TREND ACADEMIC STUDIES IN ENGINEERING



All Sciences Academy

TREND ACADEMIC STUDIES IN ENGINEERING

Editor
Asst. Prof. Dr. Umut ÖZKAYA

Trend Academic Studies in Engineering
Editor: Asst. Prof. Dr. Umut ÖZKAYA

Design: All Sciences Academy Design
Published Date: March 2025
Publisher's Certification Number: 72273
ISBN: 978-625-5954-95-4

© All Sciences Academy

www.allsciencesacademy.com
allsciencesacademy@gmail.com

CONTENT

1. Chapter **6**

Microplastic Pollution in Soil Ecosystems: Biological Disruptions and Interactions with Heavy Metals

Fatma Olcay TOPAC, Melike YALILI KILIC, Arzu TEKSOY, Sevil ÇALIŞKAN ELEREN

2. Chapter **22**

Blockchain-Based Dual-Layer System Model for Enhanced Security in Energy Trading

Zeynep TANIŞ, Ali DURUSU

3. Chapter **39**

Comparative Analysis of Cameras Compatible with Image Processing Supported Developer Cards

Kamil Aykutalp GÜNDÜZ, Ertuğrul TEKİN, Mikail AYDIN

4. Chapter **68**

Analysis of the Resistance of High Performance Concrete to Acidic Environments and Sorptivity

Tarek HADJI, Ahmed ATTIA, Taha Hocine DOUARA, Salim GUETTALA, Michèle QUÉNEUDEC

5. Chapter **88**

Design and Simulation of Rectangular Patch Antenna for Brain Monitoring Methods

Havva Demet ISLER, Ozlem COSKUN

6. Chapter **97**

Seismic Performance and Structural Assessment of Historical Yali Mosque in Izmir, Türkiye

Pınar USTA EVCI, Elifnur ŞAKALAK, Ali Ekber SEVER

7. Chapter **113**
Timer Modes for ATmega328P Microcontroller
Serhat KÜÇÜKDERMENCİ

Blockchain-Based Dual-Layer System Model for Enhanced Security in Energy Trading

Zeynep TANIŞ[*,1]

Ali DURUSU [2]

[1]Department of Electrical Engineering, Yildiz Technical University, Istanbul, Turkey
[2] Department of Electrical Engineering, Yildiz Technical University, Istanbul, Turkey
[*](zynpctnts@gmail.com) Email of the corresponding author

ABSTRACT

Local energy trading has garnered attention due to its environmental benefits and innovative role in energy management, offering advantages such as the reduction of carbon emissions, ensuring energy supply security, and increasing market competitiveness. However, energy trading among multiple prosumers, particularly in centralized systems, brings about security, privacy, and reliability issues that may lead to single-point failures and high costs. To address these challenges, this study proposes a blockchain-based, dual-layer secure P2P energy trading model. The model enhances security against fraudulent attacks through an authentication layer, while the secure trading layer incorporates an innovative consensus mechanism that minimizes the impact of malicious validators. Additionally, a rewarding mechanism is introduced to encourage prosumer participation. The model aims to raise security, privacy, and reliability standards in energy trading, demonstrating successful performance in terms of trust and data protection.

Keywords – Blockchain, Peer-To-Peer (P2p), Energy Trading, Security, Privacy, Incentive Mechanism.

INTRODUCTION

The increasing number of distributed energy producers and consumers has made Peer-to-Peer (P2P) energy trading based on renewable energy sources increasingly significant. While centralized systems face challenges such as security, cost, and privacy issues, decentralized systems and blockchain technology enable users to conduct transactions directly, offering enhanced security, data integrity, and transaction efficiency [1]. Blockchain, with its immutable transaction records and consensus mechanisms, prevents malicious interventions while ensuring authentication and data security [2]. However, challenges such as user privacy, identity spoofing, and price fluctuations remain unresolved [3]. Local energy usage reduces grid load by minimizing energy losses but requires innovative pricing mechanisms to ensure sustainable trade [4]. Consequently, P2P energy trading forms the foundation of secure, sustainable, and efficient energy systems, yet overcoming challenges such as user privacy, price stability, and trust-building remains critical [5].

