IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Blockchain-Powered Patient-Centric Medical Record Sharing

Advay Tapi, Tasmay Patil, Prajwal Telang, Harsh Toshniwal

Student, Student, Student, Student
Department of Computer Engineering,
Vishwakarma Institute Of Technology, Pune, India

Abstract -Regional healthcare systems are becoming increasingly digitalized, which implies that volumes of sensitive medical records are stored across different hospitals, laboratories, and clinics. The fragmented nature often causes delayed treatments, data breaches, and unauthorized access that seriously threaten patient privacy and safety. Traditional centralized systems are not transparent and are easily tampered with; patients do not really own their medical information. Thus, in modern healthcare, there is a dire need for an appropriate, secure, reliable, and patient-centric data-sharing mechanism. This paper is concerned with the design and implementation of a Blockchain-Based Healthcare Data Sharing and Access-Control System using Ethereum smart contracts, IPFS decentralized storage, and a React–MetaMask-based DApp interface. Accordingly, in this system, patients can safely upload medical records where the actual file is stored off-chain, while the cryptographic hash is recorded on the blockchain to ensure immutability. Physicians can request access to specific records, which a patient can then approve or reject in real time via verified blockchain transactions. Upon successful access grant, a doctor receives a secure IPFS link that is valid for only a pre-defined time interval to ensure fine-grained and controlled data sharing.The modular architecture allows the deployment of the solution across clinical, research, or telemedicine environments that require continuous protection of sensitive patient data. Given its light and cost-effective nature, the system needs only a browser enabled by MetaMask and an Ethereum test network, with no other complementary communication modules. Experimental results confirm that the smart contract is reliable, the access expiration logic is correct, and the verification of file integrity is precise through IPFS hashing. The integration of Blockchain enriches system transparency, privacy, and auditability by recording logging of access events in real time. In this regard, this work shows how decentralized ledger technology can be used to build secure, scalable, and user-controlled healthcare data-sharing solutions that effectively increase patient trust and medical interoperability.

Keywords- Blockchain, Healthcare Data, Smart Contracts, IPFS Storage, DApp, Ethereum, Access Control, MetaMask

I. INTRODUCTION

Within the past few years, healthcare data management has grown as an important building block for modern digital medical systems. It considers the accuracy of diagnosis, continuity of care, and timely decision-making. Traditional healthcare information systems are characterized by fragmentation, lack of interoperability, and limited transparency-each factor contributing to a compromise in quality patient care. Medical records are usually maintained in various isolated, centralized databases controlled by different hospitals or laboratories, not allowing patients or healthcare professionals to share information securely whenever required.

Moreover, the storage of data in a centralized location raises severe vulnerability to data breaches, unauthorized access, and manipulation. It may lead to exposure, misuse, or alteration of sensitive patient information regarding prescription, laboratory reports, or diagnostic images without accountability. Current systems raise many questions concerning privacy and trust, as patients have little control over who accesses their health records and for what reasons. Such limitations create the need for an architecture that can safely and verifiably make access to medical data transparent and decentralized, while at the same time empowering the patients.

These challenges have turned the spotlight toward blockchain-based healthcare solutions. Blockchain offers an immutable, tamper-proof ledger that enhances data integrity and eliminates single points of failure. Integration with smart contracts will allow automation of access control so that only the authorized user-for example, registered doctors-can request a view of particular medical records. Each action, such as upload, request, approval, or revocation, is recorded on the blockchain, thus allowing full traceability and improving trust between stakeholders.

Ethereum, along with decentralized storage like IPFS, represents a robust architecture for health data management securely. Smart contracts allow fine-grained permissions, whereas IPFS stores medical files efficiently in an encrypted manner without overloading the blockchain. Patient identity and consent are handled through wallet addresses connected via MetaMask to make sure that the user is in full control over their own data. The frontend is made using React to provide users with an easy-to-use interface for record upload, approval requests by doctors, and viewing file access logs in real time. This work proposes a low-cost, patient-centric, decentralized blockchain-enabled healthcare data-sharing system that is designed to ensure secure record exchange between patients and doctors. The proposed DApp helps in maintaining privacy, prevents unauthorized access, and ensures trust through immutable logging, whether the patient is physically present in the hospital or interacting remotely via a digital platform.

