International Journal of Advanced and Applied Sciences

Journal homepage :http://www.ijaas.in

The blockchain-based design and implementation of a framework for remote data management

Abdulrahman Alreshidi *

College of Computer Science and Engineering, University of Ha'il, Hail, Saudi Arabia

ARTICLE INFO

Article history:
Received 30 November 2024
Received in revised form
15 April 2025
Accepted 29 April 2025

Keywords:
Blockchain architecture
Decentralized data management
Smart contracts
Satellite data sensing
Data security

ABSTRACT

Blockchain technology has recently emerged as a disruptive solution for secure data storage, transfer, and management across various fields such as remote sensing, space exploration, and sustainable energy systems. In this study, we design, develop, and assess a blockchain-based system for managing remotely sensed data. Our approach removes the need for central authorities and improves data security and retrieval through decentralized data management. By using blockchain algorithms and smart contracts, the proposed system ensures transparent and verifiable tracking of data sensing processes and communications. We apply our method to a case study involving satellite data sensing and develop a proof-of-concept prototype using Ethereum's TESTNET platform. To evaluate the effectiveness of our solution, we conduct a cost analysis focusing on (i) energy consumption and (ii) storage efficiency of smart communication contracts. This approach offers a promising way to improve the management and security of data in critical applications. The main contributions of this research are: (a) the design of a blockchain-based architecture, (b) the development of algorithms to support this architecture, and (c) experimental evaluation using satellite sensing data. Our work aims to advance research on blockchain-based data management and supports the development of new decentralized systems for future data management needs.

1. Introduction

In recent years, 5G (the 5th Generation network) technologies have seen significant advancements that have led a race towards the 6G technologies for wireless communication (Ji et al., 2021). The 5G technologies promise enhanced reliability, reduced data latency, increased data transmission throughput, stable connectivity, and broader coverage for remote data sensing (Muthulakshmi and Chitra, 2024). Despite the potential offered by 5 G-enabled communication systems, data security, and privacy remain central for the successful implementation and adoption of such systems in the smart systems context (Khan et al., 2020). Securing remote sensing of communication data is a critical challenge, as it involves collaboration among multiple entities, necessitating accurate data management, change tracking, and data temper-proofing (Ahmad et al., 2023). However, existing centralized solutions suffer from inefficiencies, inadequate updating methods, and the risk of unauthorized alterations. These limitations and emerging challenges demand a secure and decentralized infrastructure that can manage remotely sensed data to increase the trustworthiness of decentralized communications and data sensing (Hammad et al., 2023). This poses a critical challenge for efficiently and securely managing, and processing remotely sensed data.

Context of Research: Blockchain technology employs a consensus process to create a distributed ledger shared across its network to ensure security and complete decentralization without third-party verification (Razzaq, 2024). In blockchain systems, the data blocks (a.k.a 'miner nodes') digitally sign, verify, and validate each transaction thus rendering the ledgers tamper-proof with timestamping for secure data management. Various sectors such as industrial automation, banking, accounting, logistics, supply chain, and healthcare systems have leveraged blockchain-based solutions to address secure and efficient transmission of big data (Slimani and Hedjam, 2022; Ma et al., 2023) and ensure

trustworthiness due to robust and decentralized infrastructure offered by blockchains, as illustrated in Fig. 1. In In blockchain systems, smart contracts are implemented as self-executing algorithms executed by a network of untrusting nodes to offer tamper resistance for data. Smart contracts transform blockchains into distributed computing architectures, enabling the cost-effectiveness and reusability of blockchain-based decentralized data management. Ethereum is a prominent blockchain platform that activates smart contracts by assigning transactions to an Ethereum-implemented smart contract and executing it based on provided inputs (Ahmad et al., 2022). Ethereum utilizes Ether as the crypto protocol (synonymously, the cryptocurrency), and each network member is identified by a unique Ethereum address.

Challenges and Research Objectives: Blockchain technology is often attributed to a multitude of challenges including inefficiencies in handling extensive data, energy inefficiency in executing transactions, and complex implementations. However, enabling the storage of document hashes within the blockchain instead of the documents themselves can help overcome the issues of transaction costs, i.e., increased performance and decreased gas consumption. Specifically, in blockchains, the data uploaded to the Inter-Planetary File System (IPFS) as a protocol to share data in a peer-to-peer network generates a hash that also secures the smart contract for content retrieval based on the hash generated (Verma et al., 2025). The available solutions of remote sensing based on distributed are predominantly centralized which limits user control and susceptibility to data loss or tampering. One of the central challenges for this research is '*how to leverage blockchain technology to develop a decentralized mechanism that can devoid a third-party authentication to enhance scalability and security of remotely sensed data*' (Ahmadisheykhsarmast et al., 2023). Managing versions of transmitted data in decentralized storage demands a uniform log, necessitating innovative solutions.

