International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 2, Mar-Apr-2026, ISSN (Online): 2395-566X

Blockchain-Based Police Complaint Management System for Secure and Transparent FIR Registration

Mrs. N. Nikhitha[1], Malla Sudarsan Sai Sunny[2], Guthula Surya Sindhu[3], Neelapalli Sri Durga Abhilasha[4], Govada Pavan Sai[5], Palisetti Siva Ram[6]

[1]Assistant Professor, Department of CSE (Data Science) In Pragati Engineering College, Surampalem, Andhra Pradesh, India,

[2,3,4,5,6] UG Students Department of CSE (Data Science) In Pragati Engineering College, Surampalem, Andhra Pradesh, India.

ABSTRACT:

The increasing rate of criminal activities and the limitations of existing police complaint systems highlight the need for a more transparent, secure, and efficient method for managing complaints and First Information Reports (FIRs). In many cases, complaints remain unreported or are not officially registered due to procedural delays, corruption, or lack of proper documentation systems. Although online portals such as the Crime and Criminal Tracking Network and Systems (CCTNS) have been introduced, they still operate on centralized architectures that may suffer from issues such as single points of failure, limited transparency, and vulnerability to data tampering. To address these challenges, this study proposes a blockchain-based police complaint management system designed to provide secure, decentralized, and tamper-proof storage of complaint records. In the proposed system, complaint details and FIR records are encrypted and stored using the InterPlanetary File System (IPFS), while the corresponding hash values are recorded on a blockchain network to ensure immutability and data integrity. The decentralized nature of blockchain technology ensures that complaint records cannot be altered or deleted without network consensus, thereby preventing unauthorized modifications and enhancing system transparency. Additionally, timestamped blockchain entries provide verifiable proof of complaint submission, enabling citizens to demonstrate that their complaint was officially recorded even if authorities deny receiving it. By integrating blockchain with distributed file storage technologies, the proposed system enhances trust between citizens and law enforcement agencies while ensuring secure and transparent management of police complaints. The framework also supports the broader goals of e-governance by improving accountability, data security, and accessibility in public service systems.

Keywords: Blockchain Technology, Police Complaint Management System, First Information Report (FIR), InterPlanetary File System (IPFS), Decentralized Systems, E-Governance, Data Security.

I. INTRODUCTION

The rapid growth of digital technologies has significantly influenced the development of modern e-governance systems aimed at improving transparency, efficiency, and accessibility in public services. Among these services, the police complaint management system plays a crucial role in maintaining law and order by enabling citizens to report criminal activities and seek justice through formal legal procedures. In India and many other countries, criminal complaints are registered through documents such as the First Information Report (FIR) and Non-Cognizable Report (NCR). These reports serve as the foundation for initiating legal investigations and ensuring that crimes are officially recorded within the criminal justice system.

Despite the availability of online complaint portals and digital record management systems, many police departments still rely on traditional manual procedures for registering complaints. In several cases, FIRs are handwritten and stored in centralized databases maintained by individual police stations or state authorities. Such systems often suffer from issues including delays in complaint registration, lack of transparency, data manipulation, and difficulties in accessing complaint records. Additionally, centralized systems are vulnerable to single points of failure and potential security breaches, which may compromise the integrity and availability of critical legal records [3], [4].

To improve the management of criminal records and police complaints, the Government of India introduced the Crime and Criminal Tracking Network and Systems (CCTNS) as part of its e-governance initiative. The primary objective of CCTNS is to integrate police stations across the country through a centralized digital platform for recording and managing crime-related information. Although the system has improved the digitization of crime records, it still operates using centralized architecture, which may limit transparency and create potential risks related to data tampering or unauthorized access to sensitive information [1], [2].

In recent years, blockchain technology has emerged as a promising solution for addressing challenges related to data security, transparency, and trust in digital systems. Blockchain is a decentralized and distributed ledger technology that records transactions across multiple nodes in a network, ensuring that once data is stored, it cannot be altered or deleted without consensus from the network participants. The immutability and cryptographic security of blockchain make it particularly suitable for applications that require secure record keeping and tamper-proof data management. The first practical application of blockchain technology was introduced through Bitcoin by Satoshi Nakamoto, demonstrating the feasibility of decentralized digital transaction systems [5].

