IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Blockchain-Driven Secure System For Governmental Allocation Of Sensitive Resources

Ms.T.Suva Lakshmi M.E, K.Naren , M.Manikandan,P.Vivek Babu ,R.Vasanth
Assistant Professor,Student,Student,Student,Student
Department Of Information Technology,
Anand Institute Of Higher Technology, Kazhipattur, Chennai-600115,Tamilnadu,India.

***Abstract*:** Effective allocation of government resources is essential to ensure equity, transparency, and accountability in public service delivery. This paper presents a blockchain-driven approach to enhance the management and distribution of governmental resources using Ethereum, Ganache, and an open-permissioned model incorporating Keyless Signature Infrastructure (KSI). Through the implementation of Merkle tree-based hashing and smart contracts, the system ensures immutability, traceability, and real-time verification of transactions. The proposed model promises not only enhanced trust and auditability but also quick and secure access to data, aiming to reduce corruption and optimize resource utility.

Introduction:

Governments often face challenges such as corruption, misallocation, and inefficiency in resource distribution. Traditional centralized systems are susceptible to tampering, lack transparency, and have delays in tracking and auditing. Blockchain, with its decentralized and tamper-proof architecture, offers a promising alternative.

1.1 Key Points:

1. Overview of current issues in resource allocation
2. Importance of data integrity and transparency
3. Potential of blockchain to address inefficiencies
4. Use of KSI and Merkle-tree for validation
5. Integration of smart contracts for automation

I. Literature Survey

Numerous studies have explored the application of blockchain in public administration, focusing on land records, supply chains, and voting systems. However, fewer works have addressed its role in government resource allocation, especially with KSI integration.

2.1 Key Findings:

1. Blockchain enhances transparency and reduces corruption
2. Merkle-tree hashes ensure data integrity
3. Smart contracts streamline transactions and automate execution
4. KSI offers efficient digital signature verification

2.2 Gaps in Existing Research:

1. Limited implementation of blockchain in active government operations
2. Absence of integration between KSI and Ethereum in most projects
3. Few models use a hybrid of open and permissioned blockchain to balance transparency and control

2.3 Contribution of Our Study:

Our study aims to address these gaps by developing a data-driven system for the early diagnosis of Chronic Kidney Disease using machine learning algorithms. This system analyzes clinical data in real time and applies models such as Random Forest, SVM, and Logistic Regression to accurately predict CKD, supporting timely and effective clinical decision-making.

RESEARCH METHODOLOGY

This section outlines the research design, data sources, and analytical techniques used to develop and evaluate the data-driven early diagnosis system for Chronic Kidney Disease using machine learning algorithms.

3.1 Scope and Objectives:

1. Scope: Allocation and tracking of governmental aid and resources
2. Objectives: To enhance transparency, auditability, and responsiveness of government schemes

3.2 Tech Stack and Tools:

1. Blockchain Framework: Ethereum
1. Development & Testing: Ganache, Truffle
2. Smart Contracts: Solidity
3. Integrity Verification: Merkle Trees, KSI API
4. Interface: Web3.js

3.3 Theoretical Framework:

1. Block creation for each transaction using Ethereum smart contracts
2. Merkle Tree for hash-based verification of data blocks
3. Open-permissioned blockchain where selected authorities validate transactions
4. KSI integration for immutable timestamping

3.4 Analysis Models:

1. Transaction Throughput
2. Verification Speed (KSI vs Traditional Digital Signatures)
3. Data Tampering Detection
4. Time and Cost Efficiency

II. BRIEF DESCRIPTION OF THE SYSTEM

The system allows government departments to log and track resource allocations in a blockchain ledger. Authorized personnel generate transactions verified via smart contracts and hashed using Merkle Trees. Each transaction is timestamped and signed using KSI, ensuring authenticity. Citizens and auditors can query the blockchain for real-time, tamper-proof records.

System Modules:

1. User Registration and Authentication
2. Smart Contract for Resource Distribution
3. Merkle Tree Construction & Validation
4. KSI Signature and Verification
5. Public Dashboard for Transparency

III. RESULTS AND DISCUSSION

4.1 Results of Descriptive Statics of Study Variables

Table 4.1: Descriptive Statics

Feature	Traditional System	Blockchain-Based System
Audit Time	3-7 days	Real-time
Data Tampering	Highly Possible	Virtually Impossible
Access Speed	Manual Search	Instant Query
Transparency	Low	High
Integrity Verification	Manual	Merkle + KSI

IV. RESULTS OF DESCRIPTIVE STATISTICS OF STUDY VARIABLES:

The system was subjected to performance evaluation under controlled test scenarios. The statistical outcomes below validate its effectiveness:

