Article | Received 31 August 2024; Accepted 28 October 2024; Published 13 November 2024
https://doi.org/10.55092/blockchain20240007

Security scheme design of intelligent lighting system based on blockchain

Yongbin Zhao[1,*], Cong Men[1], Xiao Yang[2] and Xiangyang Liu[3]

[1] Hebei Key Laboratory of Electromagnetic Environmental Effects and Information Processing, Cyberspace Security, Shijiazhuang Tiedao University, Shijiazhuang, China
[2] Hebei Provincial Tax Service, State Taxation Administration, Shijiazhuang, China
[3] Shijiazhuang Second Research Institute, Shijiazhuang, China

* Correspondence author; E-mail: zhaoyb@stdu.edu.cn.

Abstract: Intelligent lighting systems achieve high energy efficiency through precise control and serve as vital tools for reducing carbon emissions, providing essential data for carbon trading. However, data exchange between the lighting system and the carbon trading system presents several challenges. For instance, data may be maliciously tampered with, and frequent unauthorized access threatens the normal operation of carbon trading. Therefore, this paper proposes a security framework for intelligent lighting systems based on blockchain technology. The framework utilizes a dual-chain structure of Hyperledger Fabric and Ethereum to address the issues of blockchain storage expansion and transaction efficiency, employing smart contracts to ensure the effective processing of lighting data. The security requirements for intelligent lighting data are thoroughly studied and analyzed. Additionally, this paper presents a key distribution scheme based on the RSA encryption algorithm to ensure trusted access control within the system. Through detailed analysis and practical verification of the scheme's security and performance, the framework not only effectively prevents data tampering but also ensures data authenticity and the smooth operation of the system during carbon trading, providing robust support for the security and privacy protection of intelligent lighting systems.

Keywords: blockchain; intelligent lighting; smart contract; key distribution; carbon trading markets; Hyperledger Fabric; Ethereum

1. Introduction

Intelligent lighting systems have become essential components in modern energy management and sustainability initiatives. These systems leverage advanced technologies to optimize lighting conditions based on factors such as human presence, ambient light levels, and predefined settings, significantly reducing energy consumption and carbon emissions.

Features like automatic dimming and remote control facilitate energy conservation by ensuring that lighting is used efficiently only when needed [1]. Intelligent lighting has been widely adopted across various sectors, including commercial buildings [2], industrial environments [3], and urban infrastructure [4]. Furthermore, the integration of the Internet of Things (IoT) with the concept of smart cities has accelerated the adoption of these systems, enhancing user experience while promoting energy efficiency [5]. For example, Yuan *et al.* [6] developed an innovative remote control solution that enables real-time monitoring and management of lighting systems, effectively reducing energy waste. Figure 1 illustrates the development stages of intelligent lighting systems.

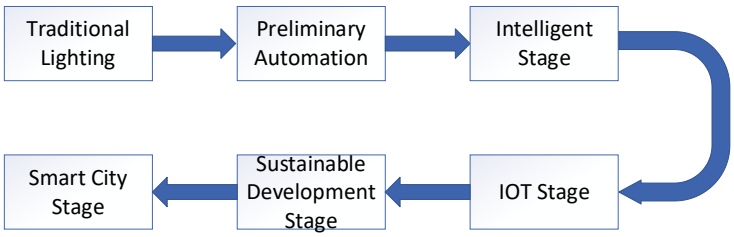

Figure 1. Development stage of intelligent lighting system.

As the complexity of intelligent lighting systems increases, the data generated—including information on electricity consumption, lighting usage patterns, fault detection, and maintenance records—becomes crucial for optimizing energy efficiency and operational performance. Concurrently, the global push for energy conservation and carbon emission reduction has led to the establishment of carbon markets [7], such as the European Union Emissions Trading System (EU ETS) [8], the Regional Greenhouse Gas Initiative (RGGI) [9], and China's carbon market pilot programs. The integration of intelligent lighting systems with these carbon markets underscores the critical need to ensure the security and reliability of lighting data [10]. Unauthorized tampering with this data can undermine the accuracy of carbon credits and disrupt the proper functioning of carbon trading mechanisms. Thus, securing intelligent lighting data has become an urgent priority.

Blockchain technology [11], with its decentralized, tamper-proof, and transparent features, offers a promising solution for enhancing the security of intelligent lighting systems. Operating as a distributed ledger, blockchain enables immutable data records that are trusted across multiple participants without requiring a central authority. This decentralized nature makes blockchain particularly suitable for environments where data integrity and transparency are critical. However, despite its potential, several challenges exist in applying blockchain technology to intelligent lighting systems on a large scale, especially when integrated with IoT and carbon markets.

The motivation for this research stems from the growing need for secure, efficient, and scalable solutions in intelligent lighting systems, particularly as these systems become intertwined with carbon trading platforms. Traditional lighting systems face significant challenges in addressing data security, performance, and reliability—all essential for accurately measuring energy consumption and calculating carbon credits. This paper aims to tackle these challenges by proposing a decentralized framework based on blockchain technology.

First, one primary limitation of blockchain technology is its performance, particularly in terms of transaction throughput. Most blockchain networks, such as Bitcoin and Ethereum, have limited capacity due to their consensus mechanisms. For example, Bitcoin processes only 7 transactions per second, while Ethereum handles approximately 15 transactions per second [12]. These limitations hinder blockchain's scalability, especially in IoT environments where intelligent lighting systems generate large volumes of real-time data. The inability of current blockchain architectures to process high transaction volumes in real time could lead to delays and inefficiencies in lighting control and carbon market integration.

Second, access control and key management represent critical challenges. Traditional access control mechanisms, such as public key infrastructures (PKI) and centralized certificate authorities (CA), are vulnerable to security risks and can undermine the decentralized nature of blockchain. These centralized models create single points of failure that are susceptible to attacks, complicating the implementation of a robust and scalable access control system for intelligent lighting environments that leverage blockchain technology. A decentralized and secure key management scheme is essential to prevent unauthorized access and ensure the integrity of lighting data.

Third, smart contract security is a fundamental concern in blockchain-based systems. Smart contracts automate decisions and actions within blockchain environments, making them key components for managing intelligent lighting systems. However, vulnerabilities in smart contract code can lead to severe security breaches, causing financial and operational damage. It is therefore vital to design secure, reliable, and efficient smart contracts to ensure the success of blockchain-enabled intelligent lighting solutions.

This research aims to develop a comprehensive, decentralized solution that enhances the security, performance, and reliability of intelligent lighting systems. Specifically, the research focuses on addressing the following objectives:

(1) Improving Blockchain Scalability: Exploring methods to optimize blockchain performance and transaction throughput to handle the high data volume and real-time processing requirements of intelligent lighting systems.

(2) Enhancing Security and Access Control: Developing a decentralized access control mechanism based on blockchain technology, emphasizing secure key management and the elimination of single points of failure.

(3) Securing Smart Contracts: Designing and implementing secure smart contracts that automate the management of lighting systems while mitigating the risks of code vulnerabilities and security breaches.

By addressing these objectives, this research seeks to provide a secure, scalable, and efficient framework for integrating intelligent lighting systems with carbon trading platforms, contributing to global efforts in energy conservation and emission reduction.