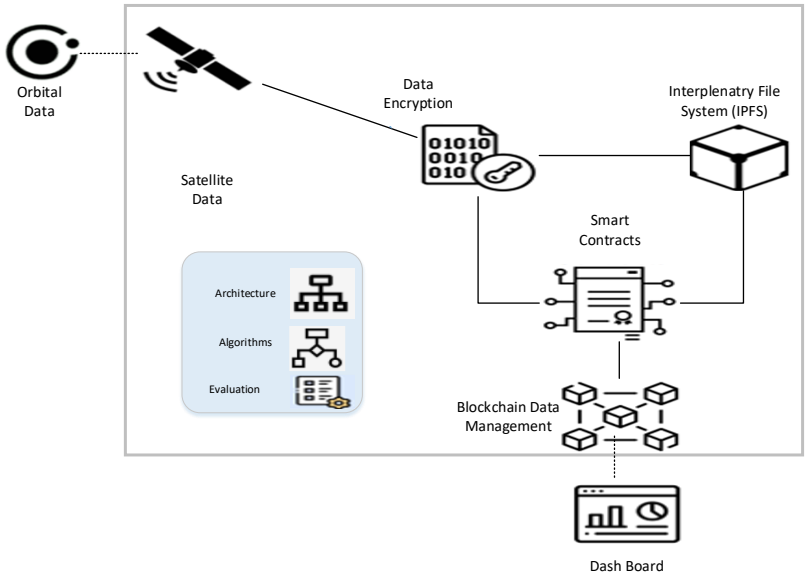

Fig. 1: An illustrative view of the proposed solution

Proposed solution and contributions: In this study, blockchain-driven solution has been proposed to measure remote sensing data based on the concept of document sharing, striving to establish a dependable, decentralized system overviewed in Fig. 1. Fig. 1, as a generic view of the solution synopsis the core component of the proposed solution in terms of encrypting satellite data, IPFS, and smart contracts that are managed by blockchain solution. The dashboard for data analytics and orbital data is outside the scope and boundary of this solution. Fig. 1 employs cryptographic methods to safeguard user identities and data transmission (Ahmed and MacCarthy, 2023; Razzaq et al., 2022), the system mitigates record manipulation, and smart contracts automate the workflow, fostering controlled or uncontrolled data transfer while facilitating decentralized communication among diverse parties, such as approvers and developers. Based on the introductory details and the solution view in Fig. 1, we outline the primary contributions:

- Blockchain architecture - representing solution blueprint - that exploits smart contracts to ingest, manage, and transmit to support remote data sensing in decentralized systems.
- Algorithmic-based implementation of the architecture to automate and customize the solution as a proof of-the-concept prototype for the proposed solution.
- Experimental validations for evaluating the efficiency of the system in terms of gas consumption and data storage cost of the smart contract-based transaction of decentralized data.

The solution proposed in this research aims to progress state-of-the-art decentralized data management by applying blockchain technology. The

solution synergizes blockchain technology and big data systems via an architectural framework that can guide researchers and practitioners to architect, implement, and validate emerging solutions of big data management using blockchain technology.

Paper organization: Section 2 presents the context as background details and a research method to conduct this study. Section 3 presents the proposed architecture for blockchain-oriented secure sensing of remotely sensed data. Section 4 presents algorithmic details to implement the proposed architecture. Section 5 provides validation of the solution. Section 6 concludes the paper and highlights some potential dimensions for future research.

2. Research context: Blockchain systems and data sensing

This section presents the research context and research method before elaborating on the technical details of the solution. First, we present the research context in terms of blockchain systems and remote data sensing to define the fundamental concepts such as blockchain systems in Section 2.1, remote data sensing in Section 2.2, and blockchain-based remote data sensing in Section 2.3 illustrated in Fig. 2. Second, we discuss the research method that provides a systematic and incremental, i.e., stepwise approach to conduct this research in Section 2.4, as shown in Fig. 3. We outline the fundamental concepts, core terminologies, and the overall methodology that is used later in the paper to discuss the proposed solution, based on the illustrations in Figs. 2 and 3.

2.1. Blockchain systems

Blockchain systems have revolutionized the landscape of digital transactions and data management by providing a decentralized, transparent, and secure framework, as in Fig. 2. Distinct from traditional centralized systems, blockchain technology ensures that data is distributed across a network of computers, eliminating the need for central authority and enhancing trust among participants (Fahmideh et al., 2022). This is achieved through cryptographic techniques and consensus algorithms that validate and record transactions immutably on a public ledger. A notable example of blockchain's application is in the financial sector (Zhao et al., 2016), where cryptocurrencies like Bitcoin and Ethereum leverage blockchain to facilitate peer-to-peer transactions without intermediaries. The potential and application areas of blockchain extend beyond transactions, finance, and healthcare and it is widely used across domains to optimize the transparency, accountability, and safety of critical data. The robust nature of blockchain can resist and withstand unauthorized access and withstanding data tempering thus making it an ultimate technological choice for data temper-proofing (Abbas et al., 2024).