This study proposes a novel secure energy trading model to address the security and privacy issues encountered in existing energy trading systems. The proposed model leverages a robust blockchain-based infrastructure to enable prosumers (users who both produce and consume energy) to conduct energy transactions securely, transparently, and with privacy preservation. The primary contributions of this research are as follows:

- A secure and efficient energy trading system has been designed using blockchain technology.
- An off-chain, mutual authentication process has been developed to protect against potential fraud and cyberattacks.
- An incentive mechanism has been introduced to encourage prosumers to contribute more energy, and an effective consensus mechanism has been proposed for the selection of energy validators.
- The theoretical foundations of the proposed model, along with its benefits in terms of security and privacy, have been discussed in detail.

RELATED WORKS

Blockchain has distributed and decentralized structure, provides a verifiable interaction environment among trustless users and is widely utilized in decentralizing energy markets. In this context, the Secure Payment Blockchain framework was developed to address issues such as privacy, transaction load, and reliance on Trusted Third Parties in energy trading, offering a secure platform through atomic meta-transactions and anonymous meter verification [6]. In the Industrial Internet of Things (IoT) environment, the $\mathsf{FeneChain}$ model was proposed to ensure security based on principles of user privacy, energy quality, and fairness, utilizing a consortium blockchain structure and time-bound commitment mechanisms [2]. Blockchain has also been evaluated as a viable solution for data security in the healthcare sector and for managing information stored in the cloud [7]. In decentralized smart grids, transaction security has been ensured through multi-signatures and anonymous messaging [8], while platforms have been proposed to allow users to transparently monitor their electricity consumption [9]. To support renewable energy trading, the NRGcoin digital currency was developed to balance energy production and consumption and facilitate green energy trading [10]. Blockchain-based approaches also offer measures to protect the privacy of trading information and prevent attacks based on geographic location and trading volumes [11]. Simulations conducted with local P2P energy trading platforms have shown that trading has limited effects on network performance [12]. Blockchain-based smart contracts enable direct and reliable trading between producers and consumers [13], supporting energy trading between prosumers and consumers to create a trustworthy trading ecosystem [14]. Furthermore, the consortium blockchain model enhances transparency and security in energy trading by incorporating a proof-of-stake protocol and the "elecoin" cryptocurrency [15].

The rise of distributed energy producers and consumers has made secure P2P energy trading essential. However, public blockchain-based models face security risks due to the lack of authentication, leading to identity spoofing

and eavesdropping attacks. While blockchain enhances transparency and decentralization, it does not fully ensure data security or prevent fraud. Consortium blockchains offer authentication but remain vulnerable to single points of failure. Therefore, integrating blockchain with robust security mechanisms is crucial for developing secure and efficient P2P energy trading platforms.

BLOCKCHAIN TECHNOLOGY

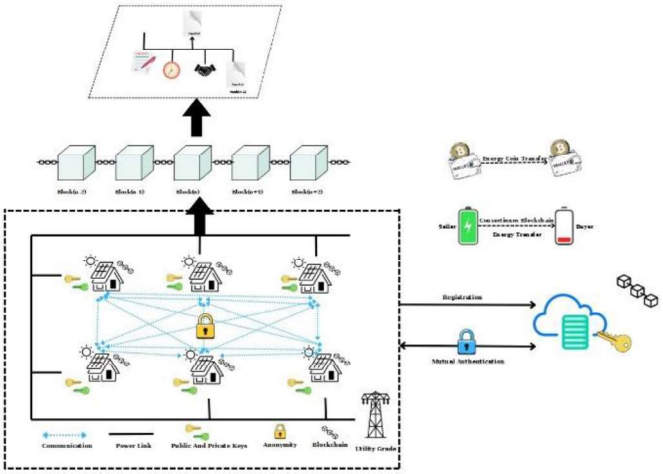
Blockchain technology, developed by Satoshi Nakamoto in 2008, is a distributed ledger designed for secure information sharing without a central authority [1]. Nodes have access and validation rights over the database, while data is secured through public-private key cryptography, digital signatures, and hashing. Blocks are linked via hash pointers to ensure integrity, and consensus algorithms, particularly Proof of Work (PoW), verify and permanently add blocks through high computational power. This structure provides transparency, decentralization, and data security [16].

A. Structure and Key Features of the Blockchain System

Blockchain technology can be defined as a distributed ledger system that enables the creation of secure, transparent, and immutable digital records [17]. This technology operates on a network of interconnected nodes, designed to ensure the accuracy and reliability of transactions without the need for a central authority [18]. Blockchain records each transaction in a digitally encrypted format, and these records are stored in a ledger that is accessible and verifiable by all participants [19].

