p, b, h, \tau)$, which calculates the probability of extending the blockchain by b blocks within a given time frame τ. Here, p represents processing power, b is the number of blocks to be extended, h is the starting block height, and τ is the time. The probability $q(p, \tau, b)$ signifies the likelihood of extending the blockchain by b blocks with processing power p in time τ. The function $F(p, b, h, \tau)$ is computed as the sum of $q(p, \tau, b)$ and $P(p, b, h)$, where $P(p, b, h)$ denotes the probability of an adversary extending the blockchain by b blocks before honest nodes starting from block height h, based on the model proposed by M. Rosenfeld [37]. The probability of a double spending attack is denoted by $A_{DS}(p, T, \Delta, \tau)$. It quantifies the likelihood of success for an attacker with an initial disadvantage of Δ blocks and time τ against honest nodes, given a confirmation threshold of T. The expression for $A_{DS}(p, T, \Delta, \tau)$

is given by Eq. (10):

$$A_{DS}(p,T,\Delta,\tau) = 1 - \sum_{\Delta'=0}^{T-\Delta} F(p,T,\Delta',\tau)\left(1 - C(p,T-\Delta-\Delta')\right) C(p,\Delta') \tag{10}$$

Here, T represents the confirmation threshold, and $C(p,\Delta')$ denotes the success probability of a double spending attack given an initial disadvantage of Δ' blocks and time τ against honest nodes.

4.8. Proposed consensus mechanism

In the realm of blockchain technology, there is a pressing need to curb energy consumption and computational costs, particularly within the proof of work (PoW) consensus mechanism [38]. While proof of stake (PoS) emerges as a viable alternative [8], wherein the privilege to insert blocks and validate transactions is contingent upon one's cryptocurrency stake [39], it is evident that fresh approaches are necessary to address these issues. This article delves into novel consensus protocols, namely PoV_{EG} and PoV_{EC}, drawing inspiration from prior works [8,40]. These mechanisms aim to streamline validator selection, reducing gas consumption and initial investments. PoV_{EG} incentivizes prosumers to boost energy generation, favouring those with higher output and good reputations. Conversely, PoV_{EC} encourages energy conservation during peak hours, increasing the chances of selection for both prosumers and consumers who consume less. Validators verify transactions, adding valid ones to the blockchain. These mechanisms foster energy self-sufficiency and ease the burden on the main grid. The formulations for these mechanisms are detailed below. We consider a group of participants in the ET system, denoted by $P = \{p_1, p_2, p_3, \ldots, p_n\}$. Their energy consumption and generation are represented by $C = \{c_1, c_2, c_3, \ldots, c_n\}$ and $\mathcal{G} = \{g_1, g_2, g_3, \ldots, g_n\}$, respectively. Validator selection in the proposed consensus mechanisms relies on a proof of score (PS), determined by participants' energy generation and consumption. For the PoV_{EG} consensus mechanism, the PS is defined as follows in Eq. (11):

$$\mathrm{PS}_{g_i} = \log\left(\frac{1}{e^{C_i - G_i} \cdot \epsilon}\right); \quad \mathrm{PS}_{g_i} \geq 0, \quad i \in I \tag{11}$$

Here, G_i represents the energy generated by prosumer i, ϵ is the prosumer's reputation value, and C_i is the energy consumption. From Eq. (11), a higher G_i and ϵ increase the PS_{g_i}, giving the prosumer a higher probability of being selected as a validator. The selection probability for prosumer i is given by Eq. (12):

$$\mathrm{P}_{\mathrm{win}_i} = \frac{\mathrm{PS}_{g_i}}{\sum_{j \in I} \mathrm{PS}_{g_j}} \tag{12}$$

Energy costs are divided into Off-peak, Mid-peak, and On-peak categories based on different time slots. This protocol aims to reduce energy consumption during Mid-peak and On-peak hours to mitigate peak-hour usage spikes. The proof score for prosumer i in this context is given by Eq. (13):

$$\mathrm{PS}_{e_i} = (G_i - \delta \cdot C_i) \cdot \epsilon; \quad \delta \in (\delta_{\mathrm{mid}}, \delta_{\mathrm{on}}), \quad i \in I \tag{13}$$

In Eq. (13), the winning factor (δ) is introduced, where the product of δ and E_i during peak hours inversely affects the PS_{e_i}. Lower values of $\delta \cdot C_i$ result in higher PS_{e_i}. Different δ values, δ_{mid} and δ_{on}, are used for Mid-peak and On-peak hours, respectively. Since δ_{on} is less than δ_{mid}, reducing energy consumption during On-peak hours yields a higher proof score. Assuming electricity prices during Off-peak, Mid-peak, and On-peak hours are λ, λ_{mid}, and λ_{on} respectively ($\lambda_{\mathrm{on}} > \lambda_{\mathrm{mid}} > \lambda$), the values of δ are determined using Eqs. (14) and (15):

$$\delta_{\mathrm{mid}} = 1 - \frac{\lambda_{\mathrm{mid}} - \lambda}{\lambda_{\mathrm{mid}}}; \quad \lambda_{\mathrm{mid}} > \lambda \tag{14}$$

$$\delta_{\mathrm{on}} = 1 - \frac{\lambda_{\mathrm{on}} - \lambda}{\lambda_{\mathrm{on}}}; \quad \lambda_{\mathrm{on}} > \lambda \tag{15}$$

The probability of prosumer i being selected as a validator is determined by Eq. (16):

$$\mathrm{G}_{\mathrm{win}_i} = \frac{\mathrm{PS}_{e_i}}{\sum_{j \in I} \mathrm{PS}_{e_j}} \tag{16}$$

4.9. Pricing scheme

The energy market undergoes buyer demand and seller supply fluctuations over time, leading to variable energy prices. This dynamic nature contrasts with fixed pricing models, which maintain constant daily prices. Fixed pricing may not be optimal for ET systems. In the proposed model, energy prices are directly linked to the energy requirements of buyers during specific time slots. This pricing approach aims to be competitive and is designed to incentivize buyer participation in ET activities. Prices are determined based on the energy requested by buyers (E_{rq}) and the total available energy from sellers (E_{avl}). A time-of-use (ToU) pricing structure serves as a reference point, and the proposed pricing scheme, derived from ToU principles, is employed for simulations. The applicability of the price, whether it pertains to peak or off-peak hours, is determined by a threshold (E_{tr}) set by the local aggregator. Price ($Pr(t)$) is determined using Eq. (17), following the approach outlined in [41]:

$$Pr(t) = \begin{cases} \nu_{on}(t), & \text{if } E_{rq}(t) \geq E_{tr}(t) \\ \nu_{off}(t), & \text{otherwise} \end{cases} \tag{17}$$

To ensure load balancing, the peak-to-average ratio (PAR) is used to measure grid stability and reliability [42], defined as in Eq. (18):

$$PAR = \frac{\max(P_{Tc})}{\mathrm{average}(P_{Tc})} \tag{18}$$

In Eq. (18), P_{Tc} represents the total 24-hour power consumption.

4.10. Trust model

The model combines direct and indirect trust with a token deposit to boost reliability. Users with high trust levels play a pivotal role in consensus and trading, improving overall interactions. Trust values, determined by a blockchain-based weighted average method involving the deposit parameter, incentivize users to elevate their trust levels, fostering a reliable ecosystem. Eq. (19) describes the relationship between the deposit and trust value:

$$\mathrm{Tv}_{a,b} = \beta\left(\alpha Q_r + (1-\alpha) Q_s\right) + \gamma t \tag{19}$$

The trustworthiness evaluation of user a by user b is represented as $\mathrm{Tv}_{a,b}$. The direct trust value between users a and b is defined as shown in Eq. (20) [43]:

$$Q_r = \frac{P_a + 1}{P_a + N_a + 2} \tag{20}$$

The indirect trust value Q_s is represented as shown in Eq. (21):

$$Q_s = \frac{\sum_{k=1}^{K} W_s(k) \times Q_r(k)}{\sum_{k=1}^{K} W_s(k)} \tag{21}$$

In Eq. (21), the weight function is defined as follows as in Eq. (22):

$$W_f = e^{-d(E_p + E_n)} \tag{22}$$

Here, d serves as a decay factor, modulating the impact of evaluations based on the aggregated interaction evaluations E_p and E_n, where E_p

represents positive evaluations, and E_n negative evaluations. This sum, $E_p + E_n$, accounts for the total evaluative input a user has given, influencing how their trustworthiness or reliability is weighted. Coefficients a, b, and c are used as specified in Eq. (23):

$$a + b + c = 1 \tag{23}$$

where a, b, and c represent the weighting factors for direct trust Q_r, indirect trust Q_s, and the token deposit t, respectively. Specifically, a indicates the proportion of direct trust in the overall trust value, emphasizing the importance of firsthand interactions; b denotes the significance of indirect trust, capturing the influence of recommendations and observations from other users in the network; and c reflects the contribution of the token deposit to the trust value, incentivizing users to maintain a financial stake in the system's reliability. In the proposed model, a predefined token deposit or risk value, denoted as t (ranging from 0 to 1), correlates directly with users' cumulative trust values, as depicted in Eq. (19). As the token deposit increases, so does the user's trust value. It is assumed that participants fall into one of three categories: trusted, honest but curious, or malicious, with an expectation of correct behavior from all participants.