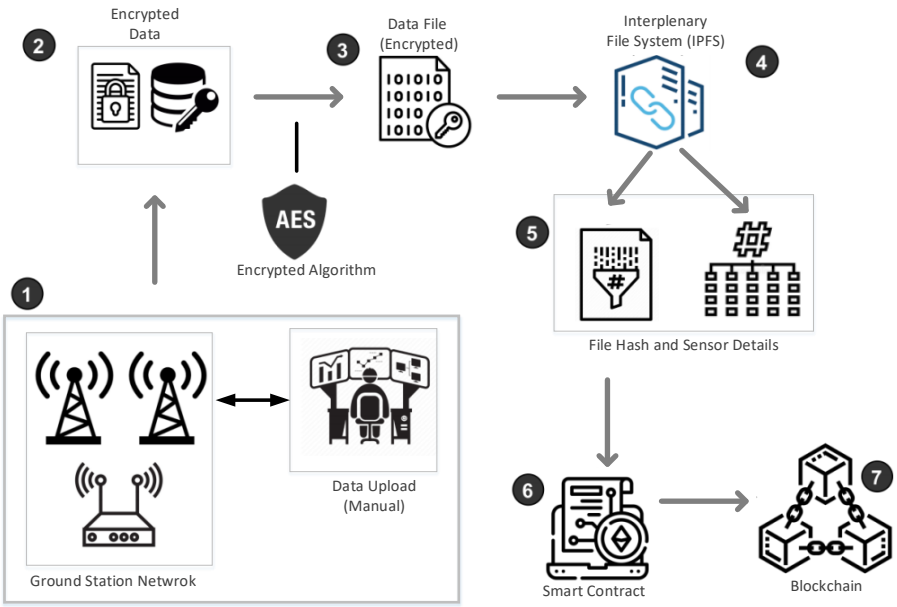

Fig. 2: Research context: Illustrative overview of blockchain-based data sensing

2.2. Remote data sensing

Remote data sensing, as a concept accumulates, several sensing sensors, technologies, software, and platforms to ingest data from data emitting nodes that are deployed at remote and geographically distributed locations. With the emergence of 5G technologies, Unmanned Aerial Vehicles (UAVs), the remote data sensing nodes can be deployed on satellites and UAVs to collect a multitude of data such as temperature, humidity, underwater levels, and so on. One of the central application areas of remote data sensing is environmental monitoring which collects data from the environmental factors and provides predictive analytics for disaster prediction and prevention. For instance, the NASA

Earth Observing System (EOS) satellites provide critical data used in climate research and weather forecasting (Khan et al., 2024). In urban planning, it supports the development of smart cities by monitoring infrastructure health and traffic patterns. The integration of remote sensing with other emerging technologies including but not limited to the Internet of Things (IoT) and machine learning further enhances its capabilities, allowing for more classy data analysis and predictive modeling. For example, IoT-enabled remote sensors can continuously monitor environmental conditions and transmit data for real-time analysis (Pu and Xu, 2025), improving decision-making processes. Remote data sensing represents a crucial tool for advancing scientific research, improving resource management, and enhancing the overall understanding of our environment.

2.3. Blockchain in secure remote data sensing

As overviewed in Fig. 2, each remote sensing dataset in the Interplanetary File System (IPFS) is assigned a cryptographic hash to encode and secure the data. IPFS, a distributed peer-to-peer content-based protocol, integrates smart contracts (SM) with blockchain data, offering benefits like speed, accuracy, transparency, trust, efficiency, and security. To ensure security, the datasets are encrypted with 256-bit encryption before uploading to IPFS. It reduces storage needs, bandwidth costs, and facilitates fast data downloads and large data sharing without duplication. Data files larger than 256 KB are divided and stored as multiple IPFS objects linked to the original file. IPFS decentralizes datasets, reducing server load, and the entire encrypted dataset is stored in IPFS. Fig. 2 provides an overview of the system processes. Once approved, users can upload data and use a secret key for decryption. The administration that controls the data server can process data and set dynamic secrets for uploading to IPFS. The ground station network can access binary data from remote sensing satellites. This data is encrypted using AES, saved as a CSV file, and uploaded to IPFS, which provides a file hash key. Smart contracts save this key and related info on the blockchain ledger. Authorized researchers or users with a registered blockchain address can access the data through the platform. The data is retrieved as cipher text and decrypted information.

2.4. Research method

A generic and phase-wise view of the research method is provided in Fig. 3 which indicates three phases of the research method. Each of the phases is detailed below, as per the illustration of methodological steps in Fig. 3.

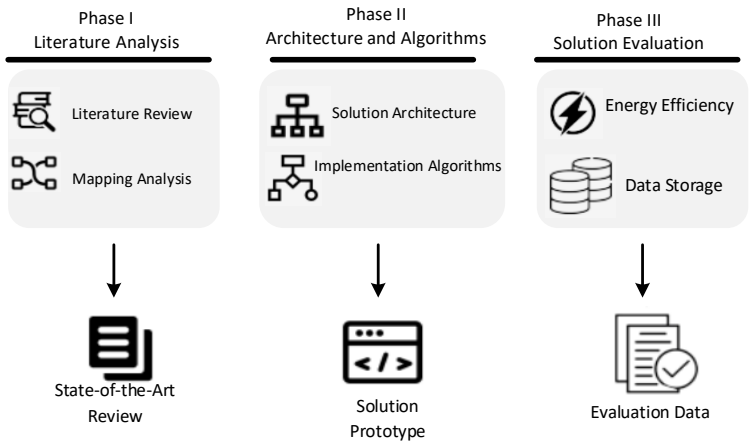

Fig. 3: Phase and steps of the research method

- **Phase I-** Literature Analysis: Our research journey commences with an extensive literature review to gain a profound understanding of the existing published research and analyze state-of-the-art in the field. This initial phase focuses on conducting a thorough comparative analysis between the existing solutions and our proposed approach. You can delve deeper into the findings of this literature review in Section 6, where we provide a comprehensive discussion.
- **Phase II-** Architecture Representation and Algorithmic Design: In the subsequent stage, we transition from knowledge gathering to the creation of a blueprint for our solution's architecture. Simultaneously, we design the algorithms that constitute the core of our approach. Section III offers a detailed insight into the architectural aspects, while the modularized implementation of our algorithms is elaborated upon in Section 4.
- **Phase III-** Solution Evaluation: The final stage of our research methodology focuses on rigorously evaluating the efficiency and suitability of our proposed solution. This phase, outlined in Section 4, ensures that our approach not only aligns with our research objectives but also proves its mettle in addressing real-world challenges.

