International Journal of Creative and Open Research in Engineering and Management
ISSN: **3108-1754 (Online)**
Volume 02 Issue 04 April-2026 | Impact Factor: 3.5

Blockchain Based Digital Document Management System with off-Chain Storage using Hybrid Approach

Dr. Gajanan Badhe[1], Dr. Maithili Arjunwadkar[2]
[1, 2] PES Modern Institute of Business Studies, Pune, Maharashtra, India.
Corresponding Author Email: badhe.gm@gmail.com | ORCID: https://orcid.org/ 0009-0000-6749-2554

How to Cite this Article:

Badhe, G. (2026). Blockchain Based Digital Document Management System with off-Chain Storage using Hybrid Approach. International Journal of Creative and Open Research in Engineering and Management, 02(04). https://doi.org/10.55041/ijcope.v2i4.606

https://doi.org/10.55041/ijcope.v2i4.606

Abstract—

The growing requirements for secure and efficient digital document management has highlighted the shortcomings of conventional centralized systems, such as susceptibility to document forgery, limited transparency, and exposure to cyber threats. This research proposes a Blockchain-based digital document management system using hybrid approach that leverages decentralized ledger technology to address these challenges. The system utilizes smart contracts to automate digital document issuance, validation, and transfer while ensuring data integrity and eliminating the need for intermediaries. Every document is represented as a unique digital token, preventing duplication and enabling traceability throughout its lifecycle. The proposed design integrates Blockchain platforms such as Ethereum and decentralized storage systems like IPFS, and user-friendly decentralized applications to enhance usability and performance. Experimental analysis demonstrates that the system significantly reduces frauds, improves transparency, and enforces appropriate document verification policies. Although challenges such as scalability and transaction costs remain, the findings indicate that Blockchain technology offers a robust and innovative solution for digital document management and verification systems, with potential applications across various industries including education, legal, governance.

Keywords—

Digital Document management, decentralized ledger, Blockchain technology, hybrid approach, off-chain storage, InterPlanetary File System technology.

I. INTRODUCTION

The rapid digitization of organizational workflows has significantly increased the reliance on Document Management Systems (DMS) for storing, processing, and sharing critical information across domains such as education, healthcare, governance, and enterprise operations. Traditional DMS architectures are predominantly centralized, which introduces several limitations including single points of failure, vulnerability to cyberattacks, lack of transparency, and difficulties in ensuring data integrity and trust among distributed stakeholders [1], [5]. These challenges become more pronounced in environments where document authenticity, traceability, and secure sharing are essential, such as academic credential verification and medical data management [2], [3], [10].

One of the major concerns in conventional systems is the susceptibility of digital documents to unauthorized access, tampering, and forgery. Centralized databases rely heavily on institutional trust and are prone to insider threats or external breaches, making them inadequate for applications requiring high levels of security and auditability [1], [4]. Moreover, the growing volume of digital data imposes scalability constraints, as storing large files directly within traditional or blockchain-based systems can lead to increased latency, higher costs, and reduced system efficiency [5]. These issues highlight the need for a more robust, distributed, and secure framework for managing digital documents.

Blockchain technology has emerged as a promising solution to address these limitations by providing a decentralized, immutable, and transparent ledger for recording transactions and metadata. Its inherent characteristics—such as cryptographic security, consensus mechanisms, and tamper-resistant storage—enable trustworthy record-keeping without reliance on centralized authorities [4], [5]. However, blockchain alone is not well-suited for storing large volumes of data due to scalability and performance constraints. Storing entire documents on-chain can lead to increased storage overhead and transaction costs, making it inefficient for real-world document management applications [5].

To overcome these limitations, the integration of blockchain with the InterPlanetary File System (IPFS) has gained significant attention as a hybrid approach. IPFS is a decentralized, peer-to-peer storage system that uses content-addressing mechanisms to store and retrieve data efficiently [8]. In a hybrid Blockchain–IPFS framework, large documents are stored off-chain in IPFS, while their corresponding cryptographic hashes or Content Identifiers (CIDs) are recorded on the blockchain. This approach ensures data integrity, as any modification to the stored document results in a change in its hash, which can be easily detected through blockchain verification [8].

The hybrid architecture not only enhances security and integrity but also improves scalability and cost-efficiency. By offloading bulky data to IPFS and maintaining only essential metadata on-chain, the system reduces storage overhead and optimizes performance. Additionally, smart contracts can be employed to enforce access control policies, automate document verification processes, and maintain audit trails, thereby enhancing transparency and accountability in document transactions [6], [9]. This decentralized verification mechanism eliminates the need for intermediaries and enables trustless interactions among users.