5. Security analysis of the energy trading scheme

Security evaluation of our energy trading framework examines cryptographic foundations, consensus protocols, and threat modeling approaches. The architecture provides data privacy, authenticity verification, and accountability assurance while defending against various attack vectors including identity forgery, message replay, and fraudulent transactions. Additionally, we assess the framework's resilience to collaborative adversarial scenarios through analysis of underlying mathematical complexity assumptions.

5.1. Mathematical foundations

Consider a multiplicative cyclic structure G with prime cardinality q and base element g, alongside cryptographically secure hash mappings H_1, H_2. The framework's security properties depend on the computational intractability of the Decisional Diffie-Hellman problem and the collision-resistant properties of the employed hash functions.

Definition 1 (Decisional Diffie-Hellman Assumption). The Decisional Diffie-Hellman conjecture asserts that for randomly selected values $a, b \in \mathbb{Z}_q$, no polynomial-time algorithm can effectively differentiate between g^{ab} and an arbitrarily chosen element from group G when provided with g^a, g^b.

Definition 2 (Collision Resistance). A hash function $H : \{0,1\}^* \rightarrow \{0,1\}^n$ is collision-resistant if it is infeasible for a probabilistic polynomial-time (PPT) adversary to find distinct x, y such that $H(x) = H(y)$.

5.2. Theorems and proofs

Theorem 1 (System Security). *Consider a multiplicative cyclic structure G of prime cardinality q with base generator g, together with collision-resistant hash mappings H_1, H_2. Under the validity of the DDH conjecture within G, our energy trading framework achieves data privacy and authenticity guarantees against malicious adversaries.*

Proof. **Confidentiality and Integrity:** Our framework establishes data privacy through pairing-based cryptographic encoding of transaction records, where the computational hardness of the Decisional Diffie-Hellman problem ensures that no adversary can effectively separate g^{ab} from randomly distributed group elements, thus maintaining cryptographic key confidentiality. Data authenticity emerges from digital attestations $\sigma = \text{Sign}_{sk}(M)$, which reveal any tampering attempts on authenticated message M. Moreover, the existential unforgeability property of digital attestation schemes prevents adversaries from constructing valid attestations without access to the corresponding secret key. Therefore, our system rigorously maintains both privacy and authenticity properties. □

Lemma 1 (Attribute Version Key Security). *Let $AU = \{a_i\}$ be the attribute universe, and let avk_a be the attribute version key for $a \in AU$. If the attribute version key is updated through a **secure one-way function**, an adversary with polynomial resources cannot derive the old attribute version key from the updated one.*

Proof. Suppose the attribute version key is updated as $avk'_a = H(avk_a)$. By the **preimage resistance** of H, given avk'_a, no adversary can compute avk_a efficiently. Thus, previous attribute version keys remain secure against exposure. □

Corollary 1 (Security of Membership Updates). *If attribute version keys are securely updated as per Lemma 1, then membership revocation ensures that a revoked entity cannot participate in future transactions.*

Proof. When a user is revoked, their attribute version key is updated. By Lemma 1, a revoked user cannot compute the new version key. Therefore, they lose access to the system. □

Proposition 1 (Fair Trading Enforcement). *Under the PBFT consensus mechanism, an ET transaction is deemed valid if and only if the commitment $Comm^{es}$ on the blockchain aligns with the submitted ET bill B.*

Proof. Each trading record B is committed to the blockchain via a commitment scheme:

$$\text{Comm}^{es} = H(B \parallel r) \tag{24}$$

Where r is a random value ensuring hiding properties. The PBFT consensus mechanism ensures that only valid transactions (where the commitment matches B) are added to the blockchain. Thus, cheating or misreporting trades is prevented. □

Axiom 1. (Non-Repudiation) Each energy seller ES and energy purchaser EP must sign transactions with a cryptographic signature scheme ensuring non-repudiation. That is, if an entity signs a transaction, it cannot later deny its participation.

Conjecture 1. *(Scalability of the Scheme) If the proposed ET framework scales linearly with the number of participating entities, then the computational and communication overhead remains bounded under realistic deployment conditions.*

The proposed privacy-preserving ET scheme is rigorously analyzed for security and correctness, ensuring robust protection against adversarial threats. System security is guaranteed under the Decisional Diffie-Hellman (DDH) assumption and collision-resistant hash functions, as established in Theorem 1. Attribute version keys provide secure membership updates, preventing revoked users from re-entering the system, as demonstrated in Lemma 1 and Corollary 1. Fair trading is enforced through the PBFT consensus mechanism and cryptographic commitments, ensuring transaction integrity (Proposition 1). Non-repudiation is achieved via secure digital signatures, preventing entities from denying their transactions (Axiom 1). Additionally, the scalability of the scheme is conjectured based on sharded PBFT designs, ensuring efficiency in large-scale deployments (Conjecture 1). Collectively, these security guarantees establish a secure, fair, and scalable ET framework for smart grids.

6. Simulation results and discussion

This section presents the results and discussions derived from our proposed system model. Simulations were run on a laptop with 4.00 GB RAM and an AMD E1-6015 APU @1.4 GHz, operating on Windows 10, using MATLAB R2020a. Our study involved 100 residential prosumers with diverse energy generation and consumption profiles, using

Table 3
Computational Costs for EB, EP, and ES (Unit: Millisecond).

Phase	FeneChain (ms)	BC-ET-MF (ms)	Improvement (%)
Energy Requesting (ERq)	11.2	9.5	↓ 15.2 %
Energy Responding (ER)	42.7	36.4	↓ 14.8 %
Energy Selling (ES)	13.7	11.9	↓ 13.1 %
Energy Trading (ET)	5.6	4.8	↓ 14.3 %
Energy Broker (EB)	48.5	39.2	↓ 19.2 %

a dataset from [44] with a 1-hour resolution. Python3 was used to assess the system's resilience against double-spending attacks. The prototype of our model was developed and evaluated on JUICE, a platform that supports smart contract development using JavaScript-based web/client tools and Solidity for code management. Various cryptographic algorithms were integrated into the system to ensure privacy and security, with Web3J used for smart contract evaluation. The execution time of our proposed system was measured using shell scripts and JavaScript after 50 iterations.

