©2025 Published in 11th International Symposium on Intelligent Technologies in
Engineering and Science 16-18 May 2025 (ISITES2025 Diyarbakır - Turkey)

Design of a Reliable Communication Infrastructure Based on Blockchain Technology for Smart Grids

[1]Samet Ayan , [2]Esra Kızılelma, [3]Yasemin Muzıroğlu and *Musa Balta

[1,2,3,4] Faculty of Computer and Information Sciences, Department of Computer Engineering, Sakarya University, Turkey

Abstract

A smart grid is an automatic, flexible, and sustainable system integrated with communication and information technologies within the energy sector. It dynamically manages energy flow and provides a high-quality energy network by enabling real-time, bidirectional information transfer from energy production to consumption. Among its goals are the efficient use of energy and the integration of renewable energy sources. According to NIST standards, it encompasses seven main domains: generation, transmission, distribution, consumption, service provider, marketing, and operations. Consumption areas, such as home and industrial area networks, can be exposed to various attack vectors due to their complex structures. Traditional security methods may be insufficient against new-generation cyberattacks and zero-day attacks. Therefore, within the scope of this study, a blockchain-based secure communication system was designed to protect consumers against cyber threats. The aim was to enhance data communication security using blockchain technology. The data obtained from the smart grid was first stored in a .txt file and then integrated into the blockchain using IPFS technology. Subsequently, we reviewed the information by examining the data on the blockchain. In the first phase of our project, we created a smart contract using the Solidity language and established a connection via the Ethereum virtual machine to transfer the data. However, due to the excessive amount of data, adding data to the blockchain through Solidity became challenging. Therefore, we used this method solely for data verification purposes. The data transfer was successfully completed using IPFS technology.

Key words: Smart Grid, Energy Management, Blockchain Technology, Cybersecurity, Real-Time Information Flow

1. Introduction

Traditional electrical distribution systems have several shortcomings, such as the inability to incorporate green energy sources, high costs, supply-demand imbalances, and high carbon emissions. To address these issues, there is a growing need to transition to smart grid systems. Smart grids enhance energy efficiency and reduce harmful environmental emissions by using data collection, analysis, and management technologies to maintain a balance between energy production and consumption. However, the various network protocols and devices used in smart grids can lead to security vulnerabilities. This is where blockchain technology comes into play. With its distributed and decentralized structure, blockchain enhances the security of smart grids, providing protection against cyberattacks. Blockchain's features, such as distributed data storage and identity verification, secure data communication within smart grids and optimize the energy supply and distribution processes. This integration not only improves the efficiency of smart grids but also facilitates the

*Corresponding author: Musa Balta, Address: Faculty of Computer and Information Sciences, Department of Computer Engineering, Sakarya University, 54187, Sakarya/Türkiye. E-mail address: mbalta@sakarya.edu.tr, Phone: +0264 295 5646

integration of renewable energy sources, contributing to the creation of a more sustainable energy infrastructure.[1-4]

In this context, this study presents a blockchain-based framework for advanced metering infrastructures (AMI) in smart grids. The proposed infrastructure model offers significant contributions to smart grids through the use of blockchain technology. Firstly, blockchain enables the transparent recording and sharing of energy production and consumption data, making energy management more efficient. Additionally, with distributed ledger technology, transactions are conducted securely and quickly without the need for a central authority. This makes energy trading and distribution more flexible and reliable. Blockchain also plays an effective role in the verification and tracking of energy sources, allowing data such as renewable energy certificates and carbon footprints to be accurately monitored. The security, transparency, and efficiency provided by this technology greatly contribute to the sustainable and effective operation of smart grids.[5-14]

In the following sections of the study, the relationship between blockchain technology and smart grids will be discussed in Section 2, followed by an explanation of the methodology used in the study in Section 3.