Despite its advantages, the integration of blockchain and IPFS introduces new challenges related to data privacy, encryption, access control, and interoperability. For instance, IPFS does not inherently provide encryption, necessitating the use of advanced cryptographic techniques such as hybrid encryption schemes to secure stored content. Furthermore, issues such as network latency, data availability, and governance of decentralized systems must be addressed to ensure practical adoption [10]. The proposed Hybrid Blockchain–IPFS framework aims to enhance document management systems by addressing critical challenges related to security, integrity, and decentralization. By combining the immutable and transparent nature of blockchain with the scalable and efficient storage capabilities of IPFS, the framework provides a resilient, tamper-proof, and decentralized solution for modern document management.

II. PROBLEMS IN DIGITAL DOCUMENT MANAGMENT

Existing research highlights that traditional document management systems suffer from centralization, lack of transparency, and vulnerability to data manipulation [1]. Blockchain-based solutions have been proposed to improve trust and security in digital systems, particularly in education and credential verification [2], [3].

However, early blockchain implementations faced scalability challenges due to the need to store large amounts of data directly on-chain [5]. Studies on smart contracts demonstrate their ability to automate secure

transactions, but also highlight complexities in implementation and performance overhead [6], [9].
Recent approaches integrating IPFS with blockchain address storage limitations by offloading large files to decentralized storage systems [8]. Additionally, blockchain-based healthcare systems such as MedShare demonstrate the effectiveness of decentralized data sharing but reveal challenges related to privacy and interoperability [10].
These limitations motivate the need for a hybrid architecture that balances security, scalability, and efficiency.

III. DESIGN OF DIGITAL DOCUMENT MANAGEMENT SYSTEM

A. System Overview

The proposed system adopts a three-layer hybrid architecture integrating blockchain technology with the InterPlanetary File System (IPFS) to achieve secure, scalable, and decentralized document management. The architecture is divided into the layers such as user Interface Layer, Blockchain Layer, and IPFS Storage Layer. Each layer performs a distinct function while collectively ensuring data integrity, confidentiality, and efficient storage.

1. User Interface Layer

The User Interface (UI) Layer acts as the interaction point between users and the system. It provides functionalities such as user authentication, document upload, access requests, and retrieval operations. Users, including administrators and employees, interact with the system through web or application interfaces.

When a user uploads a document, the UI layer initiates the process by capturing the file and associated metadata (such as ownership, timestamp, and access permissions). The document is then forwarded for encryption before being sent to the storage layer. Similarly, during retrieval, the UI layer handles user requests and displays the decrypted document after verification. This layer ensures usability and secure access by integrating authentication mechanisms such as public-key cryptography and role-based access control [6]. It also interacts with smart contracts in the blockchain layer to validate permissions and enforce policies [9].

2. Blockchain Layer

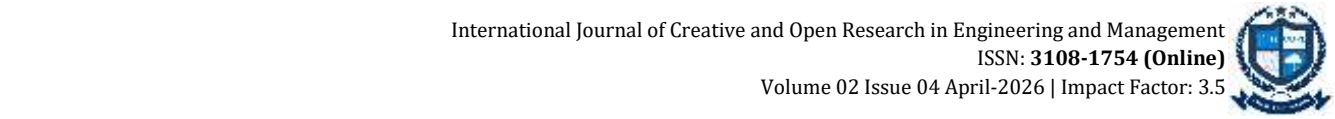
The Blockchain Layer is responsible for maintaining secure and immutable metadata records. Instead of storing actual documents, the blockchain stores hashed references (Content Identifiers - CIDs) and associated metadata such as document ownership, access rights, and timestamps. A hybrid blockchain approach is employed, combining permissioned blockchain for access control, smart contract execution, and audit logging, public blockchain for ensuring transparency and immutability. Smart contracts automate processes such as permission verification, access control, and logging of user actions. Once metadata is recorded, it cannot be altered, ensuring data integrity and non-repudiation [4]. The use of blockchain significantly enhances trust by eliminating the need for centralized authorities and enabling decentralized validation through consensus mechanisms [5]. The storing only metadata on-chain reduces storage overhead and improves scalability, as large files are not directly stored on the blockchain [7].

