A Secure Blockchain-Based Mobile Application Framework for Art Authentication and Empowerment

Himaniben Gajjar[1], Dr.JayeshJ.Gamar[2]

Assistant Professor, B.P.College of Computer Studies, Kadi SarvaVishwavidyalaya,GH Road, Sector 23, Gandhinagar, Gujarat, India[1]
Assistant Professor,Vitthalbhai Patel& Rajratna P.T.Patel Science College,Vallabh Vidyanagar, Anand, Gujarat, India[2]

prof.himani@gmail.com[1], dr.jayeshgamar@gmail.com[2]

Abstract. Digital art platforms can face issues with authentication, ownership verification, and intellectual property protection due to their centralized approach. Such issues mainly affect artists living in rural areas with less accessible digital technology. This paper will present a secure mobile application framework using blockchain technology for art authentication and empowerment.
The proposed system utilizes a mobile application, the concept of blockchain, and the idea of a smart contract to develop a tamper-proof authentication and an open and transparent management for the art ownership system. Digital art is stored in an encrypted off-chain space, and the cryptographic hashes and metadata information about the digital art is placed in the blockchain for data integrity and verification. Security analysis and performance analysis verify the efficiency and scalability of mobile art authentication in the proposed system. Through the facilitation of a secure and decentralized process for the verification of artworks by use of mobile technology, the proposed framework enables digital inclusion, which empowers artists, especially those in rural areas, to safeguard their creative properties.

Keywords: Blockchain, Mobile Application Framework, Art Authentication, Smart Contracts, Cybersecurity, Digital Provenance, Rural Empowerment, Decentralized Systems

I. INTRODUCTION

Due to rapid advancements in technology, a paradigm shift has been noted in the way that artworks are created, distributed, and monetized. Artists are now using mobile applications and websites to reach out to the world at large about their creations. Nevertheless, central systems tend to suffer from various disadvantages such as unauthorized duplication of the artworks, lack of ownership information, and data manipulation.
It is vital for any artwork to go through authentication and provenance validation. The conventional digital art marketplace relies greatly on centralized systems, which pose risks such as failure due to single point of failures and data manipulation among other security vulnerabilities. Consequently, authentication and provenance validation remain a challenge due to this vulnerability. The issue of ownership and transactions is another concern that has come with the challenges that exist in the current situation.

Blockchain technology stands out as an ideal solution to address some of these concerns due to its decentralized and tamper-proof nature. Blockchain provides a reliable and decentralized platform for keeping records of ownership and transactions without depending on any trusted parties. Smart contracts provide an additional layer of trust to this solution.Mobile applications provide an easy-to-use environment for both artists and consumers. Therefore, it is evident that mobile applications make the best platform for implementing any secure authentication system for art pieces. In addition, it should be noted that the storage of large digital artworks in blockchain is impossible. It means that off-chain encryption should be used to ensure scalability and efficiency.

Taking into account all the above-listed points, the current research proposes a new model for building an application based on blockchain technology. This application will help to ensure the recording of provenance in an immutable way and guarantee a transparent process of ownership verification and secure access to digital artworks.

The major contributions of the current research study include:

- Creation of a decentralized and mobile framework to authenticate art in a safe manner.
- The use of smart contracts to facilitate ownership management and verification automatically.
- Using off-chain private storage will help avoid blockchain's excessive overhead issues.
- It has been confirmed that the suggested method will have no security or efficiency concerns.

http://doi.org/10.63766/spujstmr.26.000076

Artistic and crafty practices offer a crucial source of income and job for many rural communities. Nevertheless, artisans are usually left out of secure digital systems that are essential for securing intellectual property rights, building trust with consumers, and so forth. In such an atmosphere, economic empowerment becomes difficult due to challenges like piracy, lack of ownership proofs, and interference by middlemen. The mobile application system developed by this team and which is capable of exploiting the potential of blockchain is specifically designed to address all these challenges, making it a safe, transparent, and decentralized system for authentication and ownership of art. Through mobile technology and blockchain documentation, artisans are getting access to a better platform for authenticating their art and engaging with digital markets.

