International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Blockchain-Based Business Intelligence System Architecture for a Trusted Open Budget Initiative

Harouna Naroua[1], Moussa Habiboulaye*[2], Chaibou Kadri[3]

Submitted:10/08/2025 **Revised**: 28/09/2025 **Accepted**: 12/10/2025

Abstract*:* This paper presents an innovative decision support system architecture that integrates blockchain technology to ensure the authenticity, traceability, and non-repudiation of data in the context of public finance. In contrast to traditional architectures limited to ETL processes, data warehouses, application server, and user interfaces, this approach introduces a blockchain layer to secure datasets. The system generates a cryptographic fingerprint (hash) for each dataset, signs it with a private key, and records the pair (hash, hash_signed) within the blockchain. This design allows users to independently authenticate datasets using the public key, thereby guaranteeing data integrity even in the event of central server failure. The proposed architecture was implemented on Ubuntu 22.04, and the experimental results demonstrate the technical feasibility of this solution for critical decision-making systems requiring high availability and maximum confidence in data.

Keywords: *Decision Support System, Data Warehouse, Blockchain, Cryptography*

1. Introduction

Faced with the significant production of data in the health field, accompanied by the difficulties of managing and exploiting this data, Lopes, Tiago and Santos conducted a study on the implementation of an adaptive decision-making system [1]. To this end, they proposed a new architectural approach, organized into 3 main layers. The first for standardization and data processing, the second and the third for prediction and optimization, thus offering a decision support system regularly updated in accordance with the company context. Figure 1 presents the architecture of the proposed system.

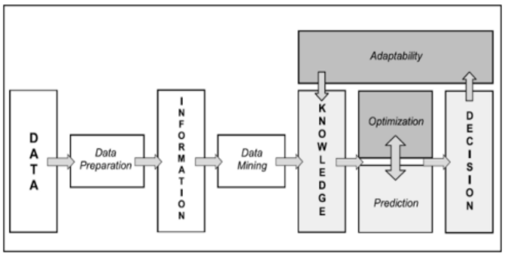


Fig. 1. Adaptive Architecture of a Decision Support System [1].

Common decision support systems, as defined by Rashidi and Behbahani [2] are viewed as:

- the art of leveraging data, they have four components, including a data warehouse, a data transformation layer into information and knowledge, a performance evaluation layer and a user interface as shown in figure 2;
- services, they have three components namely, analytics and reporting services, data management services and integration services where the sources can be relational databases, flat files or other sources as shown in figure 3.

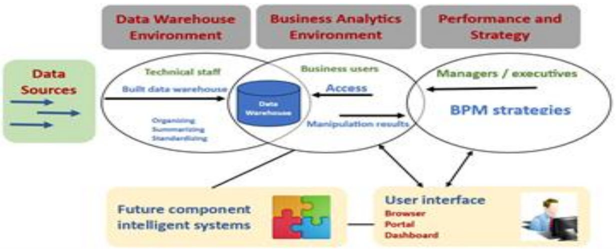


Fig. 2. A High-Level Architecture of Business Intelligence [2].

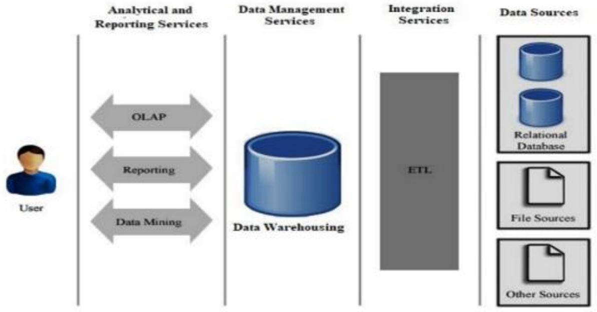


Fig. 3. Business Intelligence Architecture [2].

Rashidi and Behbahani [2] demonstrated that the architectures of

1 Faculty of Sciences and Technology, Abdou Moumouni University, Niger
ORCID ID: https://orcid.org/0000-0003-4512-4971
2 Faculty of Sciences and Technology, Abdou Moumouni University, Niger
3 Faculty of Sciences and Technology, Abdou Moumouni University, Niger
** Corresponding Author Email: musa_habibou@yahoo.com*

decision support systems nowadays, are not able to exploit big data, as a combination of structured and unstructured data. Organizations that use these traditional decision support systems with the types of big data face enormous difficulties. To do this, they proposed a new architecture of decision support system capable of supporting big data. The said architecture, as presented in figure 4, has four layers, the components of traditional decision support systems and coupled big data management tools.