The rest of the paper is organized as follows. Section 2 reviews previous studies related to the proposed framework. In Section 3, we describe the overall architecture of the security scheme for the blockchain-based smart lighting system. Section 4 provides a detailed overview of the design concept of the proposed dual-chain architecture, as well as the implementation of smart contracts and key distribution strategies. In Section 5, we conduct

experiments to validate the effectiveness of the system and perform a comprehensive analysis of its performance and security. In the final section, we summarize the key findings of the research and engage in a thorough discussion.

2. Review

2.1. Current research

Intelligent lighting represents a convergence of comprehensive technologies. Building on existing lighting systems, it integrates information technologies such as the Internet of Things (IoT), big data, and cloud computing to achieve intelligent, digital, and user-centered lighting management. Intelligent lighting not only meets people's needs for illumination but also promotes energy-saving practices, aligning with energy conservation and emission reduction goals.

The integration of blockchain with IoT has garnered significant attention in intelligent lighting systems. IoT-enabled intelligent lighting facilitates real-time monitoring and dynamic control of lighting conditions, substantially reducing energy consumption by adjusting lighting based on occupancy and ambient light levels. Research by Heydarian A *et al.* [13] demonstrated that these systems optimize energy usage while enhancing user satisfaction through personalized lighting settings. Additionally, Kolahan A [14] explored blockchain-based smart contracts to automate lighting control in response to real-time conditions such as occupancy and daylight availability, ensuring secure management of lighting data through blockchain’s transparency and trust.

Despite these advancements, blockchain performance limitations present challenges. Muhammad Salek Ali [15] noted that current platforms like Bitcoin and Ethereum suffer from low transaction throughput and scalability issues, making them less suitable for handling the vast amounts of real-time data generated by IoT devices in intelligent lighting systems. To address this, Gianpiero [16] examined the application of fully homomorphic encryption (FHE) within blockchain-based intelligent lighting systems. FHE allows encrypted data processing, ensuring data security without compromising system performance. Yuning Qi [17] suggested that combining blockchain with FHE could significantly enhance the security, scalability, and efficiency of intelligent lighting systems, particularly in smart city environments.

Other studies have also focused on optimizing the intelligent control of lighting systems. For instance, Hussain M [18] applied machine vision technology, utilizing the YOLOv5 algorithm for dynamic control based on personnel distribution, while Jebeniani *et al.* [19] investigated digital twin models for street lighting to improve energy efficiency and remote control capabilities. Zarindast *et al.* [20] employed unsupervised machine learning to create personalized lighting schedules based on user data, enhancing the user experience. While these works underscore the role of technology in creating responsive and efficient lighting systems, they often lack in-depth exploration of security mechanisms.

Expanding on these innovations, Ghadi *et al.* [21] examined the integration of federated learning with IoT technology to enhance smart city applications. They highlighted federated

learning's potential to support areas such as traffic management and environmental monitoring while addressing the technical and privacy challenges posed by large-scale IoT networks. This approach illustrates the ongoing evolution of intelligent lighting systems and their integration with cutting-edge technologies to meet both energy efficiency and security needs.

2.2. Research gap

While significant progress has been made in integrating blockchain with IoT-enabled intelligent lighting systems, key challenges remain unresolved. One critical research gap lies in the performance bottlenecks of blockchain technology when applied to real-time lighting control systems. Most studies have focused on the application of smart contracts for automation but have not fully addressed how to enhance blockchain's capacity to handle the high volume of transactions and real-time data generated by intelligent lighting systems. Scalability issues, such as low transaction throughput, continue to limit the widespread implementation of blockchain in this context.

Another significant gap is in security management. Although some studies have proposed using multi-key fully homomorphic encryption (MKFHE) to enhance data security, comprehensive solutions for key management and secure access control within blockchain-enabled intelligent lighting systems are still lacking. The centralized nature of traditional public key infrastructures (PKI) poses security risks by creating single points of failure, contradicting the decentralized ethos of blockchain technology. Furthermore, the security of smart contracts, which are integral to automating intelligent lighting systems, has not been sufficiently addressed, particularly regarding their vulnerability to code exploitation.

Finally, there is limited exploration of blockchain's role in integrating intelligent lighting systems with carbon trading markets. As these systems become more intertwined with carbon markets, ensuring the integrity and accuracy of lighting data will be crucial for calculating carbon credits accurately. Current research lacks detailed frameworks that securely connect lighting data with carbon markets, highlighting an important avenue for future investigation.

Addressing these research gaps will require a multidisciplinary approach that combines advancements in blockchain scalability, cryptographic techniques like MKFHE, and robust access control mechanisms. Additionally, enhancing smart contract security is essential to prevent exploitation and ensure reliable, automated management of intelligent lighting systems across diverse applications, including energy conservation and carbon trading.

3. Overall architecture of intelligent lighting system security solution based on blockchain

Overall Architecture: According to the division of IoT system architecture, the overall architecture of the intelligent lighting system can be organized into four longitudinal layers: the perception layer, communication layer, control layer, and application layer. Additionally, there is a management and support layer, as illustrated in Figure 2.

Perception Layer: Located at the base of the architecture, this layer is essential for achieving "intelligence" [22]. It is equipped with advanced environmental sensing

capabilities, responsible for collecting physical events and data from the environment. Commonly used sensing technologies include noise detectors, brightness sensors, and infrared sensors. This layer primarily detects lighting conditions and provides control services.

Communication Layer: Serving as the information channel for the intelligent lighting system, this layer is a crucial component. It facilitates communication with the Internet through gateways and routing, allowing data messages to be transmitted. Participants in this interaction obtain public and private keys from the key distribution system and use session keys to encrypt the transmitted data, ensuring that only authorized recipients can decrypt and access the information, thereby safeguarding data privacy and security.

Data Layer: Utilizing a cloud computing platform that offers advantages in network computing, distributed computing, and load balancing, this layer is responsible for storing and processing data [23]. Data is a strategic resource in the intelligent lighting system, playing a vital role in its construction. This layer employs both blockchain and cloud servers to store data, including the basic attributes of lamp nodes and information regarding lighting energy consumption.