In addition to blockchain technology, distributed storage systems such as the InterPlanetary File System (IPFS) provide efficient mechanisms for storing large files in a decentralized network. IPFS uses content-based addressing to store and retrieve files based on cryptographic hashes, ensuring data integrity and reliability. Integrating IPFS with blockchain technology allows systems to store large documents securely while maintaining a verifiable reference to the data within the blockchain network. This combination enables scalable and tamper-resistant storage of digital records in decentralized applications [6].

Motivated by these technological advancements, this study proposes a blockchain-based police complaint management system designed to enhance transparency, security, and reliability in the process of filing and managing police complaints. In the proposed system, complaint records and FIR documents are encrypted and stored using IPFS, while their corresponding cryptographic hashes are recorded on a blockchain network. This decentralized architecture ensures that complaint records remain immutable and verifiable, preventing unauthorized modifications and providing timestamped proof of complaint submissions.

The remainder of this paper is organized as follows. Section II presents a review of related research studies in blockchain-based governance and secure complaint management systems. Section III analyses the limitations of the existing police complaint management systems and introduces the proposed

decentralized framework. Section IV describes the system architecture and design methodology of the proposed blockchain-based solution. Section V explains the implementation modules and system components. Section VI discusses the experimental results and system evaluation. Finally, Section VII concludes the paper and outlines possible directions for future research.

II. LITERATURE SURVEY

In recent years, the adoption of digital technologies in governance systems has increased significantly, leading to the development of secure and transparent platforms for managing public services. One such critical area is the management of police complaints and criminal records. Traditional systems for registering and managing complaints often rely on centralized databases and manual documentation processes, which may lead to inefficiencies, lack of transparency, and potential manipulation of records. With the increasing availability of advanced technologies such as blockchain and distributed storage systems, researchers have begun exploring innovative approaches to improve the security and transparency of public service systems [3], [4].

Nakamoto introduced the concept of blockchain technology through the Bitcoin digital currency system, demonstrating the possibility of maintaining a decentralized and tamper-proof ledger of transactions across a peer-to-peer network. The core idea behind blockchain is to store data in a distributed ledger where each block is cryptographically linked to the previous block, ensuring data integrity and preventing unauthorized modifications. This decentralized architecture eliminates the need for a central authority while maintaining trust among participants in the network [5].

Several researchers have investigated the use of blockchain technology in e-governance applications to enhance transparency and accountability. Blockchain-based systems can store sensitive records securely while providing verifiable proof of transactions through cryptographic hashing and consensus mechanisms. These features make blockchain particularly suitable for applications such as digital identity management, voting systems, healthcare records, and government document management. The immutability and distributed nature of blockchain ensure that once data is recorded, it cannot be altered without the consensus of the network participants [1], [2].

In addition to blockchain technology, distributed file storage systems have been developed to improve the efficiency and reliability of storing large digital documents. The InterPlanetary File System (IPFS) is a peer-to-peer distributed file storage protocol that enables secure and decentralized storage of files using content-based addressing. Instead of storing files in a centralized server, IPFS distributes data across multiple nodes in a network, ensuring high availability and resistance to data loss. Each file stored in IPFS is assigned a unique cryptographic hash, which can be used to retrieve and verify the integrity of the stored content [6].

Researchers have also explored the integration of blockchain with IPFS to develop secure and scalable decentralized applications. In such systems, large documents or files are stored in IPFS, while the corresponding cryptographic hash is stored on the blockchain network. This approach combines the immutability of blockchain with the efficient distributed storage capabilities of IPFS, enabling the creation of secure record management systems for sensitive data. Applications of this architecture include digital certificate verification, document

authentication systems, and decentralized data storage platforms [7].

Despite these advancements, many existing police complaint management systems still rely on centralized architectures that may suffer from issues such as lack of transparency, potential manipulation of complaint records, and limited accessibility for citizens. In certain situations, complaints may not be officially recorded due to administrative delays or external pressures on law enforcement authorities. Additionally, centralized databases are vulnerable to security breaches and single points of failure, which may compromise the integrity and availability of critical legal records.

Therefore, there is a growing need for a decentralized and secure complaint management system that ensures transparency, accountability, and data integrity. By leveraging blockchain technology and distributed storage systems such as IPFS, it is possible to create a tamper-proof platform for managing police complaints and FIR records. Such systems can provide timestamped proof of complaint submissions, prevent unauthorized data modifications, and enhance trust between citizens and law enforcement agencies.