3. IPFS Storage Layer

The IPFS Storage Layer is responsible for storing the actual document files in a decentralized manner. IPFS is a peer-to-peer distributed file system where files are stored across multiple nodes and identified using cryptographic hashes known as Content Identifiers (CIDs). When a document is uploaded the file is encrypted and split into chunks, each chunk is distributed across the IPFS network and a unique CID is generated and returned. This CID is then stored on the blockchain as a reference to the file. During retrieval, the CID is used to locate and reconstruct the document from the distributed network. IPFS ensures high availability, fault tolerance, and efficient data retrieval by fetching data from the nearest available node. Its content-addressing mechanism guarantees data integrity, as any modification to the file results in a different CID [8].

5. Integrated Workflow

The integration of these three layers enables a secure and efficient workflow the UI Layer handles user interaction and request initiation, the Blockchain Layer manages metadata, access control, and verification, the IPFS Layer stores and retrieves actual documents. This hybrid approach leverages the strengths of both blockchain and IPFS, reducing blockchain storage load while ensuring secure, decentralized, and scalable document management [8].



B. System Workflow

The proposed hybrid system follows a structured workflow that integrates blockchain technology with the InterPlanetary File System (IPFS) to ensure secure storage, efficient retrieval, and data integrity. The complete process includes document upload, encryption, decentralized storage, metadata recording, and retrieval using a Content Identifier (CID).

1. User Uploads a Document

The workflow begins when a user uploads a document through the system interface. The user may be an administrator, employee, or authorized external entity. Along with the document, relevant metadata such as ownership details, access permissions, and timestamps are captured. This metadata is essential for enforcing access control and auditability within the system [1].

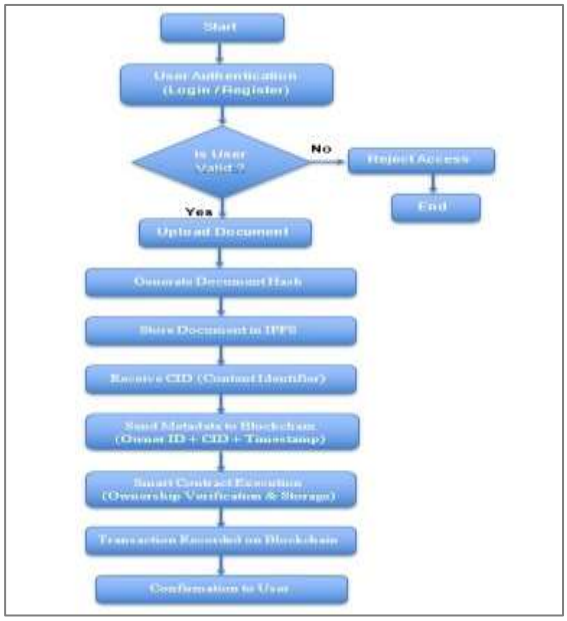


Figure 1. Document upload and store to IPFS off-chain storage.

2. Document Storage in IPFS

Before storing the document, it is encrypted using cryptographic algorithms to ensure confidentiality and prevent unauthorized access. Encryption may be performed using symmetric or asymmetric key techniques depending on the system design. After encryption, the document is transmitted to the IPFS network, where it is divided into smaller chunks and distributed across multiple nodes in a decentralized manner. This eliminates reliance on centralized storage systems and enhances fault tolerance and availability [5].

3. Generation of Content Identifier (CID)

Once the document is stored in IPFS, a unique Content Identifier (CID) is generated. The CID is a cryptographic hash derived from the content of the file, making it inherently tamper-evident. Any modification to the document results in a completely different CID, ensuring data integrity [6]. The CID serves as a reference pointer to the stored document and is used for future retrieval operations.

4. Storing CID on the Blockchain

Instead of storing the entire document on the blockchain, only the CID along with metadata (such as ownership, permissions, and timestamps) is recorded on the blockchain. This approach significantly reduces storage overhead and improves system scalability. Smart contracts are used to store and manage this metadata securely. Once recorded, the data becomes immutable and cannot be altered, ensuring transparency, integrity, and non-repudiation. The blockchain also maintains an audit trail of all transactions related to the document [9].

5. Document Retrieval and Verification Using CID

When a user requests access to a document, the system first verifies the user's permissions through the blockchain layer using smart contracts. If authorized, the CID stored on the blockchain is retrieved.

