| Volume 02 | Issue 06 | November 2026 | ISSN: 3139-1737

International Journal of Advances and Applications in Convergent Studies & Transdisciplinary (IJ-AACST)

Bridging Disciplines, Bridging Knowledge

Aligned with the Vision of NEP 2020 and UGC Guidelines

Website: https://aacstij.org || Email: journaleditor@aacstij.org

A Blockchain-Based Framework for Secure Digital Record Management: BirthChain and Soulbound Token Authentication

DOI: https://doi.org/ 10.5281/zenodo.24104261

Miss. Sheetal R. Billore[1]*, Dr. Keshao D. Kalaskar[2]

*Corresponding Author: [1] Research Scholar, Sardar Patel Mahavidyalaya, Chandrapur, Maharashtra, India
sheetalbillore123@gmail.com

[2] Professor, Dr. Ambedkar College of Arts, Commerce and Science, Chandrapur, Maharashtra, India
keshao_kalaskar@yahoo.co.in

ABSTRACT

Digital birth registration and medical-document verification require records that are authentic, traceable, and accessible only to authorized parties. Paper-based procedures and isolated databases can delay verification and complicate information exchange across institutions. This paper presents a blockchain-based framework comprising two complementary applications: BirthChain, a smart-contract-enabled workflow for birth registration and certificate management, and a Soulbound Token (SBT)-based mechanism for medical-document authentication. BirthChain coordinates an administrator, authorized hospitals, and municipal authorities through participant registration, newborn-record submission, municipal approval, and certificate issuance. The medical-document mechanism associates a document reference and SHA-256 hash with patient-related identifiers and a non-transferable credential. Verification compares the submitted document and associated identifiers with the corresponding blockchain record; a match results in a verified status, whereas a mismatch or missing credential results in an unverified status. The framework is implementation-oriented and illustrates how blockchain can support auditability and integrity checking. However, comprehensive quantitative benchmarks and large-scale field deployment evidence are not available. Therefore, the paper does not claim measured improvements in processing time, fraud reduction, or cost. Privacy protection, secure key management, interoperability, legal compliance, and operational validation remain essential before deployment.

KEYWORDS: Blockchain, BirthChain, smart contracts, digital birth certificates, Soulbound Tokens, medical-document authentication, SHA-256, digital identity.

1. INTRODUCTION

Digital records are increasingly used in public administration and healthcare. However, information is often distributed across hospitals, municipal offices, clinics, and other organizations. In birth registration, information submitted by a healthcare institution must be reviewed by the responsible authority before a certificate is issued. In medical-document workflows, a recipient needs to determine whether a document corresponds to a previously registered record and whether its contents have been altered.

© 2026 The Author(s). This article is published by the AACST in the IJ-AACST under the Creative Commons Attribution 4.0 International (CC BY 4.0) License. The authors retain copyright and grant AACST a non-exclusive license to publish, distribute, and archive the work.

Blockchain technology can maintain a shared transaction history and provide an auditable record of actions performed by authorized participants. Smart contracts can encode workflow rules, including participant registration, record submission, approval, and certificate issuance. Cryptographic hash functions support integrity checking by enabling a comparison between the digest of a submitted file and a previously registered digest. Soulbound Tokens (SBTs) are non-transferable digital credentials that can represent an association between an identity and an issued credential.

This paper brings together two related but distinct applications of blockchain-enabled record management. BirthChain addresses an administrative workflow for birth registration and digital certificate management, while the SBT-based mechanism supports the integrity verification of medical documents. The proposed approach uses blockchain as an audit and verification layer alongside off-chain document storage, rather than as a replacement for all existing information systems.

2. OBJECTIVES AND RESEARCH QUESTIONS

The objectives of this study are to present the architecture and workflow of BirthChain, explain the SBT-based medical-document verification process, and identify the technical, privacy, and governance requirements that influence responsible deployment.

- How can authorized hospitals and municipal authorities coordinate birth-registration activities through smart contracts?
- How can the integrity and credential association of a medical document be checked against a blockchain record?
- What security, privacy, interoperability, and operational limitations must be addressed before these applications can be used in practice?

3. RELATED WORK

Research on blockchain-based healthcare systems has explored secure storage, controlled access, record sharing, and auditability. Sun et al. [1] proposed a blockchain-based secure storage and access scheme for electronic medical records using the InterPlanetary File System (IPFS). Tanwar et al. [2] examined blockchain-enabled electronic healthcare records for Healthcare 4.0, while Xia et al. [3] presented a permissioned blockchain approach to sharing electronic medical records in cloud environments. These studies demonstrate the relevance of distributed verification and controlled data exchange, while also showing that secure storage, identity management, and access control remain necessary.

Blockchain has also been investigated for civil registration and birth-certificate management. A birth-notification verification model based on blockchain and smart contracts was examined for urban digitization governance [4]. More recently, a blockchain-based approach to birth-certificate delivery, traceability, and authentication was reported [5]. These works establish the relevance of tamper-evident records in civil registration processes.