II. LITERATURE REVIEW

Sharing EHRs safely and efficiently is considered the foundation for quality of care, patient safety, and medical research improvement in modern healthcare systems. Conventional data management platforms build on centralized models, controlled by either individual hospitals or vendors, which inherently introduce single points of failure with limited interoperability and high risks of unauthorized access or tampering. Blockchain technology has emerged with an immutable and distributed ledger that guarantees strong data integrity and traceability of all operations on patient records through verifiable logs in many recent studies [1]. In parallel, it allows for programmable logic on access control facilitated by smart contracts, thus enabling fine-grained permissioning and automated enforcement of sharing policies across different stakeholders, such as patients, doctors, and researchers [2].

On the other hand, existing works also identify key constraints. Due to limitations in storage, cost, and privacy concerns, storing the whole medical record directly on-chain is not feasible. To address this challenge, many framework designs adopt a hybrid architecture wherein only cryptographic hashes and metadata go on-chain, with actual medical files kept off-chain through decentralized storage systems like the InterPlanetary File System (IPFS) or secure databases [3]. This combination maintains tamper evidence since any modification to an off-chain record changes the hash, reducing on-chain bloat and transaction costs. Simultaneously, studies emphasize the need for strong encryption, pseudonymization, and key management techniques that guard sensitive health information against unauthorized disclosure, even when metadata is publicly visible on the ledger [1].

Performances and scalability are also further investigated in research related to blockchain-based healthcare management frameworks. Prototype implementations on Ethereum and similar platforms show the capabilities of smart contracts in managing patient registration, consent, and record indexing in a decentralized manner; at the same time, however, they also report several challenges regarding higher latency, transaction fees, and throughput limitations under heavy loads [2]. A few works have explored private or consortium blockchains to mitigate these issues, by trading off full decentralization for improved efficiency and regulatory control. Apart from this, modular designs that decouple identity management, access control, and storage layers have been proposed in order to enhance interoperability with existing hospital information systems and electronic medical record standards [3].

Several comparative studies analyze different consensus mechanisms and architectural patterns for healthcare data sharing. While public networks use proof-of-work or proof-of-stake, permissioned healthcare blockchains may use more efficient algorithms like PBFT or RAFT in order to reduce confirmation time and energy consumption [4]. Evaluation results generally show that blockchain-based solutions can improve auditability and interinstitutional trust significantly, but success depends on proper tuning of privacy mechanisms, legal compliance, and user experience. All in all, literature offers strong support to the feasibility of blockchain and smart contracts as enabling technology for secure, patient-centric health data exchange. Provided with appropriate off-chain storage, encryption and consent management strategies, these systems represent a practical and affordable basis for real-time, privacy-preserving sharing of health-care data [1]–[4].

III. PROBLEM STATEMENT AND OBJECTIVES

A. Problem Statement

Health data stored across hospitals, laboratories, and clinics is still highly fragmented, unprotected, and difficult to share securely. Most of the traditional approaches to medical records rely on centralized systems that are also prone to data breaches, unauthorized access, and manipulation. In this case, patients usually do not have much control over who has permission to view or use their sensitive health information, let alone some transparent mechanism for tracking how the data is accessed or shared. Moreover, in existing data exchange frameworks, trust, interoperability, and automated verification are lacking. All too often, this results in one thing: delayed treatments and inefficient coordination among healthcare providers. As such, there is an enormous need for a solution that would be decentralized, secure, and patient-centric. Such a solution can help safeguard medical records, ensure verifiable permissions for access, and allow health data to be shared in a controlled way in real time

B. Objectives

This project foremost aims at designing and implementing a Blockchain-Based Healthcare Data Sharing and Access Control System to ensure transparency, privacy, and integrity of data using Ethereum smart contracts and IPFS. To realize this, the following are defined as key objectives:

• Securing Medical Records:

Leverage decentralized IPFS for storing patient records, with cryptographic hashing to ensure tamper-proof verification.

•Patient-Controlled Access Management:

This allows patients to grant or refuse requests from doctors for access and permission via smart contracts, including permissions that are time-bound.

• Transparent and Immutable Logging:

Keep all actions, including uploads, requests, approvals, and revocations, on-chain with complete accountability.