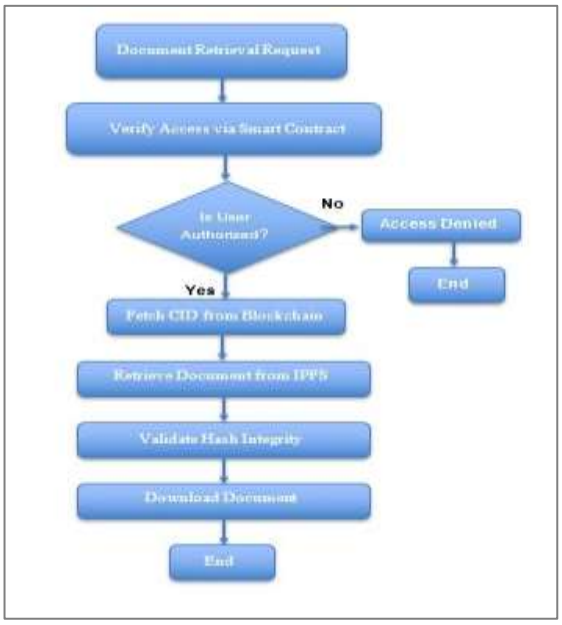


Figure 2. Document retrieval and verification using Content Identifier

Using this CID, the system fetches the encrypted document from the IPFS network. The document is then decrypted using the appropriate cryptographic keys and delivered to the user. Verification is inherently ensured because the CID matches the cryptographic hash of the retrieved content. If the file has been tampered with, the hash will not match, and the system can detect the inconsistency [6]. This workflow ensures the confidentiality through encryption, integrity via content-based hashing (CID), decentralization using IPFS storage, immutability and trust through blockchain.

By combining blockchain and IPFS, the system achieves a balance between security, scalability, and performance, making it suitable for modern decentralized document management applications [7].

C. Development of Smart Contracts

Smart contracts are self-executing programs deployed on the blockchain that automatically enforce predefined rules and conditions without the need for intermediaries. In the proposed hybrid blockchain–IPFS system, smart contracts play a critical role in managing security, trust, and automation by controlling access, verifying ownership, and validating transactions [6].

1. Access Control

Smart contracts implement fine-grained access control mechanisms to regulate who can upload, view, or modify documents. Access policies are encoded within the contract logic, ensuring that only authorized users can perform specific actions. When a user requests access to a document, the smart contract verifies the user's identity and permissions against the stored metadata (such as roles and access rights). If the conditions are satisfied, access is granted; otherwise, the request is denied. This eliminates reliance on centralized access control systems and enhances security through decentralized enforcement [6], [9]. The role-based and attribute-based access control models can be integrated into smart contracts to support dynamic and scalable permission management [6], [5].

2. Ownership Verification

Smart contracts are responsible for maintaining and verifying document ownership. Each document stored in the system is associated with an owner's identity, which is securely recorded on the blockchain along with the document's metadata and CID. Whenever an operation such as sharing, updating permissions, or transferring ownership is requested, the smart contract verifies whether the initiating user is the legitimate owner. This ensures that only authorized entities can make critical changes to the document's access or status [6], [9]. Because blockchain records are immutable, ownership information cannot be altered or forged, thereby providing strong guarantees of authenticity and non-repudiation [4], [5].

3. Transaction Validation

Smart contracts also handle transaction validation by ensuring that all operations related to documents comply with predefined rules before being recorded on the blockchain. These operations include document uploads, access requests, permission updates, and retrieval actions.

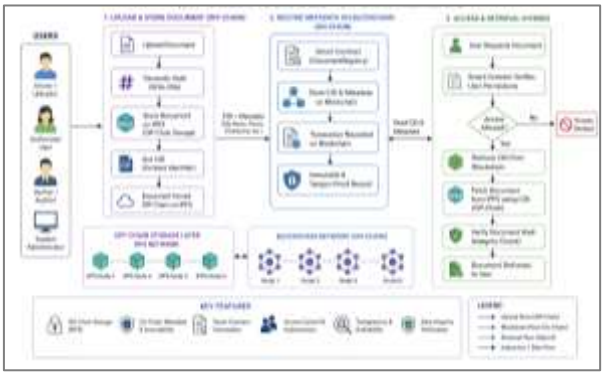


Figure 3. Digital Document Management System with off-chain IPFS and Blockchain using Hybrid Approach.

When a transaction is initiated, the smart contract verifies the authenticity of the request, checks compliance with access and ownership policies and also ensures data consistency and integrity. Only after successful validation is the transaction executed and recorded as a new block entry. This automated validation process reduces the risk of malicious activities and eliminates the need for manual verification [6]. All validated transactions are permanently stored on the blockchain, creating a transparent and auditable history of document-related activities [7]. Smart contracts enhance the system by enforcing secure and decentralized access control, ensuring accurate ownership verification and automating trustworthy transaction validation.