For medical-document authentication, recent studies have specifically considered Soulbound Tokens. Singh et al. [6] presented blockchain-enabled medical-record verification using SBTs and cloud computing. Boi et al. [7] discussed SBTs as a privacy-aware and decentralized authentication mechanism for medical-data storage. Related research emphasizes that blockchain-based healthcare solutions must address privacy, authorization, and

the maturity gap between prototypes and operational systems. The present framework combines an administrative birth-registration workflow with an SBT-supported medical-document integrity workflow.

Blockchain immutability can help preserve an audit trail and make subsequent changes detectable, but it cannot independently establish that information entered initially is accurate. Data validation, trusted institutional processes, and accountability are therefore required in both applications.

4. PROPOSED FRAMEWORK

4.1 BirthChain Architecture

BirthChain consists of three principal participant categories: an administrator, authorized hospitals, and municipal authorities. The administrator manages participant registration. Hospitals submit newborn and related registration information, and the appropriate municipal authority reviews the submission. Following approval, the workflow authorizes birth-certificate generation and electronic delivery to parents or legal guardians.

The system configuration considered in the implementation comprises eight hospitals, three municipal offices, and a central administrative entity. This represents the configured architecture used for the implementation and should not be interpreted as evidence of a district-wide operational deployment. The implementation uses Solidity smart contracts in an Ethereum development environment, with interaction through MetaMask and testing on an Ethereum test network.

The principal write functions are setHospital(), setMunicipality(), newBirth(), and approveBC(). These functions support participant registration, birth-record submission, and approval of certificate issuance. The read functions include hospital(), municipality(), birthCertificate(), and BCDetails(), which retrieve registered information without changing blockchain state.

4.2 BirthChain Workflow

- Initialization: The administrator deploys the smart contract and configures the application environment.
- Participant registration: The administrator registers hospitals and municipal authorities and assigns unique identifiers.
- Birth submission: An authorized hospital submits newborn information through newBirth(), creating a registration request and a certificate-related identifier.
- Municipal review: An authorized municipal official examines the submitted information and records the approval decision through approveBC().
- Certificate issuance: After approval, the workflow authorizes certificate generation and digital delivery. The related transaction activity is retained to support traceability and auditing.

4.3 SBT-Based Medical-Document Authentication

The medical-document authentication mechanism associates a document with a cryptographic hash, a document reference, patient-related identification information, and a non-transferable SBT credential. The document is processed using the SHA-256 hash function. During verification, the hash of the submitted document and its associated information are compared with the corresponding blockchain record. If the expected credential

is present and the hash and identifiers match, the document is assigned a verified status. A mismatch or missing credential results in an unverified status.

The medical file itself need not be stored directly on-chain. The design uses document references and off-chain storage concepts, including IPFS-style references, while recording hashes and credential metadata on the blockchain. This separation can limit direct exposure of sensitive files on a shared ledger. Nevertheless, off-chain storage requires availability and access controls, and the use of a hash does not provide confidentiality. Encryption, authorization, retention policies, and secure identity binding remain necessary.

5. METHODOLOGY AND EVALUATION APPROACH

This study follows a design- and implementation-oriented approach. It describes the architecture, smart-contract functions, participant roles, and transaction workflows of BirthChain, together with the credential issuance and verification process of the SBT-based medical-document mechanism. BirthChain is implemented using Solidity and tested with Ethereum development tools and a test network. The SBT application is presented through its credential association and document-verification workflow.

The available implementation information supports a functional description of the applications; it does not establish a comprehensive comparative benchmark. In particular, a common quantitative evaluation covering transaction throughput, confirmation latency, gas cost, failed-verification rates, user acceptance, and real-world deployment is not available. Accordingly, no numerical performance improvement or fraud-reduction rate is claimed.

A rigorous future evaluation should measure: (i) transaction confirmation latency at each workflow stage; (ii) gas or transaction cost for participant registration, record submission, approval, and verification; (iii) successful and failed verification rates for valid, altered, missing, and mismatched documents; (iv) behaviour under concurrent submissions; and (v) recovery following node, storage, or credential failure. A field pilot should additionally assess usability, administrative workload, accessibility, interoperability, and legal compliance.

6. FINDINGS AND DESIGN IMPLICATIONS

The BirthChain workflow provides a structured sequence from hospital submission to municipal approval and certificate issuance. Recording these actions on a blockchain can support traceability by allowing authorized participants to inspect the sequence of recorded transactions. Smart contracts can encode role-specific permissions for performing particular operations. These features support auditability, but the workflow remains dependent on accurate data entry, reliable identity management, and an appropriate administrative governance model.