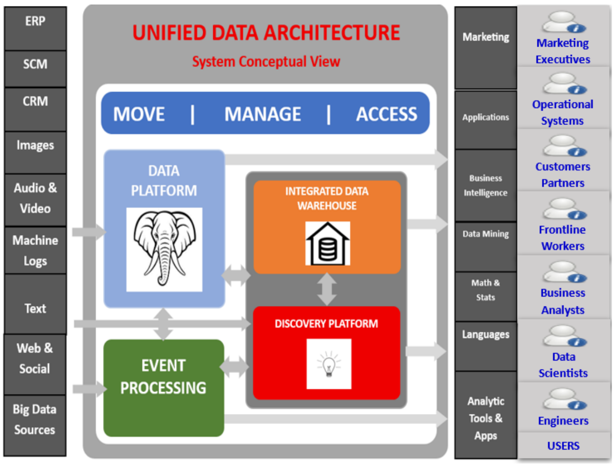


Fig. 4. A High-Level Big Data Architecture [2].

The architecture of Figure 4 is presented in detail in Figures 5 and 6, showing the integration of the big data architecture with the architectural model of traditional decision-making systems.

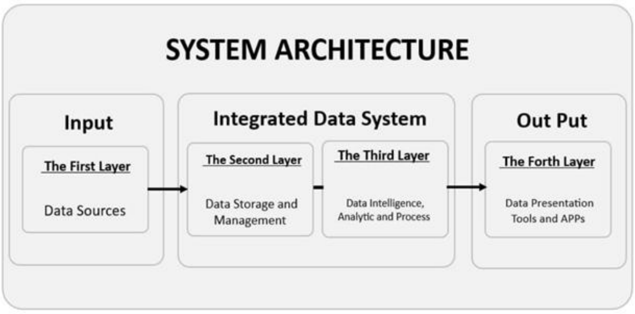


Fig. 5. Four-layered architecture of the proposed architecture with the system approach [2].

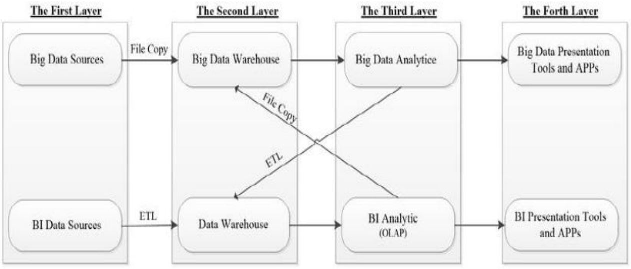


Fig. 6. New four-layer architecture, derived from the integration of Big Data architecture and traditional decision-making system architecture [2].

The possibility of managing large quantities of data in many companies and all kinds of activities, while improving the quality of data processing and the presentation of information, has led to an exploration of decision support systems [3]. During this exploration, the advantages of decision support systems, their roles and the different components that constitute them were recalled, thus proposing an information system architecture integrating a decision support system architecture as shown in figure 7.

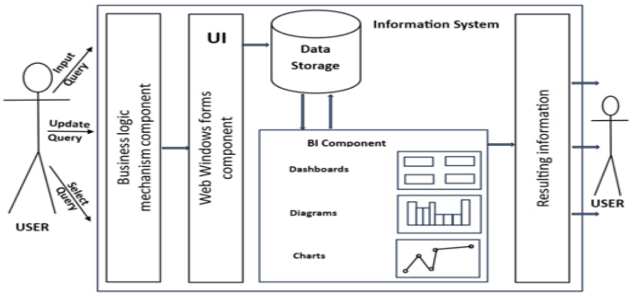


Fig. 7. Architecture of information systems with decision-making system [3].

Researchers like William, Xavier and Sergio have noticed that universities are changing their teaching model, towards a quality style based on the experience of teachers and the learning of students [4]. These factors have led schools to find a solution that would allow them to extract data from different sources and use them to make decisions that improve academic results. To do this, they proposed a roadmap for the implementation of decision-making systems for the analysis of educational data as presented in figure 8.

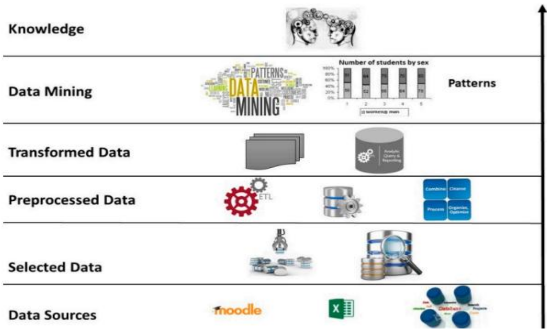


Fig. 8. Steps in implementing a decision support system [4].

Higher education institutions, like all other organizations, aware of the competitive environment in which they operate, need to make appropriate decisions in all their sectors of activities. Aware of this challenge, Boulila et al. (2018) and Sorour et al. (2020a) [5] presented a roadmap for the implementation of decision-making systems in higher education institutions following the architecture of figure 9.

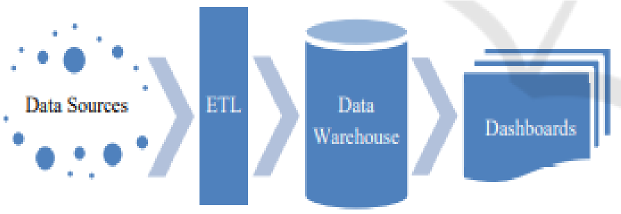


Fig. 9. Business Intelligence Architecture. Adapted from Boulila et al. (2018) and Sorour et al. (2020) [5].