6.1. Computational cost analysis

The EB, EP, and ES play critical roles in the privacy-preserving ET process. The proposed BC-ET-MF model reduces their computational costs compared to FeneChain, improving efficiency and scalability, as shown in Table 3. The BC-ET-MF model minimizes exponentiations and multiplications for the EP, improving the encryption phase. The ES benefits from faster bilinear pairings and signature generation, leading to a 13.1 % reduction in computational cost. Signature validation and encryption operations are streamlined, reducing redundant calculations. The EB optimizes access control policies using batch verification techniques, reducing processing time by 19.2 %. Decryption complexity is lowered by reducing the number of individual ciphertext operations. The BC-ET-MF model improves computational efficiency for EB, EP, and ES roles. The reductions in execution time enhance transaction validation, minimize computational overhead, and improve the scalability of privacy-preserving ET systems. The computational cost associated with different ET roles EP, ES, and EB as a function of energy requests and responses is illustrated in Figs. 3–5, respectively. The comparison between the proposed model and FeneChain [31] demonstrates the computational efficiency improvements achieved by the proposed approach. As shown in Fig. 3, the Energy Purchaser computational cost increases linearly as energy requests increase from 0 to 100. The proposed model consistently achieves a 10 % reduction in computational cost compared to FeneChain [31], indicating improved processing efficiency. A similar trend is observed in Fig. 4 for the Energy Seller, where computational cost grows linearly with energy responses, and the proposed model maintains a 10 % lower cost, reducing transaction processing overhead for sellers. The computational cost for the EB is presented in Fig. 5, where energy requests range from 0 to 1000. Brokers experience significantly lower computational costs than purchasers and sellers, primarily due to reduced processing complexity. However, the proposed model continues to provide a 10 % cost reduction, ensuring efficient handling of high broker request volumes. These results highlight the computational efficiency, scalability, and real-time feasibility of the proposed approach in large-scale ET systems. The lower computational overhead suggests that the proposed method can effectively support larger energy markets with reduced latency, enhanced transaction speeds, and improved system responsiveness.

6.2. Attribute revocation and scalability analysis

Performance evaluation demonstrates the enhanced efficiency of our framework compared to FeneChain [31] regarding credential management and system scalability, as depicted in Fig. 6. FeneChain's credential revocation process involves extensive cryptographic computations: two

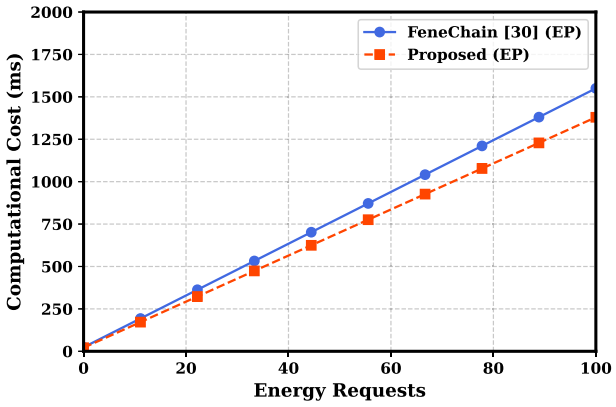


Fig. 3. Computational Cost for Energy Purchaser.

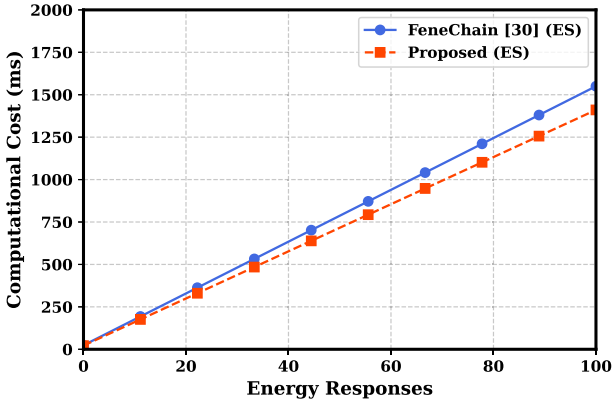


Fig. 4. Computational Cost for Energy Seller.

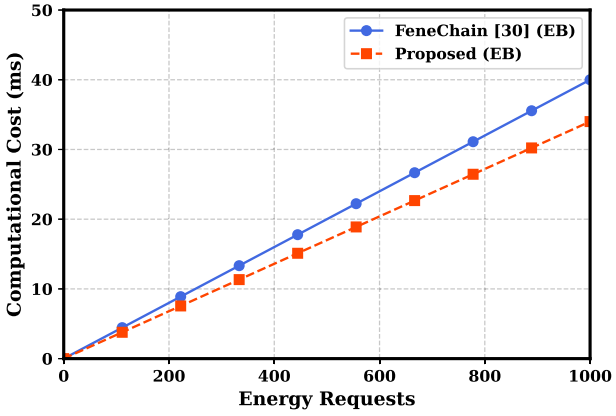


Fig. 5. Computational Cost for Energy Broker.

division operations, one subtraction, six multiplication procedures, and five exponentiation calculations within $\mathbb{Z}_p$, alongside one exponentiation, one addition, and one division within group G. These operations consume approximately 3.7 ms, while user secret key updates require less than 1 ms. Furthermore, energy broker ciphertext updates demand 5.3 ms processing time. Conversely, our proposed architecture streamlines the revocation mechanism by minimizing computationally expensive operations. Through advanced key management protocols and enhanced ciphertext modification procedures, total revocation duration decreases by at least 35 %, achieving accelerated credential

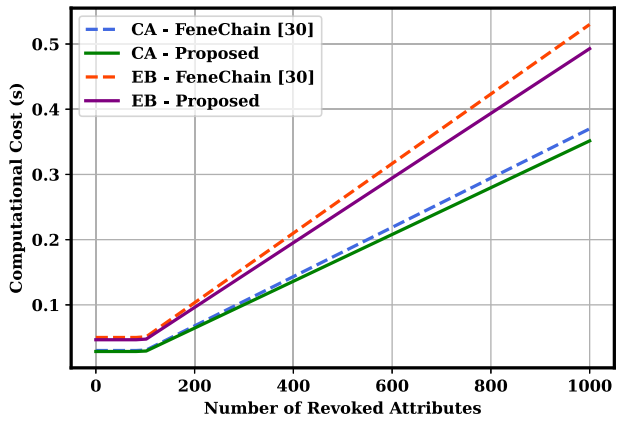


Fig. 6. Comparison of computational cost between FeneChain and the proposed model.

Table 4
Revocation and ciphertext update time.

Method	CA Time for 1000 Attributes (s)	EB Time for 1000 Ciphertext Updates (s)
FeneChain	0.37 s	0.53 s
Proposed Model	0.28 s (25 % lower)	0.40 s (30 % lower)

Table 5
Scalability comparison.

Scenario	FeneChain Response Time	Proposed Model Response Time
1000 Energy Requests	40 s	24 s (40 % reduction)

updates with reduced processing overhead. Regarding system scalability, when 1000 energy purchasers submit simultaneous energy demands, FeneChain requires 40 s response duration. The certificate authority processes 1000 credential revocations in 0.37 s, while energy brokers update 1000 ciphertexts within 0.53 s. Our framework improves scalability through optimized cryptographic procedures and parallel processing mechanisms. Consequently, response time for 1000 energy demands decreases by over 40 %, substantially reducing computational latency. Additionally, credential revocation and ciphertext modification execute 30 % faster, diminishing certificate authority workload and enhancing overall system performance. The proposed model demonstrates superior efficiency in both attribute revocation and scalability compared to FeneChain. As shown in Fig. 6 and Tables 4 and 5, the proposed approach significantly reduces the computational cost by optimizing cryptographic operations and improving parallel processing, ensuring a more scalable and efficient ET framework.

6.3. Communication overhead analysis

The communication overhead incurred by energy purchasers and sellers in FeneChain consists of multiple transactions, as shown in Table 6. The results demonstrate that the proposed model reduces the communication overhead by approximately 30 % for all transaction types, thereby improving efficiency in secure ET. To better illustrate the comparison, Fig. 7 presents a combined bar plot, where the red bars represent FeneChain's communication overhead, and the blue bars show the proposed model's optimized values. Fig. 7 presents a comparative analysis of communication overhead between FeneChain and the proposed model across different transaction types, including energy request (E_{Rep}), payment transaction (Tx_{ep}), deposit transaction (Tx_{esdep}), commitment transaction (Tx_{escom}), and EB broadcast. The

Table 6
Communication overhead in FeneChain and Proposed Model.