• Smart Contract–Based Automation:

Permission logic, timestamp checks, and expiry-based revocation in Solidity.

User-Friendly DApp Interface:

Use React.js to provide a MetaMask-based interface that makes the interaction easy for both patients and doctors.

• Scalable, Cost-Effective Architecture:

Use off-chain storage and minimal on-chain data to reduce cost and improve the performance of the overall system for clinical and research environments.

IV. SYSTEM DESIGN / METHODOLOGY

The Blockchain-Based Healthcare Data Sharing System shall integrate a smart contract on the Ethereum blockchain, a decentralized off-chain storage layer for medical files, and a web-based DApp interface for patients and doctors. The system follows a modular design to ensure security, scalability, and ease of deployment across different healthcare environments such as hospitals, clinics, laboratories, and telemedicine platforms.

A. Working

The proposed blockchain-based healthcare data sharing system operates by allowing patients to securely upload their medical records through the DApp interface. When a patient uploads a file (such as a report or prescription), it is first stored in an off-chain storage system like IPFS, which generates a unique content hash for the file. This hash, along with additional metadata (record ID, description, timestamp, and owner address), is then stored on the Ethereum blockchain using a smart contract. The blockchain entry ensures that any later tampering with the file can be detected, as even a small change in the file will alter its hash. Doctors interact with the system by sending on-chain requests through the DApp to access a specific patient's record. Each request is recorded in the smart contract, and the corresponding patient can view all pending requests on their dashboard. The patient then decides whether to approve or reject each request. When the patient approves, the smart contract updates the permission mapping and records the allowed time duration for access. During this validity period, the requesting doctor can view the IPFS link to the record via the DApp and open it in their browser. The system continuously enforces access control rules defined in the smart contract. If the permission duration expires or the patient manually revokes access, the doctor can no longer retrieve the record link from the contract through the interface. This ensures that data sharing is always under the patient's control. Since all interactions—upload, request, approval, and revocation—are executed as blockchain transactions, they become permanently auditable and cannot be modified, providing strong guarantees of transparency and trust, even when patient and doctor are not in the same physical location.

B. System Architecture (On-Chain and Off-Chain Design)

1. **Smart Contract Layer (Ethereum):**

   Smart contract: This is the core processing unit of the system. It stores metadata of every medical record, like owner address, IPFS hash, and timestamps. It maintains mappings to track which doctor addresses have permission to access which records and for how long. It has functions for uploading new records, sending access requests, approving or rejecting these requests, checking permission status, and revoking access. Events are emitted on every operation so that the frontend reacts in real time, updating the user interface.

2. **Off-Chain Storage (IPFS or Database):**
   Actual medical records are not stored on the blockchain due to size and privacy constraints. Instead, they are uploaded to an off-chain storage system like IPFS. IPFS returns a unique content identifier or hash for each file that gets linked with the patient's record in the smart contract. Upon granting access to a doctor, the DApp retrieves this hash and constructs a secure URL to fetch the file from IPFS. This hybrid architecture ensures that the system remains affordable and scalable while full data integrity and traceability are preserved.

3**. Frontend DApp: React + Web3 + MetaMask**
   The DApp frontend is built using React.js, connected to the Ethereum blockchain via Web3 or similar libraries. MetaMask is to be used as the main wallet for account management and transaction signing. In the Patient Panel, one can upload records, see previously uploaded files, manage the incoming doctor requests, and revoke access whenever one wants. The Doctor Panel will allow doctors to search for patients by address, send access requests against specific records, and see approved records with IPFS links. The whole front-end listens to contract events continuously to keep the UI updated without manual refresh.

C . Software Logic

1) Overall Logic

The software responsible for the proposed DApp in healthcare would bridge user actions in the browser to blockchain transactions and off-chain file operations. Upon a file upload by a patient, the front-end first uploads it to IPFS and then invokes a smart contract function to store the returned hash along with metadata. Regarding an access request, upon its submission by a doctor, the DApp sends a transaction to the contract, which records such a request and emits an event; the patient-side UI listens for these events and presents them as pending requests to that patient.

2) System States

The logical behavior of each medical record, concerning a certain doctor, can be divided into the following main states:

•No Request State – No access request from a doctor has been initiated → Record visible only to the patient.