Blockchain technology operates on a decentralized structure, ensuring transaction validation without a central authority [20]. This enhances system reliability by eliminating single points of failure and strengthening security. The technology fosters trust through immutable transaction records and has been shown to reduce costs and improve financial inclusion. Additionally, its role in smart grid systems has been analyzed through conceptual models, highlighting decentralization, trust, and incentivization [21]. Blockchain technology ensures the security of transactions and guarantees their immutability through the use of cryptographic algorithms. Each transaction is validated and recorded by all nodes in the network, and once confirmed, it becomes impossible to reverse or alter [22]. The impact of blockchain in providing security, transparency, and efficiency has been highlighted in fields such as smart cities, healthcare, supply chains, and IoT. Specifically, in studies related to cryptocurrency security, it has been emphasized that the distributed structure of blockchain and consensus procedures play a critical role in enhancing security, though issues such as scalability and privacy must also be addressed [23]. Blockchain technology provides transparency by recording

transactions in a publicly accessible manner, allowing them to be verified by network participants. This feature is crucial, particularly in increasing the traceability of supply chains and offering consumers the opportunity to verify the authenticity of products [24]. A transaction recorded on the blockchain is immutable and cannot be deleted. This characteristic plays a critical role in ensuring the reliability and integrity of the system [25]. In business applications and digital archiving systems, this immutability is fundamental to long-term data security [26]. Blockchain technology uses a consensus mechanism that ensures all nodes in the network agree on the current state of the ledger. This mechanism guarantees the validation and immutability of transactions, thus maintaining the consistency of the system [27]. These features of blockchain technology offer innovative solutions in areas such as energy trading and distributed systems, enhancing security, transparency, and reliability in digital systems.



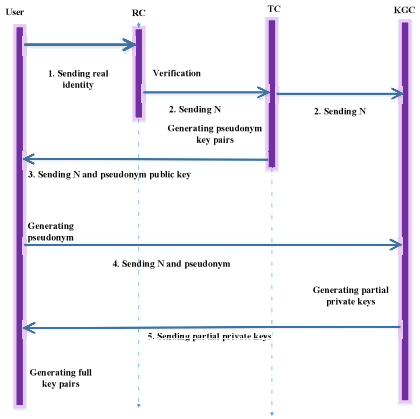


Fig.1. Proposed blockchain structure

Fig. 2. User registration phase

B. The Security Dimension of Blockchain Technology: Encountered Threats and Solutions

The applications of blockchain technology in P2P energy trading face various technical and legal challenges. Key challenges include scalability, transaction delays, and energy consumption. Specifically, as transaction volume increases on platforms such as Ethereum, there may be reductions in transaction speed and increased costs. This complicates the simultaneous energy transfer and data exchange required for P2P trading. Additionally, the PoW algorithm, with its high energy consumption, conflicts with environmental goals, prompting research into alternative consensus

mechanisms such as Proof of Stake (PoS). Another barrier is the lack of interoperability between different blockchain platforms, which leads to difficulties in data sharing and interaction [28].

Regulatory uncertainties and regional differences hinder the widespread application of blockchain in energy trading. Existing regulatory frameworks are far from being compatible with decentralized systems, making it challenging to adopt these platforms. A lack of education and trust issues further reduce user confidence in blockchain-based systems. Overcoming these barriers requires aligning regulatory frameworks, implementing standardization, and establishing educational programs. Energy-efficient consensus mechanisms like PoS and Layer-2 solutions support P2P trading by improving scalability and transaction speed [29]. Advanced smart contracts and conditional agreements enhance trading efficiency and ensure user trust. These solutions will increase the adoption of blockchain-based energy trading and enable its sustainable growth [30].

PROPOSED SYSTEM MODEL

The proposed energy trading system has two main layers: a privacy-centric authentication layer ensuring data security for prosumers and a permissioned blockchain layer enabling transparent transactions. Prosumers dynamically act as buyers or sellers based on their energy status, including users like EVs, charging stations, businesses, and households. Smart meters securely monitor energy usage, with all data immutably recorded on the blockchain. Participants undergo authentication before trading, while validators handle blockchain mining to enhance efficiency. This model ensures user privacy, data security, and efficient trading. The proposed system model is shown in Fig. 1.