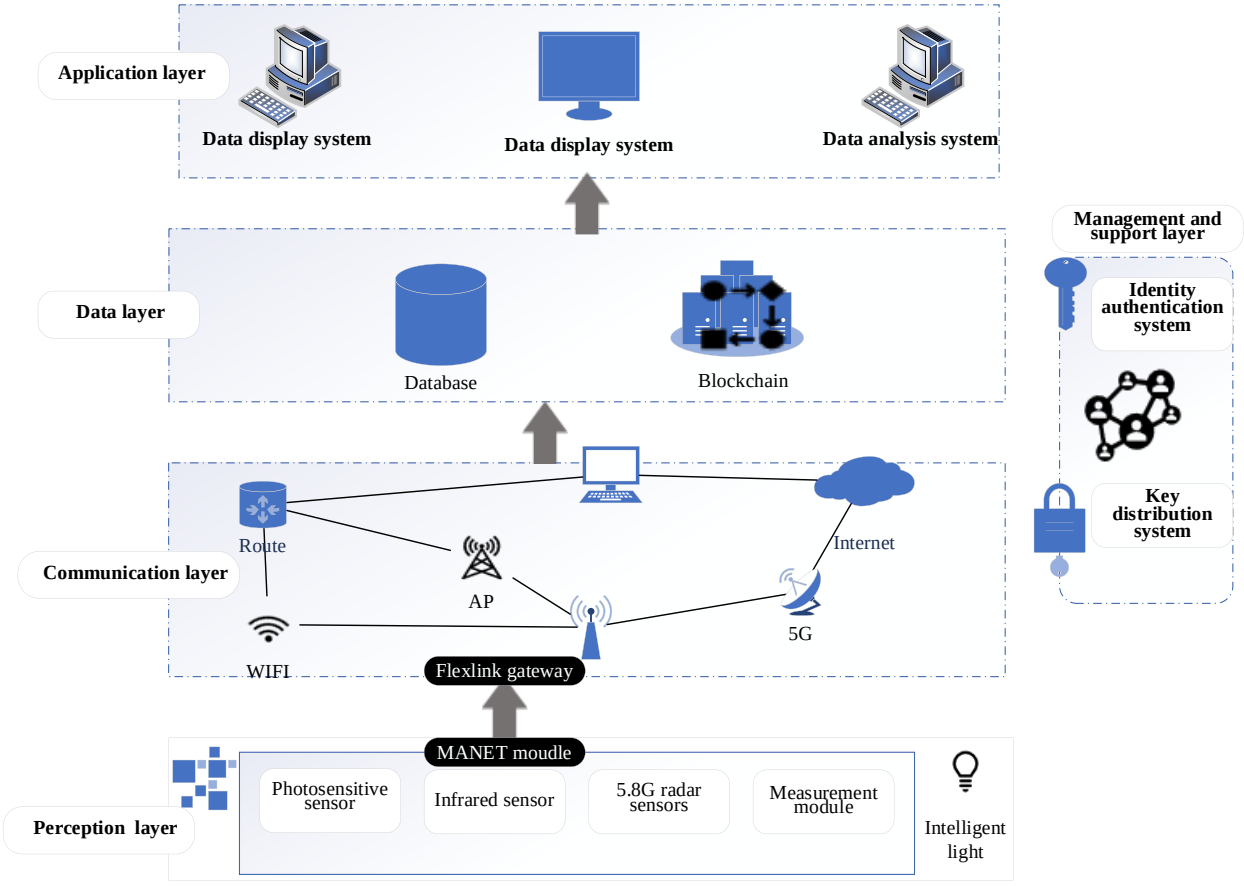

Figure 2. Overall system architecture.

Application Layer: This layer encompasses various applications built upon the perception, communication, and data layers. These applications directly present data or analysis results and support decision-making by analyzing trends and variations in the data.

Management and Support Layer: Spanning across the communication, data, and application layers, this layer ensures the authenticity and integrity of data. It distributes keys

to trusted users, addresses data privacy protection, and serves as a crucial guarantee for the normal operation of the system.

4. Detailed design of the blockchain-based security scheme for the intelligent lighting system

4.1. Hyperledger Fabric-Ethereum dual-chain design

The extensive use and frequent operation of IoT nodes have led to an expansion in data volume. To ensure the authenticity and security of IoT data, it is required that blockchain systems can withstand both large volumes of data and data authenticity checks during normal operation.

Blockchain can be categorized into public chains, private chains, and consortium chains based on application scenarios, with their characteristics shown in Table 1. Public chains have no authority restrictions and can be completely decentralized, but they have low storage efficiency; consortium chains involve only members of the consortium, offering high storage efficiency, high throughput, and good compatibility with large volumes of data.

Table 1. Comparison of the three blockchains.

Comparison item	Public chain	Private chain	Alliance chain
Centralization degree	Decentralization	Centralization	Partial centralization
Participant	Any user	Designated Users	Alliance members
Transaction speed	Slow	Fast	Fast
Advantage	High credibility	High security and low latency	Good scalability
Insufficient	High latency and low efficiency	Node limited and centralized	There is a trust issue

Hyperledger Fabric [24] is an open-source distributed ledger platform that belongs to the consortium chain, offering a high level of confidentiality, adaptability, and scalability. The Ethereum [25] public chain, widely used in the development of smart contracts and decentralized applications (DApps) [26], employs a Turing-complete programming language, enabling Ethereum to flexibly support a variety of application scenarios. Regardless of network and configuration settings, Ethereum can handle dozens to hundreds of transactions per second, with each block comprising tens to hundreds of transactions. In reality, with a large number of lights and substantial data volume, assuming several floors have 1024 lights and data is uploaded to the blockchain daily, it would require 5 blocks and take more than a minute. With the proliferation of intelligent lighting, such performance cannot meet the demand.

Due to the limited block size of blockchain and the vast number of nodes participating in public chains, they cannot handle large volumes of data. Therefore, adopting a consortium chain as the primary storage chain can alleviate the pressure on public chains. Public chains are recognized, and based on this recognition, consortium chains cannot falsify data. Public chains are completely decentralized and maintained by all nodes, so they cannot possess such

powerful computing power. Hence, to store a large amount of data while ensuring its immutability during normal operation, this paper designs a Hyperledger Fabric-Ethereum dual-chain structure [27] for support, as shown in Figure 3.

Hyperledger Fabric offers faster transaction speeds and can store large volumes of data, preventing performance degradation due to data loss and storage expansion. It is used to store all lighting data information; Ethereum is decentralized and highly trusted, but it has high latency and low efficiency. It is used to store the block digests of Hyperledger Fabric, which can greatly enhance system performance. Using the example provided for calculation, Hyperledger Fabric only requires one block for 1024 transactions on the blockchain, which takes about 1 second. The newly generated Fabric block hash is saved to Ethereum as a transaction. This dual-chain structure, leveraging the characteristics of blockchain technology, allows lighting data to be traded one-to-one with Ethereum without storage chaos and ensures efficiency. As a result, the credibility issue of intelligent lighting systems has been resolved.