A decision-making system architecture is a framework for organizing data, managing information and the technology used [6].

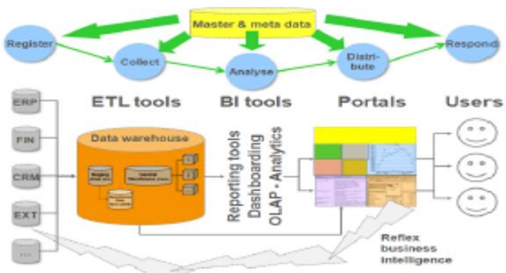


Fig. 10. Typical decision-making system architecture [6].

Djerdjouri conducted a study on the establishment of a roadmap for the implementation of decision support systems, particularly for reporting and data analysis. He pointed out that on decision-making platforms, the tasks performed are generally limited to loading of data into a repository called a data warehouse managed by one or more servers. Data preparation technologies (Extraction, Transformation and Loading) for decision support systems are known as ETL tool (Extract-Transform Load), associated with a set of engines in the form of an application server supporting the analysis and reporting needs as shown in figure 10.

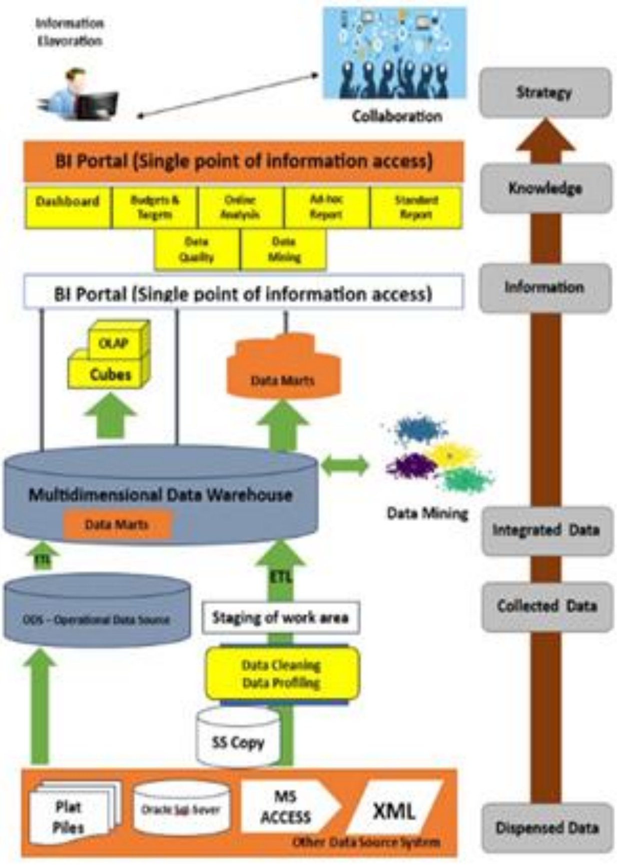


Fig. 11. Decision support system architecture [7].

In the healthcare field, the environment is developing with the inclusion of digital transformation based on traditional information systems, but also with decision support platforms, thus allowing managers and other analysts to produce reports in record time. In this context, Sang [7] presented a set of methods and technologies used in the development of decision-making systems in industry. His presentation is summarized in Figure 11.

Still, given the immeasurable nature of healthcare, implementing a transformative framework in decision-making has been a concern for Srimurali [8]. Thus, he conducted a recent study that resulted in the design of a cloud-based decision support system architecture, demonstrating the limitations of traditional on-premise systems while providing improved scalability, flexibility, and cost-effectiveness. The architecture of the proposed system is presented in figure 12.

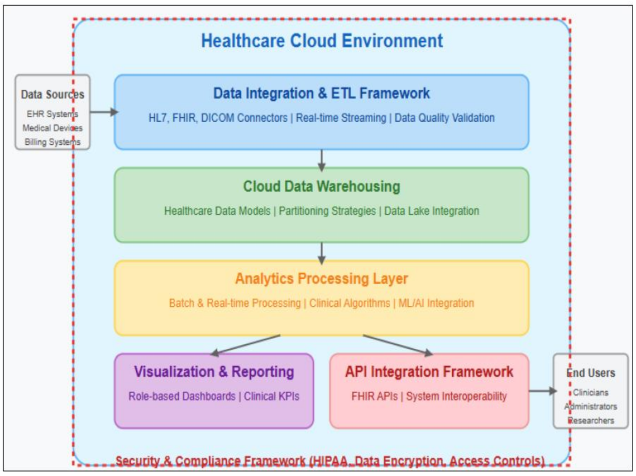

Healthcare Cloud Environment
Data Sources
EHR Systems
Medical Devices
Billing Systems
Data Integration & ETL Framework
HL7, FHIR, DICOM Connectors | Real-time Streaming | Data Quality Validation
Cloud Data Warehousing
Healthcare Data Models | Partitioning Strategies | Data Lake Integration
Analytics Processing Layer
Batch & Real-time Processing | Clinical Algorithms | ML/AI Integration
Visualization & Reporting
Role-based Dashboards | Clinical KPIs
API Integration Framework
FHIR APIs | System Interoperability
End Users
Clinicians
Administrators
Researchers
Security & Compliance Framework (HIPAA, Data Encryption, Access Controls)

Fig. 12. Cloud-based decision support system architecture [8].