3. Proposed architecture: Blockchain-oriented secure data sensing

An overall architecture view of the system is presented in Fig. 4b which reflects the system blueprint in terms of orbital data, the IPFS system,

and blockchain-based smart contracts. The overall architectural representation is mapped with the component and connector-based architecture (Sun et al., 2019) of the system as presented in Fig. 4a. For example, the orbital data component in Fig. 4b can be mapped to Orbital Data component with a transmit connector for Encrypt Data in Fig. 4a. We now present the architectural components, algorithmic background and the technologies used to implement the architecture, each detailed below.

3.1. Core architectural components

The architecture of software-intensive systems, services, and applications plays a pivotal role in outlining the blueprint for effective implementation. In Fig. 4, we present a comprehensive architectural view that delineates the overall design of our proposed solution. This architectural representation provides valuable insights into the core components and functionality of our system. As shown in Fig. 4, the proposed solution leverages Ethereum smart contracts, that act as fundamental entities ensuring the immutability of transactional records and enabling trustworthy storage and transmission of data. The architecture view projects a structural representation of the overall system as well as highlights how the security and confidentiality of the data are preserved. Specifically, Fig. 4 demonstrates a separation of concerns between data sensing, data management, and data transmission. Such separation of concerns helps to maintain the confidentiality and integrity of data. The data is securely stored in the Interplanetary File System (IPFS) and linked to the blockchain. The synergy between IPFS and blockchain ensures seamless and secure data processing. The architecture, as shown in Fig. 4, provides modularization as well as architectural components to enable remote data sensing assured with data security, transparency, and reliability of remotely sensed data.

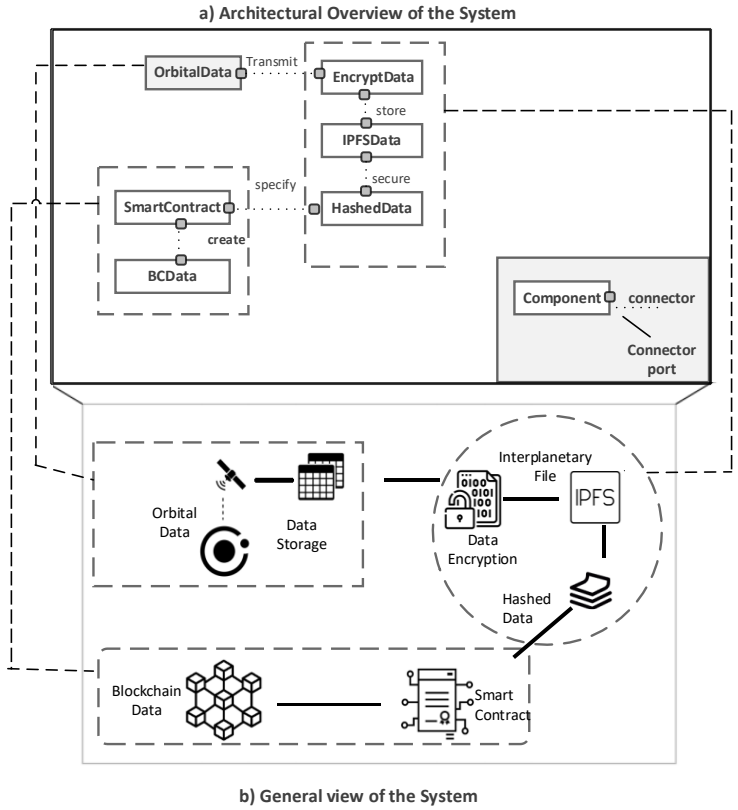

Fig. 4: Architectural overview of the proposed solution

3.2. Algorithms for architecture implementation

The proposed research and its underlying solution exploit algorithms as implementation-specific details of the architecture that are tailored to incorporate encryption, decryption, retrieval, and validation of blockchain-based security-critical data. Additionally, we incorporated a range of cutting-edge technologies, including blockchain (specifically Ethereum) for creating an immutable and transparent ledger, the Interplanetary File System (IPFS) for decentralized and secure data storage, smart contracts for automating and management, advanced encryption mechanisms (such as AES) to ensure data confidentiality and integrity, and various programming technologies and available frameworks including but not limited to Solidity, Python, and Truffle. This programming framework provides executable specifications to develop smart contracts, implement algorithms as modules of source code, and test the Ethereum contracts. This combination of algorithms and technologies formed the foundation of our research, enabling the development of a robust and secure system for managing records.

3.3. Technologies for architecture implementation

By exploiting the programming framework and the above-mentioned technologies, complemented with the principles and practices of software engineering to ensure the security and reliability of the proposed solution. In the corresponding sections, we focus on (a) architecture as a solution blueprint, (b) algorithms to modularize the implementation of the architecture, and (c) evaluate the overall solution. Fig. 4 provides an insightful visualization of our data storage process, a critical component of our blockchain-based system.The process commences when the document's owner initiates the procedure by uploading the pertinent data to the IPFS. In return, the IPFS generates a unique hash key for this document and a key with other essential details which is stored securely in the ledger of the blockchain. To ensure data integrity, i.e., correctness and security, we employ a symmetric encryption method. This method entails encrypting the data using a predefined key and transforming it into ciphertext. Subsequently, this ciphertext efficiently writes a file using a library of file streams, facilitating smooth data handling. Following the encryption and file creation phase, the encrypted file is then securely uploaded into the IPFS network. IPFS, with its decentralized architecture and content-addressable structure, not only ensures the availability and integrity of the stored data but also returns a unique hash key for this file. The file hash that acts as an identifier for the file is seamlessly preserved in the blockchain ledger along with a description of the data. Blockchain ledger not only assures the security and immutability of the data record but also enables version tracking and management for any temper-proofing.