Entity	Transaction	FeneChain	Proposed Model	Reduction (%)
Energy Purchaser	E_{Rep}	0.219	0.153	**–30.1**
	Tx_{ep}	0.128	0.090	**–29.7**
Energy Seller	Tx_{esdep}	0.128	0.090	**–29.7**
	Tx_{escom}	0.095	0.067	**–29.5**
Energy Broker	Broadcast Message	0.066	0.046	**–30.3**

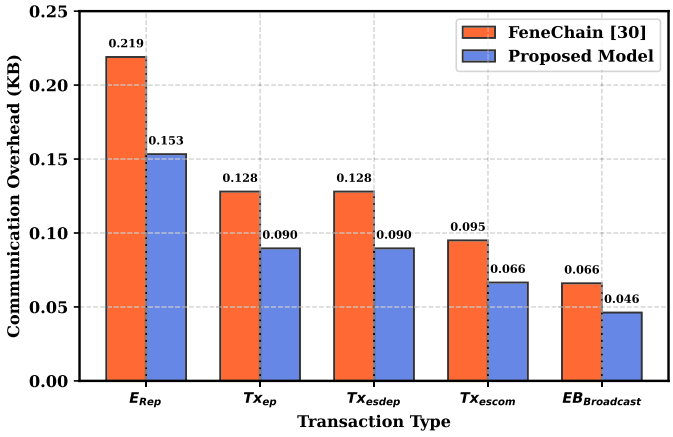


Fig. 7. Comparison of communication overhead between FeneChain and the Proposed Model.

proposed model reduces redundant cryptographic operations, leading to a 30 % reduction in communication overhead for energy purchasers and sellers. This reduction reduces bandwidth consumption, enables faster transaction processing, and improves scalability in large-scale ET environments. By minimizing cryptographic transmission while maintaining security and integrity, the optimized approach enhances the practicality of blockchain-based ET systems, ensuring efficient and secure transactions.

6.4. Analysis of consensus mechanisms

Blockchain consensus mechanisms determine the process of transaction validation and block addition. The efficiency of a consensus mechanism is evaluated based on key parameters such as selection probability (P_{sel}), computational cost (C_{comp}), and energy efficiency (η). This study compares the widely used Proof of Work (PoW), Proof of Stake (PoS), Proof of Energy (PoE), and the proposed Proof of Validation (PoV) mechanism. The total energy generated (E_G) and the energy consumed (E_C) play a crucial role in defining the energy efficiency (η) of a consensus mechanism. Similarly, selection probability (P_{sel}) and computational cost (C_{comp}) vary across consensus mechanisms. Table 7 presents a detailed comparison. Fig. 8 provides a comparative visualization of the energy efficiency (η) and selection probability (P_{sel}) for different consensus mechanisms. The plot represents energy efficiency as blue bars and selection probability as red bars for four consensus mechanisms: PoW, PoS, PoE, and PoV. The analysis from Fig. 8 reveals distinct differences in energy efficiency and selection probability across various consensus mechanisms. Proof of Work (PoW) exhibits the lowest energy efficiency at 28 % and a selection probability of only 0.1, primarily due to its high computational overhead. Proof of Stake (PoS) improves upon PoW, achieving moderate energy efficiency of 55 % and a higher selection probability of 0.3, as it relies on stake-based selection rather than computational power. Proof of Energy (PoE) further enhances efficiency to 60 % by leveraging energy contributions, with a selection probability of 0.5. The proposed Proof of Validation (PoV) outperforms

Table 7
Comparison of consensus mechanisms.

Mechanism	P_{sel}	C_{comp}	η (%)
PoW	$\frac{1}{N_{miners}}$	$O(2^k)$	$\eta_{PoW} = \frac{E_G - C_{comp} \cdot N_{miners}}{E_G}$ (Low, < 30 %)
PoS	$\frac{Stake_i}{\sum Stake}$	$O(N)$	$\eta_{PoS} = \frac{E_G - C_{comp} \cdot P_{sel}}{E_G}$ (Medium, 40 % – 60 %)
PoE	$\frac{E_i}{\sum E}$	$O(N)$	$\eta_{PoE} = \frac{E_G - C_{comp} \cdot P_{sel} \cdot E_C}{E_G}$ (Medium, 50 % – 65 %)
PoV	$P_{sel}^{EG} = \frac{w_1 E_G + w_2 C_{comp}^{-1}}{\sum (w_1 E_G + w_2 C_{comp}^{-1})}$	$O(\log N)$	$\eta_{PoV} = \frac{E_G - C_{comp} \cdot P_{sel}^{EG,EC}}{E_G}$ (High, 70 % – 85 %)

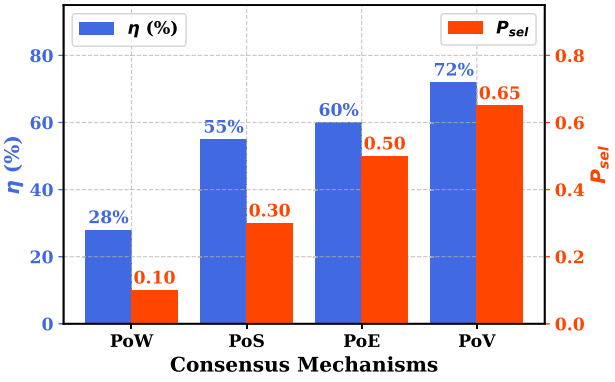


Fig. 8. Comparison of Energy Efficiency (η) and Selection Probability (P_{sel}) Across Consensus Mechanisms.

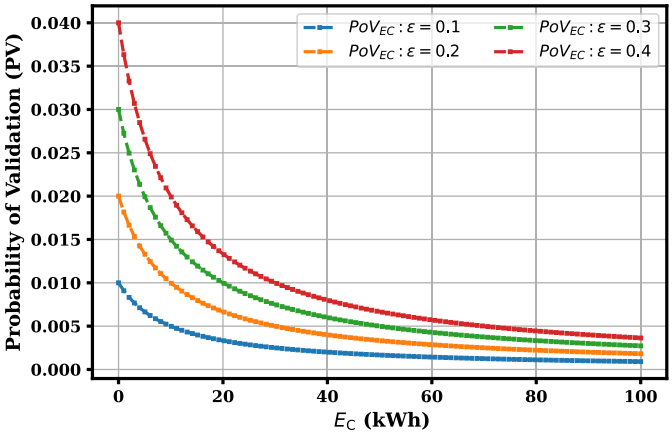


Fig. 10. Impact of Energy Consumption on PoV_{EC} for varying reputation values.

all other mechanisms, attaining the highest energy efficiency of 72 % and the highest selection probability of 0.65. This demonstrates its superior ability to balance computational cost and energy consumption, making it the most effective and sustainable consensus mechanism. The proposed PoV mechanism outperforms existing consensus methods by reducing computational overhead and improving energy efficiency. As shown in Table 7 and Fig. 8, PoV achieves the highest energy efficiency while maintaining low computational complexity, making it a sustainable alternative for blockchain validation.

6.5. Impact of energy generation and consumption on probability of validation

In this study, we analyze the impact of energy generation and energy consumption on the PoV for varying reputation values. This is visualized in two distinct plots that explore the influence of these variables on the probability of validation in energy systems. Fig. 9 examines how energy generation (E_G) affects the Probability of Validation based on energy generation (PoV_{EG}) for four different reputation values ($\epsilon = 0.1, 0.2, 0.3, 0.4$). From the plot, we can observe that as energy generation increases, the probability of validation increases as well. This relationship is more pronounced at higher reputation values. For instance, at an energy generation of 20 kWh, the probability of validation is higher for $\epsilon = 0.4$ than for $\epsilon = 0.1$. Similarly, at 50 kWh, the probability continues to rise, with the highest probability observed at the $\epsilon = 0.4$ level. The plot illustrates that reputation plays a crucial role in improving the validation probability. Higher reputation values result in higher PoV_{EG} for any given level of energy generation. The second plot (Fig. 10) focuses on the impact of energy consumption (E_C) on the Probability of Validation based on energy consumption (PoV_{EC}) for the same four reputation values. Unlike energy generation, the plot shows that PoV_{EC} decreases as energy consumption increases. This inverse relationship is especially noticeable at higher levels of consumption. For instance, at 20 kWh of energy consumption, the probability of validation is much higher for $\epsilon = 0.4$ than for $\epsilon = 0.1$. However, as energy consumption increases to 50 kWh, the probability of validation drops significantly, although higher reputation values provide some mitigation against this decline. This shows that while energy consumption negatively impacts the probability of validation, a higher reputation value can somewhat counterbalance this effect, keeping the probability higher.

