JST: Smart Systems and Devices
Volume 34, Issue 2, May 2024, 044-053

Utilizing Layer-2 Blockchain and IPFS Innovations for Establishing a Robust System for Secure Document Signing and Management

Thinh Nguyen-Cong[1*], Ngoc C. Lê[1,2]
[1] *Hanoi University of Science and Technology, Ha Noi, Vietnam*
[2] *UMMISCO Center in Southeast Asia, UMI 209, IRD, France*
[*]*Corresponding author email: nguyencongthinh1999@gmail.com*

Abstract

Data holds immense significance within any information system. In traditional setups, data typically funnels into a central server for processing and storage, rendering the entire system reliant on this singular point. The ongoing digitalization trend, particularly accelerated by the global pandemic, has ushered in many transformative shifts in various operational aspects, including the validation, storage, and electronic signing of many documents. This surge in digital transactions has amplified both the data storage requirements and the volume of data traversing the Internet, thereby heightening the potential risks associated with fraud and document tampering. Consequently, an imperative need for a robust and secure document management system arises. Blockchain technology emerges as an innovative solution poised to address these challenges. In this study, we explore the compelling advantages that Blockchain technology offers to the realm of digital document storage, culminating in the development of a secure, web-based solution for document storage and processing.

Keywords: BC-DMS, Blockchain, document management, polygon, security, IPFS, CP-ABE, layer-2 Blockchain.

1. Introduction

The rapid pace of digitalization has prompted government and private organizations to integrate online platforms into their operations, bringing unprecedented convenience for users and the agencies responsible for their processing. This shift is fueled by continuous advancements in hardware, software technologies, and widespread internet access. Management systems have evolved into efficient and user-friendly solutions, often employing a centralized server-client architecture [1]. These systems enhance operational efficiency, streamline procedures, and contribute to environmental sustainability by reducing the reliance on physical documentation [2]. The role of these systems in organizational operations and stakeholder interactions is increasingly pivotal in the ongoing digital age.

Despite the proven effectiveness of document management systems, they frequently encounter scalability challenges. As organizations grow and amass more data, maintaining efficient storage and retrieval becomes increasingly arduous. Infrastructure limitations, as discussed earlier, can hinder scalability, leading to decreased system performance and potential disruptions to business operations. Additionally, the challenge of data redundancy, previously emphasized, can escalate storage costs and complexity. Managing updates or modifications to identical documents serving multiple purposes becomes a formidable task, emphasizing the need for robust data synchronization mechanisms and stringent version control in online systems.

Ensuring cybersecurity and addressing the growing threat of cyber fraud and data tampering is crucial in modern document management. With an increasing volume of sensitive information stored digitally, the risk of unauthorized access and manipulation rises. Implementing robust cybersecurity measures, including encryption, authentication, and intrusion detection, is essential for safeguarding data integrity [3].

The absence of precise mechanisms for documenting updates and preventing fraud in current management systems emphasizes the need for enhanced audit trails and stringent document governance practices. Organizations must establish protocols for tracking alterations, ensuring transparency, and holding individuals accountable for any fraudulent activities. To mitigate vulnerabilities linked to centralized server-based document storage, exploring distributed and decentralized storage solutions is recommended [4]. These technologies enhance data security by reducing single points of failure and minimizing the potential impact of cyberattacks.

ISSN 2734-9373
https://doi.org/10.51316/jst.174.ssad.2024.34.2.6
Received: Jan 1, 2024; revised: Mar 15, 2024;
accepted: Mar 26, 2024

As the surge in internet data traffic coincides with an increase in cybercrime rates, particularly in developing nations like Vietnam, the awareness of data protection hasn't kept pace with technological advancement. Consequently, the incidence of cybercrime, including routine data breaches and cyberattacks, remains disturbingly high. Addressing this, there's a pressing need for a decentralized solution that combines convenience with robust security for tasks like storing, verifying, signing, and sharing data. This can be achieved through the seamless integration of Blockchain technology into document management systems. Leveraging Blockchain enhances document security, reducing instances of counterfeiting [3]. Blockchain, with its inherent security features and immutability, provides a secure and transparent option, particularly beneficial for individuals and organizations prioritizing online data protection [5].

In essence, integrating Blockchain technology into document management systems enhances security and provides users with unprecedented control and transparency. This innovative approach has the potential to substantially reduce the risks associated with cybercrime, creating a more secure digital landscape, particularly in rapidly evolving regions like Vietnam.

Blockchain's multifaceted architecture, combining chain, tree, and graph structures, strengthens resistance against tampering, maintaining an immutable transaction history ledger [6]. The utilization of tree and graph structures adds complexity, broadening Blockchain's applicability across diverse domains. The integrity of Blockchain relies on record immutability, achieved through Proof-of-Work (PoW) consensus algorithms. Participants, known as miners, solve intricate puzzles to validate and append transactions, ensuring their security and discouraging alteration attempts [7]. Academic literatures reflected a growing interest in the intersection of Blockchain technology and document management systems [8]. Researchers have been exploring how Blockchain can revolutionize data integrity and security, focusing on methodologies that elevate storage, retrieval, and secure dissemination of sensitive documents.

