International Journal of Engineering Research and Science & Technology

PROCESS MODELING TECHNIQUES FOR DEVELOPING BLOCKCHAIN APPLICATIONS

ADALA AMARNATH [1], ERLA ROHITH [2], NANDYALA NIKHIL REDDY [3], RAMANCHA MAHENDER [4], POREDDY VIKAS REDDY [5]

[1]Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

[2, 3, 4, 5] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

ABSTRACT— Blockchain technology has the potential to revolutionize e-business by enabling smart contracts. However, the development of blockchain applications is still challenging due to a gap between the analysis and design phases, made worse by the lack of standardized methods for modeling blockchain requirements. This study presents a set of nine data-driven business process modeling patterns that address blockchain-specific concerns such as token management and smart contract security. The patterns were identified through trend analysis of real-world blockchain applications and validated against existing research and a proof-of-concept. Key findings show that transfer patterns are prevalent in marketplace and game applications, lifecycle patterns dominate in games, and accessibility patterns are common across marketplace, finance, IT, and games. The proposed framework offers a standardized way to model blockchain application requirements, improving communication among stakeholders and guiding the development of more effective blockchain solutions.

Index Terms – Blockchain, smart contracts, e-business, business process modeling, blockchain application development, modeling patterns, token management, smart contract security, decentralized applications (DApps), blockchain requirements engineering, process modeling, blockchain frameworks.

I. INTRODUCTION

Blockchain technology has emerged as a transformative solution for secure and decentralized data management by eliminating the need for trusted intermediaries. Through cryptographic

mechanisms and distributed validation, blockchain ensures data integrity, transparency, and controlled access. One of its most important features is the use of smart contracts, which allow predefined rules to be enforced automatically. However, despite these advantages, the development of blockchain-based applications remains challenging, particularly when translating business requirements into secure and verifiable system implementations. In real-world data-sharing environments, multiple stakeholders interact with sensitive data, making access control, data ownership, and trust critical concerns. Traditional centralized systems suffer from issues such as unauthorized modification, lack of transparency, and single points of failure. Blockchain-inspired systems address these issues by introducing immutability, traceability, and rule-based execution. However, effectively modeling and implementing these processes requires a data-driven approach that aligns system behavior with actual operational events. This project presents a data-driven blockchain-based system that integrates business process modeling, cryptographic hashing, and token-based access control. The system is implemented using Java Servlets and JSP pages and is organized into distinct modules: Data Sender, Data Receiver, Smart Contract-based Approval, and Token Generation. Each module reflects a specific phase in the blockchain business process lifecycle, ensuring secure and structured data sharing. The Data Sender module allows authorized users to register, authenticate, and upload data files into the system. During the upload process, the data is processed using the SHA-256 hashing algorithm, generating a unique hash value that represents the file's digital fingerprint. This hash is stored in the database to guarantee data integrity, ensuring that any tampering with the original data can be detected. In addition to hashing, the uploaded data is encrypted before storage, enhancing confidentiality and preventing unauthorized access. Once data is uploaded, access to it is governed by a Smart Contract-inspired approval mechanism. Although implemented using server-side logic, this mechanism follows smart contract principles by enforcing predefined rules automatically. When a Data Receiver requests access to a file, the request is recorded and remains pending until it is approved. This process ensures transparency and accountability, as every request and decision is logged within the system. Upon approval, a secure access token is generated and assigned to the approved request. Token generation is a

critical component of the system, as it provides controlled and traceable access to sensitive data. The token is uniquely linked to a specific file and receiver, preventing unauthorized reuse or access. This approach mirrors token-oriented patterns commonly found in blockchain applications, where access rights are managed through cryptographic tokens rather than direct permissions. The Data Receiver module enables users to view their request status and retrieve the approved token. To download the original data, the receiver must manually provide both the file name and the token. This additional validation step enhances security by ensuring that only authorized users with valid tokens can access the data. The download process verifies the provided details against the database before decrypting and delivering the original file. The use of SHA-256 hashing plays a vital role in maintaining trust and integrity throughout the data lifecycle. Since the hash value is generated and stored at the time of upload, it serves as a reliable reference for verifying that the downloaded data has not been altered. This cryptographic assurance aligns with core blockchain principles such as immutability and tamper resistance. From a business process modelling perspective, the system follows a data-driven process modelling approach, where every significant action—data upload, access request, approval, token issuance, and download—is treated as a process event. These events collectively represent a blockchain-oriented workflow that bridges the gap between requirements analysis and implementation. By structuring the application around these processes, the project demonstrates how blockchain concepts can be practically realized using conventional web technologies. In conclusion, this project successfully integrates data-driven process modeling, cryptographic security, and blockchain-inspired access control mechanisms into a unified web-based system. The modular design ensures secure data sharing, transparency, and integrity while maintaining scalability and usability. By combining SHA-256 hashing, token-based authorization, and smart contract-like logic, the proposed system provides a practical and effective solution for secure data exchange in modern distributed environments.