III. SYSTEM ANALYSIS

A. EXISTING SYSTEM

Traditional police complaint management systems primarily rely on manual documentation and centralized digital databases to record criminal complaints such as First Information Reports (FIRs) and Non-Cognizable Reports (NCRs). In many regions, complaints are still recorded manually in police stations, where officers write FIR details in physical registers or store them in local digital systems. Although such procedures allow authorities to maintain official records of crimes, they often introduce delays and inefficiencies in complaint registration and management.

To improve the digitalization of crime records, several governments have implemented centralized e-governance systems. One such initiative is the Crime and Criminal Tracking Network and Systems (CCTNS) introduced in India. The CCTNS platform was designed to connect police stations across different states and maintain a centralized repository of criminal records and complaints. While this system has improved the accessibility of crime data and enhanced coordination among law enforcement agencies, it still operates on centralized architecture. Centralized systems may face challenges such as single points of failure, limited transparency, and potential vulnerabilities to cyber-attacks or unauthorized data manipulation [1], [2].

Furthermore, in many cases complainants are required to physically visit police stations to file their complaints. This requirement can discourage individuals from reporting crimes, particularly in situations where victims may fear intimidation or lack access to nearby police stations. Additionally, there have been instances where complaints are not officially registered due to administrative delays, external pressure, or corruption within the system. In such cases, complainants may not have sufficient proof that they attempted to report an incident.

The storage of complaint records in centralized databases also introduces concerns related to data security and record manipulation. Since centralized systems rely on a single database server or administrative authority, there is a possibility that records could be modified, deleted, or altered without proper verification. This lack of transparency can

reduce public trust in law enforcement systems and hinder the effective administration of justice [3], [4].

Recent developments in digital technologies have highlighted the importance of secure and decentralized systems for managing sensitive records. However, many existing complaint management systems have not fully adopted advanced technologies such as blockchain or distributed storage networks that can ensure data integrity and tamper-proof record keeping. As a result, existing systems continue to face challenges related to transparency, security, and accessibility of complaint records.

LIMITATIONS OF EXISTING SYSTEM

Manual and paper-based processes: Many police stations still rely on handwritten FIR records, which can lead to delays, human errors, and inefficient record management.

Centralized system architecture: Systems such as CCTNS operate on centralized databases that are vulnerable to single points of failure and potential cyber threats.

Limited transparency: Complainants often have limited visibility into the status of their complaints, which can reduce trust in the complaint management process.

Possibility of record manipulation: Centralized databases may allow unauthorized modifications or deletion of complaint records without proper verification.

Limited proof of complaint submission: If a complaint is not officially registered, citizens may lack verifiable evidence that they attempted to report an incident.

Accessibility challenges: Requiring individuals to visit police stations physically to file complaints may discourage reporting and reduce system efficiency.

A. PROPOSED SYSTEM

To overcome the limitations of the existing police complaint management systems, this study proposes a blockchain-based decentralized complaint management framework designed to improve transparency, security, and reliability in the complaint registration process.

In the proposed system, complaint records such as FIRs are encrypted and stored in the InterPlanetary File System (IPFS), which is a decentralized file storage network capable of securely storing large digital documents. Each stored file generates a unique cryptographic hash, which acts as a digital fingerprint of the document.

The corresponding hash value of the stored complaint record is then recorded on a blockchain network, creating a permanent and immutable record of the complaint. Blockchain technology ensures that once a complaint record is added to the ledger, it cannot be modified or deleted without the consensus of the network participants. This feature prevents unauthorized manipulation of complaint records and guarantees data integrity.

The decentralized architecture of the proposed system eliminates the risk of a single point of failure and ensures continuous availability of complaint records across multiple nodes in the network. Additionally, the blockchain ledger records timestamps for every complaint submission, providing verifiable proof that a complaint was filed at a specific time. This feature enables complainants to demonstrate that their complaint was officially recorded even if authorities later deny receiving it.

International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 2, Mar-Apr-2026, ISSN (Online): 2395-566X

By integrating blockchain technology with distributed storage systems such as IPFS, the proposed system enhances security, transparency, and trust in the police complaint management process. The framework aims to strengthen e-governance systems by providing a reliable platform for managing complaints while protecting sensitive information from unauthorized access or tampering [3], [5].

IV. SYSTEM DESIGN

SYSTEM ARCHITECTURE

Below diagram depicts the whole system architecture.

Fig 1. Methodology Followed for Proposed Model

Fig 1. Methodology followed for proposed model

V. SYSTEM IMPLEMENTATION

MODULES

This section describes the main implementation modules of the proposed Blockchain-Based Police Complaint Management System. The system is designed using a modular architecture that integrates user authentication, complaint submission, encryption, blockchain storage, IPFS file management, and complaint verification mechanisms. This modular approach improves the system's reliability, scalability, security, and transparency in handling police complaints and FIR records.