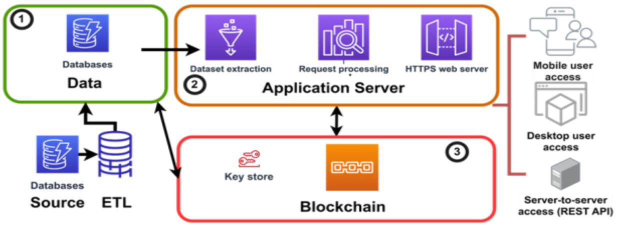
In all the literature we have reviewed, it appears that the research has been limited to the traditional facilities of decision-making systems based on architectures composed of the following layers: the data source, the ETL process, the data warehouse, the application server and the user interface. The architectures as presented in the literature have concerned less the security aspect, the reliability of the data and especially the high availability of the system. The decision-making systems of public finances, in all countries of the world are strategic infrastructures, which require a robust architecture capable of assuring users about the reliability of the data and their availability at all times, hence the need to propose an infrastructure based on the blockchain. A blockchain is a technology for storing and transmitting information at low cost, securely, transparently, and without a central control body. A blockchain refers to a secure, decentralized database space, replicated across a very large number of nodes, and containing a set of transactions. A blockchain can therefore be likened to a transparent and tamper-proof ledger [9]. In the abstract sense of the term, blockchain is a new platform technology for better verifying and recording the exchange of value between a set of interconnected users. It is a secure and transparent way to track asset ownership before, during, and after each transaction. Each transaction between parties in the network is a "block," and the cumulative set of transactions across the entire network constitutes the "chain," hence the blockchain [10]. There are a number of blockchain platforms, the most popular of which are bitcoin, Ethereum, and quorum, which is a blockchain technology based on Ethereum. There are three primary types of blockchains: consortium, public, and private [10],[11]. All three provide databases that synchronize by consensus of participants, but they differ in their degree of centralization and accessibility [11]. They are distinguished by their governance structures between participants and the nature of the blockchain [12]. Consortium blockchains are deployed in a decentralized manner across multiple hardware managed by different owners (or companies). Furthermore, data is not necessarily homogeneous among consortium nodes. The consortium blockchain brings together multiple actors but is not public and open to all. It is a hybrid blockchain in which some nodes can be made public and others private. Participants in the chain have certain rights and decisions are made collectively [13]. Public blockchains are open to any user in terms of reading (free access to the register), use (sending peer-to-peer transactions) and participation in the proper functioning of the network (validation of transactions, each participant can become a miner on a public blockchain). An example is bitcoin or Ethereum [14]. Private blockchains are blockchains where certain rights are reserved for certain users, including the right to validate transactions. In a private blockchain, only one organization can write to the blockchain and can choose who gives access to read its data. A private blockchain has several advantages over traditional databases, without constituting a disruptive innovation like public blockchains [14]. An example is Quorum, which is used in this study.

2. Proposed blockchain-based decision support system architecture

2.1. General presentation of the architecture

The new architectural approach, organized into five (5) main layers, is represented in Figure 13.

Fig. 13. Blockchain-based decision support system architecture.



It is essentially about:

1. Data source (1) and Extract Transform Load (ETL) (2) layers

Data come from primary sources such as relational databases (DBMS) or spreadsheets. The data is then processed through an ETL (Extract Transform Load) layer, which:

- Extracts source data;
- Transforms data according to system needs;
- Loads data into a main database (central collector database, called a data warehouse).

2. Data storage (main database or data warehouse)

- The main database is represented in a green box labeled "Data";
- It centralizes data ready to be used by applications;
- It serves as a repository for the application server.

3. Application Server

This server acts as an interface between users and data. It:

- Receives REST (API) requests;
- Manages user access (mobile, desktop, and server-to-server);
- Serves data from the main database.

4. Generation and recording of the hash (authentication)

Before sending the data:

- The server generates a hash (digital fingerprint) of the dataset.
- This hash is cryptographically signed using a private key of the system, we can call the signature thus obtained "hash_signed";
- The pair (hash, hash_signed) is then recorded in the blockchain layer, ensuring
  - Traceability;
  - Non-repudiation;
  - Authentication of disseminated data.

5. Blockchain Layer

- It records and keeps the pairs (hash, hash signed);
- Other components of the system can query this layer:
  - To write a new pair when issuing a dataset;
  - To read and verify that a dataset is authentic.

6. User Authentication

Two types of authentications are possible:

- Via the application server: the user sends the hash; the server verifies by consulting the blockchain;
- Autonomously: the user retrieves the copy of the blockchain, verifies the pair (hash, hash_signed) and validates with the system's public key.