This research embarks on a comprehensive exploration of the Blockchain concept, aiming to elucidate how it can be leveraged to create a prototype for a resilient and secure online document management system. The upcoming discussion will delve into the fundamental tenets of Blockchain, highlighting its capacity to mitigate susceptibility to tampering, establish a reliable framework for approving new documents, and facilitate secure document sharing [9-10]. The subsequent analysis will pave the way for practical applications, culminating in the development of a proof-of-concept system that harnesses the full potential of Blockchain technology for efficient and secure document management.

In this study, we focus on a detailed analysis of Blockchain and explore its potential applications in building a resilient online document management system. Our efforts begin by unraveling the complexities of Blockchain, establishing a strong foundation for its incorporation into our proposed system. Our goal is to showcase how Blockchain technology, with its built-in security features, can effectively reduce the risk of unauthorized document alterations. This provides a reliable platform for document approval and facilitates secure document sharing. Our contributions to addressing this challenge are outlined as follows:

1) Comprehensive Exploration of Blockchain: We provide an in-depth examination of Blockchain technology, elucidating its principles, mechanisms, and cryptographic techniques for a profound understanding of its capabilities.
2) Tamper-Resistant Document Management: We discuss the utilization of Blockchain's immutable ledger to create a document management system resistant to tampering, ensuring the integrity and authenticity of stored documents.
3) Trustworthy Document Approval Process: We delve into the design and implementation of a robust document approval mechanism using Blockchain, ensuring a transparent and trusted process for authorizing new documents.
4) Secure and Efficient Document Sharing: We investigate the integration of Blockchain for secure document sharing, facilitating easy, confidential, and efficient data exchange among authorized users.

The research paper is organized as follows: First, we examine the importance of document management systems, focusing on their role in digitalization. Second, we provide a detailed overview of document management systems and Blockchain technology, highlighting their essential features. Third, we conduct a thorough exploration of the design of the document management system integrated with Blockchain technology, including the construction and reconfiguration of the document processing workflow. Finally, we present the experimental phase and introduce a carefully crafted system prototype.

2. Theoretical Background

2.1. Overview of Blockchain

Blockchain technology originated in 2008 when an unidentified individual or group named Satoshi Nakamoto introduced it as a solution to address a fundamental challenge in digital transactions: the need for trust in intermediaries, such as banks, to facilitate secure and reliable exchanges of value [11].

Nakamoto's vision led to the creation of the Bitcoin whitepaper in 2009, laying the groundwork for Blockchain [12]. The first practical implementation occurred with the mining of the "genesis block" in January 2009, marking the official birth of the Bitcoin Blockchain. Initially designed for cryptocurrency, Blockchain has since evolved into a versatile technology with applications across various sectors, highlighting its transformative potential [9].

Blockchain, at its essence, is a decentralized digital ledger operating on a network of computers. It securely records transactions using fundamental components like "blocks" for data, "chains" linking blocks chronologically, and a network of "nodes" validating and storing transactions [13]. Notably, Blockchain employs advanced cryptographic techniques, ensuring data integrity and preventing tampering. A crucial aspect is the use of a hash function, a cryptographic tool processing data into an encrypted fixed-length string, called a hash value. Despite its resilience, hash functions may encounter key duplication (collisions), motivating ongoing efforts to enhance hashing algorithms and minimize collisions.

2.1.1. Transaction

Transactions are the fundamental building blocks of Blockchain technology, which can represent various activities, including cryptocurrency transfers, the execution of smart contracts, data storage requests, and more, depending on the Blockchain's capabilities [5]. A transaction contains several components, which are displayed in Fig. 1.

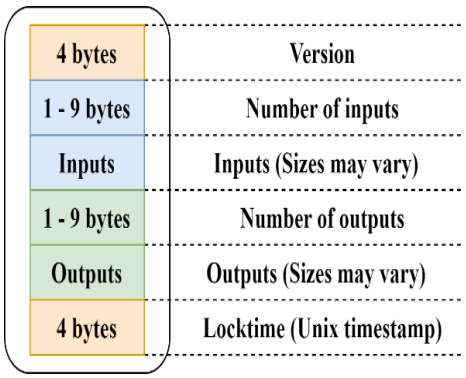

Fig. 1. Structure of a transaction.

To be successful, a transaction in the Blockchain network must go through 6 following steps:

- Step 1 - Initialization: The parties and detailed information of the transaction are recorded.
- Step 2 - Creation: One or more transactions are packaged together into a block.
- Step 3 - Broadcasting: The newly created block will be sent to all network members.
- Step 4 - Consensus: Nodes validate the transactions based on consensus mechanism.
- Step 5 - Storage: The validated block will be chained and stored in Blockchain distributed ledger.
- Step 6 - Notification: The parties involved will be notified of the transaction.