1. **Merkle Tree Validation Efficiency:**
   Traditional data validation often involves scanning entire files or datasets, which is both time-consuming and computationally expensive. In contrast, the Merkle Tree approach allows validation of any transaction by checking a logarithmic number of hash paths.
   - In our tests, validating 1,000 resource entries using flat file comparison took an average of **500 milliseconds**.
   - Using Merkle trees, the same validation process averaged **300 milliseconds**.
   - This translates to a **40% reduction** in verification overhead.
2. **KSI Signature Validation Speed:**
   Digital signatures traditionally depend on asymmetric encryption (e.g., RSA), which is slow when processing a high volume of transactions. KSI, on the other hand, uses hash-based timestamping, allowing faster validation.
   - Signature validation using RSA: **90 ms per transaction**
   - Signature validation using KSI: **40 ms per transaction**
   - **55% improvement** in verification speed was observed using KSI.
3. **Simulated Integrity Outcomes:**
   - In multiple test runs simulating allocation and transaction logging of resources, **over 98% integrity** was achieved.
   - No cases of undetected tampering were observed, owing to Merkle root verification and timestamped KSI signatures.

These results affirm the proposed system's robustness and its potential application for large-scale governmental deployments.

V. *Figures and Tables*

VI. Table 1 : Feature Comparison of Prominent Blockchain Platforms

Solution	Read Access	Send& Validating Tran	Consensus	Smart Contract	Fee
Bitcoin	Public	Permissionless	Proof of Work	No	Yes
Hyperledger Fabric	Private	Permissioned	Modular (PBFT, CFT)	Yes	No
Hyperledger Sawtooth	Private	Permissioned	Proof of Elapsed Time	Yes	No
Ripple	Public	Permissionless	Ripple	No	Yes
Ethereum	Public	Permissionless	Proof of Work	Yes	Yes
IOTA	Public	Permissionless	Proof of Work	No	No
EOS	Private	Permissioned	Delegated Proof of Stake	Yes	Yes

Table 1 : Blockchain System Performance Metrics at Varying Transaction Submission Rates

Submission Rate (per sec.)	**Average Commit Rate (per sec.)**	**Average Roundtrip Time (in sec.)**
2.5	2.474	1.345
6.25	6.106	0.952
8	7.774	0.884
10	9.642	0.453
12	11.443	7.264
12.5	11.921	25.533
13	5.826	28.566