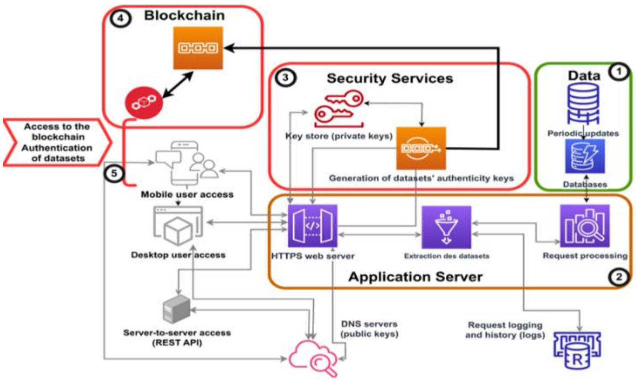
The system thus allows:

- distribution of datasets;
- Proof of authenticity accessible even without direct dependence on the server (due to the blockchain);
- Inter-system mutualization, since several sets of this type can coexist and share the same blockchain layer.

2.2. General presentation of the architecture

Figure 14 shows the technical architecture of the application.

Fig. 14. Technical architecture of the application.



1. Functional block (1) is composed of the system of relational databases which contain the data made available to users. These data are updated periodically from the management system.
2. Functional block (2) is composed of services for processing, extracting and providing the results of queries initiated by users. In addition, the domain name of the web service is authenticated on the Internet's DNS (Domain Name Service) services using a set of asymmetric keys issued by certification authorities.
3. The function of block (3) is to generate a fingerprint (hash) of any dataset served by block (2), to sign this fingerprint using a private cryptographic key (hash_signed) and to register the pair (hash, hash_signed) in the blockchain of block (4).
4. Block (4) has the function of receiving write (3) or read (5) requests from the blockchain.

2.3. Tools and Implementation

The solution was implemented on a Linux Ubuntu (22.04) server using Python (version 3.11) and Go languages. The solution also uses Nodejs and Go quorom, as well as PostgreSQL (version 17) for the database. The ETL processes are based on Pentaho data integration. The implementation consisted of retrieving these sources, extracting and compiling them, the different path configurations in the profile files, cloning, compiling, setting up the blockchain network infrastructure, creating the data warehouse and developing the application.

2.4. Functional analysis of the system

From a functional point of view, the proposed system operates according to the following mechanism:

1. Data processing chain
   - The raw data comes from a DBMS or spreadsheet (OLTP source);
   - An ETL process extracts, transforms and loads this data into a main database (central DB);
   - This database serves as a repository for applications that manipulate or restore this data.
2. Application Server
   - It receives requests from users (mobile, desktop or server-to-server API);
   - It processes requests, interacts with the database, and prepares a response dataset.

     Data security and traceability are ensured by the integration of the blockchain layer, before sending:
     - A unique fingerprint (hash) of the dataset is generated;
     - This hash is then signed by a private key: hash_signed;
     - The pair (hash, hash_signed) is recorded in a decentralized Blockchain layer.

3. User authentication:

Two mechanisms are available:
- Assisted authentication: the user submits the hash to the server. The latter is responsible for searching and verifying its authenticity using the (hash, hash_signed) pair stored in the blockchain.
- Self-authentication :
  - The user retrieves a copy of the blockchain (or a time segment, as needed);
  - The user uses the public key (already broadcasted) to check if hash_signed matches the hash of the dataset.

This check allows you to confirm that the dataset actually comes from the system, without directly consulting the database.

2.5. Advantages of the proposed new architecture

The new architecture has multiple advantages:

1. Cryptographic security of decision-making data

The integration of blockchain into the architecture of decision support systems represents a significant step forward in securing public data. The cryptographic signature mechanism of datasets via the (hash, hash_signed) pair offers robust protection against fraudulent alterations and identity theft attempts. This approach overcomes the limitations of traditional systems by creating an unalterable cryptographic proof of data authenticity, particularly crucial for public finances (health, security, etc.) where trust is paramount. The system's ability to automatically detect fraud attempts, such as in the case of fraudulent registration, significantly strengthens the overall security of the decision-making systems infrastructures.

2. Decentralization and user autonomy

The proposed architecture revolutionizes the interaction between users and decision-making systems by introducing the possibility of autonomous authentication. This feature allows users to verify the authenticity of datasets without relying on the central server, thus creating a system resilient to failures or censorship attempts. Distributing copies of the blockchain to users establishes a distributed verification mechanism that strengthens transparency and trust in the system. This partial decentralization maintains the advantages of a centralized system for data management while providing the security and availability guarantees specific to decentralized systems.

3. Performance and scalability in a big data context

The proposed architecture intelligently addresses the performance challenges inherent to blockchain systems by limiting recording to cryptographic fingerprints only rather than complete datasets. This approach optimizes the use of blockchain while maintaining its security properties, thus enabling the efficient processing of large volumes of data typical of modern decision-making systems. The clear separation between data storage (traditional database) and certification (blockchain) provides an optimal balance between performance and security. This design allows for gradual scaling of the system without compromising response times, a critical aspect for adoption in a production environment.