2.1.2. Merkle tree

In Blockchain technology, ensuring data integrity and security relies on cryptographic techniques, with the Merkle tree playing a key role. Also known as a binary hash tree or Merkle-damgard construction, this data structure organizes a large dataset into a tree of hashes, named after its creator Ralph [14]. The Merkle tree efficiently verifies data integrity in a large dataset without the need to inspect the entire dataset, a crucial feature for Blockchain where data integrity and efficiency are paramount.

Transactions are represented as leaves in the Merkle tree, with parent hashes generated based on child hashes. Branch hashes are derived from leaf hashes, and intermediate branch hashes are computed from adjacent branches [14]. This process continues until the root hash, representing the entire dataset's integrity, is included in the block.

2.1.3. Smart contracts

A “smart contract” is a set of automated protocols designed to enforce agreements between computer systems, operating without external interference or the involvement of a third-party intermediary [15]. Expressed in a programming language, these contracts enable precise, secure, and swift execution without physical meetings, relying solely on an Internet connection. Multiple languages and platforms, including Solidity, Rust, and JavaScript, exist for composing and deploying smart contracts. Despite their advantages, smart contracts face challenges like security holes due to programming mistakes and legal recognition issues in many countries [15].

2.2. Blockchain Platforms

Various Blockchain platforms are available for deploying Blockchain applications and smart contracts, each with distinct properties. Public Blockchains prioritize robust security [16], private Blockchains ensure consistent and high performance [17], and consortium Blockchains offer enhanced customization options [18]. Table 1 presents a basic comparison of Blockchain network forms, considering criteria like consensus, immutability, transparency, network design, and more.

Table 1. The differences between Blockchain taxonomies.

	Public Blockchain	Private Blockchain	Consortium Blockchain
Consensus	Only pre-selected nodes have block validation permission	Only a central entity can control validation of block	Only management organizations have block validation permission
Immutability	Transactions are less tampered	Dependent on design; transactions are more easily tampered	Dependent on design; transactions are more easily tampered
Transparency	Visible for all users	Accessible within the organization	Able for organizations in the network to access together
Network design	Decentralized	Centralized	Partially centralized
Advantages	Safe; reliable; open and clear data transparency	High TPS; high scalability; less energy consumption	High TPS; high scalability; less energy consumption
Disadvantages	Low TPS; limited scalability; high energy consumption	Permissions belong to the central entity; low security; lack of transparency	Permissions belong to management organizations; lack of transparency
Example	Bitcoin, Ethereum	Hyperledger Fabric	Hyperledger Fabric, R3 Corda.

2.2.1. Ethereum

Ethereum, a decentralized and open source Blockchain platform, was proposed by Vitalik Buterin in late 2013 and went live on July 30, 2015. Unlike Bitcoin, Ethereum is more versatile, supporting the execution of code through smart contracts. These contracts find applications in diverse fields such as finance, supply chain management, and beyond.

Ether, Ethereum's native cryptocurrency, facilitates transactions and computational services, serving as a store of value and tradable asset on cryptocurrency exchanges. The Ethereum Virtual Machine executes smart contracts, playing a crucial role in the network and enabling the development of decentralized applications. Beyond cryptocurrencies, Ethereum has made significant contributions to decentralized finance (DeFi), non-fungible tokens (NFTs), gaming, and supply chain management, showcasing its versatility and popularity for Blockchain innovation [17].

2.2.2. Hyperledger Fabric

Hyperledger Fabric, part of the Hyperledger project hosted by the Linux Foundation, is an enterprise-grade, open-source Blockchain platform tailored for developing permissioned networks. It emphasizes control and trust within known network participants, making it ideal for consortiums and private business networks [19].

This platform's modular design allows customization of components to meet specific business needs, supporting various consensus mechanisms, including Practical Byzantine Fault Tolerance (PBFT) as the default. Organizations can opt for alternatives like Raft or Kafka-based consensus for improved scalability or fault tolerance [13]. Hyperledger Fabric offers Software Development Kits (SDKs) for multiple programming languages, streamlining developer interaction with the network and application building.

With a focus on data privacy, precise access control, and scalability, Hyperledger Fabric is well-suited for industries such as supply chain management, healthcare, finance, and more. Its modular architecture and flexibility make it a robust choice for enterprise Blockchain solutions.

2.2.3. Polygon (MATIC)

Polygon, formerly Matic Network, serves as a layer 2 scaling solution for the Ethereum Blockchain, aiming to overcome challenges in scalability, transaction speed, and cost-effectiveness. Fully compatible with the Ethereum Virtual Machine (EVM), Polygon enables developers to utilize familiar tools and environments for building. Employing a Proof of Stake consensus mechanism, Polygon enhances energy efficiency and allows validators to engage in block creation and transaction validation. Transactions on Polygon's sidechains are notably faster and more cost-effective than Ethereum mainnet transactions, enhancing accessibility for developers and users engaging with decentralized applications (DApps).