The paper is structured as follows. Section II introduces the related work on authentication and secures systems using blockchain technology. Section 3 defines the problem statement and research goals.Section4 describes the proposed system design. Section 5discusses the security and privacy aspects of the proposed system, followed by a performance analysis in Section 6. Finally, Section 7 concludes this paper and suggests future work.

II. RELATED WORK

Blockchain technology has been widely explored for secure authentication, data integrity, and trust establishment in various application domains[1],[8].Recent studies suggest that blockchain-based frameworks can efficiently address problems of data tampering,unauthorized access, and opacity, thus facilitating digital asset management and authentication systems. There have been a number of research studies that have explored the concept of blockchain-supported secure infrastructure in resource-constrained settings. Decentralized healthcare systems based on blockchain technology prove that secure and efficient data management can be achieved using decentralized ledgers, which retain integrity and ensure control over access [1], [3].

A hybrid blockchain and lightweight authentication-based systems have been suggested for mobile and IoT environments that are efficient and usable [5], [6]. Fun and aesthetic usability of systems becomes important especially in mobile based art authentication applications. Moreover, the capabilities of smart contract-based systems allow for automating the enforcement of security policies making the execution of authentication and ownership trans- parent and uniform [6]. Innovative encryption techniques, such as quantum-secure blockchain-based authentication, have been integrated to enhance long-term security and defense against new threats. Future-proofing art authentication systems and trust in digital ownership records are possible with the help of these methods. The key block chain principles of distributed ledgers, cryptographic hash chaining, and decentralized consensus are the foundation of a secure digital ownership infrastructure [8].These features ensure that the recorded provenance data is immutable and traceable throughout the entire lifecycle of the asset. Moreover, the use of identity authentication and dual-chain architecture in blockchain-based trustworthy data-sharing platforms further enhances the traceability and verification of stakeholders [9].

TABLE I
SUMMARY OF EXISTING BLOCKCHAIN-BASED SECURE SYSTEMS

Ref.	Year	Application Domain	Key Technique	Main Contribution
[1]	2025	Healthcare	Blockchain-based infrastructure	Secure and cost-effective data management in resource-constrained environments
[2]	2025	Authentication Systems	Decentralized block chain framework	Tamper-proof and transparent authentication mechanisms
[3]	2024	Healthcare DataSharing	Multi-delegation blockchain architecture	Controlled and secure sharing of sensitive data
[4]	2024	Distributed Testing	Blockchain-enabled validation framework	Transparent and tamper-resistant testing processes
[5]	2025	IoMT Healthcare	Light weight hybrid block chain authentication	Efficient and mobile-friendly authentication

[6]	2025	IoT Networks	Blockchain with smart contracts	Automated enforcement of security policies
[7]	2025	Secure Authentication	Quantum-secure blockchain techniques	Enhanced security against future cryptographic threats
[8]	2008	Distributed Systems	Blockchain foundational model	Decentralized and immutable ledger architecture
[9]	2024	Trustworthy Data Sharing	Dual blockchain architecture	Identity-based authentication and traceability
[10]	2023	IoT & Federated Learning	Blockchain-secured Federated learning	Secure collaborative and distributed learning environment

Table I presents a concise summary of existing blockchain-based secure systems, which form the basis for identifying the research gaps addressed in this work. Although the studies summarized in Table II demonstrate the potential of blockchain-based secure systems, they differ significantly in functionality and applicability. Table II compares these features to clearly identify the research gap motivating this work.