4. Implications for governance and public transparency

Implementing this architecture in the context of public finance opens new perspectives for government transparency. The non-repudiation property ensures that no authentic data can be denied, thus creating a technical accountability mechanism. This enhanced transparency can promote better governance by allowing governments, managers, citizens, civil society organizations, and oversight institutions to independently verify data authenticity. The system also establishes a permanent and unalterable audit trail, facilitating current and future investigations and controls.

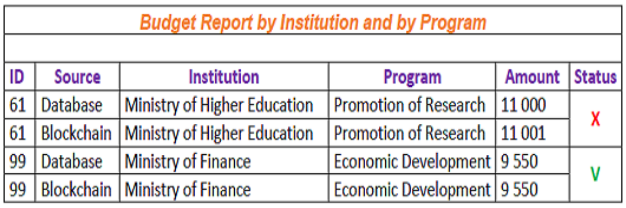
5. Advantages of the proposed system

The blockchain-based decision support system has several distinctive advantages that position it as a cutting-edge solution for critical infrastructure:

- First, the risks of data manipulation are eliminated due to the cryptographic signature mechanism. The authenticity of the datasets is guaranteed, which assures decision-makers of the absolute reliability of the information.
- Second, the operational resilience of the system allows for continued operation of verification procedures even in the event of a central server failure because users can authenticate data autonomously.
- Third, the complete traceability offered by blockchain creates an unalterable history of all data transactions, facilitating audits and compliance monitoring.
- Fourth, the interoperability of the architecture allows for mutualization between several systems sharing the same blockchain layer, optimizing infrastructure costs and the overall extension (scalability) of the system.
- Finally, the technical transparency of the system strengthens stakeholder confidence by providing independent, non-repudiable verification mechanisms, which are fundamental aspects for the acceptability of systems hosting critical information.

3. Results and Discussion

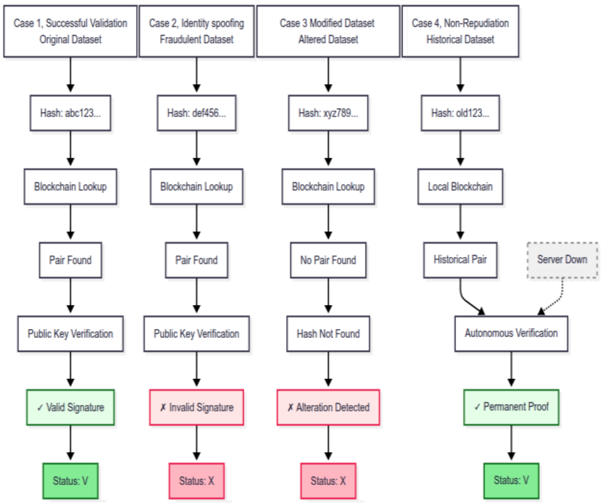
3.1. Results



Budget Report by Institution and by Program					
ID	Source	Institution	Program	Amount	Status
61	Database	Ministry of Higher Education	Promotion of Research	11 000	X
61	Blockchain	Ministry of Higher Education	Promotion of Research	11 001	
99	Database	Ministry of Finance	Economic Development	9 550	V
99	Blockchain	Ministry of Finance	Economic Development	9 550	

Fig. 15. Use Case Analysis and Property Validation.

Fig. 16. Budget report by Institutions and programs.



3.2. Discussion

Technological Innovation

This research introduces a paradigmatic rupture in the architecture of decision support systems by integrating blockchain technology as a cryptographic certification layer for datasets. Unlike traditional approaches that rely on data sources layers, ETL, data warehouse and user interface, the proposed architecture adds a fifth blockchain layer that revolutionizes digital trust management.

The main innovation lies in the hybrid certification mechanism which combines:

- Efficient storage of large data in traditional relational databases;
- Decentralized cryptographic certification via the recording of fingerprints (hash, hash_signed) in the blockchain;
- Self-authentication allows users to verify integrity without relying on the central server.

This approach overcomes the limitations of existing decision-making systems, which suffer from critical vulnerabilities: lack of anti-falsification mechanisms, total dependence on the central server, and the impossibility of proving the authenticity of data in the event of a system failure.

Experimental Validation of Security Properties

The following illustrations present the results obtained using the implementation carried out to prove the concept (proof of concept). Specifically, the aim is to demonstrate that any dataset issued by the system guarantees three fundamental security properties: authenticability, integrity and non-repudiation, and this, autonomously by the user.

Validation Protocol

To validate these properties, a rigorous protocol is followed assuming that the user has:

- a copy of the blockchain containing the pairs (hash, hash_signed)
- the public key of the sending server for cryptographic verifications.

Issuance and Certification Process

During each dataset emission, the system automatically executes:

- Generation of the SHA-256 cryptographic fingerprint of the dataset
- Signing this fingerprint with the server's private key
- Immutable recording of the pair (hash, hash_signed) in the blockchain

This procedure creates an unalterable cryptographic proof of the authenticity of the dataset at the time of its issuance.