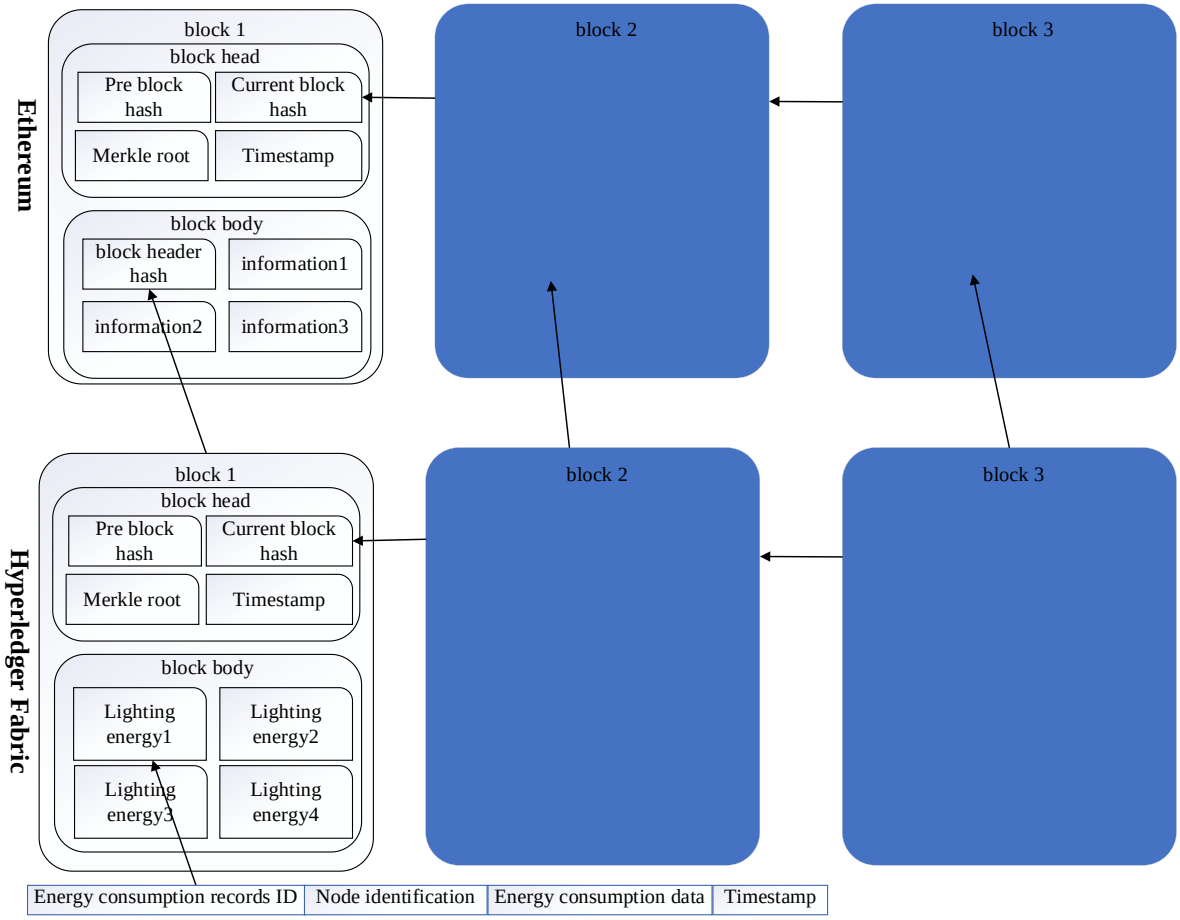

Figure 3. Hyperledger Fabric-Ethereum double chain structure.

4.2. Smart contract design

A secure smart contract is designed to counter potential attacks on smart contracts during the storage of lighting data in blockchain-based smart lighting systems. Based on common

vulnerability exploits, a secure smart contract design approach is proposed to offer a secure solution for data within blockchain-based smart lighting systems.

The blockchain operation diagram of the intelligent lighting system is shown in Figure 4.

Smart contracts are defined for transactions on the blockchain, decentralized storage interfaces are implemented, summaries of lighting data are stored, and a dual-chain structure is utilized to leverage the characteristics of the blockchain for the low-cost and efficient maintenance of data security. Among them, smart contracts encompass storage, query, verification, endorsement, and key distribution.

Sensors installed in the intelligent light nodes within the lighting system have the capability for automatic detection, collection, and upload of data, as shown in Table 2, where Emission is used for storing the lighting energy data structure, including the lighting node identification (deviceId), the hash of the node's energy consumption data Hash, and the timestamp of when the energy consumption data was generated. To uniquely determine the data generated by each IoT node, the IoT data structure should include the IoT node identifier (deviceId) and the timestamp of data generation. The IoT node identifier (deviceId) can uniquely identify the IoT node, and two fields are used to uniquely identify each transaction data.

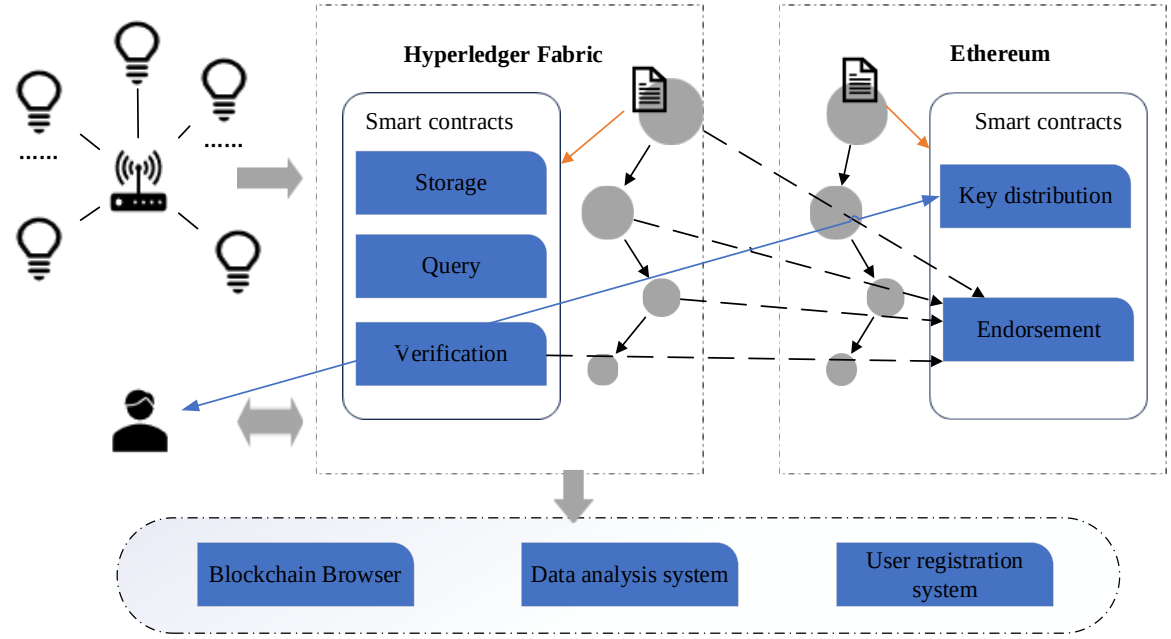

Figure 4. Blockchain operation diagram.

Table 2. Lighting energy consumption data structure.

Lighting energy consumption data structure
struct Emission {
string deviceId; / / Node identification
string dataHash; / / Lighting energy consumption data hash value
uint256 timestamp; / / Energy consumption data timestamp
}

The storage smart contract is designed to store lighting data. The process is as follows: the server first decrypts and hashes the data, then sends the hash value to the blockchain to check if the transaction has been stored. If it does not exist, the relevant information is stored on the blockchain. If it does exist, the transaction is skipped.

Algorithm 1 The storage smart contract

```
Input: lighting node identification deviceId, hash value of node energy consumption data dataHash, and energy consumption data generation time timestamp.
Output: transaction receipt or error message
begin
    if check(deviceId, timestamp) // Verify if re-upload is repeated
then
        if isDuplicate(deviceId, timestamp) then
            return "Error: Duplicate record for deviceId at given timestamp."
        end if
        memory(deviceId, dataHash, block.timestamp)  // Record lighting information
        storeData(deviceId, dataHash, block.timestamp)
        return getTransactionReceipt()  // Return transaction receipt
    else
        return "Error: Access denied or invalid input."
    end if
end
```

Querying smart contracts involves searching through node identification values and data generation timestamps. By entering the user's identity, the IoT node identification (deviceId) to be queried, and the timestamp, the smart contract first checks whether the querying user has permission. If they have permission, the data is retrieved based on the node identification (deviceId) and timestamp. If they do not have permission, an error message is returned.