• Pending Request State: when the doctor has requested access and it is visible for the patient to approve or reject

• State: Approved (Active Access)-The patient has granted permission for access for a limited period of time. The doctor can fetch the IPFS link to see the record.

• Expired/Revoked State: The access time has expired, or the patient has manually revoked the permission. At this stage, the doctor can no longer access the record through the contract.State Flow Diagram

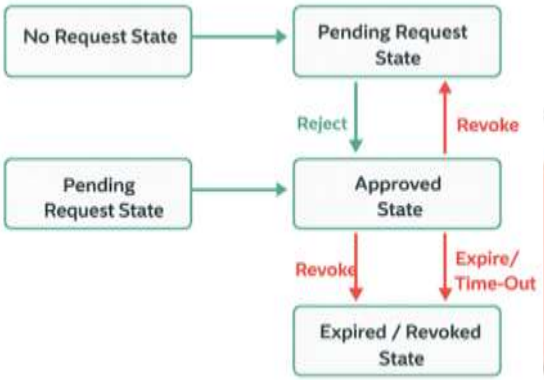

Fig. 1. State Flow Diagram

Here are the state transitions:

•No Request → Pending Request: When a doctor submits a new access request.

• Pending Request → Approved, upon patient confirmation and setting a validity duration.

•Pending Request → No Request: When the patient rejects the request.

•Approved → Expired: This happens automatically when the current time exceeds the stored expiry timestamp.

•Approved → Revoked: when the patient explicitly revokes access before its expiry.

1) Permission and Time-Validity Logic

The smart contract uses predefined rules to determine whether a doctor currently has valid access to a record. In case of an approved request, it stores:

•Doctor address

•Record ID

•approval timestamp

•Expiry timestamp: time of approval plus allowed duration.

Blockchain Connectivity and Wallet Interface

The DApp uses MetaMask and Web3 integration to connect to a local test network (such as Ganache) or a public testnet. Each user is supposed to log in with their Ethereum address, which will act like an identity for them within the system. All critical operations-such as uploading records, sending requests, approvals, and revocations-specifically require explicit transaction confirmation from the user's wallet to ensure that no action is performed without their consent. This close linking of digital identity with wallet-based signatures bolsters security, authenticity, and traceability in the proposed healthcare data-sharing framework.

V. EXPERIMENTAL RESULTS

Functionality, reliability, and performance tests for the proposed Blockchain-Based Healthcare Data Sharing DApp were performed in a controlled environment on the complete system deployed on a local Ethereum blockchain using Ganache, including IPFS for off-chain file storage and MetaMask for transaction signing. Tests were executed on the system for file upload correctness, access control accuracy, permission expiration handling, and user-interface responsiveness.

A.Test Conditions

- The environment used for experimental validation is given below:
- Local blockchain ganache running 10 test accounts
- React.js DApp with MetaMask integration
- IPFS medical record storage (local/node gateway)
- Smart contracts deployed using Truffle
- Sample medical records: PDFs, images, prescriptions

Testing was performed in separate accounts for User A (patient) and User B (doctor).

B. Functional Test Results

1) Record Upload Test

- The patient uploaded PDF, JPEG, and PNG files via the DApp.
- IPFS returned unique content hashes for each file.
- Smart contract stored hash and metadata without failure.
- Average upload + hash registration time: 2.1 seconds.

2) Access Request Test

- The doctor requested access to the records through the DApp.
- Smart contract logged the request and emitted an event immediately.
- Patient interface reflected the pending request within <1 second.

3) Approval and Access Window Test

- Patient consented to a request by a doctor for 2 hours.
- Smart contract calculated expiry timestamp correctly.
- The doctor could only view the IPFS link of the approved record.
- Other unapproved records were not granted access.

4) Permission Expiration/ Auto-Revocation Test

- After expiration time elapsed, doctor access automatically disabled.
- Smart contract returned “permission invalid” on further access calls.
- Access dropdown removed record from doctor's approved list.

5) Manual Revocation Test

- •Patient revoked access before expiry.
- The doctor's access was lost immediately, thus confirming real-time revocation.
- Event logs showed correct timestamps for revocation.