A. Secure Record and Identity Anonymization Process

To participate in energy trading on the consortium blockchain, users must complete a multi-step registration process involving the Trust Center (TC), Key Generation Center (KGC), and Registration Center (RC) to ensure secure authentication and integration into the blockchain network. A general representation is shown in Fig. 2. The user first submits their identity information ID_j to the RC, which validates the identity and generates a random number N to ensure security in subsequent cryptographic operations.

The RC forwards N to the TC, which selects another random number T, applies a hash function H_0, and computes $g^{H_0(T)\cdot N}$ reinforcing the system's cryptographic integrity. The TC then generates the public and private key pair for the user:

$$\begin{cases} PK_{pse} = g^{H_0(ID_j)} \cdot g^{H_0(H_0(T)\cdot N)} modp \\ SK_{pse} = H_0(ID_j) + H_0(g^{H_0(T)\cdot N}) \end{cases} \quad (1)$$

The RC transmits (N, PK_{pse}) to the user while securely storing SK_{pse}. The user selects a random number r and computes their anonymous identity:

$$\begin{cases} u_j = g^r modp \\ u_j' = ID_j \cdot PK_{pse}^r modp \\ ID_j' = u_j + u_j' \end{cases} \quad (2)$$

Next, the user transmits (N, ID_j') to the KGC, which selects a random value b_j and calculates:

$$B_j = b_j P$$
$$d_j = (b_j + h_{1,j}) \text{modq} \quad (3)$$

where $h_{1,j} = H_1(ID_j', B_j, P_{pub})$ is derived using a hash function, P represents the generator point in an elliptic curve system, and P_{pub} is the public key. The user's partial private key is then defined as $D_j = (d_j, B_j)$. The KGC sends D_j to the user, who verifies the equation:

$$d_j P = B_j + h_{1,j} P_{pub} \quad (4)$$

If verification succeeds, the user selects a private random value x_j and computes:

$$X_j = x_j P$$
$$Q_j = (B_j + X_j) \quad (5)$$

The final key pairs are defined as:

$$PK_j = (Q_j, B_j)$$
$$SK_j = (d_j, x_j) \quad (6)$$

If verification fails, the user must request a new D_j from the KGC to restart the process. Upon successful completion of the process, users can begin trading within the consortium blockchain, which leverages pre-selected nodes for consensus to ensure faster transactions, lower costs, and secure, tamper-evident data storage. The system guarantees privacy through the use of an anonymous identity ID_j', while public keys PK_{pse}, PK_j authenticate users and encrypt transactions, and private keys SK_{pse}, SK_j ensure only authorized participants can perform actions. This structure enables a secure, efficient, and scalable framework for decentralized energy trading.

Upon successfully completing the aforementioned process, users can begin trading within the secure and efficient framework of the consortium blockchain. By leveraging pre-selected nodes for consensus, the system ensures faster transactions, reduced costs, and secure, tamper-evident data storage. These features make consortium blockchains particularly well-suited

for small-scale power trading, offering a practical and scalable solution for decentralized energy markets.

B. Identity Authentication Process in Blockchain

Blockchain ensures secure data sharing and transaction validation through asymmetric encryption with public-private key pairs. While the public key is shareable, the private key remains confidential. Digital signatures authenticate transactions and ensure data integrity, with nodes verifying signed transactions using the sender's public key. Additionally, nodes independently validate identity, data integrity, and balance before adding transactions to the blockchain. These mechanisms enable a secure, decentralized system without a central authority, ensuring trust and transparency in transaction processing.

C. Incentive Mechanism

Blockchain-based systems ensure security, decentralization, and data integrity through asymmetric cryptography and incentive mechanisms. Transactions are encrypted, validated, and linked cryptographically, enabling a transparent and scalable system. Validators verify transactions and create blocks, earning rewards for ensuring network reliability. In energy trading, nodes are rewarded only upon successful data transmission.

1) Incentive-Based Cooperative Transmission

When cooperative nodes B, C, and D assist A in delivering message m to E, the process follows structured steps ensuring secure transmission and reward allocation.

Publishing a Transmission Task

A declares a job $A \rightarrow E: m$ and produces two arbitrary quantities, R_1 and R_2, which must remain confidential. Next, A creates a deposit to guarantee that, should the message be successfully carried to recipient E, it will award the incentives to the cooperative nodes that are acting positively; if not, A will get its deposit back.