2. The Relationship Between Blockchain and Smart Grids

2.1. Blockchain Technology

Blockchain technology is a distributed ledger system that enables the secure and transparent recording of digital data.(figure 1) Each transaction is stored in data packets called "blocks," and these blocks are linked together in a chain. Blockchain allows for the verification and recording of transactions without the need for a central authority, thereby enhancing security and data integrity. This technology offers innovative solutions across various fields, including finance, healthcare, energy, and supply chain management.[2][11-13]

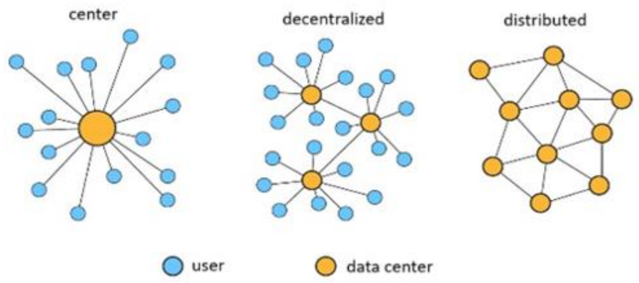

Figure 1. The decentralized and distributed structure of blockchain technology

2.2. The Contribution of Blockchain to Smart Grids

Blockchain technology is used to provide security, transparency, and efficiency in smart grids. Here are the main reasons and the protections it offers: (figure 2)[14-17]

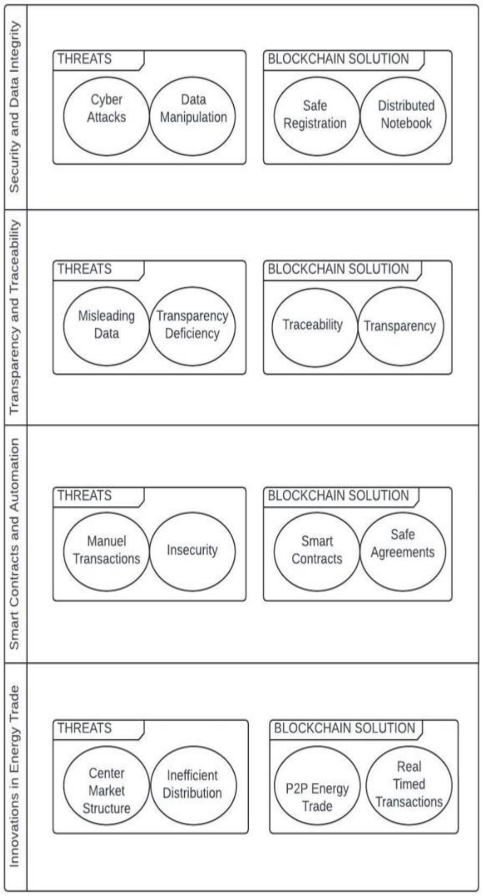

Figure 2. Blockchain solution to threats[1]

3. Blockchain as a Cyber Layer in Smart Grids

In this study, blockchain technology, presented as an infrastructure for smart grids, is defined as a securely shared and managed data community without reliance on a central authority, as illustrated in Figure 3. The blockchain structure, integrated with cloud services, facilitates the easy collection, integration, and sharing of transaction data from multiple sources.[17] Data is divided into blocks uniquely identified by cryptographic hashes and shared in a chain-like manner.[13-15]

In this process, IPFS and blockchain technologies are used in an integrated manner.[15] IPFS stores files in a decentralized structure, while blockchain securely records the hash values of these files. The steps anticipated in our study are as follows: First, data is collected from smart meters and sensors and encrypted using the RSA algorithm. The encrypted data is then uploaded to IPFS, where a unique hash value is generated. Finally, this hash value is recorded on the blockchain using a smart contract. This process contributes to ensuring the security and integrity of the data while facilitating more secure and effective data management in smart grids.[12][16]