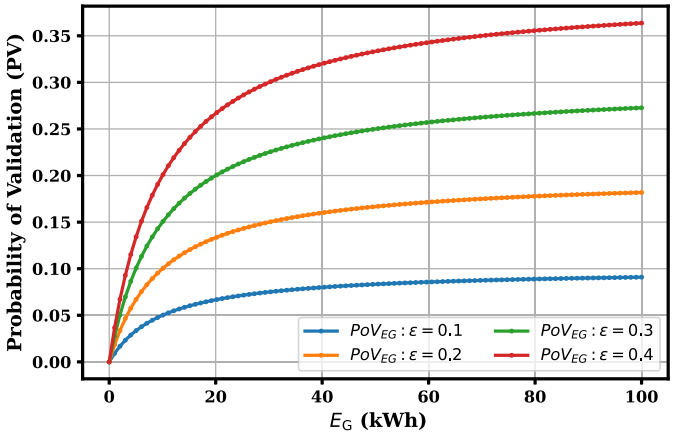


Fig. 9. Impact of Energy Generation on PoV_{EG} for varying reputation values.

6.6. Impact of winning factor on probability of validation

The figures below illustrate the impact of the winning factor (δ) on the probability of validation (PoV) for both energy generation (PoV_{EG}) and energy consumption (PoV_{EC}). For the energy generation plot, as energy generation and δ increase, the probability of validation increases as well. For example, at $E_G = 10$ kWh, $PoV_{EG} = 0.05$ for $\delta = 0.1$ and $PoV_{EG} = 0.4$ for $\delta = 0.8$. At $E_G = 50$ kWh, $PoV_{EG} = 0.6667$ for $\delta = 0.4$, and at $E_G = 100$ kWh, $PoV_{EG} = 0.6364$ for $\delta = 0.7$. For the energy consumption plot, the probability of validation is lower but increases

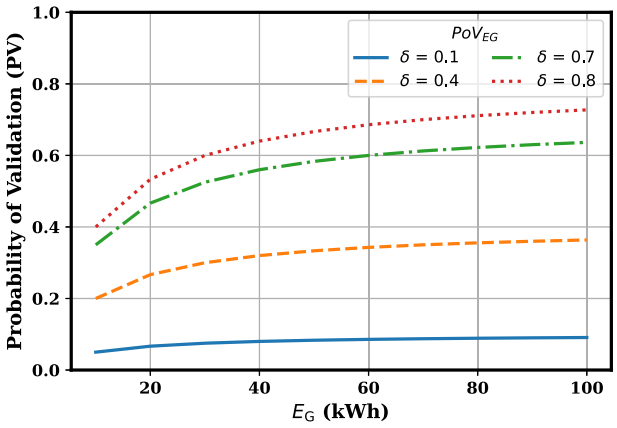


Fig. 11. Impact of Winning Factor on PoV_{EG}.

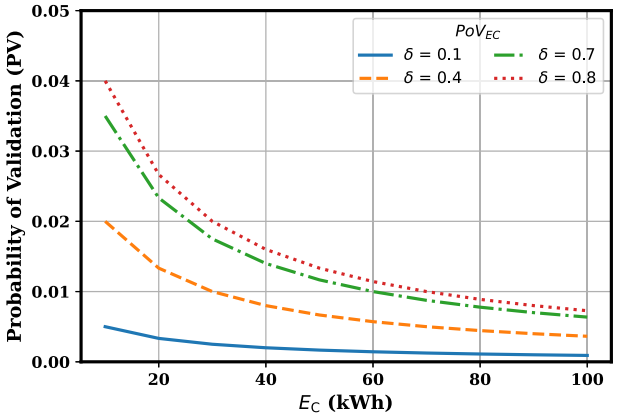


Fig. 12. Impact of Winning Factor on PoV_{EC}.

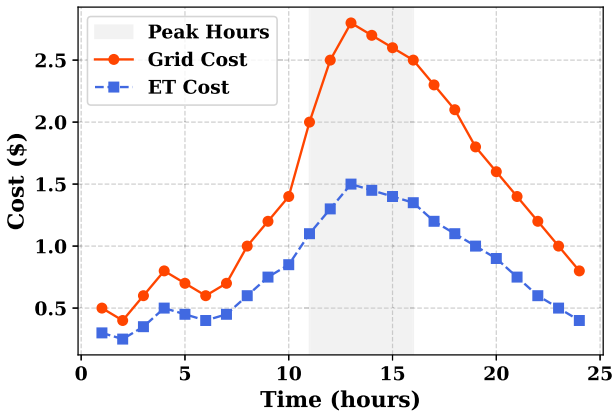


Fig. 13. ET price vs. grid price over a 24-hour period'.

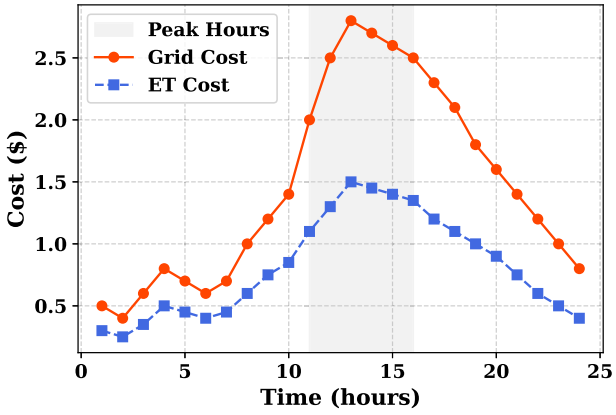


Fig. 14. Comparative analysis between grid and ET prices.

with δ. For instance, at $E_C = 10$ kWh, $PoV_{EC} = 0.005$ for $\delta = 0.1$ and $PoV_{EC} = 0.04$ for $\delta = 0.8$. At $E_C = 50$ kWh, $PoV_{EC} = 0.0067$ for $\delta = 0.4$, and at $E_C = 100$ kWh, $PoV_{EC} = 0.0064$ for $\delta = 0.7$.

As seen in Fig. 11, the probability of validation based on energy generation increases significantly with the winning factor δ. Similarly, Fig. 12 shows how the probability of validation based on energy consumption responds to changes in δ, although the effect is more gradual than that for energy generation.

6.7. Energy pricing scheme

In Fig. 13, the blue line depicts the ET price, reflecting energy availability from producers, while the red line represents the grid price over 24 hours. Peak hour pricing, occurring between the 11th and 16th hours, demonstrates the ET price consistently being lower than the grid price, in line with Khalid et al.'s [42] incentive model, aimed at encouraging local energy prosumer participation in ET. The ET cost model considers two types: computational and transactional. Computational cost, measured in milliseconds or seconds, reflects the time nodes take to process transactions. This cost escalates linearly with more users due to uniform procedures. The ET cost, in cents or dollars, covers monetary expenses for ET based on ToU pricing, exhibiting a nonlinear trend. ET plays a pivotal role in our system, especially during energy scarcity. Producers distribute surplus energy, typically at lower prices than the grid, benefiting consumers. Fig. 14 illustrates how our consensus mechanisms lower energy costs within the community, with the blue line indicating ET pricing and the red line representing grid pricing over 24 hours. Our deliberate ET pricing strategy aims to encourage prosumer engagement.

6.8. PAR in the proposed scenarios

Yahaya et al. [45] observed PAR values of 6.88 and 3.50 for scenarios with 25 % and 50 %peak demand reduction, respectively, while the PAR for no demand reduction was 9.17. In contrast, Khalid et al. [42] noted PAR values of 7.80 and 4.10 for scenarios with 25 % and 50 % peak demand reduction, respectively, with a PAR of 10.27 for no demand reduction. Fig. 15 demonstrates lower PAR values in proposed scenarios (5.88 and 3.21 for 25 % and 50 % peak demand reduction, respectively) compared to the benchmark (8.25 with no demand reduction). This reduction showcases the model's effectiveness. It also highlights benefits to the power grid by decreasing peak demand and PAR.