A. User Authentication and Authorization Module

The User Authentication and Authorization Module manages secure access to the system by verifying the identity of users before allowing them to perform any actions. The system supports different types of users such as citizens (complainants), police officers, and administrative authorities. During the login process, users are required to provide valid credentials such as username and password. The authentication mechanism verifies the credentials using secure database queries and access control policies. Once authenticated, the system assigns appropriate permissions based on the user's role. This module ensures that only authorized individuals can access sensitive information such as complaint records, FIR documents, and case details. By implementing secure authentication and role-based authorization, the system protects confidential data and prevents unauthorized access or misuse of the complaint management platform.

B. Complaint Submission and Encryption Module

The Complaint Submission Module allows citizens to file complaints online through a user-friendly web interface. The interface enables users to enter

complaint details such as the complainant's name, incident description, date, time, location, and supporting evidence or documents. Once the complaint information is submitted, the system automatically processes the data and encrypts the complaint record to protect sensitive information. Encryption ensures that only authorized individuals can access the complaint data and prevents unauthorized viewing or modification of confidential records. The encrypted complaint document, which represents the First Information Report (FIR) or complaint record, is then prepared for decentralized storage. This step ensures the confidentiality and security of complaint data before it is stored in the distributed file storage network.

C. IPFS Storage Module

The InterPlanetary File System (IPFS) Storage Module is responsible for securely storing encrypted complaint documents in a decentralized file storage network. Instead of storing complaint records in a centralized server, the IPFS system distributes files across multiple nodes in a peer-to-peer network. Each stored file generates a unique cryptographic hash, which acts as the digital fingerprint of the stored complaint document. This content-based addressing mechanism ensures that the stored file cannot be altered without changing its hash value. As a result, any unauthorized modification of complaint data becomes immediately detectable.

The IPFS module improves system reliability by ensuring that complaint records remain accessible even if certain nodes in the network fail. It also reduces the risk of data loss and enhances the scalability of the complaint management system.

D. Blockchain Integration Module

The Blockchain Integration Module is the core component of the proposed system. This module records the cryptographic hash generated by the IPFS storage system onto a blockchain network. Blockchain technology maintains a decentralized ledger where each transaction is stored in blocks that are cryptographically linked to one another. Once a block containing complaint data is added to the blockchain, it becomes immutable and tamper-proof. Smart contracts are used within this module to automate the process of recording complaint hashes on the blockchain network. These smart contracts ensure that every complaint submission is recorded with a timestamp and verification details, which provides proof that the complaint was officially registered.

The decentralized architecture of blockchain eliminates the risk of a single point of failure and ensures that complaint records cannot be modified or deleted without consensus from the network participants.

E. Complaint Verification and Case Management Module

The Complaint Verification and Case Management Module enables authorized police officers to verify and manage complaint records stored on the blockchain network.

Police personnel can access complaint details, verify the authenticity of records through blockchain hashes, and track the status of each case. Since every complaint record is linked to a timestamped blockchain entry, officers can confirm whether a complaint was officially submitted and stored in the system.

This module also allows officers to update the status of complaints, assign investigations, and generate reports related to complaint cases. The ability to verify complaint records through blockchain significantly improves transparency and

accountability within the complaint management process.

F. Complaint Tracking and Notification Module

The Complaint Tracking and Notification Module allows complainants to track the status of their submitted complaints. Users can log into the system and view updates regarding their complaint, including verification status, investigation progress, and case resolution information. Additionally, the system can send automated notifications through email or system alerts to inform users about updates related to their complaints. This feature improves communication between citizens and law enforcement authorities while enhancing transparency in the complaint handling process.

By integrating these modules, the proposed system provides a secure, decentralized, and transparent platform for managing police complaints and FIR records. The use of blockchain technology and distributed storage systems ensures the integrity, confidentiality, and reliability of complaint records while promoting trust between citizens and law enforcement agencies.

VI. RESULTS AND DISCUSSION

This section presents the implementation results and performance evaluation of the proposed Blockchain-Based Police Complaint Management System. The primary objective of the system is to improve transparency, security, and reliability in the process of registering and managing police complaints. The system integrates blockchain technology and the InterPlanetary File System (IPFS) to ensure secure storage and tamper-proof management of complaint records. The evaluation focuses on analyzing system reliability, data security, complaint verification mechanisms, and the efficiency of decentralized record management.