4. Algorithmic implementations of architecture

In the context of blockchain-based application development and the emergence of decentralized applications (DApps), a multitude of tools and technologies are synergized to develop and deliver a seamless solution. At the forefront of this toolbox is Visual Studio Code, a widely embraced open-source code editor renowned for its versatility. Application developers and academic researchers exploit the blockchain platform for not only developing and testing but also experimenting with the deployment of smart contracts and DApps. An extensive application ecosystem facilitates researchers and developers to rapidly design, develop, test, and deploy their DApps on blockchain platforms. In conjunction with the Visual Studio Code, Ganache is a valuable resource for blockchain-based application development.

It acts as an emulator for blockchain application development and deployment along with debugging the blockchain applications. In addition, MetaMask provides a web platform to execute Ethereum applications in a web-based environment. It provides a transaction vault to manage blockchain-based data management. By exploiting the Metamask, users can interact with the blockchain applications and enable wide-spread useability of the blockchain applications.

4.1. Algorithm 1: Data sensing and preservation

We provide a comprehensive demonstration and description of the remote sensing data storage process within the blockchain ledger. Each of the algorithms is detailed in terms of the inputs, the process supported by the algorithm, and the output(s) of the algorithm.

- Input(s): For the algorithm, input data is parameterized with user ID and document ID corresponding to the sensor's data.
- Processing: This technique serves as the vigorous repository for a diverse range of data types, including aerial imagery, maps, and thematic maps, all precisely recorded within the blockchain ledger through the execution of a smart contract endowed with specific additional properties for mapping. Within the blockchain, a collection of critical parameters, straddling temperature, wind speed and direction, altitude, and more, find their secure abode. These parameters are shrewdly analyzed across temporal, spectral, and spatial domains to ensure comprehensive data integration.

- Output(s): As the processing of the algorithm 1 completes, the blockchain ledger preserves the immutability of the remotely sensed data for secure storage and further processing.

Algorithm 1: Data sensing and preservation

```
1:    Input:  RS, λ, Output: R

3:    SensingData
4:    if τ == RS  then      FS ← File(γ)

6:        FB ← Buffer.form(FS)
7:        ENCRYPTED ← AES(KEY, FB)
8:        FH ← IPFS.ADD(ENCRYPTED)
9:        PRESERVE(RS, λ, Output: R)
10:
12:       = 0
```

4.2. Algorithm 2: Interface view

The algorithm is central in validating and authorizing access to the data in the blockchain ledger that is detailed below:

- Input(s): The algorithm starts with the processing of the blockchain ledger data that is provided as parameterized input to the algorithm.
- Processing: The data preserved in the blockchain ledger is accessed via parameters. Data access is managed and controlled via a mapping of user ID, facilitating personalized access. Furthermore, remote sensing specialists possess the ability to

directly access stored data, employing them as their gateway. The processing phase is marked by the versatility of data access methods, accommodating a spectrum of approaches, from user ID mapped to geologists gaining direct access to geographical image data via the user.

- Output(s): Ultimately, the output of Algorithm 2 is established as publicly accessible data, thoughtfully organized and mapped for efficient retrieval.

Algorithm 2: Data interface view

```
Input: γ, Δ
Output: RS
procedure DATA ACCESSING
    if sender(Δ) == 1 then
        FH ← GetFileHash(γ)
        ENCRYPT() ← IPFS(FH)
        γ ← DOWNLOAD(ENCRYPT())
    end if
    Update(RS)
end procedure = 0
```

5. Results and evaluation

This section overviews the experimental evaluation of the proposed solution. Our evaluation encompasses a criterion-based and experiment-driven assessment to validate the solution. We primarily focus on evaluating the functional aspects of smart contracts, with specific emphasis on energy and computational efficiency metrics. Additionally, we quantitatively measure the efficiency of data management and transmission using blockchain to validate system efficiency in handling these critical operations. Experimental evaluations also assess query response times, with a keen focus on algorithmic efficiency. While presenting the experimental results, we also need to highlight some threats to the validity of the solution.

5.1. Experimental setup

The experimental setup considers both the hardware configurations and software setup. In the hardware context, we utilized a Microsoft Windows Platform having a core i7 processor and 16 gigabytes of running memory. The hardware and software experimental setup ensure a compatible platform for solution execution. Specifically, from the evaluation perspective, we focused on system testing by implementing automation using NodeJS and ReactJS within the Visual Studio Code environment. By leveraging libraries like React, Web3, IPFS, and HTTP, we automated critical tasks, enhancing the efficiency of our evaluation. Additionally, we developed an execution script based on JavaScript to monitor processor utilization during tasks such as image uploads to IPFS and blockchain storage, providing valuable insights into system performance. For local Ethereum simulation, we seamlessly integrated the Ganache suite and incorporated the MetaMask extension to enable browser-based interactions. This setup allowed us to evaluate the system's performance in a simulated Ethereum environment.

5.2. Energy efficiency (gas consumption)

One key aspect of our evaluation was the measurement of fuel consumption, denominated in Gwei, which represents the smallest unit of Ether. By comparing these measurements to planned data uploads, we were able to assess the cost efficiency of our approach. Our detailed cost analysis presented in Table 1, included a breakdown of gas usage and Ether cost. Notably, we observed that minimizing input data resulted in reduced costs, underscoring the cost-effectiveness of our approach when compared to traditional centralized database systems. A rigorous evaluation provides an objective evaluation of the energy efficiency of the proposed solution.