TABLE II
FEATURECOMPARISONANDRESEARCHGAPANALYSIS

Ref.	Decentralization	Smart Contract Support	Mobile Compatibility	Security Mechanisms	Art Authentication Support
[1]	Yes	No	No	Yes	No
[2]	Yes	No	No	Yes	No
[3]	Yes	Yes	No	Yes	No
[4]	Yes	No	No	Yes	No
[5]	Yes	Yes	Yes	Yes	No
[6]	Yes	Yes	No	Yes	No
[7]	Yes	Yes	No	Yes	No
[8]	Yes	No	No	Yes	No
[9]	Yes	Yes	No	Yes	No
[10]	Yes	Yes	No	Yes	No
Proposed Work	Yes	Yes	Yes	Yes	Yes

As can be seen from Table II, the current frameworks based on blockchain technology solve issues related to security and decentralization, whereas the suggested framework has unique features, which include both mobile compatibility and art authentication capabilities.

III. PROBLEMSTATEMENTANDRESEARCH OBJECTIVES

A. Problem Statement

The popularity of digital platforms utilized in order to create, distribute, and trade artworks poses numerous difficulties regarding the issue of ownership verification, the authenticity check, as well as security in trading procedures. The majority of today's digital platforms for artwork trading are designed based on centralized systems that are susceptible to such problems as unauthorized replication, data manipulation, single point of failure, and inadequate levels of information transparency concerning ownership issues.

Moreover, the lack of permanent provenance records hampers the process of authentication of artworks, which leads to

ownership conflicts as well as violation of intellectual property rights. On the other hand, although mobile applications can be used to access digital art platforms, the majority of them provide low levels of security and have no trust models associated with decentralization. Thus, there is a necessity for development of a platform for artworks that would enable users to verify their artworks and guarantee safe transactions.

B. Research Objectives

The principal objective of this research project is to design and analyze an effective framework for a secure mobile application for art authentication and empowerment:

- To develop a decentralized mobile application framework based on blockchain technology for the secure authentication of art.
- To provide tamper-proof and immutable recording of ownership and provenance details of artworks.
- For the integration of smart contracts with a view to automating the verification process, management of ownership, as well as transaction
- To ensure safe and privacy-enhancing access to art-related data via off-chain encrypted storage.
- To assess the proposed framework interms of security, performance, and appropriateness for mobile environments.

IV. PROPOSED SYSTEM ARCHITECTURE AND SMART CONTRACT DESIGN

A. System Overview

Fig. 1 illustrates the overall architecture of the proposed blockchain-based mobile application framework for secure art authentication and empowerment. In this paper, a mobile-centric framework will be proposed wherein interaction between the artists and the buyers/verifiers will occur within the mobile application which acts as the front-end interface for registering, authenticating, and verifying artwork transactions. Digital artworks are encrypted and stored in off-chain storage, while their cryptographic hash values and metadata are recorded on the blockchain through smart contracts. The smart contract layer manages artwork registration, ownership verification, and ownership transfer in a decentralized and immutable manner. During authentication, ownership and provenance details are verified by matching the generated artwork hash with the hash value stored on the blockchain, ensuring secure and transparent artwork authentication without revealing confidential artwork content. Therefore, the proposed architecture is scalable, accessible, and suitable for secure digital art authentication and empowerment in resource-constrained and rural areas.

]