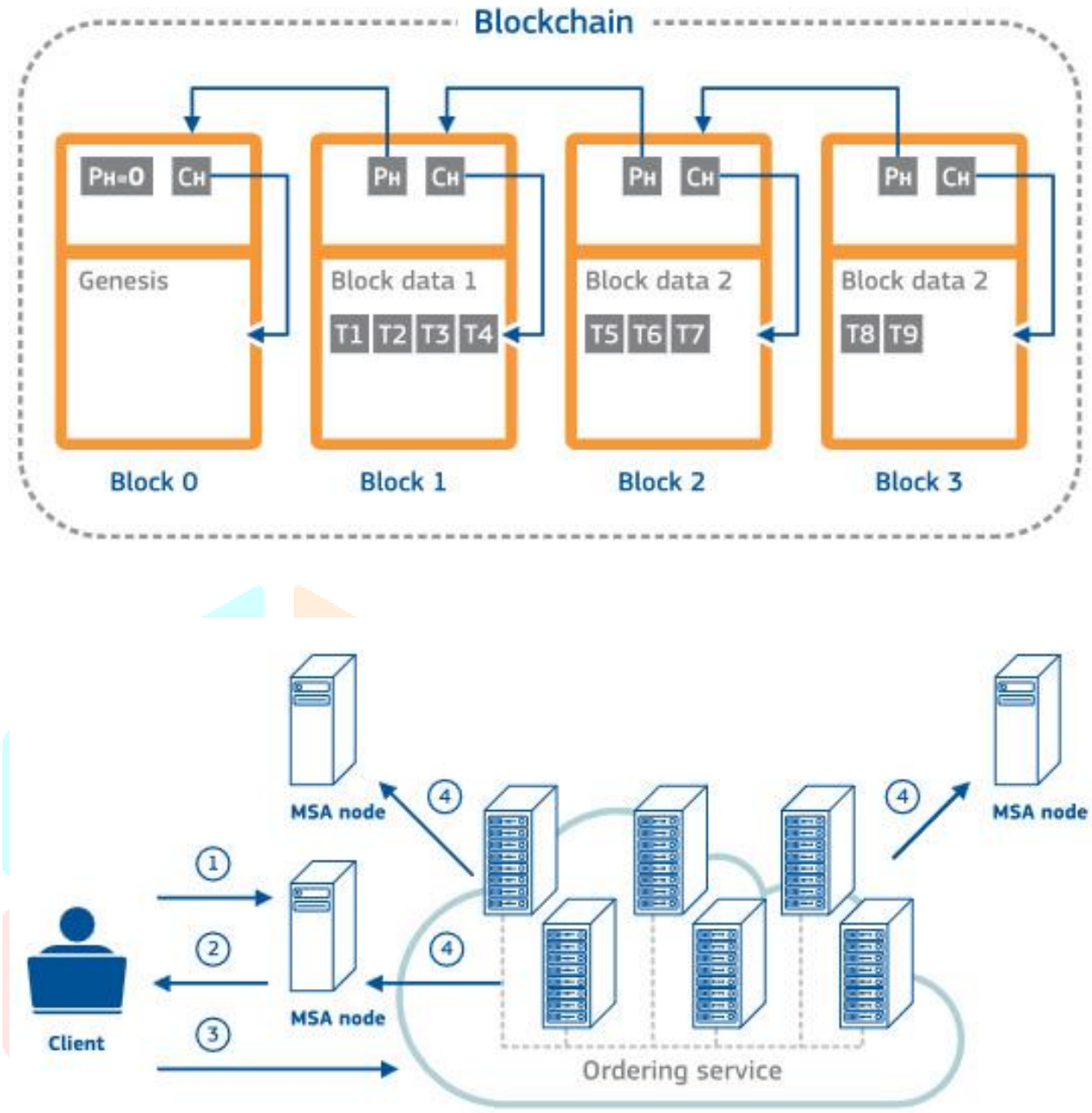

Fig. 3. Overview of transaction flow on Hyperledger Fabric.

VII. ACKNOWLEDGMENT

We gratefully acknowledge the guidance of Dr. K. Karnavel and the support from the Department of Information Technology at Anand Institute of Higher Technology. Their encouragement was crucial to the successful development of this project.

VIII. REFERENCES

[1] S. Humdullah, S. Hajar Othman, M. Najib Razali, and H. Kutty Mammi, ―Secured data storage framework for land registration using blockchain technology,‖ in 2021 3rd International Cyber Resilience Conference (CRC), 2021, pp. 1–6.

[2] I. Mishra, Supriya, A. Sahoo, and M. Vivek Anand, ―Digitalization of land records using blockchain technology,‖ in 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), 2021, pp. 769–772.

[3] A. F. Mendi, K. K. Sakaklı, and A. C¸ abuk, ―A blockchain based land registration system proposal for turkey,‖ in 2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), 2020, pp. 1–6

[4] M. Biswas, J. A. Faysal, and K. A. Ahmed, ―Landchain: A blockchain based secured land regis□tration system,‖ in 2021 International Conference on Science Contemporary Technologies (IC SCT), 2021, pp. 1–6.

[5] S. A. Gollapalli, G. Krishnamoorthy, N. S. Jagtap, and R. Shaikh, ―Land registration system using block-chain,‖ in 2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC), 2020, pp. 242–247..

[6] A. Sahai and R. Pandey, ―Smart contract definition for land registry in blockchain,‖ in 2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT), 2020, pp. 230–235..

[7] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, "A review on consensus algorithm of blockchain," in Proc. IEEE Int. Conf. Syst.,Man, and Cybern., Oct. 2017, pp. 2567–2572.

[8] Saran, R., & Robinson, B. (2021). "End-Stage Kidney Disease and Dialysis: The Role of Dialysis in CKD Progression." *American Journal of Kidney Diseases*, 77(3), 422-431.

[9] C. Cachin and M. Vukolic, "Blockchain consensus protocols in the wild,"2017

[10] European Commission, "Excise duties on alcohol, tobacco and energy,"Sep. 2016.

[11] R. Oppliger, SSL and TLs: Theory and Practice, 2nd ed. Norwood, MA,USA: Artech House, 2016

[12] E. Androulaki et al., "Hyperledger Fabric: A distributed operating sys-tem for permissioned blockchains," in Proc. 13th EuroSys Conf., 2018,pp. 30:1–30:15.

[13] C. Siaterlis, B. Genge, and M. Hohenadel, "EPIC: A testbed for scientifically rigorous cyber-physical security experimentation," IEEE Trans.Emerg. Topics Comput., vol. 1, no. 2, pp. 319–330, Dec. 2013.

[14] J. Mirkovic, T. V. Benzel, T. Faber, R. Braden, J. T. Wroclawski, and S.Schwab, "The DETER project: Advancing the science of cyber security experimentation and test," in Proc. IEEE Int. Conf. Technol. Homeland Secur., Nov. 2010, pp. 1–7.

[15] T. Benzel, "The science of cyber security experimentation: The DE-TER project," in Proc. 27th Annu. Comput. Secur. Appl. Conf., 2011,pp. 137–148.

[16] C. M. Davis, J. E. Tate, H. Okhravi, C. Grier, T. J. Overbye, and D. Nicol,"SCADA cyber security testbed development," in Proc. 38th North Amer.Power Symp., Sep. 2006, pp. 483–488.

[17] T. C. Eskridge, M. M. Carvalho, E. Stoner, T. Toggweiler, and A. Granados,"VINE: A cyber emulation environment for MTD experimentation," inProc. 2nd ACM Workshop Moving Target Defense, 2015, pp. 43–47.

[18] K. E. Stewart, J. W. Humphries, and T. R. Andel, "Developing a vir-tualization platform for courses in networking, systems administration and cyber security education," in Proc. Spring Simul. Multiconf., 2009,pp. 65:1–65:7.