Fig. 5 presents the results of the evaluation and shows the required time for uploading the data to IPFS by a user and saving it to a blockchain ledger. The evaluation of the data handling process shows the use of time for uploading and retrieving data. Fig. 6 illustrates the summary values of experimental trials based on data block sizes (in Bytes), and gas consumption. An interesting trend to observe is for example, when data upload exceeds the 600 Byte size threshold, the gas consumption (on average) records to 800717 units. On the contrary, considering the data storage of 350 Byte size, gas consumption (on average) is 322839 units. This observation reveals a direct correlation between data size and units of gas consumption, i.e., units of gas consumed have a proportionality to the size of data being uploaded or processed. An interesting observation is that even with an increased block of data size the difference between gas consumption using IPFS in the proposed solution. The experimental analysis and illustrative view in Fig. 6 show the solution's performance with varying blocks of data size and its impact on gas consumption.

Table 1: Standard gas consumption and cost of executing smart contracts

Evaluation parameter	Contract execution	Gas consumption	Ether cost
Parameter-1	Smart contracts creation (DPoH)	556046	0.01112092
Parameter-2	Smart contracts migration	25915	0.0054726
Parameter-3	Cost of initial contact	234574	0.0450474
Parameter-4	Cost of initial migration call	42363	0.0084726
Parameter average	Final cost		0.06849198

Fig. 5: Uploading the digital passport of health to the blockchain (benchmark data for DPoH creation extracted from Alreshidi (2024))

Our approach leverages the power of IPFS, a decentralized storage system seamlessly integrated with the blockchain, to safeguard and maintain remote sensing data. This harmonious combination ensures the secure preservation of crucial data while capitalizing on the blockchain's immutable ledger for transactional records. To evaluate the efficacy of the proposed solution in terms of data retrieval and storage within the blockchain ledger, we conducted a rigorous evaluation of query response times.

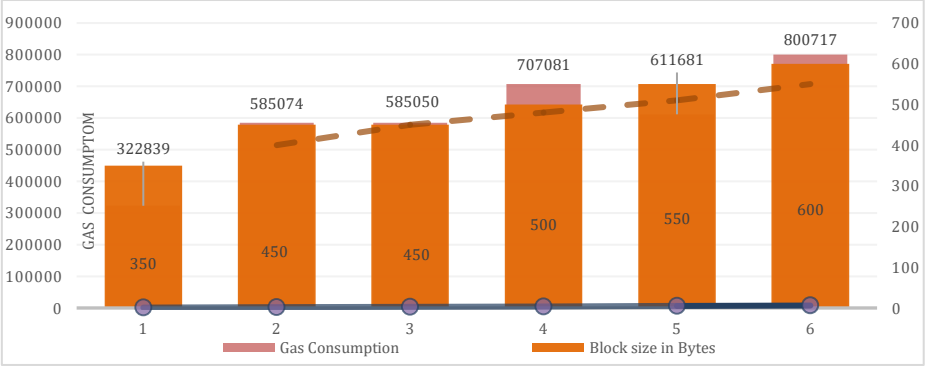

Fig. 6: Gas consumption vs. block size and transaction

This evaluation of computational efficiency, i.e., processing is that even with an increased block of data size the difference between computational efficiency using IPFS in the proposed solution. The experimental analysis and illustrative view in Fig. 7 show the solution's performance with varying blocks of data size and its impact on computational efficiency.

5.3. Summary of computational efficiency

Discussion and Conclusion of Evaluations: This evaluation encompassed two distinct tests designed to ascertain the speed at which data, stored both in IPFS and the blockchain ledger, could be swiftly retrieved in response to user queries. The compelling results of these query response time assessments are graphically depicted in Fig. 7, where execution time is represented in the horizontal axis and response time is represented in the vertical axis. The "Complete Execution" facet of the chart represents the end-to-end process, commencing with the secure storage of remote sensing data within the IPFS system and culminating in the meticulous recording of essential information within the blockchain. This inclusive approach captures vital transactional details, including the remote sensing data file hash, providing a holistic view of our system's efficiency.

6. Related research

This section provides an overview and streamlines the most relevant related work on (i) blockchain systems for digital asset management, and (ii) applications of blockchain systems in smart systems. Critical analysis and overview of the related work justifies the scope and proposed contributions. Table 2 provides a comparative analysis of the most relevant existing research in terms of data management by centralized vs decentralized systems.

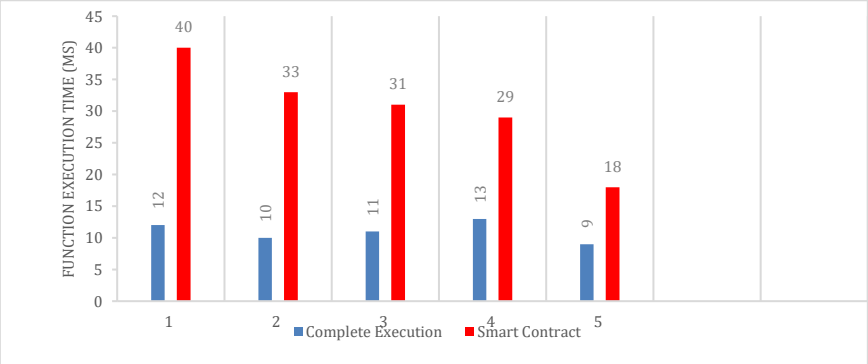

Fig. 7: A Comparative overview of data storage time IPFS vs. blockchain

6.1. Blockchain solutions for digital asset management

In the context of asset digitization, the Swedish government employed blockchain for digitizing the real estate industry particularly in managing land papers and titles. This approach aims to enhance the reliability and security of document updates and exchanges among stakeholders, enabling user identity confirmation through smart contracts (Razzaq et al., 2022). While the model is in testing, the recordskeeper has proposed a solution based on public access which is open-source and protects the documents (Japitana and Burce, 2019). This technology offers heightened security and accessibility across peer groups, unlike conventional database systems, as it creates immutable records (Kitchenham et al., 2009; Razzaq, 2022). Records Keeper provides a rigorous framework for blockchain-based document storage (Gatcha et al., 2022; Daniel and Guida, 2019), allowing validation at any time, but practical implementation of document version control remains a challenge, as summarized in Table 2.