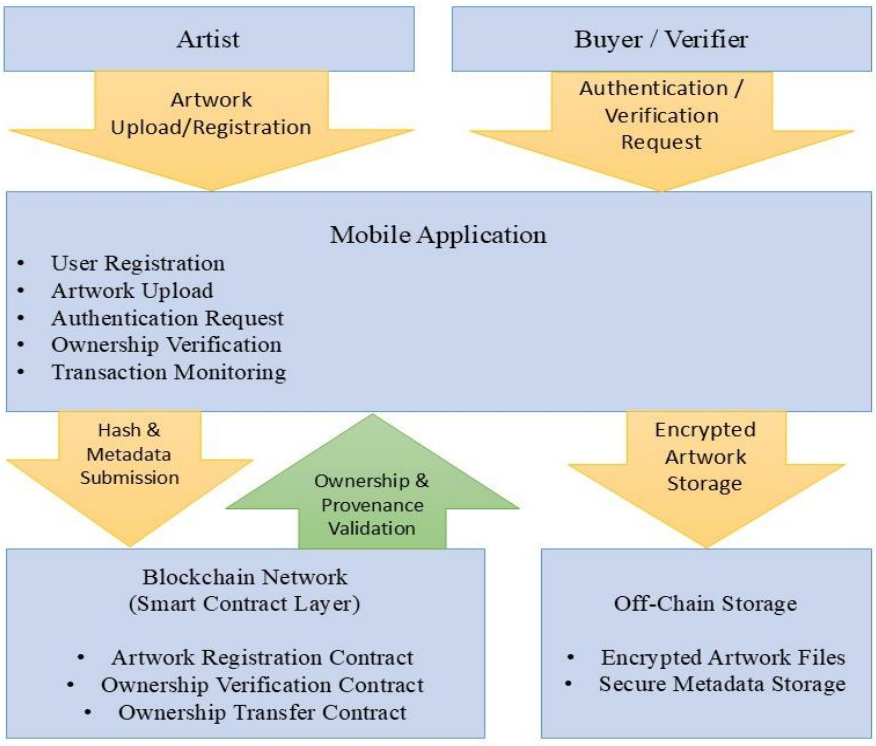

Fig.1. Architecture of the proposed blockchain-based mobile application framework for secure art authentication and empowerment. Source:

Authors' own design, created using Microsoft PowerPoint.

B. System Components

Thearchitectureismadeupoffourmainelementsthatworktogethertoprovidesecure art authentication.

MobileApplication

The main interface for artists and buyers is the mobile application. It enables the user to register for the web application, submit artwork, and verify ownership and track transactions. The application uses secure APIs to interact with the blockchain network, enabling them to authenticate the artworks and verify their provenance in real-time.

Blockchain

The decentralized ledger of a blockchain network immutably records artwork registration, ownership, and transaction history. A cryptographic hash is used to identify each artwork, ensuring integrity and preventing unauthorized modification. A decentralized system increases the trust in a system and makes it resilient.

SmartContracts

The use of smart contracts within the blockchain network helps in carrying out system functions like registration of artwork, ownership verification, and ownership transfer automatically. Smart contracts work based on pre-set rules in the blockchains making it possible for the art authentication process to have tamper-proof standards.

Off-ChainStorage

The digital files containing artwork is huge; hence, the content has been stored off-chain in an encrypted format. The blockchain only keeps the hash values and references to the content. This ensures that the amount of blockchain storage space needed is greatly minimized.

C. Implementation Details of the Proposed Framework

The mobile application framework will be implemented using the combination of the mobile front end, the blockchain network, smart contracts, and off-chain storage. In other words, the mobile application will serve as the user interface for the artists, buyers, or the verifiers. The artists will be able to register themselves, upload their artwork, and carry out ownership registration. Buyers or verifiers can authenticate the artwork and view ownership information.

The artwork file gets encrypted and saved on off-chain storage. Cryptographic hashing of the artwork is done using SHA-256. The hash value, artwork metadata, owner identity, timestamp, and off-chain storage reference get recorded on the blockchain by means of smart contracts. The blockchain does not have the full file of the artwork saved on it, making it highly scalable.

The smart contract layer fulfils three important tasks, namely artwork registration, ownership verification, and ownership transfer. While registration involves storing the hash and artwork metadata, ownership verification entails comparing the hash value of the artwork submitted against that stored on the blockchain. Finally, transfer entails changing the ownership status only when the identity of the existing owner is verified successfully.

The table below describes the implementation of the framework, including the major components and their intended purpose in the system along with suggested technology.