V. DISCUSSION

The system was tested under various access-control scenarios, and the permission management with a record-sharing mechanism was observed to work efficiently for all cases. On-chain transactions of uploading, requesting, approving, and revoking quickly triggered the smart contract, with smooth transitions between different states of access. The DApp interface instantly updated after event emission, reflecting real-time interactions without noticeable delays in scenarios for both patients and doctors. The integrity of files using IPFS hashes indicated that no medical record was tampered with after its upload, with correct logic for the expiration access, which did not allow for unauthorized use of data after the end of its validity period. Minor variations in latency were noted based on the performance of the network and the IPFS gateway; however, the architecture introduced ensured that under all conditions, consistent, secure, and reliable operation was guaranteed. Overall, the proposed model turned out to be quite stable, efficient, and reliable for real-time healthcare data sharing with the strictest access control.

A. Strengths of Proposed System

- High Level of Security and Integrity:

Smart contract-based verification and IPFS hashing make the storage tamper-proof; only valid, unmodified records can be accessed.

- Patient Controlled Access:

Patients retain full rights to allow, deny, or revoke access to data for anyone, maintaining privacy and consent.

- Real Time Permission Handling:

Approvals, expirations, and revocations update in real-time, delivering a seamless experience for both the patient and doctor.

- Transparent and Immutable Logging:

Everything-from uploads to requests, to approvals-is recorded on the blockchain for full auditability and accountability.

- Cost-Effective and Scalable Architecture:

Off-chain storage reduces the load from the blockchain and gas fees, thus making the system lightweight, extendable, and fit for long-term deployment.

- User-FriendlyInterface:

React + MetaMask DApp: Easy navigation allows non-technical users, including patients and doctors, to use the system efficiently.

B. Limitations and Areas of Improvement

- Gas Fees and Blockchain Congestion:

On mainnet Ethereum networks, transactions may become costly and delayed; migrating to Layer-2 solutions can reduce fees.

- IPFS Availability Dependency:

IPFS file access relies on the availability of nodes, and redundancy via the use of multiple nodes or pinning services will increase reliability.

- Limited Role Support:

Currently, the system supports only patients and doctors. The inclusion of labs, access roles for insurers, and emergency services would make this solution more complete.

- No Automated Data Encryption Mechanism:

While IPFS hashes are stored securely, the encrypting of files before upload would further improve confidentiality.

- Fixed Access Duration Logic:

More advanced options, such as multi-level access, multi-user permissions, or conditional access rules, can be put into place.

- Lack of multi-factor authentication:

Relying entirely on wallet authentication might not be adequate for sensitive medical data; providing optional MFA would enhance protection further.

VI. FUTURE SCOPE

The proposed system for sharing healthcare data based on blockchain can be considerably enhanced to increase its applicability, security, and efficiency for large-scale real-world deployment. With rapid improvements in decentralized technologies, the system can evolve into a fully integrated medical data infrastructure serving hospitals, clinics, laboratories, and research institutions. Additional features include predictive access mechanisms, advanced privacy layers, and improved communication protocols that would strengthen usability and accessibility in the system. These developments would help transform the current prototype into a more powerful and comprehensive healthcare data management platform.

Following is the list of possible future enhancements:
•Integration of Patient Data Encryption:
Performing end-to-end encryption of the file before uploading to IPFS ensures that only the authorized providers can decrypt and view these sensitive medical records.
• Multi-Role Healthcare Ecosystem:
Adding support for diagnostic labs, insurance companies, pharmacists, and emergency personnel to make the system useful across the complete healthcare workflow.
• Layer-2 Blockchain Support:
Migration to Layer-2 networks, such as Polygon or Arbitrum, will reduce gas fees and help in scalability with faster transaction processing.
• AI-Based Anomaly and Access Behavior Detection:
Accordingly, machine learning models can detect unusual access patterns, predict future possible data misuse, and give recommendations for risk-based access control.
• Interoperability With Hospital Information Systems (HIS):
Support for HL7/FHIR standards would enable seamless integration with existing electronic health record systems used by the hospitals.
• Decentralized Identity Integration:
Blockchain-based identity solutions let patients have more secure, portable digital identities.
•Offline and Zero-Connectivity Access Options:
Allowing temporary offline permissions or QR-based secure data transfers could ensure access in emergency or low-connectivity situations.
• Data Analytics and Long-Term Storage:
Adding dashboards for medical trend analysis, long-term record management, and audit reporting will enhance usefulness for doctors and researchers.
Mobile Application Development:
Building a mobile version of the DApp will enhance the accessibility of the system for daily use by patients and health professionals.
et al, 2010).