Data Transmission

The data transmission procedure from A to E is structured to ensure secure and verifiable communication. The message $m||E_{PK_E}(R_2)||\sigma Sig_{SK_E}(R_1)$ is sent by A. First, sender A generates two confidential random values, R_1 and R_2, which serve as authentication and verification parameters in the transaction process. A then encrypts R_2 using E's public key, denoted as $E_{PK_E}(R_2)$, and signs R_1 with its private key, expressed as $\sigma = Sig_{SK_E}(R_1)$. The message, structured as $m||E_{PK_E}(R_2)||\sigma$, is transmitted from A to relay node B, along with a transaction $Payment_{A\rightarrow B}$ recorded on the blockchain. Subsequently, cooperative nodes B, C, and D assist in forwarding the message

and create the corresponding transactions $Payment_{B\to C}$, $Payment_{C\to D}$, and $Payment_{D\to E}$, ensuring an incentive-based forwarding mechanism. Upon successful delivery, the encrypted signed acknowledgment is generated by E and sequentially transmitted back through D, C, and B, ensuring each node's participation is recorded. It is important to note that these payments represent conditional commitments, meaning actual fund transfers occur only after validation by blockchain miners, ensuring integrity and security within the incentive-based cooperative transmission system. Upon receipt, E generates an encrypted acknowledgment (ACK) as proof, relayed back through D, C, and B, verifying participation for incentive distribution.

Obtaining the Payments

Once the recipient has successfully received the data, giving the miners proof that they participated in the data should be a way to reward the good cooperative nodes transmission. In additional detail, B offers $\{E_{PK_B}(R_1), E_{PK_B}(ACK_c), PK_A, PK_C\}$; C supplies $\{E_{PK_C}(ACK_c), E_{PK_C}(ACK_D), PK_D\}$; D supplies $\{E_{PK_D}(ACK_D), E_{PK_D}(ACK_E), PK_E\}$; and E supplies $\{R_2, E_{PK_E}(ACK_E)\}$. If and only if the following requirements are met, the transactions are regarded as legitimate.

1. The random number R_2, which is supplied by E, is confirmed by,
$$H(R_2) = h_2 \quad (7)$$
2. The transaction chain from A to E may be used to discover the route that goes from A to E.
3. B is able to supply the random number R_1, which can confirm by,
$$E_{PK_B}(h_1) = E_{PK_A}(E_{PK_B}(R_1)) \quad (8)$$
4. B, C, and D are able to supply the accurate signed acknowledgments, which are confirmed by,
$$E_{PK_B}\left(E_{PK_C}(ACK_C)\right) = E_{PK_C}\left(E_{PK_B}(ACK_C)\right),$$
$$E_{PK_C}\left(E_{PK_D}(ACK_D)\right) = E_{PK_D}\left(E_{PK_C}(ACK_D)\right),$$
$$E_{PK_D}\left(E_{PK_E}(ACK_E)\right) = E_{PK_E}(E_{PK_D}(ACK_E)) \quad (9)$$

By enforcing these conditions, the incentive mechanism ensures fair compensation for cooperative nodes while maintaining security and data integrity within the blockchain-based energy trading system.

SIMULATION RESULTS AND DISCUSSION

In this section, the simulation results of the proposed model are discussed. MATLAB 2020a was used for the implementation of the model and the execution of the simulations. The simulations considered 100 energy users, and it was assumed that the energy consumption and production of the users varied from one another.

D. Privacy and Security Analysis

The proposed system ensures privacy and security through robust authentication, transaction verification, and data integrity mechanisms. Protection against impersonation attacks is achieved by utilizing anonymous certificates and digital signatures, allowing users to generate one-time private keys that verify their identity while preserving anonymity. These keys are deactivated after authentication, preventing linking attacks, privacy breaches, or unauthorized access to user resources. Encryption mechanisms safeguard data against interception or tampering, ensuring secure communication between senders and receivers. A consensus mechanism enhances security by selecting validators carefully, excluding malicious or inefficient nodes, and preventing attackers from gaining control over the network. One-time public keys are generated for each transaction, deactivated upon completion, thereby eliminating linking attacks and reinforcing anonymity. The blockchain structure maintains integrity and transparency, as each block references the previous one, making unauthorized modifications computationally infeasible. Asymmetric encryption ensures that only authorized users with the corresponding private key can access data, preventing malicious interference. These combined measures establish a secure, transparent, and privacy-preserving environment where transaction data remains protected, identities remain confidential, and the system remains resilient against security threats.