6.2. Blockchain in smart city systems

Iron Mountain, a global organization, employs blockchain technology to securely save and manage digital data and ensure the network storage is reliable. This blockchain-assisted framework serves as an audit trail or version tracking system, allowing approved network members to monitor changes, overcoming concerns about digital asset authenticity and reliance on untrustworthy third parties (Daniel and Guida, 2019). Eleks Labs has created a unique technique using Ethereum to secure document transmission for various types of sensitive data, eliminating the need for third-party intermediaries. Their permissionless blockchain enables safe storage and transmission of documents, including legal agreements, with cryptographic technology and Ethereum-enabled smart contracts ensuring security and efficiency (Kitchenham et al., 2009; Razzaq, 2022).

Conclusive Summary: We now conclude the comparison of the most relevant existing research based on 4-point criteria organized as rows of Table 2 and 3-features presented as the columns of Table 2. Considering the recent research and development on big data for remote sensing, capable developments are emerging. For example, based on the criteria in Table 2, a typical example of such a case is Analysis Ready Data (ARD) which is recommended by the Committee on Earth Observation Satellites (CEOS), although challenges remain in data aligning formats with ARD standards. The data-sharing policies have revealed two significant shortcomings. These developments offer the potential for addressing existing data-sharing challenges (Razzaq, 2022; Ahmad et al., 2023) and fostering a more cooperative and data-rich environment within the field, driving progress and innovation in remote data sensing (Jobarteh and Neethirajan, 2025). Table 2 provides an objective and criteria-based comparison of key factors for centralized and decentralized data management.

Table 2: Comparison of centralized vs decentralized data management systems

Core feature	Identity management	Blockchain identity management
Data governance	Central management	Distributed
Identity evolution	Information update on servers is a method to achieve this	Identity change permitted is possible but more challenging when it's under central control
Security key management	Resetting a password helps recover a lost one	Data lost in case the key is lost
Data storage	Central data server	Computation decentralized
Data management	Users are under threat of identity loss or identity stolen	Users can retain personal data

7. Conclusions and future research

This paper advocates for the system using blockchain technology to support efficient management of remote-sensed data in a decentralized network. Primary Contributions: The paper proposed blockchain-based architecture, supporting algorithms, and criteria-based evaluations to enable a decentralized platform for securing large-scale remotely sensed data, via IPFS

and smart contracts. Synergizing blockchain with IPFS ensures resilience, security, and full decentralization, eliminating the need for trusted third parties. We implemented and used the online test platform of Remix IDE for testing smart contracts. Our experimental implementation demonstrated the system's efficiency, data encryption, improved data provenance, and enhanced security. Our innovations include securing remote sensing data without third-party authentication, a systematic development process, and a prototype platform on the test network of Ethereum using smart contracts.

Potential Dimensions for Future Research: The potential dimensions of future research can be organized into the following two main categories.

- Expansion and applicability of the solution into other application domains such as smart healthcare, financial technology (FinTech), and smart city systems.
- Diverse use cases and case studies systematically investigate the applicability of the proposed solution. In this regard, empirical validations are required that relieve experimentation and use cases to establish guidelines and practical steps to architect, implement, and validate blockchain-based solutions for decentralized data management.

Compliance with ethical standards

Conflict of interest

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

References

Abbas A, Alroobaea R, Krichen M, Rubaiee S, Vimal S, and Almansour FM (2024). Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things. Personal and Ubiquitous Computing, 28(1): 59-72. https://doi.org/10.1007/s00779-021-01583-8

Ahmad A, Khan AA, Waseem M, Fahmideh M, and Mikkonen T (2022). Towards process centered architecting for quantum software systems. In the IEEE International Conference on Quantum Software, IEEE, Barcelona, Spain: 26-31. https://doi.org/10.1109/QSW55613.2022.00019 **PMCid:PMC9250254**

Ahmad A, Malik AW, Alreshidi A, Khan W, and Sajjad M (2023). Adaptive security for self-protection of mobile computing devices. Mobile Networks and Applications, 28(2): 653-672. https://doi.org/10.1007/s11036-019-01355-y

Ahmad A, Waseem M, Liang P, Fahmideh M, Aktar MS, and Mikkonen T (2023). Towards human-bot collaborative software architecting with ChatGPT. In the Proceedings of the 27th International Conference on Evaluation and Assessment in Software Engineering, ACM, Oulu, Finland: 279-285. https://doi.org/10.1145/3593434.3593468

Ahmadisheykhsarmast S, Senji SG, and Sonmez R (2023). Decentralized tendering of construction projects using blockchain-based smart contracts and storage systems. Automation in Construction, 151: 104900. https://doi.org/10.1016/j.autcon.2023.104900

Ahmed WA and MacCarthy BL (2023). Blockchain-enabled supply chain traceability–How wide? How deep? International Journal of Production Economics, 263: 108963. https://doi.org/10.1016/j.ijpe.2023.108963

Alreshidi A (2024). Blockchain-based decentralised management of digital passports of health (DPoH) for vaccination records. International Journal of Advanced Computer Science and Applications, 15(6): 1440-1448. https://doi.org/10.14569/IJACSA.2024.01506144