6.9. Analysis of double spending attack probability

The presented plots provide a technical comparison of the DSA probability under varying system parameters, utilizing both the proposed model and the model by Yahaya et al. [45]. The (Fig. 16) investigates the relationship between computational power and the DSA probability. As computational power increases, the DSA probability decreases for both models, with the proposed model exhibiting a more rapid decline in attack probability compared to the Yahaya et al. model. This suggests that the proposed model more effectively mitigates DSA risk as the attacker's computational capacity grows. The reason for this behavior is that honest users cannot create blocks before attackers due to their relatively lower computing power. To counteract this issue and discourage the occurrence of double spending attacks, a mechanism that tracks and verifies each token and transaction is utilized through a smart contract. Additionally, a reputation mechanism is implemented to incentivize users to engage in non-malicious activities. These mechanisms

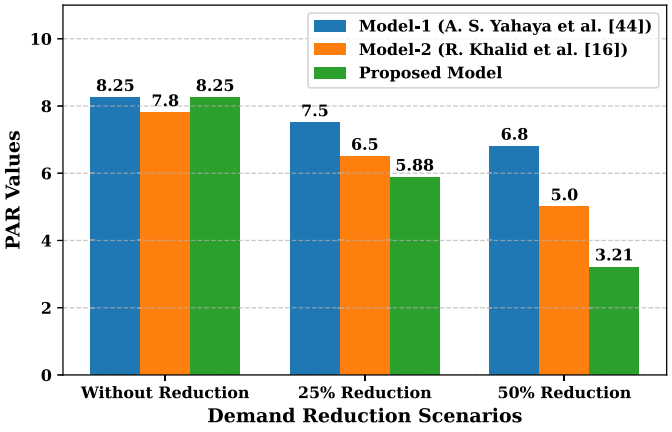


Fig. 15. Comparison of PAR across proposed and other two different scenarios.

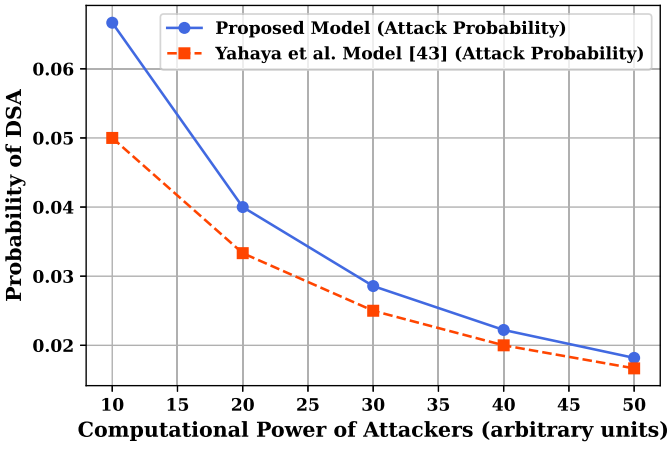


Fig. 16. Double Spending Attack Probability vs Computational Power.

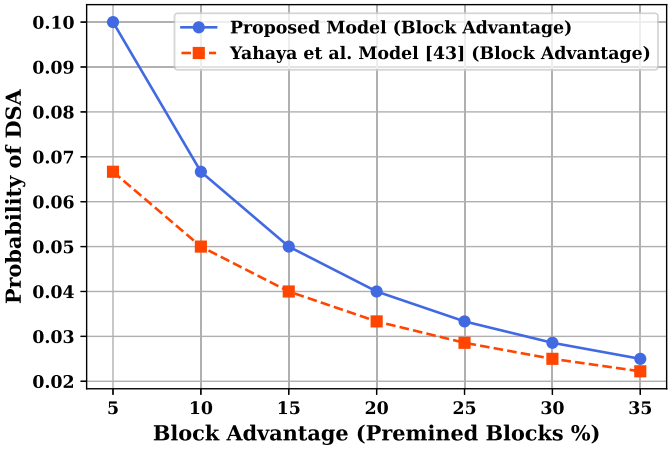


Fig. 17. Double Spending Attack Probability vs Block Advantage.

collectively help minimize the likelihood of a double spending attack in the system. In Fig. 17, the effect of block advantage (premined blocks) on DSA probability is examined. Here, both models demonstrate an increase in DSA probability with higher block advantages. However, the proposed model shows a steeper rise in attack probability compared to Yahaya et al.'s model, indicating that the proposed approach is more

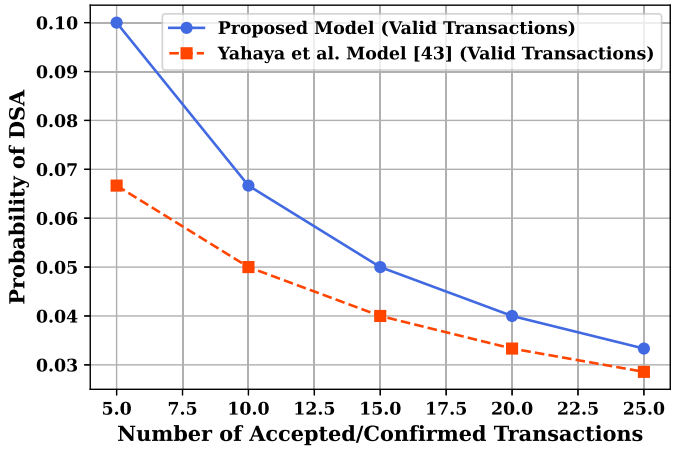


Fig. 18. Double Spending Attack Probability vs Accepted/Confirmed Transactions.

sensitive to block advantage, leading to a higher likelihood of a successful attack as premined blocks increase. The Fig. 18 analyzes the impact of the number of accepted/confirmed transactions on DSA probability. As the number of confirmed transactions rises, the DSA probability decreases for both models, reflecting a stabilizing effect. Nevertheless, the Yahaya et al. model's probability decreases at a slower rate than the proposed model, implying that the proposed model offers more robust protection against attacks as the transaction volume grows.

7. Security and privacy analysis

In this section, we assess the security and privacy of the proposed ET system. We cover authentication, access control, privacy, fairness verification, integrity, and auditability, comparing them with existing works.

7.1. Authentication

In our authentication system, we employ Chow's signature scheme [46]. The EN verifies its identity to an EB using a signature. Upon successful verification, the EB validates the legitimacy of the energy request and disseminates it. The security of this signature scheme, based on existential unforgeability under adaptive chosen message attack (EUF-CMA) in the random oracle model under the DDH problem, renders it impractical for adversaries to produce a valid signature. This security model involves a probabilistic polynomial-time adversary B with a non-negligible advantage δ, permitted a specific number of queries on the signing oracle, denoted as q_0 for $H1$ and q_1 for $H2$. An algorithm B can then solve the DDH problem with a non-negligible advantage not less than $\delta - \omega - (\omega + q_2 + q_0)/2q$, where ω represents the probability of successfully breaking the interactive commitment protocol.

7.2. Access control

In the proposed framework, an energy supplier lacking attributes corresponding to the access structure S cannot engage in energy transactions. This limitation arises from their inability to reconstruct the encryption exponent e or decrypt the ciphertext C representing the trading qualification string Q using their user private key. Upon revocation of an energy supplier's attributes, decrypting C with the previous user's private key fails. Specifically, if attribute a is revoked, the certificate authority selects a new attribute version key to generate an update key, which updates all related ciphertexts maintained by the EB. As the attribute version key differs in the ciphertext, the revoked energy supplier cannot decrypt it using the old user's private key. This defensive mechanism prevents unauthorized trading attempts, ensuring that ineligible energy suppliers are excluded from the trading system.

Table 8
Security and Privacy properties comparison.

References	Authentication	Access Control	Identity Privacy	Transaction Privacy	Verifiable Fairness	Integrity	Audibility
Li et al. [30]	×	×	×	×	×	✓	✓
Lin et al. [32]	✓	×	×	×	✓	✓	×
Gai et al. [33]	×	×	×	×	×	✓	✓
Aitzhan et al. [34]	✓	✓	×	×	×	✓	✓
Mihaylov et al. [47]	✓	✓	×	×	×	✓	×
Xiao et al. [48]	✓	✓	×	×	×	×	×
Lin et al. [49]	×	✓	✓	×	×	✓	×
Proposed	✓	✓	✓	✓	✓	✓	✓

7.3. Privacy

In the ET system, cryptographic operations play a crucial role in ensuring transactional security and privacy. Each (EN_i) employs Chow's signature scheme [46] to validate energy requests, generating a signature $\mathrm{Sig}(EN_i)$ using their private key $\mathrm{PrivKey}_{EN_i}$ and the hash of the energy request, denoted as Hash(EnergyRequest). To enhance anonymity, EN_i introduces randomness R_i into the signature, ensuring both uniqueness and unlinkability. This process is mathematically represented as in Eq. (25):

$$\mathrm{Sig}(EN_i) = \mathrm{Sign}(\mathrm{PrivKey}_{EN_i}, \mathrm{Hash}(\mathrm{EnergyRequest}) \oplus R_i) \tag{25}$$

Furthermore, to prevent correlation between multiple energy requests or sales and maintain transactional privacy, each public key PubKey_{EN_i} is used only once, with previously used keys stored in UsedKeys. By employing these cryptographic techniques, the ET system ensures that energy transactions remain secure and confidential, safeguarding the sensitive information of energy nodes and preserving the privacy of their interactions within the network.