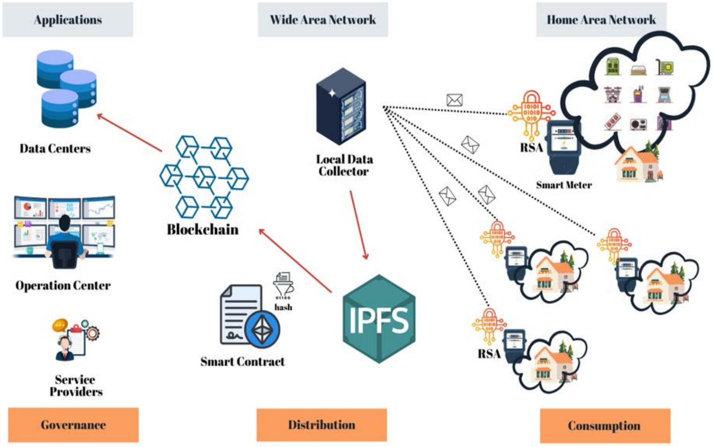

Figure 3. Integrating blockchain technology into smart grids

In smart grids, data transfers through the AMI infrastructure are made from smart meters to a central location. However, storing data in a single location and transmitting it in one direction can sometimes create security vulnerabilities and serve as attack vectors for intruders. In blockchain technology, there is no single central system like in smart grids. Instead, all computers on the blockchain can access the data simultaneously. In addition to accessing the data, it is also possible to obtain information about which user performed the transactions, when they were performed, and during which time intervals changes occurred.[3][4][12]

As a distinct feature of this technology, transactions are immutable; if a correction is needed, a new record is added to the system instead of modifying the existing one. This requires slightly more storage space, but it ensures that all data is preserved and all activities are visible. In a smart meter system, since data is stored in a single location, it can be manipulated following an attack, and it may not be possible to identify which user made the changes if the altered data is not associated with a specific user's personal actions.Therefore, in blockchain technology, all transactions on smart meters can be conducted using an identity number instead of personal data such as first name or last name.[12]

Any transaction performed here is encrypted using mathematical calculations, specifically hash functions, and recorded on the blockchain. The character strings generated by hash functions consist of letters and numbers. Even the smallest change in the data results in a different string, and the data prior to modification is also preserved in the records. Since manipulated or altered data cannot be deleted and every action is recorded with this technology, historical data can be reviewed after an attack. The locations of manipulated data can be easily identified, and the size of the data to be examined post-attack can be reduced.[17] In blockchain technology, all transactions are verified by users, and records become permanent.

In the context of the study, the integration of data from smart grids into smart contracts within the blockchain infrastructure is described, including the steps of directing data to the Ethereum virtual machine and then to the blockchain and console application.[16][17]

3.1. Data Flow / Data Source Identification

First, it is necessary to define the data flow of the information obtained from the smart grid (such as measurement data from a device, readings from a sensor, or data from a system). Particularly within the consumption area, obtaining both the information and process data from devices like PLCs, RTUs, HMIs, and sensors in industrial networks, as well as IoT-based smart home appliances in residential networks, is essential due to requirements related to energy efficiency, sustainability, and security [18].

3.2. Data Processing / Encryption / Signing

After asset management, the obtained data should be converted into a format that can be accepted by the smart contract. At this stage, factors such as data validation, data security, and data quality should also be considered.

To integrate data into the blockchain, the data must be signed. The signing process is used to ensure the integrity of the data and to confirm that it has not been altered afterward. Data signing is typically performed using encryption algorithms [18-22]:

- *Homomorphic Encryption*
- *AES (Advanced Encryption Standard)*
- *RSA (Rivest-Shamir-Adleman)*
- *ECC (Elliptic Curve Cryptography)*
- *S/MIME (Secure/Multipurpose Internet Mail Extensions)*
- *SHA-256 (Secure Hash Algorithm 256-bit)*

After experimenting with various encryption algorithms to meet the requirements of smart grid infrastructures (such as security needs, performance, compliance, deployment, and ease of operation), the use of the RSA algorithm was deemed appropriate for the study. Additionally, for compatibility purposes, all platforms and systems used in the study were reconfigured to be compatible with the RSA algorithm. The algorithm's ease of deployment and operation has also reduced application and system complexity.