Polygon outperforms alternative Blockchains, especially layer 1, by effectively addressing network scalability challenges through diverse scaling solutions like sidechains and plasma chains. Sidechains operate alongside the mainchain, allowing

independent transactions on separate chains and updating the mainchain's asset state as needed, easing the mainchain's processing load. Plasma chains, organized hierarchically, form a tree-like structure with child chains connected to a mainchain, containing transactions within the plasma chain and occasionally committing to the mainchain. By shifting transactions to Layer 2, Polygon offers lower fees compared to Ethereum, making it cost-effective for frequent and microtransactions. With reduced congestion, an improved consensus mechanism, and compatibility with the EVM virtual machine, Polygon ensures faster confirmation times and seamless interoperability with EVM-based decentralized applications. A performance comparison table highlights Polygon's advantages over other prominent Blockchains.

3. System Architecture Model

Our research focuses on creating an efficient system using the Polygon Blockchain to streamline document management, validation, and sharing. The envisioned workflow starts with a basic document template, serving as the basis for generating unique documents with a distinct Signature (hash) crucial for verification. The system consists of three core components: document generation, verification, and sharing.

3.1. System Components

The Blockchain-based document management system (BC-DMS) using Polygon Blockchain can be divided into several key components, each serving a specific role in the system.

3.1.1. Polygon Blockchain

Polygon functions as the decentralized ledger housing crucial data and executing smart contracts through the Ethereum Virtual Machine (EVM). Key components within the Polygon Blockchain encompass:

- Smart contracts: Deployed on Polygon, they oversee document ownership, access control, and other functionalities;
- Accounts: Users' Ethereum wallet addresses serving as their identities within the system;
- Transaction history: Document-related actions such as uploads, updates, and access requests which are recorded as transactions on the Blockchain.

Smart contracts form the core of the document management system, establishing rules for ownership, access control, and document-related actions. They facilitate document ownership by diligently monitoring addresses that possess specific documents. Additionally, smart contracts provide robust access control, allowing users to specify who can access and modify documents, and under what conditions. Moreover, the system employs comprehensive event logging, meticulously recording document-related actions and events on the Blockchain for transparency and traceability. Furthermore, these smart contracts seamlessly integrate with encryption, incorporating logic for encryption and decryption to augment document security, ensuring a robust and secure framework.

3.1.2. Document storage layer

Document files, such as PDFs or images, are typically not directly stored on the Polygon Blockchain due to limitations in storage size and cost considerations. Instead, a blend of centralized and decentralized file storage solutions is employed. The Interplanetary File System (IPFS) functions as a decentralized storage system, generating unique content addresses in the form of hashes to reference documents within smart contracts [20]. In instances of slow international network connections or disconnections caused by fiber optic cable breakages, centralized cloud storage serves as a backup option to restore data. While the utilization of centralized storage for backups may seemingly compromise system security, in practice, users interact solely with data streams stored on IPFS. The system exclusively engages with cloud storage for data recovery during emergency situations. Furthermore, data undergoes encryption before storage to ensure that the system's security remains unaffected.

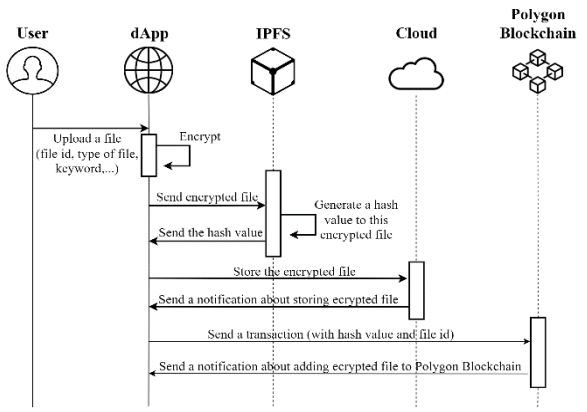

Fig. 2. 3-layer document storage model.

Our system design incorporates a three-tier storage architecture, comprising IPFS, Cloud, and Polygon Blockchain (as illustrated in Fig. 2). The initial layer, IPFS, functions as the repository for the encrypted documents, with its management facilitated by Content Identifiers (CIDs). The Cloud serves as the repository for system backups. Simultaneously, the Polygon Blockchain plays a dual role, serving as the storage location for CIDs and as the platform for executing functions within smart contracts, including tasks such as minting documents and signing them.

Table 2. A detailed performance comparison table between popular Blockchain networks.