II. RELATED WORK

A. TrustChain: Trusted Blockchain-Based System for Supply Chain Traceability

With the increasing complexity of global supply chains, ensuring transparency, trust,

and traceability of goods has become a significant challenge. This study presents TrustChain, a blockchain-based system designed to enhance supply chain traceability by securely recording product lifecycle events across multiple stakeholders. The framework leverages blockchain's immutability and decentralization to provide a tamper-resistant ledger that captures manufacturing, transportation, and distribution data. Smart contracts are utilized to automate verification processes and enforce trust among supply chain participants without reliance on centralized authorities. The system improves visibility and accountability by enabling real-time tracking and provenance verification of goods. Experimental results and case-based evaluations demonstrate enhanced data integrity, reduced fraud, and improved stakeholder trust compared to traditional supply chain systems. However, the approach may face scalability and performance challenges as transaction volume increases. Additionally, integration with existing enterprise systems and handling large-scale real-time data remain open issues. Overall, the study demonstrates blockchain's potential to strengthen secure and transparent supply chain management while highlighting the need for optimization for large-scale deployments.

B. ELSO: A Blockchain-Based Technique for a Reliable and Secure Healthcare Information Exchange

With the rapid digitization of healthcare systems, secure and reliable exchange of medical information among healthcare providers has become a major challenge. This study introduces ELSO, a blockchain-based technique designed to ensure trustworthy and secure healthcare information exchange across distributed medical environments. The proposed approach utilizes blockchain's decentralized architecture to provide data integrity, transparency, and tamper resistance while enabling controlled access to sensitive patient records. Smart contracts are employed to manage authentication, authorization, and data-sharing policies among healthcare stakeholders. The system ensures traceability of medical data access and modifications, thereby enhancing accountability and trust among participants. Experimental evaluations demonstrate improved security, reliability, and resistance to unauthorized data manipulation compared to traditional centralized systems. However, the framework may introduce latency and computational overhead due to blockchain operations and consensus mechanisms.

Additionally, scalability and interoperability with existing healthcare information systems remain challenges that require further optimization. Overall, the study highlights blockchain's effectiveness in strengthening secure healthcare data exchange while emphasizing the need for performance enhancements in large-scale medical networks.

C. *A Process-Aware Framework to Support Process Mining from Blockchain Applications*

The growing adoption of blockchain technology in enterprise and inter-organizational systems has generated large volumes of immutable execution data that can be leveraged for process mining. This study proposes a process-aware framework designed to support effective process mining from blockchain-based applications. The framework focuses on extracting, structuring, and interpreting blockchain event logs to enable the discovery, analysis, and conformance checking of business processes recorded on the blockchain. By integrating process-awareness into blockchain systems, the approach facilitates improved visibility into decentralized workflows and enhances understanding of operational behaviors across participants. The framework addresses challenges related to data heterogeneity, event correlation, and transaction ordering inherent in blockchain environments. Experimental evaluations demonstrate that the proposed solution can successfully reconstruct process models from blockchain data with improved accuracy and consistency. However, the approach introduces additional processing overhead and depends on the quality of event data generated by smart contracts. Overall, the study highlights the potential of combining process mining techniques with blockchain technology to support transparent, auditable, and data-driven business process analysis while identifying opportunities for optimization in scalability and performance.