3.3. Writing Smart Contracts

After completing the data flow and processing stages, a smart contract should be written. This smart contract will receive and process the data, then record and store the results on the blockchain. The steps to be used for integrating blockchain technology into the smart grid with the use of smart contracts are as follows:[23]

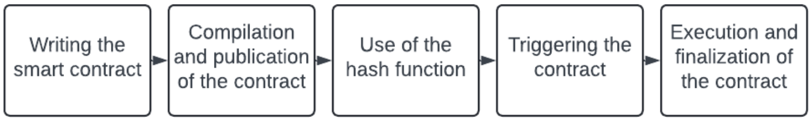
Writing the smart contract
Compilation and publication of the contract
Use of the hash function
Triggering the contract
Execution and finalization of the contract

Figure 4. Smart contract methods

These steps provide a general overview of the use of smart contracts. However, the specifics of their implementation and sequence may vary depending on the particular smart grid structures.

3.4. Integration with Smart Contracts

The smart contract is directed to the Ethereum Virtual Machine (EVM). The smart contract processes the data and generates results, which are then recorded on the blockchain.[10][22]

The most commonly used virtual machine for executing blockchain-based smart contracts is the Ethereum Virtual Machine (EVM).[10] It is a platform that operates on the Ethereum blockchain, where smart contracts are created, processed, and executed. Ethereum is known as a decentralized blockchain platform and provides infrastructure not only for smart contracts but also for the cryptocurrency Ether (ETH). Ethereum supports smart contracts and uses the Solidity programming language. The EVM is a virtual machine specifically designed to execute and process smart contracts written in Solidity. This study also uses the EVM. Some reasons for the preference of EVM can be summarized as follows:[10]

- *Compatible and Widespread:* The EVM is the virtual machine underlying Ethereum and is compatible with the Ethereum ecosystem.
- *Solidity Support:* The EVM supports Solidity, the programming language specifically designed for Ethereum smart contracts. Solidity is used to write smart contracts for Ethereum.[22]
- *Deterministic and Secure:* The EVM has a deterministic structure, meaning it always produces the same outputs for the same inputs. This ensures that smart contracts operate predictably and securely. The EVM is protected against known security vulnerabilities and provides isolation to prevent faulty smart contracts from harming the network.
- *Turing Complete:* The EVM can perform complex computations and allows smart contracts to have more intricate business logic. This enables the development of a variety of applications and increases functionality.

To send data from the virtual machine to the Ethereum network, the following steps will be followed:[10][22]

- *Connecting to the Ethereum Network:* To connect the virtual machine to the Ethereum network, an Ethereum client is needed.[10] In this context, Geth is used as the Ethereum client. This client provides access to the Ethereum network and broadcasts transactions to the blockchain.
- *Data Processing and Preparation:* The data in the virtual machine needs to be converted into a format suitable for sending to the Ethereum network. Typically, sending data to the Ethereum network involves creating a special transaction and using a data field within that transaction to carry the data.
- *Wallet and Signature:* To perform transactions on the Ethereum network, a wallet is required.[10] This wallet represents your Ethereum account and allows you to sign transactions.
- *Creating and Publishing the Transaction:* After processing and signing the data, a transaction needs to be created to send the data to the Ethereum network.
- *Transaction Confirmation and Blockchain Addition:* The transaction will be validated by miners on the Ethereum network and will be added to the blockchain. This process involves the transaction

being propagated across the network, selected by miners, and included in a block on the blockchain. Once the transaction is added to the blockchain, the data will be stored in a location accessible by your smart contract on the Ethereum network.

3.5. Blockchain Stages

The blockchain stages involve the steps necessary to add a new block to the blockchain. These steps may include mining, validation, reward for validation, processing of the data added to the blockchain, data alignment, and maintenance of the blockchain structure. The typical steps to add a new block to the blockchain generally include:[23]

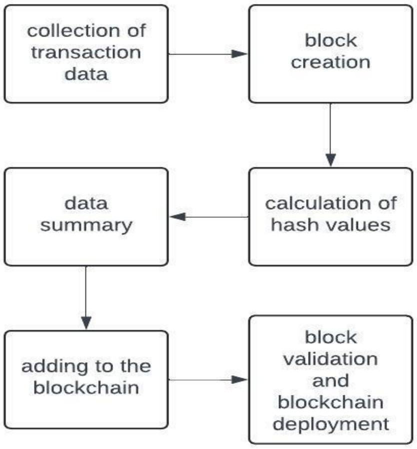
collection of transaction data
block creation
calculation of hash values
data summary
adding to the blockchain
block validation and blockchain deployment