	Ethereum	Hyperledger Fabric	Polygon
Native token	ETH	-	MATIC
Programming language	Solidity	Rust, C, C++	Golang, Solidity, Vyper
Transaction speed (TPS)	13-15 per second	3000 per second	Almost 7000 per second
Consensus Mechanism	Proof of Work	PBFT, RAFT	Proof of Stake Plasma-based sidechain
Architecture	Stateful architecture	Modular architecture	Multichain architecture
Scalability	Limited scalability	Limited scalability, only used for organizations.	Multichain solutions offer better scalability.
Cost per transaction	Average $6.5	-	Average $0.015

3.1.3. Encryption layer

Documents must undergo encryption to guarantee the security and confidentiality of information before any sharing occurs. The encryption layer manages the encoding and decoding processes of the document's content. Encryption keys can be securely stored, with access restricted solely to authorized users or smart contracts. The utilization of CP-ABE (Ciphertext Policy Attribute-Based Encryption) is proposed for incorporation into this system's architecture due to its notable characteristics, which enhance security and access control.

CP-ABE offers flexibility in access management, ensuring that only authorized users, or entities possessing the necessary attributes, can decrypt and access sensitive information. This attribute-based approach aligns well with the diverse access requirements of modern systems, making CP-ABE a preferred choice for bolstering security in the proposed system architecture. The integration of CP-ABE and Blockchain forms a robust security framework for the entire system (shown in Fig. 3).

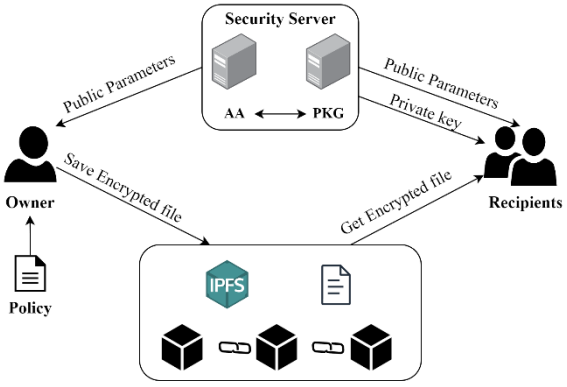

Fig. 3. The integration of CP-ABE and Blockchain.

3.1.4. User authentication and identity

Users need a way to authenticate themselves within the system. Ethereum wallet addresses can serve as their identities. Additional identity verification methods may be integrated, depending on system requirements.

Ethereum wallet login based on managing private keys aligns with decentralization principles and provides users with enhanced security and control over their assets. Users are often required to manage their private keys. Ethereum wallets use cryptographic keys for secure login. Private keys, which are kept securely by the user, are required to access the wallet and authenticate transactions. The model of the login process using the private key is illustrated in Fig. 4. This adds an extra layer of security compared to traditional username and password systems. Managing private keys without relying on a centralized wallet provider gives users full control over their assets.

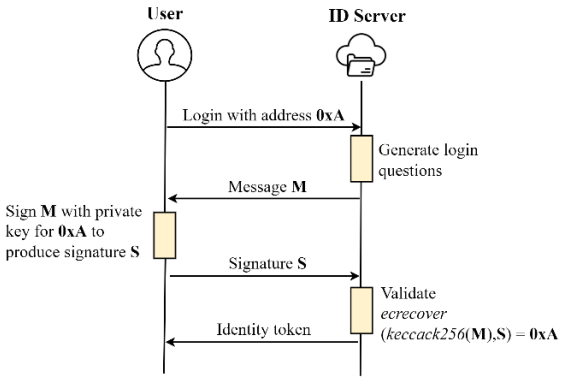

Fig. 4. Model login with Ethereum wallet.

3.1.5. Others

User interface (UI) is the front-end of the system that allows users to interact with the document management platform. Users can directly upload, access, and manage documents through the UI. It communicates with the Polygon Blockchain through a Web3.js library or a similar Ethereum integration

library. The backend server handles various tasks, including user authentication, document encryption/decryption, file storage, and interaction with the Polygon Blockchain. It communicates with the Polygon network through nodes or an API service.

3.2. System Architecture

A Blockchain-based document management system architecture utilizes distributed ledger technology for secure and transparent document storage. Smart contracts define ownership, access control, and document actions. Encrypted documents are stored in decentralized storage (e.g., IPFS), with references on the Blockchain. Documents function as NFTs on the Blockchain. User interactions occur through a friendly interface, enabling uploads, access requests, and management. The Polygon Blockchain (or other EVM-compatible networks) ensures data integrity. This architecture prioritizes security, privacy, and auditability, making it ideal for trust-centric applications like legal, healthcare, or finance (shown in Fig. 5).

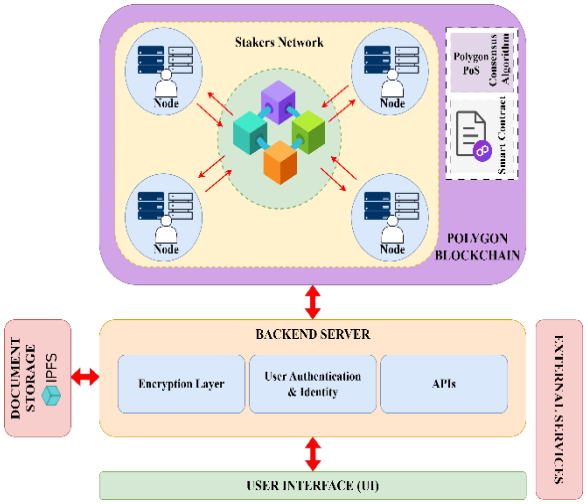

Fig. 5. Basic architecture of Blockchain-based Document Management.