E. Results of the Incentive-Penalty Mechanism

The proposed incentive-penalty mechanism has been developed to ensure the fair, transparent, and sustainable operation of the energy system. This mechanism increases the active participation of prosumers in the system while effectively deterring malicious behaviors. The results demonstrate that this approach not only enhances individual user motivation but also contributes significantly to the community energy balance.

As shown in Fig. 3(a), it is evident that the incentives given for each non-malicious transaction increase in parallel with the number of transactions. This increase is due to the rewards given in the form of digital currency for every valid transaction made by energy prosumers. These digital currencies can be used to purchase energy and create a cyclical economic benefit among prosumers. In particular, the continuous increase in these incentives establishes a strong motivational mechanism that supports prosumers in

contributing more to the system. On the other hand, the measures taken against malicious activities also demonstrate the effectiveness of the mechanism. In Fig. 3(a), it can be seen that the incentive amount for malicious transactions is zero across all time periods. This ensures that users engaged in malicious activities do not receive any rewards from the system. Thus, while ensuring that the system maintains a fair structure, malicious behaviors are effectively deterred.

Fig. 3(b) highlights the positive relationship between energy contributions and the rewards received. As energy contributions increase, the rewards also rise significantly. This situation not only encourages prosumers to provide more energy to the system but also makes a significant contribution to maintaining the energy balance within the community. This increase in energy supply not only supports the sustainability of the system but also leads to lower energy prices, providing economic benefits to all users. The proposed mechanism does not only incentivize positive user participation in the system; it also provides a strong structure in terms of reliability and transparency. In this context, increasing transparency and reliability in the energy trading system plays a critical role in establishing trust among users. The rewards provided through digital currencies and the prevention of malicious behaviors allow users to manage their energy consumption and production habits more efficiently.

In conclusion, the incentive-penalty mechanism fosters a fairer, more reliable, and more sustainable energy trading environment by benefiting both individual users and the community. This mechanism not only increases prosumers' active participation but also supports the increase of energy supply, lowering prices, and balancing community energy. These results strongly demonstrate that the proposed system offers not only technological but also economic and social benefits.

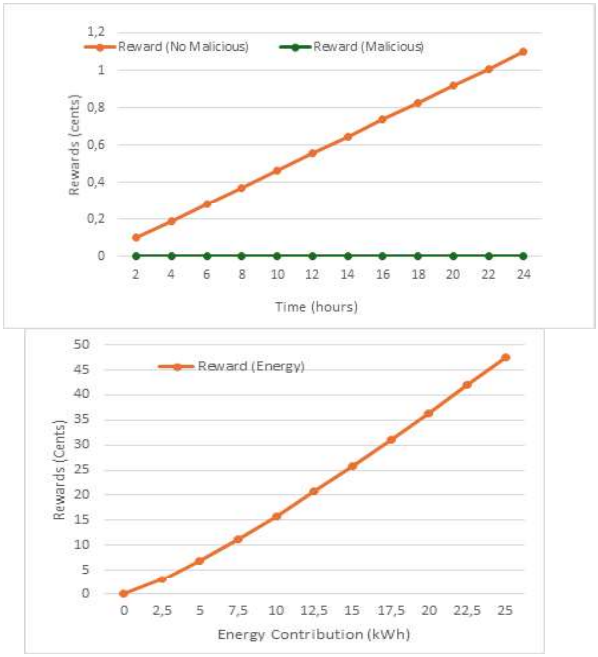


Fig. 3. Reward Systems: (a) Malicious vs. Non-Malicious Activities
(b) Impact of Energy Contribution

CONCLUSION

This study proposes an innovative two-layer P2P energy trading model that simultaneously addresses the security, privacy, and efficiency requirements in energy transactions. The model utilizes blockchain technology's reliability and transparency to optimize identity authentication and manage secure trading transactions. The algorithm, based on an incentive and penalty mechanism, detects and isolates malicious users while encouraging active participation from energy prosumers. This mechanism enhances security, promotes transparency, and strengthens the sustainability and efficiency of the energy ecosystem. Simulation results demonstrate that the proposed model offers significant advantages over traditional methods, improving security and increasing participation in energy trading. The contributions of this study are twofold. First, it optimizes critical parameters such as security and privacy within the trading process, establishing a more reliable infrastructure. Second, by enhancing participation, it facilitates the integration of renewable energy sources and supports the transition to more sustainable energy systems. In the future, the model's integration with various distributed energy systems could establish a new standard in energy trading, with significant scientific and

practical impact. This study provides a pioneering contribution to energy trading and lays a solid foundation for future research.