TABLE III
IMPLEMENTATION DETAILS OF THE PROPOSED FRAMEWORK

Component	Suggested Technology	Purpose
Mobile Application	Android / Flutter	User interface for artists, buyers, and verifiers
Blockchain Network	Ethereum / Hyperledger Fabric	Immutable storage of artwork hash and ownership records
Smart Contract	Solidity / Chaincode	Artwork registration, verification, and ownership transfer
Off-chain Storage	IPFS / Encrypted Cloud Storage	Secure storage of encrypted artwork files
Hashing Algorithm	SHA-256	Artwork integrity and authenticity verification

Component	Suggested Technology	Purpose
User Authentication	Wallet-based login / Digital identity	Secure user access and ownership control
Encryption	AES-based encryption	Protection of artwork before off-chain storage

D. Smart Contract Design

The core method of execution for the designed framework would be the use of smart contracts, which implement authentication and ownership policies based on certain conditions on the blockchain. Agreement for New Art on Blockchain: This smart contract ensures the recording of the art piece on the blockchain network. When an art piece is uploaded to the blockchain system, a hash, which is unique to the artwork, along with other metadata is created and stored on the blockchain.
Ownership Verification Contract: The purpose of this smart contract is to verify the authenticity of the art piece using the hash value submitted and hash value present in the blockchain.
Ownership Transfer Contract: Using this smart contract, it is possible to manage the ownership of the artwork in a secure and auditable manner.

E. Workflow of the Proposed Framework

Operation procedure of integrated architecture:

- The artists use the mobile app for registering and uploading artworks.
- Artworks are stored on an off-chain system after encryption, and a digital hash code is generated.
- The hash code and its associated metadata are registered using a smart contract for artwork registration on blockchain.
- Buyers/verifiers of the artwork will check the ownership of artwork using blockchain from the mobile app.
- Ownership of artwork is transferred through smart contracts, and transaction updates are also done automatically using smart contracts.This process offers safe credentials, clear ownership, and convenient access through mobile apps.

V. SECURITY AND PRIVACY ANALYSIS

The blockchain-based mobile application framework proposed tackles several security and privacy challenges involved in the authentication, verification of ownership, and transaction processing for the digital art pieces. The security analysis will be based on the factors such as data integrity and access control, privacy protection, risks at the blockchain level, and vulnerabilities in the smart contracts.

A. Data Integrity and Access Control: In the proposed system, the hash values of the artworks and other relevant ownership data are stored in the blockchain. As we know that once the data is recorded in the blockchain, it is practically impossible to change. Every artwork has a unique cryptographic hash value that changes when there is any modification in the artwork file. Hence, the integrity of the art piece can be checked by comparing the hash values of the artwork stored on the blockchain against the new one.

B. Privacy Preservation and Ownership Protection: The entire artwork is not directly uploaded to the blockchain. Rather, the artwork is encrypted and stored in an off-chain storage location, whereas the hash values, metadata, and storage location are stored in the blockchain itself. This helps reduce the amount of sensitive artwork data exposed and ensures user privacy. The usage of encrypted off-chain storage also saves blockchain storage resources while maintaining artwork integrity.

C. Blockchain and Smart Contract Attack Analysis: While blockchain is a decentralized and immutable technology, there exist various types of threats for any blockchain-based system. Possible attacks and solutions are therefore considered within the proposed solution framework.

TABLE IV
BLOCKCHAIN AND SMART CONTRACT ATTACK ANALYSIS

Attack / Threat	Possible Risk	Mitigation Strategy
51% Attack	Malicious control over blockchain consensus may alter transaction history	Use of a permissioned or consortium blockchain with trusted validators

Attack / Threat	Possible Risk	Mitigation Strategy
Sybil Attack	Fake identities may create false ownership or verification requests	Strong identity verification and wallet-based authentication
Replay Attack	Reuse of old, valid transactions may cause unauthorized actions	Use of nonce, timestamp, and transaction validation
Private Key Compromise	Unauthorized ownership transfer may occur if user keys are stolen	Secure wallet management, multi-factor authentication, and a key recovery mechanism
Reentrancy Attack	A smart contract may be repeatedly called before a state update	Use of the checks-effects-interactions pattern and reentrancy guards
Front-running Attack	Transaction order manipulation may affect ownership transfer	Commit-reveal mechanism and transaction ordering control
Integer Overflow / Underflow	Incorrect contract execution due to arithmetic errors	Use of safe arithmetic libraries and updated compiler versions
Smart Contract Bugs	Incorrect ownership logic may lead to false authentication	Smart contract testing, auditing, and formal verification
Denial-of-Service Attack	Attackers may overload verification or transaction requests	Rate limiting, access control, and distributed storage support
Metadata Leakage	Public metadata may reveal sensitive ownership information	Store only the minimum required metadata on-chain