Algorithm 2 The querying smart contract

```
Input: user identity userId, node identity deviceId, and time timestamp.
Output: query results or error message.
begin
    if checkPermission(userId) // Verify whether userId has permissions
then
        Emission [] emissions = getEmissions(deviceId, timestamp)
// Query energy consumption records based on node ID and data generation time
        return emissions
    else
        return "Notice: User " + userId + " does not have permission to query."
    end if
end
```

The block endorsement smart contract is designed to endorse the newly generated block hash value from Fabric to Ethereum. Input the block hash produced by Fabric, and the smart contract outputs the transaction receipt corresponding to the block, storing this receipt in Ethereum. Acting as the primary storage chain, the consortium chain is granted endorsement authority by the public chain. However, the consortium chain is unable to engage in data fraud due to the endorsement from the authorized public chain.

Algorithm 3 The blockchain endorsement smart contract

```
Input: blockHash.
Output: transaction receipt or error message.
begin
    if isValidBlockHash(blockHash)
then
        memory[blockHash] = true   //Record block hash
        storeEndorsement(blockHash)
        return getTransactionReceipt()  //Return transaction receipt
    else
        return "Error: Invalid block hash."
    end if
end
```

Verification smart contracts are utilized by regulators to authenticate the data's veracity using this algorithm. By entering the user's identity, the identification of the IoT node to be queried, and the timestamp, the smart contract will return results indicating the authenticity of the verification data or error alerts, contingent upon whether the user possesses regulatory authority.

Algorithm 4 The verification smart contracts

```
Input: user identity userId, node identity deviceId, and data generation time timestamp.
Output: verification results error message.
begin
    if hasRegulatoryAuthority(userId)  // Verify whether userId has permissions
then
        bool isVerified = verifyData(deviceId, timestamp)
        if isVerified
then
            return "Verification successful: The data is authentic." // Return verification result
        else
            return "Verification failed: The data is not authentic."
        end if
    else
        return "Notice: User " + userId + " does not have regulatory authority to verify."
    end if
end
```

The key distribution smart contract is where users apply for public and private keys, as well as digital certificates. If a user already possesses a valid certificate, they can utilize it directly. If the certificate is invalid, they may apply for an update.

Algorithm 5 The key distribution smart contracts

```
Input: user UID.
Output: public key certificate and private key, or error message.
begin
    if isValidUser(UID)  // Verify whether the user is valid
then // Pass identity verification
        ID = authenticateUser(UID) // Generate public and private keys
        PublicKey, PrivateKey = generateKeys(ID)
        distributeKeys(PublicKey, PrivateKey)
        return PublicKey, PrivateKey   // Return public key certificate
    else
        return "Notice: User UID is invalid or not authenticated."
    end if
end
```

4.3. Design of the key distribution scheme

As a distributed ledger, blockchain achieves consensus among participating network nodes through consensus algorithms, without the need for trusted third parties. It features decentralization, security, reliability, and programmability; the RSA algorithm is highly secure, has a wide range of application scenarios, publicly available algorithm standards, and is applicable to distributed systems, ensuring the security of information transmission.

To ensure the security of data access, the key distribution scheme is built on the blockchain's distributed mechanism and the RSA [28] algorithm, with blockchain replacing the centralization of trusted institutions (Trusted Authority, TA). Due to the blockchain's immutability and transparency, once identity information is added to and modified on the blockchain, there will be no disputes in the central mode [29].

The main work of the key distribution contract is identity authentication and key issuance, in which the RSA algorithm is used to generate public and private keys:

The contract generates two large prime sums randomly and calculates them pq

$$\mathrm{n} = \mathrm{p} \times \mathrm{q} \tag{1}$$

$$\varphi(\mathrm{n}) = (\mathrm{p} - 1) \times (\mathrm{q} - 1) \tag{2}$$

Generate an integer *e*, *e* and *r* less than r and calculate *d* by the following formula:

$$\mathrm{ed} \equiv 1(\mathrm{mod}\ \mathrm{r}) \tag{3}$$

The public key and the private key are made available here.$PK = (N, e), SK = (N, d)$.

When users register on Ethereum, they generate a unique user identifier (*UID*). When applying for a public or private key for the first time, the following steps occur (the flowchart is shown in Figure 5):

(1) Initial Request: The user sends their *UID* along with access permissions, denoted as M, to the address of the key distribution smart contract and invokes the contract.

(2) Verification: Upon receiving the *UID* and *M*, the contract verifies their validity. If the *UID* is invalid, the contract halts and returns an error message to the user. If the

UID is valid, the contract proceeds to check whether a valid key pair already exists for the user on the blockchain.

(3) Key Generation:

(a) If a valid key pair exists, the contract returns the user's public and private keys and terminates the process.

(b) If no valid key pair is found, the contract generates a new key pair (public key *PK* and private key *SK*) along with an expiration timestamp *T*, representing the validity period of the user's identity credentials.

(c) This information (*PK*, *SK*, *T*) is securely stored on the blockchain, with the blockchain server maintaining the user's credentials and certificate pairs. The contract then returns the newly generated keys and other relevant information to the user.

(4) Key Update and Revocation:

(a) The process for updating the user's public key or revoking and reissuing keys follows a similar flow to the initial key request, with the main difference being the parameters submitted in the request.

(b) The key distribution contract interprets the user's intent based on the parameters provided, performing the appropriate action and returning the result.

(c) To ensure the authenticity of key update or revocation requests, users must include the transaction hash from their previous key application in the request. This hash is privately stored by the user, making it possible to verify that the request originated from the rightful user, thus ensuring its authenticity.

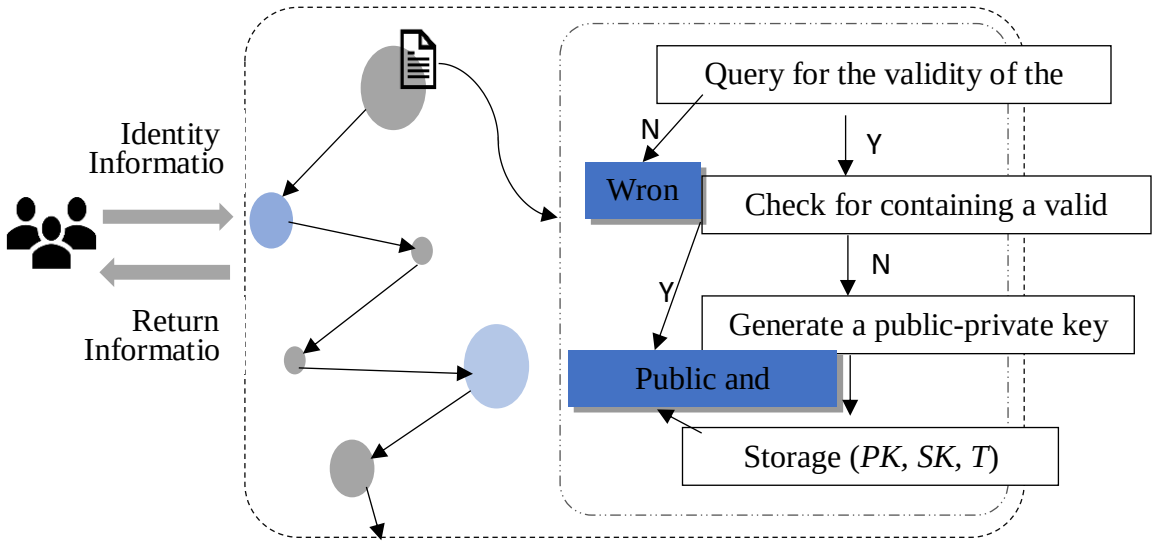

Figure 5. Public key distribution mechanism.