REFERENCES

[1] J. Li, Z. Zhou, J. Wu, J. Li, S. Mumtaz, X. Lin, H. Gacain, and S. Alotaibi, "Decentralized On-Demand Energy Supply for Blockchain in Internet of Things: A Microgrids Approach," IEEE Trans Comput Soc Syst, vol. 6, no. 6, pp. 1395–1406, Dec. 2019, doi: 10.1109/TCSS.2019.2917335.

[2] M. Li, D. Hu, C. Lal, M. Conti, and Z. Zhang, "Blockchain-Enabled Secure Energy Trading with Verifiable Fairness in Industrial Internet of Things," IEEE Trans Industr Inform, vol. 16, no. 10, pp. 6564–6574, Oct. 2020, doi: 10.1109/TII.2020.2974537.

[3] W. Wang, D.T. Hoang, P.Hu, Z.Xıong, D.Nıyato, P.Wang, Y.Wen, and D.I. Kim, "A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks," IEEE Access, vol. 7, pp. 22328–22370, 2019, doi: 10.1109/ACCESS.2019.2896108.

[4] N. Saxena, S. Grijalva, V. Chukwuka, and A. V. Vasilakos, "Network Security and Privacy Challenges in Smart Vehicle-to-Grid," IEEE Wirel Commun, vol. 24, no. 4, pp. 88–98, Mar. 2017, doi: 10.1109/MWC.2016.1600039WC.

[5] S. Park, J. Lee, S. Bae, G. Hwang, and J. K. Choi, "Contribution-Based Energy-Trading Mechanism in Microgrids for Future Smart Grid: A Game Theoretic Approach," IEEE Transactions on Industrial Electronics, vol. 63, no. 7, pp. 4255–4265, Jul. 2016, doi: 10.1109/TIE.2016.2532842.

[6] A. Dorri, F. Luo, S. S. Kanhere, R. Jurdak, and Z. Y. Dong, "SPB: A secure private blockchain-based solution for distributed energy trading," IEEE Communications Magazine, vol. 57, no. 7, pp. 120–126, Jul. 2019, doi: 10.1109/MCOM.2019.1800577.

[7] "DEPARTMENT: Cloud and the Law Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?" [Online]. Available: www.computer.org/cloud

[8] N. Z. Aitzhan and D. Svetinovic, "Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams," IEEE Trans Dependable Secure Comput, vol. 15, no. 5, pp. 840–852, Sep. 2018, doi: 10.1109/TDSC.2016.2616861.

[9] J. Gao, K.O. Asamoah, E.B. Sifah, A. Smahi, Q. Xia, H. Xia, X.Zhang, and G.Dong , "GridMonitoring: Secured Sovereign Blockchain Based Monitoring on Smart Grid," IEEE Access, vol. 6, pp. 9917–9925, Feb. 2018, doi: 10.1109/ACCESS.2018.2806303.

[10] M.Mihaylov, S. Jurado, N. Avellana, K. V. Moffaert, I.M. Abril, and A. Nowe, " NRGcoin: Virtual Currency for Trading of Renewable Energy in Smart Grids," EEM 14 : 11th International Conference on the European Energy Market : Energy for future : Kraków, Poland, 28-30 May 2014. IEEE, 2014.

[11] K. Gai, Y. Wu, L. Zhu, M. Qiu, and M. Shen, “Privacy-preserving energy trading using consortium blockchain in smart grid,” IEEE Trans Industr Inform, vol. 15, no. 6, pp. 3548–3558, Jun. 2019, doi: 10.1109/TII.2019.2893433.

[12] B. P. Hayes, S. Thakur, and J. G. Breslin, “Co-simulation of electricity distribution networks and peer to peer energy trading platforms,” International Journal of Electrical Power and Energy Systems, vol. 115, Feb. 2020, doi: 10.1016/j.ijepes.2019.105419.

[13] D. Han, C. Zhang, J. Ping, and Z. Yan, “Smart contract architecture for decentralized energy trading and management based on blockchains,” Energy, vol. 199, May 2020, doi: 10.1016/j.energy.2020.117417.

[14] I. A. Umoren, S. S. A. Jaffary, M. Z. Shakir, K. Katzis, and H. Ahmadi, “Blockchain-based energy trading in electric-vehicle-enabled microgrids,” IEEE Consumer Electronics Magazine, vol. 9, no. 6, pp. 66–71, Nov. 2020, doi: 10.1109/MCE.2020.2988904.