D. Overall Security Justification: Blockchain immutability, smart contracts' automation, encryption for off-chain data storage, and hashing provide better security for the proposed framework. This model lessens the dependence on centralized authorities and gives clear evidence of the integrity of ownership proofing. However, there is a need for adequate testing, key management, identity validation, and setup of a blockchain network.

VI. PERFORMANCE EVALUATION

Performance assessment of the proposed blockchain-based mobile application framework is performed according to certain metrics that can be used in the mobile environment and decentralized environment. Metrics considered during assessment include storage overhead, transaction latency, smart contracts execution fee, mobile device response time, and scalability.
The proposed framework stores only hash values of the artwork, its metadata, time stamp, ownership information, and storage information on the blockchain, while the artwork itself is stored offline.

TABLE V
QUANTITATIVE AND FUNCTIONAL PERFORMANCE COMPARISON

Performance Metric	Centralized Art Platform	Proposed Blockchain-Based Framework
Artwork storage	Full file stored centrally	Encrypted file stored off-chain
Storage overhead	High	Low
Ownership verification	Platform-dependent	Smart contract-based
Transaction transparency	Limited	High
Tamper resistance	Medium	High
Provenance tracking	Limited	Immutable and traceable

Performance Metric	Centralized Art Platform	Proposed Blockchain-Based Framework
Scalability	Medium	High
Mobile accessibility	Platform-dependent	Mobile-centric

Based on the comparative parameters presented in Table V, Fig. 2 illustrates the relative performance of the centralized art platform and the proposed blockchain-based mobile application framework.

Fig. 2 presents relative comparative scores based on framework-level analysis. The proposed framework offers better storage management, transparency, provenance tracking, tamper resistance, and scalability by combining blockchain records, smart contracts, cryptographic hashing, and encrypted off-chain storage.
Overall, the proposed framework is suitable for secure and mobile-based art authentication, particularly for artists and users in resource-constrained environments. Full prototype implementation, gas cost analysis, transaction confirmation time, and real-time mobile response validation are considered as future work.

VII. CONCLUSION AND FUTURE WORK

This paper describes a secure and blockchain-based mobile application framework for art authentication and empowerment. The proposed framework uses blockchain technology and smart contracts to provide tamper-proof and transparent ownership information while ensuring secure and decentralized authentication of digital artworks. The two main objectives of using mobile connectivity with off-chain encrypted storage to contest unauthorized copying, ownership and trust in centralized art platforms will be proposed in this work. The framework can deliver significant rural empowerment benefits that can help artists and artisans located in rural areas, which often suffer from a lack of secure digital infrastructure and intellectual property protection. With the mobile-friendly framework design, artists can verify their artworks via accessible mobile devices. At the same time, using blockchain technology in provenance creates trust and transparency without any middleman. The framework's ability to preserve the integrity of data, along with its confidentiality and access control using cryptographic techniques, is proven by security analysis. The proposed framework aids in promoting secure digital livelihoods, equitable access to technology, and economic empowerment of artists, especially in rural areas, in conformity to the Sustainable Development Goals or SDG 8 (Decent Work and Economic Growth), SDG 9 (Industry, Innovation and Infrastructure), and SDG 10 (Reduced Inequalities). The performance analysis shows that the proposed approach is suitable for mobile platforms. Further, it ensures a reasonable transaction delay, low storage cost, and the response of the system is also optimum, which shows the feasibility of the framework in the real world. In future studies, this framework can be enhanced by incorporating artificial intelligence methods for the automatic analysis of artwork similarity, forgery detection, and artwork style classification. Extensions may include cross-chain interoperability, integration with decentralized art markets, or sophisticated access control policies for community art environments. This will help make the proposed framework more effective in creating secure and scalable digital platforms for empowering rural areas.