Use Case Analysis and Property Validation

Case 1: Successful Authentication (Authentic Dataset), figure 15.

Scenario: Legitimate dataset not altered since its issuance

Validation process:

- The user calculates the SHA-256 hash of the received dataset
- The user looks up this hash in the local copy of the blockchain
- The user extracts the corresponding (hash, hash_signed) pair
- The user uses the public key to verify that hash_signed actually comes from the sending server
- The user compares the calculated hash with the one stored in the blockchain.

Result: Positive authentication (status = 'V'), figure 16.

Demonstrated Property: Authentication, the system cryptographically proves the legitimate origin of the data.

Case 2: Detection of Fraud by Spoofing, figure 15.

Scenario: A malicious entity attempts to pass off fraudulent data as legitimate

Security innovation: The system automatically detects this attempt because:

- The fraudulent entity does not have the private key of the legitimate server
- The generated hash_signed signature cannot be validated by the official public key
- Cryptographic verification consistently fails

Result: Fraud detection (status = 'X'), figure 16.

Demonstrated property: Spoofing Resistance - Protection against impersonation attempts

Case 3: Data Alteration Detection, figure 15.

Scenario: Dataset modified (accidentally or maliciously) after its issuance

Detection mechanism:

- Any modification, no matter how small, radically changes the SHA-256 hash
- The hash of the corrupted dataset does not match any entry in the blockchain
- The lack of correspondence immediately reveals the alteration

Result: Tampering Detection (status = 'X'), Figure 16.

Demonstrated Ownership: Integrity - Guarantee that the data has not been modified

Case 4: Historical non-repudiation, figure 15.

Scenario, major innovation: verification of an old dataset, even if the sending server is no longer available or the dataset has been deleted on the sending server.

- Cryptographic proof remains valid indefinitely in the blockchain

- No dependency on the issuing server for validation
- Impossibility for the issuer to deny having produced the dataset

Result: Permanent validation of authenticity (regardless of the subsequent status of the server that issued the dataset)

Demonstrated Ownership: Non-repudiation - Indisputable and permanent proof of the origin of the data

Competitive Advantages of Architecture

Operational Resilience

Unlike traditional systems, the proposed architecture maintains authentication capabilities even in the event of (i) central server failure, (ii) denial of service attack or (iii) destruction of centralized infrastructure.

Controlled Decentralization

The architecture preserves (i) the performance of relational databases for storage, (ii) the security of the blockchain for certification and (iii) the autonomy of users for verification.

Scalability and Interoperability

The architecture allows (i) sharing of the blockchain layer between several systems, (ii) progressive scaling without performance degradation and (iii) integration with existing infrastructures.

Impact on Digital Governance

This technical innovation opens up new perspectives for:

- Increased transparency due to:
  - o verification of data by all stakeholders
  - o traceability of modifications and emissions
  - o an automated and permanent audit mechanism
- Technological empowerment through:
  - o the impossibility of denying the emission of data (non-repudiation)
  - o detection of attempts to manipulate data
  - o proof of process integrity
- Systemic Trust through:
  - o reducing dependence on institutional trust
  - o validation of authenticity
  - o a distributed consensus mechanism for verification that relies on public-key cryptographic algorithms.

The implementation successfully demonstrates that the proposed architecture is innovative for decision support systems by providing robust cryptographic guarantees while preserving operational performance. This innovation constitutes a change of paradigm towards decision-making systems infrastructures where trust emanates from verifiable cryptographic proofs rather than mere institutional assurances.

The experimental validation confirms that the system effectively meets the critical challenges of security, transparency and resilience that characterize the needs of the 21st century public infrastructure.

4. Conclusion

This article presents a contribution to the evolution of decision support systems by proposing an innovative architecture that addresses the contemporary challenges of security, trust, and transparency in data management. The judicious integration of blockchain technology into a traditional decision-making system architecture demonstrates that it is possible to reconcile operational performance and robust cryptographic guarantees. The proposed approach overcomes the limitations of conventional decision-making systems by introducing automated dataset certification mechanisms. These mechanisms guarantee the authenticity, non-repudiation and traceability of data. The cryptographic signature system coupled with decentralized fingerprint recording establishes a new paradigm of digital trust particularly suited to critical data sharing infrastructures. NodeJS and GoQuorum technologies validates the technical feasibility of this advanced architecture. The results obtained confirm the effectiveness of the system in detecting data alterations, preventing fraud through identity theft and ensuring non-repudiation of the datasets issued. This technical validation paves the way for operational deployment in production environments. Beyond the technical aspects, this study contributes to strengthening digital systems by providing users and control institutions with tools for autonomous authentication of critical data. This independent verification capacity constitutes an innovative accountability mechanism that can transform relationships between stakeholders by strengthening their trust in shared data. There are many potential expansion opportunities for this architecture. The system's native interoperability makes it possible to consider its generalization to other application areas requiring similar guarantees of trust and traceability, such as public health, education, justice, civil status, or security. This contribution is part of a broader approach to modernizing digital infrastructures, where cryptography and distributed technologies are becoming essential tools for system governance in the 21st century. The proposed architecture thus provides a solid foundation for the development of trustworthy, transparent, and resilient information systems.