[15] J. Yang, A. Paudel, and H. B. Gooi, “Compensation for Power Loss by a Proof-of-Stake Consortium Blockchain Microgrid,” IEEE Trans Industr Inform, vol. 17, no. 5, pp. 3253–3262, May 2021, doi: 10.1109/TII.2020.3007657.

[16] P. T. Duy, T. T. Hien, V.-H. Pham, H. Chi, M. City, and V. Nam, “A survey on Blockchain-based applications for reforming data protection, privacy and security.”

[17] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System.” [Online]. Available: www.bitcoin.org

[18] W. Li, M. He, and S. Haiquan, “An Overview of Blockchain Technology: Applications, Challenges and Future Trends,” in ICEIEC 2021 - Proceedings of 2021 IEEE 11th International Conference on Electronics Information and Emergency Communication, Institute of Electrical and Electronics Engineers Inc., Jun. 2021, pp. 31–39. doi: 10.1109/ICEIEC51955.2021.9463842.

[19] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, “Everything You Wanted to Know about the Blockchain: Its Promise, Components, Processes, and Problems,” IEEE Consumer Electronics Magazine, vol. 7, no. 4, pp. 6–14, Jul. 2018, doi: 10.1109/MCE.2018.2816299.

[20] W. Cai, Z. Wang, J. B. Ernst, Z. Hong, C. Feng, and V. C. M. Leung, “Decentralized Applications: The Blockchain-Empowered Software System,” 2018, doi: 10.1109/ACCESS.2017.DOI.

[21] A. Aderibole, A. Aljarwan, M. H. Urrehman, H.H. Zeineldin, T.Mezher, K.Salah, E. Damiani, and D. Svetinovic, “Blockchain Technology for Smart Grids: Decentralized NIST Conceptual Model,” IEEE Access, vol. 8, pp. 43177–43190, 2020, doi: 10.1109/ACCESS.2020.2977149.

[22] H. Guo and X. Yu, “A survey on blockchain technology and its security,” Blockchain: Research and Applications, vol. 3, no. 2, Jun. 2022, doi: 10.1016/j.bcra.2022.100067.

[23] S. M. Idrees, M. Nowostawski, R. Jameel, and A. K. Mourya, “Security aspects of blockchain technology intended for industrial applications,” Electronics (Switzerland), vol. 10, no. 8, Apr. 2021, doi: 10.3390/electronics10080951.

[24] C. Bai and J. Sarkis, “A supply chain transparency and sustainability technology appraisal model for blockchain technology,” Int J Prod Res, vol. 58, no. 7, pp. 2142–2162, Apr. 2020, doi: 10.1080/00207543.2019.1708989.

[25] D. Ahmad, N. Lutfiani, A. D. A. Rizki Ahmad, U. Rahardja, and Q. Aini, “Blockchain Technology Immutability Framework Design in E-Government,” Jurnal Administrasi Publik : Public Administration Journal, vol. 11, no. 1, pp. 32–41, Jun. 2021, doi: 10.31289/jap.v11i1.4310.

[26] S. Rashidibajgan and T. Hupperich, “Utilizing blockchains in opportunistic networks for integrity and confidentiality,” Blockchain: Research and Applications, vol. 5, no. 1, Mar. 2024, doi: 10.1016/j.bcra.2023.100167.

[27] C. Zhang, C. Wu, and X. Wang, “Overview of blockchain consensus mechanism,” in ACM International Conference Proceeding Series, Association for Computing Machinery, May 2020, pp. 7–12. doi: 10.1145/3404512.3404522.

[28] M. A. C. L. Gunarathna, R. J. Yang, and A. Song, “Diverse distributed renewable energy trading paradigms: a business model review,” 2022, Routledge. doi: 10.1080/09640568.2021.1877640.

[29] V. K. Saini, C. S. Purohit, R. Kumar, and A. S. Al-Sumaiti, “Proof of Work Consensus Based Peer to Peer Energy Trading in the Indian Residential Community,” Energies (Basel), vol. 16, no. 3, Feb. 2023, doi: 10.3390/en16031253.

[30] A. Chiarini and L. Compagnucci, “Blockchain, Data Protection and P2P Energy Trading: A Review on Legal and Economic Challenges,” Dec. 01, 2022, MDPI. doi: 10.3390/su142316305.