Figure 5. Blockchain phases

A General Overview of How Hash Functions Are Used is as Follows:[11][18][19]

• *Data Hashing:* Data from the smart grid system is summarized using a hash function. For example, a hash function like RSA can be used. This creates a unique summary of the data.
• *Block Creation:* The data summarized using the hash function is combined into a block. This block is used as a data structure with the hash value of the previous block. Blocks are added sequentially to form a linked chain.
• *Blockchain Validation:* Before creating the next block, the hash value of the current block is computed and added to the data section of the next block. This ensures the integrity of each block and verifies that the chain has not been tampered with.
• *Transaction Verification:* Hash functions are used to verify transactions. Transactions are summarized with a hash function and added to blocks. To verify a transaction, you can compare the transaction's summary with the summaries in the blockchain.
• *Data Integrity Check:* Hash functions are used to ensure data integrity. If any data in a block is altered, the hash value will change. This is used to check data integrity and detect changes.
• *Mining and Consensus:* Hash functions play a crucial role in the mining process and consensus mechanisms. For example, the Proof of Work (PoW) consensus algorithm requires miners to use hash functions to reach a specific target.

Data is stored and validated on a distributed blockchain network. This network typically uses a consensus mechanism and works to ensure the accuracy of the data among participants. A consensus mechanism is a method used to achieve a common agreement among all nodes in the blockchain network and manage the transaction verification process. This mechanism is used to validate the validity of transactions on the blockchain, oversee the addition of new blocks, and ensure the reliability of the network.[19]

Blockchain networks operate on a decentralized structure, working over a distributed network with multiple nodes. Agreement must be reached among these nodes to ensure that transactions on the network are carried out correctly and reliably. The consensus mechanism facilitates this agreement and ensures that everyone shares the same database. Consensus mechanisms can vary across different blockchain networks.[18][19]

Conclusion and Future Work

The smart grid paradigm represents the next step in the evolution of electrical grids, contributing to environmental protection and the efficient use of resources. Since it involves a process, many grids still integrate both old and new technologies. This heterogeneous structure also introduces security vulnerabilities.[15][17][20]

In this study, the integration of cryptographic science and blockchain technology into the smart grid system aims to create a secure, flexible, and scalable network system. The goal is to enhance the reliability of data transfer, reduce the use of traditional systems, and decrease the green carbon footprint through the development of this new and modern network system. The contributions of this study to the literature can be summarized as follows:[20]

1. Modern and Scalable Grid System;

The creation of smart grid infrastructure using blockchain technology has established a coherent system that facilitates effective communication and data sharing between energy production, distribution, and consumption.[15]

2. Encrypted Data Transfer;

Data sent in plaintext from the consumption domain to the management domain is encrypted using efficient and rapid encryption methods to ensure secure transmission.[15][21]

3. Reduction of Security Vulnerabilities;

Utilizing the distributed data storage feature of blockchain helps maintain data integrity, enhance security, and reduce the risk of attacks on a single central point.[11][15][23]

For future work, continuous improvements to smart grid systems will be made to increase energy efficiency, and blockchain-based smart management strategies will be developed to optimize energy consumption. One such strategy involves developing an effective key management system integrated with blockchain, tailored for smart grids, to securely manage and update encryption keys. Another area of focus is the integration of security protocols for authentication and access control, preventing unauthorized access, and developing a comprehensive security solution to detect data security breaches.

Acknowledgements

This project was supported by Tübitak 2209-A.

References

[1] Wang W, Xu Y, Khanna M. Cyber security in the Smart Grid: Survey and challenges. Computer Networks. 2013;57(5):1344–1371. doi:10.1016/j.comnet.2012.12.017.

[2] Dehalwar V, Kolhe ML, Deoli S, Jhariya MK. Blockchain-based trust management and authentication of devices in smart grid. Cleaner Engineering and Technology. 2022;8:100481. doi:10.1016/j.clet.2022.100481.