This method not only secures the key generation and distribution process but also simplifies key management for users, ensuring seamless and secure operations on the blockchain.

5. Experiments and analysis

5.1. Experimental environment and results

This paper takes the data security issues of blockchain-based smart lighting as the starting point and applies emerging blockchain technology to propose three unresolved problems: security issues caused by centralization and lack of identity authentication in the key system of smart lighting data transmission; once a smart contract is deployed, it cannot be changed, and malicious behavior in the developed network environment can lead to huge losses; the storage space of the blockchain is limited and cannot withstand massive data storage. In the experiment, the complex had 3 gateways, each with about 30 light nodes. The experimental results are depicted in Figure 6, which accurately presents the data of each lighting node and the blockchain-related receipt as proof of data integrity and authenticity.

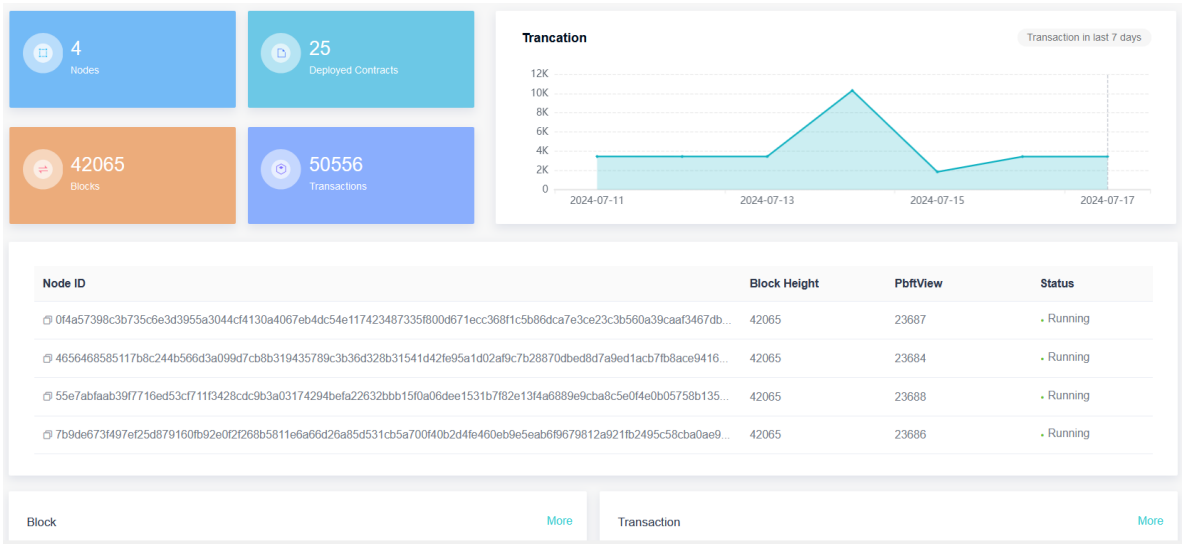

Figure 6. Results of the simulation experiments.

5.2. Performance analysis

Considering that the blockchain can only store this transaction after the transaction consensus, that is, the smart contract cannot perform complex or uncertain random work, it is impossible for the smart contract to perform key generation and other operations. In order to realize a distributed system, KGC implements key distribution and update, and issues certificates, but does not store any key information. KGC stores the generated or updated keys or certificates in the form of transactions on the blockchain, and the blockchain maintains its reliability and authenticity. As shown in Table 3 below, this solution differs in the algorithms and functions used.

Table 3. Solution function comparison.

	Blockchain	KGC	Digital Signature	Public Key Encryption	Certificate Application	Identity Authentication	Key Negotiation
Literature [30]	√	√	√	√	√	√	-
Literature [31]	√	-	√	-	√	-	-
This program	√	√	√	√	√	√	√

In the literature [30], digital signature and public key encryption algorithm are combined to design a decentralized identity authentication and key management scheme based on blockchain, in which KGC is only responsible for the generation of the first key, and the subsequent key update is completed by the user himself and stored on the blockchain in the form of transactions, which can realize certificate application and identity authentication. In the literature [31], digital signature algorithm and secure multi-party computing are used, multiple participants generate partial keys respectively, and the user synthesizes the key by himself, and the authenticity of the key is maintained by blockchain, realizing certificate application. In this scheme, KGC is responsible for key generation and update, generating digital certificates, and blockchain stores keys and certificates. Combining digital signature and public key encryption algorithm, it can realize the three functions of certificate application, identity authentication and key negotiation.

In this system, the acquisition of lighting energy consumption data is real-time, and the time consumed is disregarded. The timing of data upload primarily depends on network factors, hence the performance overhead is mainly associated with the upload, query, and verification of energy consumption data. Performance testing for smart contracts for upload, query, and verification is conducted using tape. As shown in Figures 7 and 8, it can be observed that the execution time of the smart contract increases with the growth of test data. Due to the gradual increase in time, the running time of the smart contract is within a reasonable range.

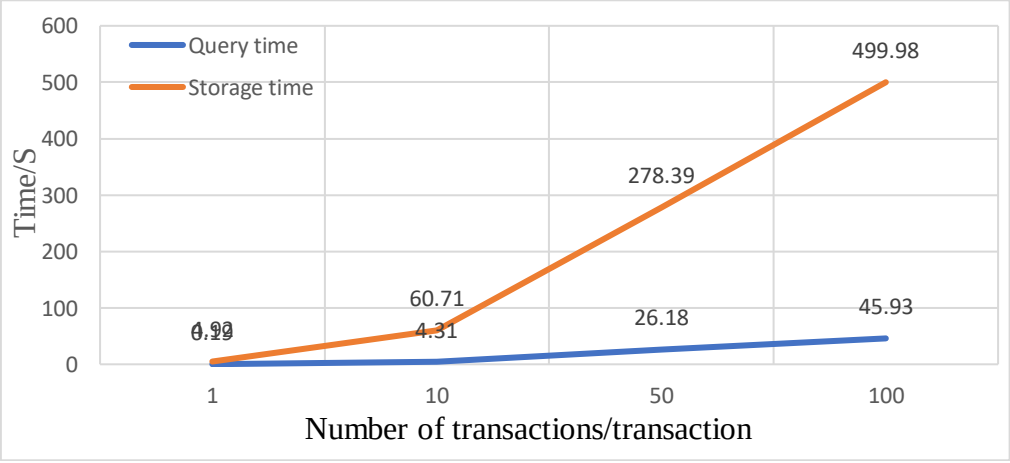

Figure 7. Comparison of storage time and query time.

As can be seen from Figure 7, the execution time of smart contracts increases with the increase of test data, and the storage time is always greater than the query time. It can be seen from the figure that, in general, the running time of smart contracts is within a reasonable time range.