By integrating smart contracts, the system achieves higher levels of security, transparency, and efficiency,

making it suitable for decentralized document management applications [8].

IV. TOOLS & TECHNIQUES USED

The design of a blockchain-based digital document management system integrates concepts from blockchain technology, cryptography, and modern web development. The Ethereum platform is commonly adopted as the core infrastructure because of its well-established ecosystem and robust support for smart contracts. These smart contracts are developed using the Solidity programming language, enabling the implementation of application logic for document submission, storage, and verification. The system architecture consists of users and authorized verifiers interacting through a decentralized application (DApp) interface, typically developed using frontend frameworks such as React.js. This interface connects to smart contracts deployed on the Ethereum network through Web3.js, facilitating seamless communication between the user interface and the blockchain layer. Smart contracts manage the core functionalities, including document handling and validation, while the blockchain maintains transparency and ensures that records remain tamper-proof. To optimize performance and reduce on-chain storage costs, only document metadata is stored on the blockchain, whereas the actual files are maintained in off-chain storage systems like IPFS. This hybrid approach balances efficiency with security. The digital wallet such as MetaMask is utilized for user authentication and to manage blockchain transactions securely.

The system's user interface is generally developed using modern frameworks like React.js, which support the creation of dynamic and intuitive decentralized applications (DApps). To enable communication between the frontend and the blockchain network, libraries such as Web3.js are utilized, allowing users to interact with smart contracts via their digital wallets. Wallets like MetaMask play a key role in user authentication and secure transaction handling, as they safely store private keys and help manage digital assets. Security and data protection are maintained through cryptographic methods, including hashing techniques (such as SHA-256) and public-key encryption, ensuring both data integrity and safe transactions. For smart contract development and testing, tools like Truffle are commonly used to compile, deploy, and validate contracts, while Ganache offers a local blockchain environment for testing, simulation, and debugging purposes.

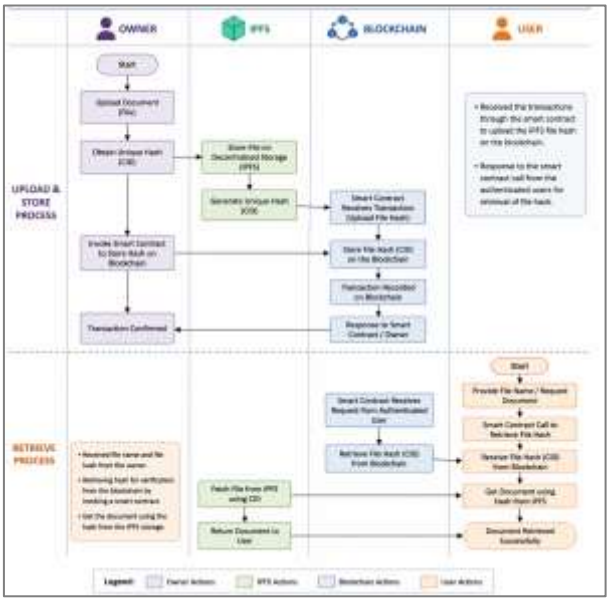


Figure 4. Digital Document Management System (Hybrid Approach using Blockchain and Off-chain IPFS storage)

To improve efficiency and reduce the load on the blockchain, the InterPlanetary File System (IPFS) is employed as an off-chain decentralized storage solution for digital documents, enhancing data availability and fault tolerance. Consensus algorithms such as Proof of Work and Proof of Authority are implemented to maintain agreement across network participants. The gas optimization strategies are applied to minimize transaction fees and enhance overall system performance. Strong security measures, including code reviews and vulnerability assessments, are essential to protect smart contracts from potential exploits and to reduce system failures or unresponsive states.

V. RESULT AND ANALYSIS

The deployment of a hybrid blockchain-based digital document management system shows distinguished enhancements across multiple aspects. A key result is the prevention of document tampering and duplication, as each record is uniquely registered and secured by the immutable characteristics of blockchain technology. This guarantees authenticity and helps minimize potential financial risks for both service providers and users. The system also promotes a high level of transparency, since all activities are recorded on a distributed ledger that can be independently verified by participants, thereby strengthening trust and ensuring fairness in document handling and validation. By

integrating smart contracts, many operations are automated, which lowers administrative expenses and reduces reliance on intermediaries. The system effectively mitigates unauthorized modifications by enforcing strict access control policies through smart contracts, ensuring that only permitted users can view or manage documents. The availability of real-time online verification significantly decreases processing time and eliminates additional costs associated with third-party verification services, while providing a secure and decentralized environment. However, challenges such as transaction fees, commonly known as gas costs, remain a concern, especially during periods of network congestion when these costs may increase. Future work should concentrate on enhancing scalability, minimizing operational expenses, and encouraging broader user adoption of the system.