Acknowledgements

This research was supported by Abdou Moumouni University and the Ministry of Economy and Finance of Niger Republic. We thank our colleagues from Advintech Niger and the Financial Computer Department who provided insight and expertise that greatly assisted the research. Special thanks to M. Khalid Alkassoum, General Director of Advintech for practical assistances with appropriate techniques, methodology and comments that greatly improved the manuscript.

Author contributions

Habiboulaye MOUSSA: Realized the conceptualization of the solution, the experiments and the design of the research plan, organized the study, participated in data collection and data processing, participated in data-analysis and contributed to the writing of the manuscript.

Harouna NAROUA: Coordinated and designed the research methodology, participated in all the experiments, and contributed in the writing of the manuscript.

Chaibou KADRI: Participated in all the experiments and contributed in the writing and reviewing of the manuscript.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] João Lopes, Tiago Guimarães, Manuel Filipe Santos, (2020), "Adaptive Business Intelligence. A New Architectural Approach", International Workshop on Healthcare Open Data, Intelligence and Interoperability

(HODII) November 2-5, 2020, Madeira, Portugal. ScienceDirect, University of Minho, Centro ALGORITMI, Braga, Portugal, Procedia Computer Science 177 (2020) 540-545, pp.542.

[2] H. Rashidi, M. R. Behbahani Nejad, (2023), "A Novel Architecture Based on Business Intelligence Approach to Exploit Big Data", Journal of Electrical and Computer Engineering Innovation, 11(1): 85-102, 2023, pp.89-90. Journal homepage: http://www.jecei.sru.ac.ir. Doi: 10.22061/JECEI.2022.8565.529.

[3] Yalova Kateryna, Muzychka Kyrylo, (2023), "Business intelligence as a part of the information systems architecture", International Scientific Journal «Grail of Science», № 27, DOI: https://doi.org/10.36074/grail-of-science.12.05.2023.046, pp.285-286.

[4] William Villegas-Ch, Xavier Palacios-Pacheco, Sergio Luján-Mora, (2020), "A Business Intelligence Framework for Analyzing Educational Data", p6. www.mdpi.com/journal/sustainability.

[5] Sequeira, N., Reis, A., Branco, F. and Alves, P. (2023), "Roadmap for Implementing Business Intelligence Systems in Higher Education Institutions: Exploratory Work", In Proceedings of the 20th International Conference on Smart Business Technologies (ICSBT 2023), pp.162-169, SBN:978-989-758-667-5, ISSN:2184-772X, DOI:10.5220/0012118000003 552.

[6] Djerdjouri Mohamed "Data and Business Intelligence Systems for Competitive Advantage: prospects, challenges, and real-world applications", Mercados y Negocios, 2020, no. 41, Enero-Junio, ISSN: 1665-7039 2594-0163, Universidad de Guadalajara, México, https://www.redalyc.org/articulo.oa?id=571 861494009, id=571861494009, pp7-8.

[7] Sang Young Lee (2018), "Architecture for Business Intelligence in the Healthcare Sector", 4th International Conference on Advanced Engineering and Technology (4th ICAET), IOP Conference Series Materials Science and Engineering 317(1):012033, pp1-2. DOI:10.1088/1757-899X/317 /1/012033.

[8] Srimurali Krishna Chillara, (2025) "Leveraging cloud-based BI architecture for scalable healthcare analytics: A technical framework for transformation", World Journal of Advanced Engineering Technology and Sciences, 2025, 15(01), pp2291, 2293, DOI: https://doi.org/10.30574/wjaets.2025.15.1.0489.

[9] Mohiuddin Ahmed (2020), "Blockchain in Data Analytics", Academic Centre of Cyber Security Excellence, School of Science, Edith Cowan University, Australia, ISBN (10): 1-5275-4429-X ISBN (13): 978-1-5275-4429-1.

[10] Abby Johnson, (2017), "An Introduction to Blockchain", darden business publishing, UVA-F-1810, pp2-3.

[11] Vrushali Kulkarni Supriya Thakur Aras, "Blockchain and its applications - a detailed survey," International journal of computer Application, vol. 80, no. 3, 2017.

[12] Shadab Alam (2023), " The Current State of Blockchain Consensus Mechanism: Issues and Future Works", International Journal of Advanced Computer Science and Applications, Vol. 14, No. 8, p84.

[13] Omar Dib, Kei-Leo Brousmiche, Antoine Durand, Eric Thea, Elyes Ben Hamida, (2018), " Consortium Blockchains: Overview, Applications and Challenges ", International Journal on Advances in Telecommunications, vol 11 no 1 & 2, p52. http://www.iariajournals.org/telecommunications

[14] Herath H.M.A.D., Ahamed Sabani M.J. & Shafana M.S., (2021), " Identifying Suite Type of Blockchain for Application: Public and Private ", International Conference on Science and Technology, p182, ISBN: 978-624-5736-17-1.