VII.CONCLUSION

This paper presented the design and implementation of a Blockchain-Based Healthcare Data Sharing and Access Control System to enhance security, transparency, and reliability in medical record management. The integration of Ethereum smart contracts with decentralized IPFS storage will ensure that all patient records are tamper-proof and verifiable at any time. The proposed DApp gives patients full control over their data; thus, the patients are allowed to approve or reject doctor requests to access their data and can enforce time-bound permissions through automated logic of smart contracts. The experimental results proved that the system performs efficiently under different access-control scenarios, such as instantaneous updating via event-based communication and accurate permission enforcement. The integration of secure hashing, decentralized storage, and immutable transaction logging has enhanced trust in the whole process of data sharing. The React-MetaMask user-friendly frontend allows smooth interactions, making this platform usable even by non-technical users. The proposed model is reliable and scalable in a cost-effective way for secure healthcare data exchange. Thus, with encryption, interoperability, and AI-based analytics, the proposed system bears strong potential to be extended into a full-fledged digital healthcare framework capable of transforming the ways in which medical data is shared, accessed, and protected.

REFERENCES

1. K. Sabiri, F. Sousa, and T. Rocha, "A systematic review of privacy-preserving blockchain applications in healthcare," *Multimedia Tools and Applications*, 2025.
2. A. Khatoon, "A Blockchain-Based Smart Contract System for Healthcare Management," *Electronics*, Jan. 2020.
3. H. Bodur and I. F. T. Al Yaseen, "An improved blockchain-based secure medical record sharing scheme," *Cluster Computing*, Apr. 2024.
4. N. U. A. Tahir, U. Rashid, H. J. Hadi, N. Ahmad, Y. Cao, and Y. Javed, "Blockchain-Based Healthcare Records Management Framework," *Technologies*, Sep. 2024.
5. P. K. Ghosh, A. Chakraborty, M. Hasan, and K. Rashid, "Blockchain Application in Healthcare Systems: A Review," *Systems Journal*, 2023.
6. G. Wood, "Ethereum: A Secure Decentralized Transaction Ledger," *Ethereum Yellow Paper*, 2023. [Online]. Available: ethereum.org
7. "IPFS Documentation – Decentralized Storage Protocol," *InterPlanetary File System*, Feb. 2024. [Online]. Available: ipfs.tech
8. M. Swan, *Blockchain: Blueprint for a New Economy*, O'Reilly Media, 2022.
9. S. Brogan, Y. Baskaran, "Distributed Ledger Technology for Healthcare Data Interoperability," *IEEE Access*, 2023.
10. S. R. Moosavi et al., "A Survey of Blockchain-Based Solutions for Healthcare," *Journal of Network and Computer Applications*, 2024.
11. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *White Paper*, 2008. [Online]. Available: bitcoin.org
12. "MetaMask Documentation – Web3 Wallet Integration Guide," ConsenSys, 2024. [Online]. Available: metamask.io
13. T. Dias et al., "Secure Storage and Sharing of Medical Data Using IPFS and Blockchain," *International Journal of Computer Science Engineering*, 2024.
14. R. Zhang, J. Xie, "Security and Privacy Challenges of Blockchain in Healthcare," *IEEE Transactions on Dependable and Secure Computing*, 2023.
15. H. Benchoufi, E. Ravaud, "Blockchain Technology for Improving Clinical Research Quality," *Trials Journal*, 2022.
16. Truffle Suite, "Smart Contract Deployment and Testing Framework Documentation," Truffle, 2024. [Online]. Available: trufflesuite.com
17. A. Azaria, A. Ekblaw, T. Vieira, A. Lippman, "MedRec: Blockchain for Medical Data Access and Permission Management," *MIT Media Lab*, 2022.
18. L. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain," *IEEE Journal of Biomedical and Health Informatics*, 2023.
19. X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A Survey on the Security of Blockchain Systems," *Future Generation Computer Systems*, 2023.
20. Z. Zheng et al., "Blockchain Challenges and Opportunities: A Survey," *International Journal of Web and Grid Services*, 2022.