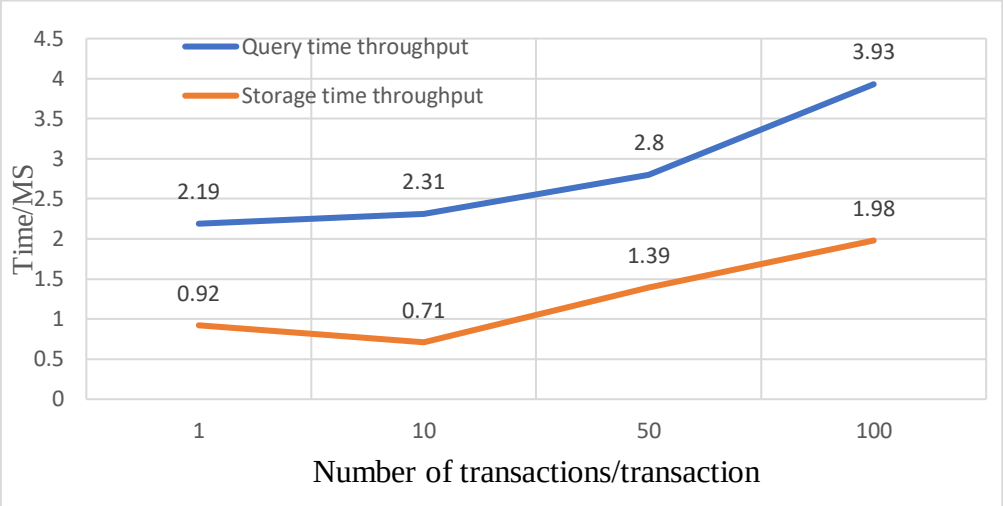

Figure 8. Comparison of storage time and query time throughput.

As can be seen from Figure 8, under the premise of the same number of transactions, the query throughput is greater than the storage throughput, and the trend changes of query throughput and storage throughput are basically the same.

5.3. Safety analysis

The blockchain-based smart lighting solution proposed in this article is practical and highly secure, addressing the data security issues in the current context of IoT data inflation and meeting the needs for data auditing. The security of the key system and smart contracts in this scheme has been analyzed. As a distributed ledger, blockchain inherently has features such as decentralization and immutability. Modifying data requires a significant amount of cost and resources, thereby enhancing the authenticity and reliability of IoT data stored on the blockchain. The blockchain-based key distribution and negotiation scheme adds communication security to the open network environment, preventing the possibility of data tampering and forgery, and improving the authenticity and reliability of data. At the same time, it combines IoT technology, with sensors automatically collecting and uploading data, and identity authentication technology to ensure the authenticity of the data source.

The security scheme design of the smart lighting system based on blockchain in this article is highly secure, mainly reflected in the following aspects.

Blockchain technology has decentralization, immutability, and traceability. A blockchain is a chain of blocks linked together, with each block containing the hash value of the previous block. Modifying data stored on the blockchain disrupts the chain structure, increases the cost and difficulty of data modification, and ensures the authenticity and reliability of data on the chain [32].

The dual-chain structure using consortium chains [33] and public chains [34] can ensure the reliability of the system, and all participants joining the system require review by consortium members, greatly reducing the chances of malicious nodes [35] participating. And through the supervision of public chains, the possibility of managers tampering with data is greatly reduced, preventing intentional fraud and further enhancing the security of the system.

IoT nodes or users use a distributed key system [36], and their identity information is stored in the blockchain. The decentralization and immutability of the blockchain ensure the reliability of their identity. The identity stored on the blockchain has an expiration date, which also ensures the validity of the identity. The use of blockchain key distribution avoids the centralization of traditional key distribution mechanisms, is resistant to DDOS attacks [37], and ensures secure and reliable data access mechanisms through the use of public key certificates.

Data is not stored in plaintext but in its hash value on the blockchain, maintaining the consistency of the stored data structure and ensuring data privacy. Before data exchange, users first authenticate and negotiate with the blockchain to obtain the session key [38] and encrypt the data with the session key. In the public network, the encrypted data protects data privacy.

In response to common vulnerabilities in smart contracts, security mechanisms have been designed for all smart contracts in this scheme, using two security detection methods: symbolic execution [39] and intermediate representation [40], namely the Mythril detection tool and the Slither detection tool, to detect all smart contracts in the system. Based on the test results and manual review analysis, the smart contract has passed the security check, as shown in Table 4.

Table 4. Vulnerability classification and detection results.

Vulnerability classification	Vulnerability types	Mythril	Slither
Solidity Code layer	Reentrant vulnerability	√	√
	Integer overflow vulnerability	√	√
	Permission control vulnerability		√
	Exception handling vulnerability	√	
	Denial of service vulnerability	√	√
	Type confusion vulnerability		√
	Unknown function call vulnerability		√
	Delegate call vulnerability		√
EVM Execution layer	Short address vulnerability		
	Call stack overflow vulnerability		√
	Tx.Origin loophole	√	√
Blockchain system layer	Block parameter dependency vulnerability	√	√
	Timestamp dependency vulnerability	√	

6. Conclusion

This paper discusses the data security issues in the blockchain-based smart lighting system, and proposes effective solutions for the centralization of the key system, the immutability of smart contracts, and the limitation of blockchain storage space. By designing the dual-chain structure of the alliance chain-permissioned public chain and the key distribution and negotiation scheme based on blockchain, this paper not only enhances the security of the system, but also provides a detailed design and implementation of the security mechanism of the smart contract. In addition, the comprehensive analysis of performance and security shows that the scheme has a high application value while achieving the expected goals.

In the subsequent implementation process, in order to improve the user experience and system performance, it is necessary to further optimize and adjust the scheme. First, develop a more intuitive user interface and data verification interface to meet the needs of different users, thereby improving the data display effect and operation convenience. Secondly, considering the data volume and throughput issues in the IoT environment, it is necessary to conduct in-depth testing of the carrying capacity of the device and the network to ensure that the system can still maintain stability when facing a large number of data node connections, and prevent data loss and equipment failure.

Looking to the future, with the continuous development of blockchain technology, smart lighting systems will make further breakthroughs in data security, privacy protection, and user experience. Researchers and engineers should continue to explore more efficient algorithms and protocols to meet the growing application needs and technical challenges. Through multi-party collaboration and innovation, smart lighting systems are expected to play a more important role in the construction of smart cities and provide users with safer and more efficient smart lighting solutions.

Acknowledgments

This work was supported by Hebei Province Construction Science and Technology Research Guiding Plan Project (2024-2159).

Conflicts of Interests

The authors declared that they have no conflicts of interests.

Authors' Contribution

Supervision, Formal analysis, Conceptualization, Methodology, Writing-Original draft preparation, Writing- Reviewing and Editing, Z. Y. B.; Conceptualization, Data curation, Software, Writing-Original draft preparation, M. C.; Conceptualization, Visualization, Investigation, Software, Writing- Original draft preparation, Y. X.; Conceptualization, Methodology, Writing- Reviewing and Editing, L. X. Y.; All authors have read and agreed to the published version of the manuscript.

References

[1] Wang W. Research on energy management method of intelligent lighting in office buildings. *IOP.Conf. Ser.: Earth Environ. Sci.* 2019, 242(6):062036.

[2] Odiyur Vathanam GS, Kalyanasundaram K, Elavarasan RM, Hussain Khahro S, Subramaniam U, *et al*. A review on effective use of daylight harvesting using intelligent lighting control systems for sustainable office buildings in India. *Sustainability* 2021, 13(9):4973.

[3] Zhao H. Intelligent management of industrial building energy saving based on artificial intelligence. *Sustainable Energy Technol. Assess*. 2023, 56:103087.