VI. DISCUSSIONS

This work presented a hybrid blockchain–IPFS framework for secure, decentralized, and scalable document management. By combining the strengths of blockchain technology and the InterPlanetary File System, the proposed system addresses critical challenges associated with traditional centralized storage solutions, including data tampering, limited scalability, and lack of transparency. The architecture separates responsibilities across layers, where the blockchain layer ensures immutability, trust, and secure metadata management, while the IPFS layer provides efficient, distributed storage for large documents. Instead of storing complete files on-chain, only cryptographic references in the form of Content Identifiers (CIDs) are recorded, significantly reducing storage overhead and improving system performance. This design not only enhances scalability but also maintains strong guarantees of data integrity and authenticity. The integration of smart contracts further strengthens the system by automating key processes such as access control, ownership verification, and transaction validation. These self-executing mechanisms eliminate the need for intermediaries, reduce human intervention, and ensure that all operations are executed in a transparent and tamper-proof manner. An encryption techniques applied before storage ensure confidentiality, making the system suitable for handling sensitive data across multiple domains. The proposed workflow demonstrates how documents can be securely uploaded, stored, verified, and retrieved using a combination of decentralized technologies. The use of IPFS ensures high availability and fault tolerance, while blockchain provides a permanent and auditable record of all interactions. Together, these technologies create a reliable and trustworthy ecosystem for document management. The applicability of the system across diverse domains such as academic certificate verification, healthcare records, legal documentation, government systems, and supply chain management highlights its versatility and practical relevance. In each of these areas, the hybrid approach enhances efficiency, reduces fraud, and builds trust among stakeholders. The hybrid blockchain–IPFS model represents a significant step toward next-generation decentralized document management systems. It successfully balances security, scalability, and performance, making it a promising solution for modern digital infrastructures. With future enhancements such as AI integration, improved persistence mechanisms, and performance optimization, the system has the potential to evolve into a highly intelligent, robust, and widely adoptable platform for secure data management.

VII. CONCLUSION

This study demonstrates how blockchain technology can significantly improve traditional digital document management systems by making them more secure, efficient and decentralized. It effectively tackles major concerns such as document tampering, unauthorized modifications, and trust issues, offering a dependable alternative to existing approaches. The incorporation of smart contracts allows automated handling of essential operations, thereby reducing manual effort and operational complexity while maintaining accountability. The proposed system shows better performance in terms of efficiency, instant verification, and user confidence, making it suitable for diverse real-world applications. Despite these advantages, issues like scalability and transaction expenses remain important challenges. This paper highlights the limitations of traditional document management systems and proposes a hybrid blockchain–IPFS as off-chain storage as a solution. The proposed system represents a promising approach for next-generation document management systems. The approach uses blockchain to store metadata and IPFS to store actual documents, reducing storage overhead and improving scalability. By storing only Content Identifiers (CIDs) on the blockchain, the system ensures data integrity and efficient retrieval. Smart contracts automate important

functions such as access control, ownership verification, and transaction validation. The system provides high reliability, transparency, and resistance to tampering. It can be applied in areas like education, healthcare, legal systems and supply chains management.

REFERENCES

[1] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," *Applied Innovation Review*, no. 2, pp. 6–19, 2016.

[2] A. Grech and A. F. Camilleri, "Blockchain in education," Joint Research Centre (JRC), European Commission, 2017.

[3] M. Sharples and J. Domingue, "The Blockchain and Kudos: A Distributed System for Educational Record," in *Proc. European Conference on Technology Enhanced Learning*, 2016.

[4] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[5] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congress on Big Data*, 2017, pp. 557–564.

[6] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[7] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, 2014.

[8] J. Benet, "IPFS—Content addressed, versioned, P2P file system," *arXiv preprint arXiv:1407.3561*, 2014.

[9] N. Szabo, "Smart contracts: Building blocks for digital markets," 1996.

[10] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain," *IEEE Access*, vol. 5, pp. 14757–14767, 2017.

[11] M. Swan, *Blockchain: Blueprint for a New Economy*. O'Reilly Media, 2015.