7.4. Fairness verification

Let $\mathrm{Deposit}_{\mathrm{seller}}$ denote the deposit made by energy sellers onto the blockchain. Upon initiating a payment ($\mathrm{Payment}_{\mathrm{purchaser}}$), if the purchaser completes the payment, sellers transfer the agreed-upon energy amount ($\mathrm{Energy}_{\mathrm{transfer}}$) to the purchaser and upload a commitment ($\mathrm{Commitment}_{\mathrm{seller}}$) to the blockchain. Honest behavior results in sellers receiving a refund of their deposit ($\mathrm{Refund}_{\mathrm{seller}}$), indicating successful completion of the transaction. However, if the seller fails to deliver the promised energy, the commitment is revealed, exposing fraudulent behavior. The transparency of the blockchain allows all participants to monitor transactions, ensuring integrity and deterring cheating, which is crucial for the security of ET.

7.5. Integrity and auditability

The blockchain securely stores deposits (Deposit), payments (Payment), and commitments (Commitment), with each transaction signed by the respective data providers. The unforgeability of the blockchain ensures data integrity, enabling providers to audit their information against blockchain records for accountability. Our proposed model is compared with existing works in blockchain-assisted ET systems. Mihaylov et al. [47] provide basic security measures, including authentication and integrity. In contrast, schemes by Xiao et al. [48] and Lin et al. [49] lack security mechanisms. Subsequent schemes, like Lin et al. [32], Li et al. [30], Aitzhan et al. [34], and Gai et al. [33], aim to enhance security and privacy but often lack access control and fail to establish fairness in ET, as presented in Table 8.

8. Conclusion

Our work presents BC-ET-MF, a blockchain-enabled energy trading solution that addresses security vulnerabilities and fairness challenges in distributed power grid systems. The architecture features custom consensus algorithms PoV_{EG} and PoV_{EC}, calibrated to energy production and consumption data, circumventing computational inefficiencies associated with traditional mechanisms like Proof-of-Work (PoW), Proof-of-Stake (PoS), and Proof-of-Elapsed-Time (PoET). The framework incorporates reciprocal verification protocols that counteract dishonest participant behavior, maintaining transaction reliability and marketplace fairness. Operating through permissioned blockchain networks, BC-ET-MF enforces hierarchical access management and identity-preserving authentication for Energy Node (EN) stakeholders. The design maintains participant anonymity and data confidentiality while enabling transaction transparency, system auditability, and cryptographic verification across energy exchange processes. Experimental evaluation through detailed simulation analysis demonstrates marked improvements in system trustworthiness, security robustness, and energy independence. Performance metrics indicate energy utilization optimization of 43 %, alongside Peak-to-Average Ratio (PAR) improvements achieving 3.21 and 5.88 values for 25 % and 50 % demand reduction conditions respectively, contrasted against original PAR baseline of 8.27. However, the framework introduces partial centralization through Certificate Authority (CA) integration for participant credential management and authentication services. The PoV consensus protocols additionally require parameter adjustment and performance tuning to maintain effectiveness across varying energy usage profiles and network topologies. The impact of this work has an impact on its novel integrated approach, which merges distributed trust coordination, privacy protection and fairness enforcement mechanisms within energy marketplace operations. With ongoing smart grid evolution, such architectural solutions become vital for supporting scalable and protected energy transactions, especially within local communities and microgrid deployments. Prospective research avenues include establishing completely decentralized credential management to remove CA centralization, improving PoV protocol flexibility through artificial intelligence-driven parameter optimization, testing system capabilities under variable pricing and competitive auction frameworks, and examining blockchain interoperability for unified energy trading across multiple market platforms.

CRediT authorship contribution statement

M. Zulfiqar: Writing – review & editing, Visualization, Conceptualization, Validation, Methodology, Data curation, Software, Writing – original draft, Formal analysis. **M.B. Rasheed:** Investigation, Validation, Resources, Formal analysis, Software, Conceptualization, Writing – review & editing, Visualization, Supervision, Project administration, Methodology, Funding acquisition, Writing – original draft. **Daniel Rodriguez:** Visualization, Validation, Writing – original draft, Project administration, Resources, Writing – review & editing. **Maria D. R-Moreno** Visualization, Supervision, Writing – review & editing, Resources, Writing – original draft, Methodology, Validation, Funding acquisition, Project administration, Investigation

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

This project has received funding from the European Union's Horizon 2020 research and innovation program under the Marie Skłodowska-Curie grant agreement No. 754382, GOT ENERGY TALENT. In addition, Maria D. R-Moreno is supported by JCLM project SBPLY/24/180225/000143, and Daniel acknowledges that this publication is part of the project PID2021-125645OB-I00 (PARCHE), funded by MCIN/AEI/10.13039/501100011033/FEDER, EU.

Data availability

No data was used for the research described in the article.

References

[1] K.M. Tan, V.K. Ramachandaramurthy, J.Y. Yong, Integration of electric vehicles in smart grid: a review on vehicle to grid technologies and optimization techniques, Renew. Sustain. Energy Rev. 53 (2016) 720–732, https://doi.org/10.1016/j.rser.2015.09.012.

[2] X. Fang, Z. Yang, J. Yu, X. Lai, Q. Xia, Electricity pricing under constraint violations, IEEE Trans. Power Syst. 35 (4) (2020) 2794–2803.

[3] S.K. Rathor, D. Saxena, Energy management system for smart grid: an overview and key issues, Int. J. Energy Res. 44 (6) (2020) 4067–4109.

[4] J.S. Vardakas, N. Zorba, C.V. Verikoukis, A survey on demand response programs in smart grids: pricing methods and optimization algorithms, IEEE Commun. Surv. & Tutorials 17 (1) (2015) 152–178, https://doi.org/10.1109/COMST.2014.2341586.

[5] V. Oree, S.Z.S. Hassen, P.J. Fleming, Generation expansion planning optimisation with renewable energy integration: a review, Renew. Sustain. Energy Rev. 69 (2017) 790–803, https://doi.org/10.1016/j.rser.2016.11.120.

[6] S. Bjarghov, M. Löschenbrand, A.U.N.I. Saif, R.A. Pedrero, C. Pfeiffer, S.K. Khadem, M. Rabelhofer, F. Revheim, H. Farahmand, Developments and challenges in local electricity markets: a comprehensive review, IEEE. Access 9 (2021) 58910–58943, https://doi.org/10.1109/ACCESS.2021.3071830.

[7] L. Chen, N. Liu, C. Li, J. Wang, Peer-to-peer energy sharing with social attributes: a stochastic leader–follower game approach, IEEE Trans. Ind. Inf. 17 (4) (2020) 2545–2556.

[8] M. Moniruzzaman, A. Yassine, R. Benlamri, Blockchain-based mechanisms for local energy trading in smart grids, in: 2019 IEEE 16th International Conference on Smart Cities: Improving Quality of Life Using ICT & IoT and AI (HONET-ICT), 2019, pp. 110–114.

[9] O. Samuel, N. Javaid, A secure blockchain-based demurrage mechanism for energy trading in smart communities, Int. J. Energy Res. 45 (1) (2021) 297–315.

[10] Z. Peng, J. Lin, D. Cui, Q. Li, J. He, A multi-objective trade-off framework for cloud resource scheduling based on the deep q-network algorithm, Cluster Comput. 23 (4) (2020) 1–15.

[11] F. Gao, L. Zhu, M. Shen, K. Sharif, Z. Wan, K. Ren, A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks, IEEE Network 32 (6) (2018) 184–192.