A. Performance Evaluation of Complaint Management System

The proposed system was implemented using modern web technologies and blockchain integration to evaluate its ability to securely manage complaint records. The system allows citizens to register complaints through an online interface, after which the complaint data is encrypted and stored in IPFS. The cryptographic hash generated by IPFS is then recorded on the blockchain network to ensure immutability and transparency.

The system was evaluated based on several performance factors including complaint submission time, record verification time, system security, and reliability of decentralized storage.

Table 1. Performance Evaluation of the Proposed Complaint Management System

System Component	Performance Result
Complaint Submission Time	1.8 seconds
IPFS File Storage Time	2.4 seconds
Blockchain Hash Recording	1.2 seconds
Complaint Verification Time	0.9 seconds
Data Integrity	100% Verified
Tampering Detection	Successfully Detected

From the experimental results, it can be observed that the proposed system efficiently processes complaint submissions and securely stores complaint records in the decentralized storage network. The integration of blockchain ensures that all complaint records remain immutable and protected from unauthorized modifications.

B. Blockchain Record Verification Analysis

Blockchain technology plays a critical role in ensuring the integrity and authenticity of complaint records. Each complaint submitted through the system generates a unique cryptographic hash that is stored on the blockchain ledger along with a timestamp

.

Fig. 2. Blockchain Complaint Verification Process

Fig. 2. Blockchain Complaint Verification Process

The blockchain ledger records all complaint transactions in a distributed network of nodes. Once a complaint record is added to the blockchain, it becomes practically impossible to alter or delete the record without consensus from the network participants.

The timestamped blockchain records provide verifiable proof that a complaint was submitted at a specific time. This feature is particularly important in situations where authorities may deny receiving a complaint. Citizens can use the blockchain record as evidence that the complaint was officially registered in the system.

The experimental results show that the blockchain network successfully validates complaint records while maintaining high levels of security and transparency in the complaint management process.

C. Complaint Record Integrity Analysis

To evaluate the security of complaint records stored in the system, data integrity analysis was performed using cryptographic hashing mechanisms provided by IPFS and blockchain.

Fig. 3. Complaint Record Integrity Verification

Fig. 3. Complaint Record Integrity Verification

The analysis demonstrated that any attempt to modify the stored complaint data results in a mismatch between the original hash stored on the blockchain and the newly generated hash from the modified file. This mismatch immediately indicates that the data has been tampered with.

The decentralized storage architecture ensures that complaint records remain consistent across all nodes in the network. Since each record is cryptographically secured, unauthorized alterations are automatically detected by the system.

The results confirm that the proposed system effectively maintains the integrity, transparency, and reliability of police complaint records, ensuring that sensitive legal documents remain protected against unauthorized access or manipulation.

By integrating blockchain technology and decentralized file storage, the proposed framework provides a robust solution for secure complaint management and enhances trust between citizens and law enforcement agencies [1], [2], [5].

VII. CONCLUSION AND FUTURE WORK

This study proposed a blockchain-based police complaint management system designed to improve transparency, security, and accountability in the complaint registration and investigation process.

Traditional complaint management systems often rely on centralized databases that are vulnerable to data manipulation, unauthorized access, and lack of transparency. Such limitations can lead to loss of public trust and inefficiencies in handling sensitive complaints. The proposed framework addresses these challenges by leveraging blockchain technology to create a decentralized and tamper-resistant platform for complaint recording and verification [1], [2].

In the proposed system, complaints submitted by citizens are securely stored using cryptographic techniques, and a unique hash value is generated for each complaint record. This hash is recorded on the blockchain network, ensuring that once the complaint data is stored, it cannot be altered without detection. The decentralized nature of blockchain guarantees that complaint records remain transparent and verifiable across multiple nodes, thereby preventing unauthorized modification or deletion of information. This mechanism significantly improves data integrity, accountability, and trust in the complaint management process [3], [4].

The system also introduces an integrity verification mechanism that compares stored complaint data with blockchain-recorded hash values. If any attempt is made to tamper with the complaint records, the mismatch in hash values immediately reveals the modification. This capability ensures reliable evidence management and strengthens the credibility of digital complaint records. Additionally, blockchain technology helps maintain an immutable audit trail, allowing authorities to track complaint handling processes in a secure and transparent manner [5], [6].