Daniel F and Guida L (2019). A service oriented perspective on blockchain smart contracts. IEEE Internet Computing, 23(1): 46-53. https://doi.org/10.1109/MIC.2018.2890624

Fahmideh M, Grundy J, Ahmad A, Shen J, Yan J, Mougouei D, Wang P, Ghose A, Gunawardana A, Aickelin U, Abedin B (2022). Engineering blockchain-based software systems: Foundations, survey, and future directions. ACM Computing Surveys, 55(6): 1-44. https://doi.org/10.1145/3530813

Gatcha M, Messelmi F, and Saadi S (2022). An anisotropic diffusion adaptive filter for image denoising and restoration applied on satellite remote sensing images: A case study. Engineering, Technology and Applied Science Research, 12(6): 9715-9719. https://doi.org/10.48084/etasr.5363

Hammad M, Iqbal J, Hussain S, Ullah SS, Uddin M, Malik UA, Abdelhaq M, and Alsaqour R (2023). Blockchain-based decentralized architecture for software version control. Applied Sciences, 13(5): 3066. https://doi.org/10.3390/app13053066

Japitana MV and Burce MEC (2019). A satellite-based remote sensing technique for surface water quality estimation. Engineering, Technology and Applied Science Research, 9(2): 3965-3970. https://doi.org/10.48084/etasr.2664

Ji B, Wang Y, Song K, Li C, Wen H, Menon VG, and Mumtaz S (2021). A survey of computational intelligence for 6G: Key technologies, applications and trends. IEEE Transactions on Industrial Informatics, 17(10): 7145-7154. https://doi.org/10.1109/TII.2021.3052531

Jobarteh B and Neethirajan S (2025). Leveraging satellite data for greenhouse gas mitigation in Canadian poultry farming. Smart Agricultural Technology, 10: 100704. https://doi.org/10.1016/j.atech.2024.100704

Khan A, Ahmad A, Rahman AU, and Alkhalil A (2020). A mobile cloud framework for context-aware and portable recommender system for smart markets. In: Mehmood R, See S, Katib I, and Chlamtac I (Eds.) Smart infrastructure and applications: 283-309. EAI/Springer Innovations in Communication and Computing, Springer, Cham, Switzerland. https://doi.org/10.1007/978-3-030-13705-2_12

Khan AA, Laghari AA, Alroobaea R, Baqasah AM, Alsafyani M, Bacarra R, and Alsayaydeh JAJ (2024). Secure remote sensing data with blockchain distributed ledger technology: A solution for smart cities. IEEE Access, 12: 69383-69396. https://doi.org/10.1109/ACCESS.2024.3401591

Kitchenham B, Brereton OP, Budgen D, Turner M, Bailey J, and Linkman S (2009). Systematic literature reviews in software engineering–a systematic literature review. Information and software technology, 51(1): 7-15. https://doi.org/10.1016/j.infsof.2008.09.009

Ma C, Li J, Wei K, Liu B, Ding M, Yuan L, Han Z, and Poor HV (2023). Trusted AI in multiagent systems: An overview of privacy and security for distributed learning. Proceedings of the IEEE, 111(9): 1097-1132. https://doi.org/10.1109/JPROC.2023.3306773

Muthulakshmi S and Chitra R (2024). Interplanetary file system and blockchain for secured smart grid networks. The Journal of Supercomputing, 80(5): 5900-5922. https://doi.org/10.1007/s11227-023-05680-8

Pu X and Xu F (2025). Low-rank adaption on transformer-based oriented object detector for satellite onboard processing of remote sensing images. IEEE Transactions on Geoscience and Remote Sensing, 63: 1-13. https://doi.org/10.1109/TGRS.2024.3524578

Razzaq A (2022). Blockchain-based secure data transmission for Internet of underwater things. Cluster Computing, 25(6): 4495-4514. https://doi.org/10.1007/s10586-022-03701-4

Razzaq A (2024). A Web3 secure platform for assessments and educational resources based on blockchain. Computer Applications in Engineering Education, 32(1): e22677. https://doi.org/10.1002/cae.22677

Razzaq A, Mohsan SAH, Ghayyur SAK, Alsharif MH, Alkahtani HK, Karim FK, and Mostafa SM (2022). Blockchain-enabled decentralized secure big data of remote sensing. Electronics, 11(19): 3164. https://doi.org/10.3390/electronics11193164

Slimani Y and Hedjam R (2022). A hybrid metaheuristic and deep learning approach for change detection in remote sensing data. Engineering, Technology and Applied Science Research, 12(5): 9351-9356. https://doi.org/10.48084/etasr.5246

Sun J, Zhang Y, Wu Z, Zhu Y, Yin X, Ding Z, Wei Z, Plaza J, and Plaza A (2019). An efficient and scalable framework for processing remotely sensed big data in cloud computing environments. IEEE Transactions on Geoscience and Remote Sensing, 57(7): 4294-4308. https://doi.org/10.1109/TGRS.2018.2890513

Verma P, Srivastava R, and Kumar S (2025). Blockchain technology: Applications and challenges. In: Sridhar V, Rani S, Pareek PK, Bhambri P, and Elngar AA (Eds.), Blockchain for IoT Systems: 1-12. Chapman and Hall/CRC, New York, USA.

Zhao JL, Fan S, and Yan J (2016). Overview of business innovations and research opportunities in blockchain and introduction to the special issue. Financial Innovation, 2: 28. https://doi.org/10.1186/s40854-016-0049-2