[3] Benmalek M, Challal Y, Derhab A, Bouabdallah A. VerSAMI: Versatile and Scalable key management for Smart Grid AMI systems. Computer Networks. 2018;132:161–179. doi:10.1016/j.comnet.2018.01.010.

[4] Radoglou-Grammatikis PI, Sarigiannidis PG, Lagkas T, Moscholios I. Securing the Smart Grid: A Comprehensive Compilation of Intrusion Detection and Prevention Systems. IEEE Access. 2019;7:46595–46620. doi:10.1109/ACCESS.2019.2909807.

[5] Paar C, Pelzl J. Understanding Cryptography: A Textbook for Students and Practitioners. Springer; 2010. p. 87.

[6] Paar C, Pelzl J. Understanding Cryptography: A Textbook for Students and Practitioners. Springer; 2010. p. 173.

[7] Paar C, Pelzl J. Understanding Cryptography: A Textbook for Students and Practitioners. Springer; 2010. p. 239.

[8] Li Y, Zhang P, Huang R. Lightweight Quantum Encryption for Secure Transmission of Power Data in Smart Grid. IEEE Access. 2019;7:36285–36293. doi:10.1109/ACCESS.2019.2909807.

[9] Paar C, Pelzl J. Understanding Cryptography: A Textbook for Students and Practitioners. Springer; 2010. p. 293.

[10] Ethereum Foundation. Ethereum Virtual Machine (EVM) Documentation. Available at: https://ethereum.org/en/developers/docs/evm/. Accessed: June 3, 2025.

[11] TÜBİTAK Bilim Genç. Blokzincir Nedir, Nasıl Çalışır? Available at: https://bilimgenc.tubitak.gov.tr/makale/blokzincir-nedir-nasil-calisir. Accessed: June 3, 2025.

[12] Li Y, Zhang P, Huang R. Lightweight Quantum Encryption for Secure Transmission of Power Data in Smart Grid. IEEE Access. 2019;7:36285–36293. doi:10.1109/ACCESS.2019.2909807.

[13] Miglani A, Kumar N, Chamola V, Zeadally S. Blockchain for Internet of Energy management: Review, solutions, and challenges. Computer Communications. 2020;151:395–418. doi:10.1016/j.comcom.2020.01.014.

[14] Tushar W, Saha TK, Yuen C, Morstyn T, Poor HV, Wood K. Peer-to-peer trading in electricity networks: An overview. Renewable and Sustainable Energy Reviews. 2021;137:110600. doi:10.1016/j.rser.2020.110600.

[15] Saxena N, Grijalva S. Blockchain Technology for Smart Grids: Implementation, Management, and Security. IET Digital Library; 2021.

[16] Teng F, Zhang Q, Wang G, Li H. A comprehensive review of energy blockchain: Application scenarios and development trends. International Journal of Energy Research. 2021;45(7):9734–9756. doi:10.1002/er.7109.

[17] Miglani A, Kumar N, Chamola V, Zeadally S. Blockchain for Internet of Energy management: Review, solutions, and challenges. Computer Communications. 2020;151:395–418. doi:10.1016/j.comcom.2020.01.014.

[18] Kumar R, Tripathi R, Tripathi P. A Review of Hash Function Types and their Applications. International Journal of Computer Applications. 2021;183(42):1–7.

[19] Singh S, Sharma M, Singh R. Hash-MAC-DSDV: Mutual Authentication for Intelligent IoT-Based Cyber-Physical Systems. International Journal of Computer Applications. 2021;183(42):8–15.

[20] Zhou Q, Huang H, Zheng Z. Blockchain Technology Research and Application: A Literature Review and Future Trends. Future Generation Computer Systems. 2021;117:1–15. doi:10.1016/j.future.2020.12.019.

[21] Zhang Y, Wang Y, Li H. A systematic review of blockchain for energy applications. Energy Reports. 2024;10:1234–1245. doi:10.1016/j.egyr.2024.03.001.

[22] Solidity Documentation. Solidity v0.8.26. Available at: https://docs.soliditylang.org/en/v0.8.26/. Accessed: June 3, 2025.

[23] IBM Corporation. IBM Blockchain. Available at: https://www.ibm.com/blockchain. Accessed: June 3, 2025.