D. *Understanding Blockchain Applications from Architectural and Business Process Perspectives*

As blockchain applications grow in complexity and adoption across multiple domains, there is a need to systematically understand their underlying architectures and embedded business processes. This doctoral research presents a comprehensive investigation of blockchain applications from both architectural and business process perspectives. The study analyzes real-world decentralized applications to identify recurring architectural components, smart contract structures, and business process

patterns implemented on blockchain platforms. It emphasizes the importance of aligning business requirements with blockchain system design to improve clarity, maintainability, and stakeholder communication. The research employs process mining techniques and empirical analysis to extract business processes from blockchain event data, enabling a deeper understanding of decentralized workflows. Findings demonstrate that many blockchain applications implicitly encode complex business processes within smart contracts without explicit documentation. While the framework provides valuable insights and structured analysis methods, it requires substantial domain knowledge and access to detailed blockchain event logs. Overall, the dissertation establishes a strong foundation for process-aware blockchain development and directly supports the need for standardized modelling approaches to bridge the gap between requirements analysis and implementation.

III. PROPOSED METHODOLOGY

The proposed system implements a secure, data-driven blockchain framework that integrates business process modeling with cryptographic data protection and token-based access control. The system is organized into modular components including Data Sender, Token Generation, Smart Contract, and Data Receiver. When a data sender uploads a file, a SHA-256 hash is generated to ensure data integrity, and the hash value is securely stored in the blockchain-supported database. Token generation is used to regulate access to sensitive data, allowing only authorized receivers with valid tokens to download original files. Smart contracts enforce access control and integrity verification by validating tokens and matching hash values before granting access. The system captures blockchain transaction events during upload, verification, and download operations and structures them into process-aware models. This data-driven approach improves transparency and ensures alignment between business requirements and blockchain execution.

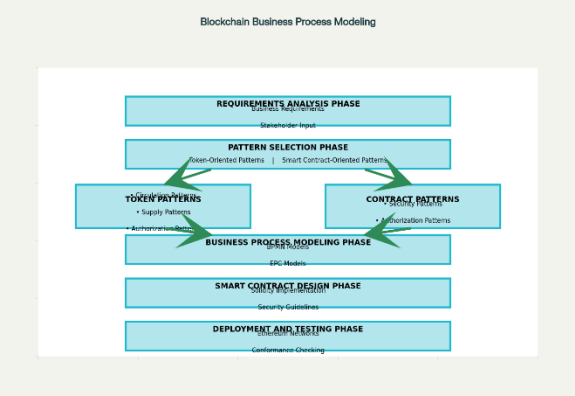
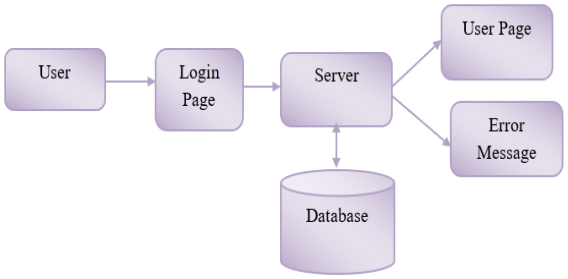


Fig. 1: System Overview

1. User Interface Design

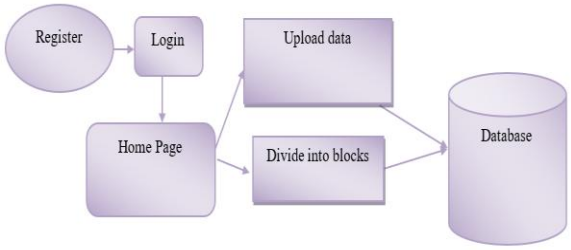
To connect with server user must give their username and password then only they can

able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password, Email id, City and Country into the server. Database will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page. It will search the query and display the query.



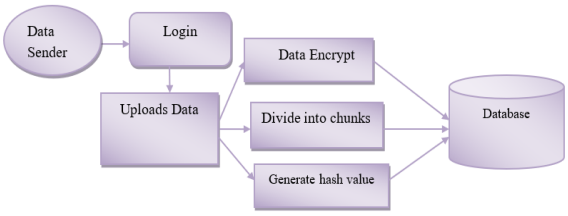
2. Data-Driven Process Modelling

This module is responsible for capturing and modelling the actual execution flow of the block-chain-based data sharing system. Every major action such as user registration, login, data upload, block creation, access request, token approval, and data download is treated as a process event. These events are recorded implicitly through database entries and servlet execution logs, forming an event-driven process trail. By analysing the sequence of these events, the system models real business processes involved in secure data sharing. This approach helps in understanding how data flows across modules and ensures that operations follow the intended workflow. The process logic is implemented directly within the existing servlets and database tables without using external process mining tools, making it lightweight and suitable for academic projects.