The document management process involves several key steps, ensuring a comprehensive and secure workflowing:

1) Uploading: Users initiate the process by uploading documents, selecting a file from local storage, and optionally adding authorized signers.

2) Encryption: Documents undergo encryption using secure algorithms to maintain confidentiality and prevent unauthorized access.

3) Storing in IPFS: Encrypted documents are uploaded to IPFS, generating a unique Content Identifier (CID) for decentralized storage.

4) Minting: The CID and signers list are minted on the Blockchain, linking the document to its IPFS location without storing content on-chain. The signers list verifies authorized signers.

5) Organization: Minted documents are organized, often with metadata like titles, descriptions, tags, and categories for efficient identification.

6) Access Control: Smart contracts enforce access control rules, defining permissions and access levels for each document.

7) Search and Retrieval: Users can search for documents using keywords, metadata, or full-text search, and the system retrieves relevant documents.

8) Signing: Authorized signers approve or reject documents through smart contracts, with the system calling the Blockchain via web3.js for document retrieval. After signing, the transaction hash is stored in the server (Fig. 6).

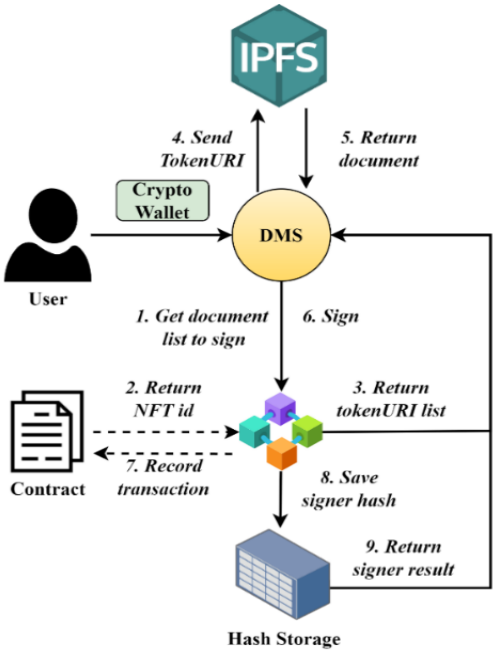

Fig. 6. Signing process model of Blockchain-based document management system.

4. Implementation

To initiate the document management and signing process, one can commence by uploading the document to the system. Within our system framework, documents are categorized into two types: those necessitating signatures (with associated signer lists) and archived documents that don't require signing. Our emphasis lies on ensuring simplicity and clarity, aiming to streamline the document upload procedure for enhanced ease and accuracy.

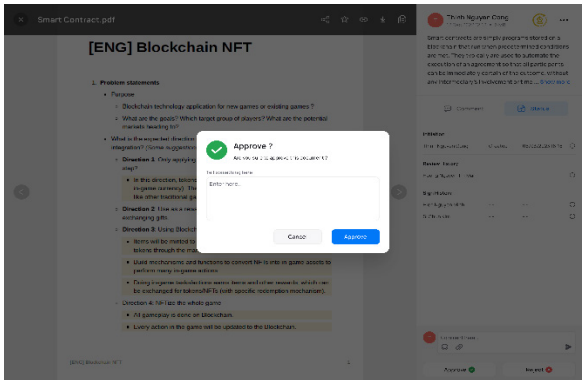

Fig. 7. Implementation of signing process.

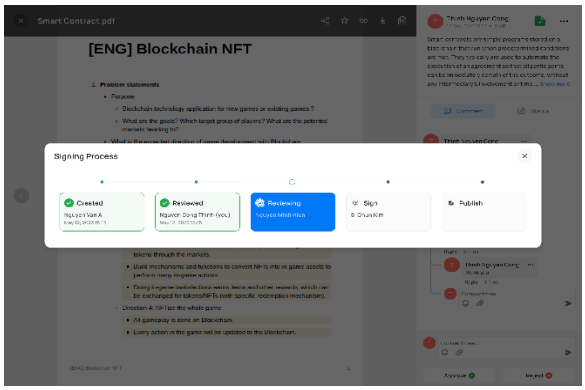

Fig. 8. Statuses of document signing process.

To authenticate information before granting approval for a document, the approver has the capability to access comprehensive document details retrieved from the 3-layer document storage. The decoding process is executed based on user attributes. The system architecture is meticulously crafted to enable users to endorse documents leveraging Blockchain technology and incorruptible smart contracts. It's important to note that only individuals explicitly listed in the document signers' roster possess the authority to approve/reject the document with the interface illustrated in Fig. 7. This authorization mechanism is made possible through our innovative architecture, which relies on the 3-layer document storage model, the integration of CP-ABE and Blockchain, and the login model utilizing Ethereum wallet addresses. The status of the document's approval process is displayed publicly and transparently to individuals in the system (shown in Fig. 8).