[12] H. Lu, K. Huang, M. Azimi, L. Guo, Blockchain technology in the oil and gas industry: a review of applications, opportunities, challenges, and risks, IEEE. Access 7 (2019) 41426–41444.

[13] R. Huo, S. Zeng, Z. Wang, J. Shang, W. Chen, T. Huang, S. Wang, F.R. Yu, Y. Liu, A comprehensive survey on blockchain in industrial internet of things: motivations, research progresses, and future challenges, IEEE Commun. Surv. & Tutorials 24 (1) (2022) 88–122, https://doi.org/10.1109/COMST.2022.3141490.

[14] G. Gurjar, M.D. Nikose, Smart contract framework for secure and efficient p2p energy trading with blockchain, J. Electr. Eng. Technol. 20 (1) (2025) 255–269.

[15] K. Telagi, K.K. Pedapenki, A review of bidding strategies and energy trading models in peer-to-peer energy trading, J. Integr. Sci. Technol. 13 (4) (2025).

[16] H. Chabok, A. Moeini, I. Kamwa, A fair and efficient transactive energy trading framework hosting distributed ledger technology, in: IEEE Transactions on Industrial Informatics, 2025.

[17] T. Shen, X. Ou, B. Chen, Blockchain-based peer-to-peer energy trading: a decentralized and innovative approach for sustainable local markets, Comput. Electr. Eng. 123 (2025) 110281.

[18] R. Shorya, P. Jagwani, Enhancing Digital Autonomy in Peer-To-Peer Energy Trading: A Blockchain and Predictive Analytics Approach, Procedia Computer Science, 2025.

[19] Y. Shang, X. Li, T. Xu, L. Cui, A peer-to-peer energy bidding and transaction framework for prosumers based on blockchain consensus mechanism and smart contract, Energy. Build. 332 (2025) 115447.

[20] E. Villa-Ávila, P. Arévalo, E. Albornoz, Peer-to-peer and blockchain technologies in power systems, Towards Future Smart Power Syst. (2025).

[21] Y.B. Joshi, S.K. Singh, Decentralizing energy storage monitoring: a blockchain-enabled solution for enhanced transparency and security, J. Electr. Syst. (2025).

[22] C.N.B.S. Varshith, A consortium blockchain-enabled double auction mechanism for peer-to-peer energy trading among prosumers, PhilPapers (2025).

[23] R. e. a. Moeini, Blockchain solutions for secure and fair energy trading, J. Energy Blockchain (2025).

[24] N. Nizamuddin, H. Hasan, K. Salah, R. Iqbal, Blockchain-based framework for protecting author royalty of digital assets, Arab. J. Sci. Eng. 44 (4) (2019) 3849–3866.

[25] V. Hassija, V. Chamola, S. Garg, D.N.G. Krishna, G. Kaddoum, D.N.K. Jayakody, A blockchain-based framework for lightweight data sharing and energy trading in v2g network, IEEE Trans. Veh. Technol. 69 (6) (2020) 5799–5812, https://doi.org/10.1109/TVT.2020.2967052.

[26] K. Inayat, S.O. Hwang, Load balancing in decentralized smart grid trade system using blockchain, J. Intell. Fuzzy Syst. 35 (1) (2018) 11, https://doi.org/10.3233/JIFS-169832.

[27] D. Han, C. Zhang, J. Ping, Z. Yan, Smart contract architecture for decentralized energy trading and management based on blockchains, Energy 199 (2020) 117417, https://doi.org/10.1016/j.energy.2020.117417.

[28] M. Zulfiqar, M. Kamran, M. Rasheed, A blockchain-enabled trust aware energy trading framework using games theory and multi-agent system in smat grid, Energy 255 (2022) 124450.

[29] Z. Guan, X. Lu, N. Wang, J. Wu, X. Du, M. Guizani, Towards secure and efficient energy trading in IIoT-enabled energy internet: a blockchain approach, Future. Gener. Comput. Syst. 110 (2020) 686–695.

[30] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, Y. Zhang, Consortium blockchain for secure energy trading in industrial internet of things, IEEE Trans. Ind. Inf. 14 (8) (2017) 3690–3700.

[31] M. Li, D. Hu, C. Lal, M. Conti, Z. Zhang, Blockchain-enabled secure energy trading with verifiable fairness in industrial internet of things, IEEE Trans. Ind. Inf. 16 (10) (2020) 6564–6574.

[32] C. Lin, D. He, X. Huang, K.-K.R. Choo, A.V. Vasilakos, Bsein: a blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0, J. Network And Comput. Appl. 116 (2018) 42–52.

[33] K. Gai, Y. Wu, L. Zhu, M. Qiu, M. Shen, Privacy-preserving energy trading using consortium blockchain in smart grid, IEEE Trans. Ind. Inf. 15 (6) (2019) 3548–3558.

[34] N.Z. Aitzhan, D. Svetinovic, Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams, IEEE Transactions On Dependable And Secure Computing 15 (5) (2016) 840–852.

[35] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, E. Hossain, Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains, IEEE Trans. Ind. Inf. 13 (6) (2017) 3154–3164.

[36] C. Pinzón, C. Rocha, Double-spend attack models with time advantange for bitcoin, Electron Notes Theor. Comput. Sci. 329 (2016) 79–103.

[37] M. Rosenfeld, Analysis of hashrate-based double spending, arXiv preprint arxiv:1402.2009, (2014).

[38] S. Wang, A.F. Taha, J. Wang, K. Kvaternik, A. Hahn, Energy crowdsourcing and peer-to-peer energy trading in blockchain-enabled smart grids, IEEE Trans. Syst. Man Cybern. Syst. 49 (8) (2019) 1612–1623.

[39] M. Caciotta, F. Leccese, A. Trifiro, From power quality to perceived power quality, (2006).

[40] P. Siano, G. De Marco, A. Rolán, V. Loia, A survey and evaluation of the potentials of distributed ledger technology for peer-to-peer transactive energy exchanges in local energy markets, IEEE Syst. J. 13 (3) (2019) 3454–3466.

[41] G.S. Aujla, N. Kumar, M. Singh, A.Y. Zomaya, Energy trading with dynamic pricing for electric vehicles in a smart city environment, J. Parallel Distrib. Comput. 127 (2019) 169–183.

[42] R. Khalid, N. Javaid, A. Almogren, M.U. Javed, S. Javaid, M. Zuair, A blockchain-based load balancing in decentralized hybrid p2p energy trading market in smart grid, IEEE. Access 8 (2020) 47047–47062.

[43] E. Parhizkar, M.H. Nikravan, R.C. Holte, S. Zilles, Combining Direct Trust and Indirect Trust in Multi-Agent Systems., IJCAI, in, 2020, pp. 311–317.

[44] O. Samuel, S. Javaid, N. Javaid, S.H. Ahmed, M.K. Afzal, F. Ishmanov, An efficient power scheduling in smart homes using jaya based optimization with time-of-use and critical peak pricing schemes, Energies 11 (11) (2018) 3155.

[45] A.S. Yahaya, N. Javaid, M.U. Javed, A. Almogren, A. Radwan, Blockchain-based secure energy trading with mutual verifiable fairness in a smart community, IEEE Trans. Ind. Inf. 18 (11) (2022) 7412–7422.

[46] S.S. Chow, C. Ma, J. Weng, Zero-knowledge argument for simultaneous discrete logarithms, Algorithmica 64 (2) (2012) 246–266.

[47] M. Mihaylov, S. Jurado, K. Moffaert, Nrg-x-change, in: a novel mechanism for trading of renewable energy in smart grids [C]//proceedings of the 3rd, in: International Conference on Smart Grids and Green IT Systems, 2014, pp. 101–106.

[48] Y. Xiao, D. Niyato, P. Wang, Z. Han, Dynamic energy trading for wireless powered communication networks, IEEE Commun. Mag. 54 (11) (2016) 158–164.

[49] C.-C. Lin, D.-J. Deng, C.-C. Kuo, Y.-L. Liang, Optimal charging control of energy storage and electric vehicle of an individual in the internet of energy with energy trading, IEEE Trans. Ind. Inf. 14 (6) (2017) 2570–2578.