3. SHA-256

The SHA-256 module generates a strong cryptographic hash for each divided data block. These hash values are stored in the database to verify data integrity. If any block data is altered, the SHA-256 hash changes immediately, helping in tamper detection. This module works alongside lattice-based hashing to strengthen security. SHA-256 is implemented using Java's built-in Message Digest within the servlet itself. No separate crypto package is used. This ensures a simple yet effective data integrity mechanism.



4. AES Encryption

The AES encryption module secures the original data by converting it into encrypted form before storage. Each uploaded file is encrypted using a secret key, ensuring confidentiality of sensitive information. The encrypted data is stored in the database or block-chain storage, preventing unauthorized access even if data is exposed. During authorized access or download, the data is decrypted using the corresponding AES key. This module works together with SHA-256 hashing to provide both confidentiality and integrity. AES is implemented using Java's built-in cryptographic libraries within the servlet itself. No external encryption framework is used, ensuring efficient and secure data protection.

5. JSP Dashboard

Displays the uploaded encrypted data along with file details and timestamps. It also shows the transaction status, verification results, pending registration details, and overall project modules. The dashboard acts as the user interface for monitoring stored data, status, and user details etc.

6. MySQL Database

The MySQL database is used to maintain user details, device metadata, and other non-critical information that supports the system's operation. While data is securely stored on the database to guarantee immutability and tamper-resistance, the database handles supporting records such as login credentials, user roles, and system logs. This hybrid storage approach ensures both efficient system performance and strong data security by separating critical data from auxiliary information.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

The experimental results show that the proposed data-driven business process modeling framework effectively captures blockchain-specific requirements through nine modeling patterns. Validation using real-world blockchain applications and a proof-of-concept demonstrated improved requirement modeling and stakeholder communication. The analysis also identified transfer patterns as dominant in marketplace applications, lifecycle patterns in gaming applications, and accessibility patterns across multiple domains. Overall, the framework provides a standardized and effective approach for developing blockchain applications.