5. Experimental Results

In summary, our presentation of a prototype for a secure document management system, leveraging the capabilities of the Polygon network and IPFS, signifies a noteworthy advancement in document management.

To prove the effectiveness of the Polygon network, the author deployed the system simultaneously on both the Ethereum and Polygon Blockchain networks with the following results: the average transaction confirmation time on Ethereum is about 12.20 seconds, while for Polygon, it is only about 2.43 seconds. As a result, the latency period for transactions on Polygon is significantly lower (see details in Fig. 9).

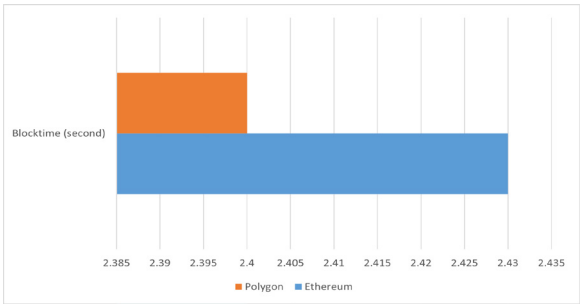

Fig. 9. Comparison of average transaction confirmation times on the Ethereum and Polygon Blockchain networks.

Moreover, to evaluate the effectiveness of the Polygon Blockchain-based document management and signing system, the author evaluates the average time (in seconds) for basic operations such as uploading, tracing, signing and sharing documents. Based on comparison with conventional document management systems such as Google Drive and SharePoint, the results are visually depicted in Fig. 10. From the graph, we can see the impressive data retrieval capabilities thanks to the use of the IPFS distributed file storage system and quick block information retrieval on the Blockchain network. Splitting data to store across multiple nodes on IPFS makes retrieving data simultaneously from multiple nodes significantly faster than with conventional database storage. Document uploading to our system is slower than Google Drive or SharePoint (1.1 seconds behind Google Drive, 0.7 seconds behind SharePoint). This delay is due to the need to split and store the document across multiple nodes on the IPFS network, followed by creating a transaction stored on the Blockchain using the resulting hash. While this process lowers transaction costs and maintains data security, it does slightly extend upload times.

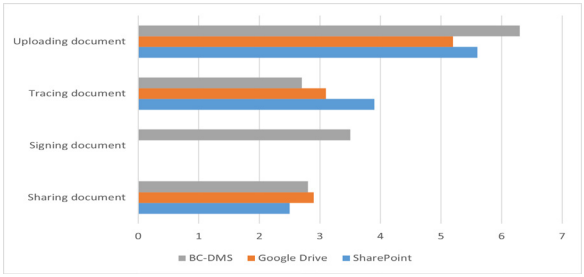

Fig. 10. The performance comparison of the main functions of document management and signing system BC-DMS and other popular document management systems.

6. Conclusion and Future work

In summary, our presentation of a prototype for a secure document management system, leveraging the capabilities of the Polygon network and IPFS, signifies a noteworthy advancement in document management technology. This pioneering integration of Blockchain scalability and decentralized storage not only simplifies document-related processes but also guarantees data security, transparency, and cost-effectiveness. The potential applications of such a system are extensive, spanning various industries that require secure and efficient document handling, ranging from finance to healthcare and beyond. As organizations increasingly seek agile and trustworthy solutions, the amalgamation of Polygon and IPFS in document management provides a glimpse into the future of secure and scalable data management.

While our architecture establishes a robust foundation, there exist numerous avenues for future development and enhancement. Primarily, prioritizing the improvement of user interfaces and experiences is crucial to maintaining a user-friendly and accessible system. Furthermore, ongoing research can delve into advanced encryption techniques to fortify document security. Addressing scalability concerns remains pivotal, prompting exploration into additional layer 2 solutions or Blockchain networks capable of accommodating larger user bases. Additionally, integrating with other Blockchain-based applications and services will broaden the ecosystem's utility. Lastly, investigating the potential of machine learning and artificial intelligence to optimize document categorization, retrieval, and data analysis within the system promises to unlock new dimensions of efficiency and insight. Overall, the journey towards a perfected, Blockchain-based document management system persists, offering even greater advantages for organizations and users alike.

References

[1] V. S. Abbasova, Main concepts of the document management system required for its implementation in enterprises, ScienceRise, pp. 32-37, Feb. 2020. https://doi.org/10.21303/sr.v0i1.1149.

[2] B. Prebreza, D. Gotseva, and P. Nakov, A study of documents management system based on web, case study: University, in 2021 29th National Conference with International Participation (TELECOM), Sofia, Bulgaria, pp. 85-89, Oct. 2021. https://doi.org/10.1109/TELECOM53156.2021.9659663.