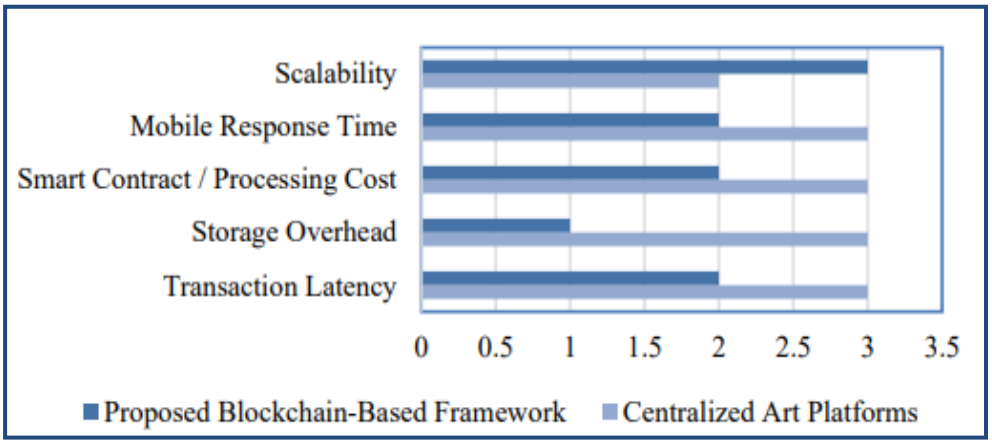

Fig. 2. Relative performance comparison of the proposed blockchain-based framework and centralized art platforms across transaction latency, storage overhead, processing cost, mobile response time, and scalability. Source: Authors' own analysis.

REFERENCES

[1] J. Lafuente et al., "SiliconHealth: A blockchain-based secure healthcare infrastructure for resource-constrained environments," arXiv preprint arXiv:2601.09557, 2025.
[2] X. Zhang et al., "Blockchain adoption for secure authentication in energy trading systems," Energy Research & Social Science, vol. 113, 2025.
[3] Kumar et al., "Blockchain-based secured data sharing using multi-delegation architecture in healthcare systems," IEEE Access, 2024.
[4] M. Rossi et al., "BCTestingPlus: A blockchain-empowered framework for distributed and transparent testing," Inventions, vol. 10, no. 4, 2024.
[5] Ahmed et al., "A lightweight hybrid authentication framework for IoMT-based e-healthcare applications," Scientific Reports, vol. 15, 2025.
[6] R. Patel et al., "A hybrid blockchain and smart contract framework for secure IoT networks," Frontiers in Blockchain, 2025.
[7] Y. Chen et al., "Quantum-secure blockchain-based authentication for future digital systems," Scientific Reports, vol. 15, 2025.
[8] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
[9] H. Liu et al., "Blockchain-empowered trustworthy data sharing with identity-based authentication," ACM Transactions on Internet Technology, 2024.
[10] H. Wu et al., "Blockchain-empowered secure federated learning for IoT applications," IEEE Transactions on Consumer Electronics, 2023.
[11] G. Wood, "Ethereum: A secure decentralized generalized transaction ledger," Ethereum Yellow Paper, 2014.
[12] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," IEEE Access, 2016.
[13] M. Crosby et al., "Blockchain technology: Beyond bitcoin," Applied Innovation Review, 2016.
[14] J. Moubarak, E. Filiol, and M. Chamoun, "On blockchain security and relevant attacks," in Proc. IEEE International Conference on Internet Technology and Secured Transactions, 2018.
[15] M. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," Telematics and Informatics, 2019.
[16] P. Kaur et al., "Blockchain-based mobile applications: A survey," IEEE Access, 2020.
[17] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in Internet of Things: Challenges and solutions," Computer Communications, 2017.