Overall, the proposed framework demonstrates how blockchain technology can enhance the efficiency, security, and reliability of police complaint management systems. By ensuring data immutability and decentralized verification, the system can help reduce corruption risks, prevent data manipulation, and improve public confidence in law enforcement processes.

Future research may focus on integrating smart contracts to automate complaint verification and case management workflows. Further improvements may include incorporating identity verification mechanisms, secure authentication techniques, and integration with national digital governance platforms. In addition, deploying the system on scalable blockchain infrastructures and integrating advanced technologies such as Artificial Intelligence for complaint categorization and analytics can further enhance the effectiveness of the proposed platform in large-scale law enforcement environments [7], [8].

REFERENCES

1. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.
2. M. Swan, Blockchain: Blueprint for a New Economy, Sebastopol, CA, USA: O’Reilly Media, 2015.
3. M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, “Blockchain Technology: Beyond Bitcoin,” Applied Innovation Review, no. 2, pp. 6–19, 2016.
4. A. Dorri, S. S. Kanhere, and R. Jurdak, “Blockchain in Internet of Things: Challenges and Solutions,” IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8076–8086, 2019.
5. K. Christidis and M. Devetsikiotis, “Blockchains and Smart Contracts for the Internet of Things,” IEEE Access, vol. 4, pp. 2292–2303, 2016.

6. Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in Proc. IEEE International Congress on Big Data, 2017, pp. 557–564.
7. M. Conoscenti, A. Vetrò, and J. C. De Martin, "Blockchain for the Internet of Things: A Systematic Literature Review," IEEE/ACS International Conference on Computer Systems and Applications, 2016.
8. Y. Yuan and F. Y. Wang, "Blockchain and Cryptocurrencies: Model, Techniques, and Applications," IEEE Transactions on Systems, Man, and Cybernetics, vol. 48, no. 9, pp. 1421–1428, 2018.
9. A. Tapscott and D. Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World, New York: Penguin, 2016.
10. W. Viriyasitavat and D. Hoonsopon, "Blockchain Characteristics and Consensus in Modern Business Processes," Journal of Industrial Information Integration, vol. 13, pp. 32–39, 2019.
11. T. M. Fernández-Caramés and P. Fraga-Lamas, "A Review on Blockchain Technologies for an Advanced and Cyber-Resilient Automotive Industry," IEEE Access, vol. 7, pp. 17578–17598, 2019.
12. M. Pilkington, "Blockchain Technology: Principles and Applications," in Research Handbook on Digital Transformations, Edward Elgar Publishing, 2016.
13. D. Drescher, Blockchain Basics: A Non-Technical Introduction in 25 Steps, Berkeley, CA, USA: Apress, 2017.
14. K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for AI: Review and Open Research Challenges," IEEE Access, vol. 7, pp. 10127–10149, 2019.
15. M. Casino, T. K. Dasaklis, and C. Patsakis, "A Systematic Literature Review of Blockchain-Based Applications," Telematics and Informatics, vol. 36, pp. 55–81, 2019.
16. N. Kshetri, "Blockchain's Roles in Meeting Key Supply Chain Management Objectives," International Journal of Information Management, vol. 39, pp. 80–89, 2018.
17. P. K. Sharma, M. Y. Chen, and J. H. Park, "A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT," IEEE Access, vol. 6, pp. 115–124, 2018.
18. M. Xu, X. Chen, and G. Kou, "A Systematic Review of Blockchain," Financial Innovation, vol. 5, no. 27, 2019.
19. G. Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger," Ethereum Project Yellow Paper, 2014.
20. H. Treiblmaier, "The Impact of the Blockchain on the Supply Chain: A Theory-Based Research Framework," Supply Chain Management, vol. 23, no. 6, pp. 545–559, 2018.
21. S. Underwood, "Blockchain Beyond Bitcoin," Communications of the ACM, vol. 59, no. 11, pp. 15–17, 2016.
22. A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On Blockchain and Its Integration with IoT," Future Generation Computer Systems, vol. 88, pp. 173–190, 2018.
23. M. S. Ferdous, M. J. Chowdhury, and M. A. Hoque, "A Survey of Consensus Algorithms in Public Blockchain Systems," IEEE Access, vol. 8, pp. 57655–57684, 2020.
24. A. Ekblaw, A. Azaria, J. Halamka, and A. Lippman, "A Case Study for Blockchain in

Healthcare: MedRec Prototype," IEEE Open & Big Data Conference, 2016.

25. V. Buterin, "A Next Generation Smart Contract and Decentralized Application Platform," Ethereum White Paper, 2014.