[3] R. Prakash, V. Anoop, and S. Asharaf, Blockchain technology for cybersecurity: A text mining literature analysis, International Journal of Information Management Data Insights, vol. 2, no. 2, pp. 100112, Nov. 2022. https://doi.org/10.1016/j.jjimei.2022.100112.

[4] Y. Zhu, C. Lv, Z. Zeng, J. Wang, and B. Pei, Blockchain-based decentralized storage scheme, Journal of Physics: Conference Series, vol. 1237, issue 4, pp. 042008, Jun. 2019. https://doi.org/10.1088/1742-6596/1237/4/042008.

[5] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, An overview of Blockchain technology: Architecture, consensus, and future trends, in 2017 IEEE International Congress on Big Data (BigData Congress), pp. 557-564, Jun. 2017. https://doi.org/10.1109/BigDataCongress.2017.85.

[6] L. Hughes, Y. Dwivedi, S. Misra, N. Rana, V. Raghavan, and V. Akella, Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda, International Journal of Information Management, vol. 49, pp. 114-129, Dec. 2019. https://doi.org/10.1016/j.ijinfomgt.2019.02.005.

[7] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, On the security and performance of proof of work Blockchains, in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS '16, (New York, NY, USA), pp. 3-16, Association for Computing Machinery, Oct. 2016. https://doi.org/10.1145/2976749.2978341.

[8] X. Zhao, Z. Zhang, R. Hu, J. Liu, X. Yang, R. Zhang, and H. Gao, Blockchain technology based digital document management system design, in 2022 7th Asia Conference on Power and Electrical Engineering (ACPEE), pp. 440-446, Jun. 2022. https://doi.org/10.1109/ACPEE53904.2022.9783819.

[9] M. Das, X. Tao, and J. C. P. Cheng, A secure and distributed construction document management system using Blockchain, In Proceedings of the 18th International Conference on Computing in Civil and Building Engineering, vol. 98, pp. 850-862, Springer International Publishing, July. 2020. https://doi.org/10.1007/978-3-030-51295-8_59.

[10] M. Das, X. Tao, Y. Liu, and J. C. Cheng, A Blockchain-based integrated document management framework for construction applications, Automation in Construction, vol. 133, pp. 104001, Jan. 2022. https://doi.org/10.1016/j.autcon.2021.104001.

[11] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, Where is current research on Blockchain technology? —a systematic review, PLOS ONE, vol. 11, pp. 1-27, Oct, 2016. https://doi.org/10.1371/journal.pone.0163477.

[12] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, Cryptography, Mar. 2009. [Online] Available: https://bitcoin.org/bitcoin.pdf.

[13] S. J. Alsunaidi and F. A. Alhaidari, A Survey of Consensus Algorithms for Blockchain Technology, 2019 International Conference on Computer and Information Sciences (ICCIS), Sakaka, Saudi Arabia, pp. 1-6, May. 2019. https://doi.org/10.1109/ICCISci.2019.8716424.

[14] M. Bosamia and D. T. Patel, Current trends and future implementation possibilities of the merkel tree, International Journal of Computer Sciences and Engineering, vol.6, issue.8, pp. 294-301, Aug. 2018. https://doi.org/10.26438/ijcse/v6i8.294301.

[15] M. Bartoletti and L. Pompianu, An empirical analysis of smart contracts: Platforms, applications, and design patterns, Lecture Notes in Computer Science, vol. 10323, Nov. 2017, pp. 494-509. https://doi.org/10.1007/978-3-319-70278-0_31.

[16] F. Eigelshoven, A. Ullrich, and B. Bender, Public Blockchain-a systematic literature review on the sustainability of consensus algorithms, Twenty-Eighth European Conference on Information Systems (ECIS2020) - A Virtual AIS Conference, pp. 1-19, Jun. 2020. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1201&context=ecis2020_rp.

[17] M. Valenta and P.G. Sandner, Comparison of Ethereum, Hyperledger Fabric and Corda, FSBC Working Paper, Frankfurt School Blockchain Center: Hessen, vol.8, pp. 1-8, Jun. 2017. https://api.semanticscholar.org/CorpusID:46991541.

[18] K. Wüst and A. Gervais, Do you need a Blockchain?, in 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), pp. 45-54, Nov. 2018. https://doi.org/10.1109/CVCBT.2018.00011.

[19] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolic, and J. Yellick, Hyperledger fabric: A distributed operating system for permissioned Blockchains, Association for Computing Machinery, New York, pp. 1-15, Apr. 2018. https://doi.org/10.1145/3190508.3190538.

[20] N. Nizamuddin, H. R. Hasan, and K. Salah, "Ipfs-Blockchain-based authenticity of online publications," in Blockchain - ICBC, Springer International Publishing, vol. 10974, pp. 199-212, Jun. 2018. https://doi.org/10.1007/978-3-319-94478-4_14.