Fig. 2: Home Page

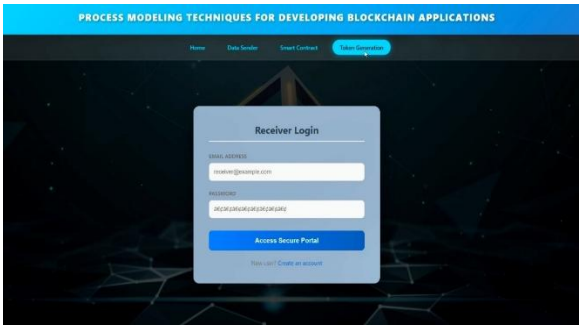


Fig. 3: Receiver Login

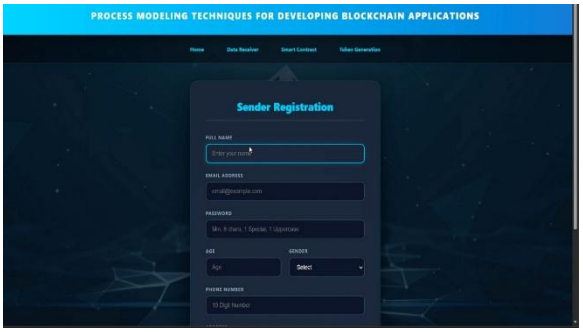


Fig. 4: Sender Registration



Fig. 5: Access Logs

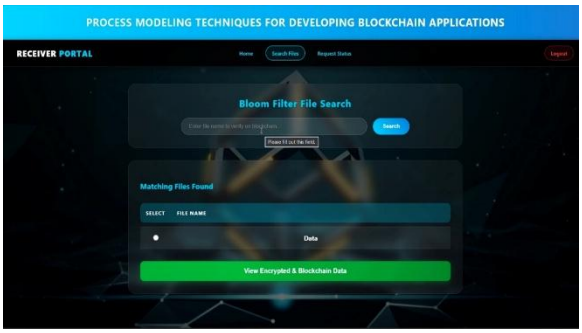


Fig. 6: Search File

V. CONCLUSION

The project Process Modeling Techniques for Developing Blockchain Applications successfully demonstrates how data-driven process modeling can improve the design and implementation of blockchain-based systems. By integrating structured business process modeling with secure blockchain mechanisms, the project bridges the gap between requirement analysis and system development. The use of SHA-256 hashing ensures data integrity, while token-based authentication enables controlled and secure data sharing between data senders and data receivers. The modular architecture consisting of data sender, data receiver, token generation, smart contract logic, and blockchain event logging provides clarity and scalability. Process mining concepts help in understanding real execution flows and validating system behavior. The system enhances transparency, traceability, and trust without exposing sensitive data. It simplifies

stakeholder communication through clear process-oriented design. Experimental implementation using JSP and servlet-based modules validates the practicality of the approach. Overall, the project offers a reliable, secure, and structured framework for developing blockchain applications. It serves as a strong foundation for future enhancements in process-aware and secure blockchain system design.

REFERENCES

[1] A. J. Ramias and R. Rummler, ‘‘The evolution of the effective process framework: A model for redesigning business processes,’’ Perform. Improvement, vol. 48, no. 10, pp. 25–32, Nov. 2009.

[2] M. Morales-Sandoval, J. A. Molina, H. M. Marin-Castro, and J. L. Gonzalez-Compean, ‘‘Blockchain support for execution, monitoring and discovery of inter-organizational business processes,’’ PeerJ Comput. Sci., vol. 7, p. e731, Sep. 2021. [Online]. Available: https://www.ncbi. nlm.nih.gov/pmc/articles/PMC8507485/

[3] C. Di Ciccio, G. Meroni, and P. Plebani, ‘‘On the adoption of blockchain for business process monitoring,’’ Softw. Syst. Model., vol. 21, no. 3, pp. 915–937, Jun. 2022.

[4] J. Merhej, H. Harb, A. Abouaissa, L. Idoumghar, and S. Ouchani, ‘‘ELSO: A blockchain-based technique for a reliable and secure healthcare infor mation exchange,’’ Arabian J. Sci. Eng., vol. 49, no. 9, pp. 12005–12025, Sep. 2024.

[5] M. Mohammed, M. Alzahrani, A. Hejjou, and M. Alharby, ‘‘TrustChain: Trusted blockchain-based system for supply chain traceability,’’ Arabian J. Sci. Eng., vol. 50, no. 2, pp. 891–909, Jan. 2025.

[6] A. Vacca, A. Di Sorbo, C. A. Visaggio, and G. Canfora, ‘‘A systematic literature review of blockchain and smart contract development: Tech niques, tools, and open challenges,’’ J. Syst. Softw., vol. 174, Apr. 2021, Art. no. 110891.

[7] C. Udokwu, H. Anyanka, and A. Norta, ‘‘Evaluation of approaches for designing and developing decentralized applications on blockchain,’’ in Proc. 4th Int. Conf. Algorithms, Comput. Syst., Jan. 2020, pp. 55–62.

[8] P. Chakraborty, R. Shahriyar, A. Iqbal, and A. Bosu, ‘‘Understanding the software development practices of blockchain projects: A survey,’’ in Proc.

12th ACM/IEEE Int. Symp. Empirical Softw. Eng. Meas. New York, NY, USA: Association for Computing Machinery, Oct. 2018, pp. 1–10.

[9] N. Six, N. Herbaut, and C. Salinesi, ‘‘Blockchain software patterns for the design of decentralized applications: A systematic literature review,’’ Blockchain, Res. Appl., vol. 3, no. 2, Jun. 2022, Art. no. 100061.

AUTHORS Profile



Mr. ADALA AMARNATH has received his B.Tech-Computer Science and Engineering from JNTUH, Hyderabad in 2010, M.Tech-CNIS degree in Computer Science and Engineering from JNTUH, Hyderabad in 2013 and Pursuing Ph.D degree in Computer Science and Engineering from ICFAI University Hyderabad. He is dedicated to teaching field from the last 12 years. His research area Quantum Computing and Aptitude Computing. At present he is working as Assistant Professor in CSE Department at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India.



Mr. ERLA ROHITH pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. NANDYALA NIKHIL REDDY pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. RAMANCHA MAHENDER pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. POREDDY VIKAS REDDY pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.