[4] Scorpio M, Laffi R, Masullo M, Ciampi G, Rosato A, *et al*. Virtual reality for smart urban lighting design: Review, applications and opportunities. *Energies* 2020, 13(15):3809.

[5] Caragliu A, Del Bo C, Nijkamp P. Smart cities in Europe. *J. Urban. Technol*. 2011, 18(2):65–82.

[6] Yuan J， Jiao ZM， Jian-Bo YU， Bin WU， Jing W, *et al*. GPRS and ZigBee based remote intelligent distributed control system for LED lighting. *Computer Engineering Des.* 2015, 36(1):108–114

[7] Tao M, Poletti S, Sheng SM, Wen L. Nexus between carbon, stock, and energy markets in New Zealand: An analysis of causal domains. *Energy* 2024, 299:131409.

[8] Di Foggia G, Beccarello M, Arrigo U. Assessment of the European Emissions Trading System's impact on sustainable development. *Sustainability* 2023, 16(1):223.

[9] Lamb RL, Hurtt GC, Boudreau TJ, Campbell E, Carlo EAS, *et al*. Context and future directions for integrating forest carbon into sub-national climate mitigation planning in the RGGI region of the U.S. *Environ. Res. Lett*. 2021, 16(6):063001.

[10] Jin D, Hannon C, Li Z, Cortes P, Ramaraju S, *et al*. Smart street lighting system: A platform for innovative smart city applications and a new frontier for cyber-security. *Electr. J.* 2016, 29(10):28–35.

[11] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. 2008. Available: https://bitcoin.org/bitcoin.pdf (accessed on 17 January 2024).

[12] Yuan Y, Wang FY. Blockchain: The state of the art and future trends. *Acta. Automatica. Sinica*. 2016, 42(4):481–494.

[13] Heydarian A, Pantazis E, Wang A, Gerber D, Becerik-Gerber B. Towards user centered building design: Identifying end-user lighting preferences via immersive virtual environments. *Autom. Constr.* 2017, 81:56–66.

[14] Kolahan A, Maadi S R, Teymouri Z, Schenone C. Blockchain-based solution for energy demand-side management of residential buildings. *Sustainable Cities Soc.* 2021, 75: 103316.

[15] Ali M S, Vecchio M, Pincheira M, Dolui K, Antonelli F, *et al*. Applications of blockchains in the Internet of Things: A comprehensive survey. *IEEE Commun. Surv.*

Tutorials 2018, 21(2):1676–1717.

[16] Costantino G, De Vincenzi M, Martinelli F, Matteucci, I. A privacy-preserving solution for intelligent transportation systems: Private driver DNA. *IEEE Trans. Intell. Transp. Syst.* 2022, 24(1):258–273.

[17] Qi Y, Bi J, Peng H, Li L. Efficient Homomorphic Encryption for Multi-key Compressed Sensing in Lightweight Cloud-based Image Processing. *IEEE Sens. J.* 2024.

[18] Hussain M. YOLO-v5 variant selection algorithm coupled with representative augmentations for modelling production-based variance in automated lightweight pallet racking inspection. *Big Data Cognit. Comput.* 2023, 7(2):120.

[19] Jebeniani H, Araoud Z, Canale L, Zissis G. Approach of "Digital Twins" applied to smart urban lighting: from concept to application. In *IEEE Sustainable Smart Lighting World Conference & Expo,* Mumbai, 2023.

[20] Zarindast A, Wood J, Sharma A. A data-driven personalized smart lighting recommender system. *arXiv* 2021, arXiv:2104.02164.

[21] Ghadi YY, Mazhar T, Shah SFA, Haq I, Ahmad W, *et al.* Integration of federated learning with IoT for smart cities applications, challenges, and solutions. *PeerJ Comput. Sci.* 2023, 9: e1657.

[22] Wu H. Image Self-coding algorithm based on IoT perception layer. *Mob. Inf. Syst*. 2022(1), 9910655.

[23] Zhang Y, Geng P. Multi-task assignment method of the cloud computing platform based on artificial intelligence. *Comput. Intel. Neurosc*. 2022(1):1789490.

[24] Liu W, Zhang D, Mu C, Zhao X, Zhao J. Ring-overlap: a storage scaling mechanism for Hyperledger fabric. *Appl. Sci*. 2022, 12(19):9568.

[25] Jayapal C, Xavier AR, Arunachalam P. Capitalizing on blockchain technology for efficient crowdfunding: an exploration of Ethereum's smart contracts. *Int. J. Safety Secur. Eng.* 2023, 13(4):723–729.

[26] Samreen NF, Alalfi MH. An empirical study on the complexity, security and maintainability of Ethereum–based decentralized applications (DApps). *Blockchain Res. Appl.* 2023, 4(2):100120.

[27] Song L, Wang X, Wei P, Lu Z, Wang X, *et al*. Blockchain-based flexible double-chain architecture and performance optimization for better sustainability in agriculture. *Comput. Mater. Continua* 2021, 68(1):1429–1446.

[28] Gupta N, Jain AK. RSA based consensus algorithm for resource-constrained distributed devices. *Internet Technol. Lett*. 2023, 6(6):e471.

[29] Yap KY, Chin HH, Klemeš JJ. Blockchain technology for distributed generation: A review of current development, challenges and future prospect. *Renew. Sust. Energ. Rev*. 2023, 175:113170.

[30] Yao YY, Chang XL, Zhen P. Decentralized identity authentication and key management scheme based on blockchain. *Cyberspace Secur.* 2019, 10(06):33–39.

[31] Yu Y, Li Z, Tu J. Distributed identity password management based on blockchain. *Appl. Electron. Technol.* 2023, 49(08):98–102.

[32] Dwivedi SK, Amin R, Vollala S. Blockchain based secured information sharing protocol in supply chain management system with key distribution mechanism. *J. Inf. Secur. Appl.* 2020, 54:102554.

[33] Zhang W, Huo X, Bao Z. A secure and efficient multi-domain data sharing model on consortium chain. *J. Supercomput.* 2023, 79(8):8538–8582.

[34] Liu Y, Zhang Y, Lin Z, Wang Z, Wang X. Simulation method for blockchain systems with a public chain. *Sensors* 2022, 22(24):9750.

[35] Saeed A, Javed MU, Almogren A, Javaid N, Jamil M. Employing blockchain and IPFS in WSNs for malicious node detection and efficient data storage. *Wirel. Netw.* 2024, 30:2313–2328.

[36] Baouch M, López-Ramos JA, Schnyder R, Torrecillas B. An active attack on a distributed Group Key Exchange system. *arXiv* 2016, arXiv:1603.09090.

[37] Li M, Zhou H, Deng S. Parallel path selection mechanism for DDoS attack detection. *J. Netw. Comput. Appl*. 2024, 230:103938.

[38] Long Y, Peng C, Tan W, Chen Y. Blockchain-assisted full-session key agreement for secure data sharing in cloud computing. *J. Parallel Distrib. Comput.* 2024, 193:104943.

[39] Borodin AE, Dudina IA. Intraprocedural analysis based on symbolic execution for bug detection. *Program. Comput. Softw*. 2021, 47(8):858–865.

[40] Li X, Wang L, Xin Y, Yang Y, Chen Y. Automated vulnerability detection in source code using minimum intermediate representation learning. *Appl. Sci.* 2020, 10(5):1692.