The SBT mechanism provides an integrity check by comparing the current SHA-256 digest of a medical document with the digest recorded previously. A matching digest supports the conclusion that the compared file content is consistent with the registered version. It does not independently establish that the clinical information is medically correct, that the issuer's identity was properly validated, or that the document has remained confidential. These requirements need separate controls and validation.

Both applications use blockchain as a verification and audit layer rather than as a complete replacement for existing databases. A privacy-conscious architecture should place only the minimum necessary metadata on-chain and retain sensitive files in access-controlled storage. Storing personal or medical information directly on an immutable ledger may complicate correction, deletion, and compliance obligations. These design considerations are consistent with wider findings on privacy-preserving blockchain-based healthcare data sharing [6], [7].

7. SECURITY, PRIVACY, AND OPERATIONAL CONSIDERATIONS

- Identity binding: Hospital accounts, municipal officials, patients, and credential issuers must be authenticated reliably.
- Role-based permissions: Registration, submission, approval, credential issuance, and verification should be restricted to authorized roles.
- Key lifecycle management: Key generation, secure storage, rotation, recovery, and revocation procedures must be defined.
- Privacy: Full medical documents and unnecessary personally identifiable information should not be placed on-chain.
- Data correctness: Information must be validated at the point of entry; immutability preserves recorded data but does not make incorrect input accurate.
- Off-chain availability: Document references and IPFS-style storage require persistence, access control, backup, and recovery plans.
- Interoperability: Interfaces and data formats should be defined for existing hospital information systems, municipal databases, and certificate services.
- Governance and compliance: Responsibility for errors, disputes, consent, retention, and applicable legal requirements must be established before deployment.

Scalability, interoperability, privacy, key management, regulatory compliance, and operational deployment are central conditions for evaluating the suitability of the proposed applications. They should be treated as core design requirements rather than as secondary implementation details.

8. LIMITATIONS AND FUTURE WORK

The evidence presented is primarily implementation- and prototype-oriented. A broad operational deployment or controlled field study has not been established for the two applications. The available information does not provide sufficient quantitative data to claim a measured reduction in processing time, a specific fraud-prevention rate, or a defined cost saving. Such outcomes require systematic evaluation.

Future work should test the smart contracts under larger and more varied workloads, conduct independent security audits and attack simulations, and evaluate document verification using altered and mismatched files.

Further studies should assess key loss, credential revocation, storage failure, and recovery procedures. Integration testing should examine interoperability with existing record systems. Privacy assessment should include metadata leakage and the implications of linking patient identifiers with immutable credentials. Finally, pilot studies involving authorized institutions and intended users are needed to evaluate usability and administrative feasibility.

9. CONCLUSION

This paper presents a blockchain-based framework for two digital-record applications: BirthChain for birth registration and certificate management, and an SBT-based mechanism for medical-document integrity verification. BirthChain uses smart contracts to coordinate hospital-submitted birth records, municipal validation, and certificate issuance. The medical-document mechanism associates documents with SHA-256 hashes and non-transferable credentials to support verification against a registered blockchain record.

The framework illustrates how blockchain can provide an auditable transaction history and structured verification workflows. These capabilities do not eliminate the need for accurate input data, privacy-preserving storage, secure identity and key management, interoperability, and institutional governance. Since comprehensive performance measurements and real-world deployment evidence are not available, claims about efficiency, cost reduction, or fraud prevention should be made only after further experiments and field validation.

10. REFERENCES

[1] J. Sun, X. Yao, S. Wang, and Y. Wu, “Blockchain-based secure storage and access scheme for electronic medical records in IPFS,” IEEE Access, vol. 8, pp. 59389–59401, 2020, doi: 10.1109/ACCESS.2020.2982964.

[2] S. Tanwar, K. Parekh, and R. Evans, “Blockchain-based electronic healthcare record system for healthcare 4.0 applications,” Journal of Information Security and Applications, vol. 50, Art. no. 102407, 2020, doi: 10.1016/j.jisa.2019.102407.

[3] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, “BBDS: Blockchain-based data sharing for electronic medical records in cloud environments,” Information, vol. 8, no. 2, Art. no. 44, 2017, doi: 10.3390/info8020044.

[4] “A novel block chain method for urban digitization governance in birth registration field: A case study,” International Journal of Environmental Research and Public Health, vol. 19, no. 15, Art. no. 9309, 2022, doi: 10.3390/ijerph19159309.

[5] T. T. M. Eddy, B. B. Georges, N. E. P. Salomon, and E. M. V. Boniface, “Birth certificates delivery, traceability and authentication using blockchain technology,” International Journal of Advanced Computer Science and Applications, vol. 15, no. 9, 2024, doi: 10.14569/IJACSA.2024.0150957.

[6] P. Singh et al., “Blockchain-enabled verification of medical records using soul-bound tokens and cloud computing,” Scientific Reports, vol. 14, Art. no. 24830, 2024, doi: 10.1038/s41598-024-75708-3.

[7] B. Boi, F. Cirillo, M. De Santis, and C. Esposito, “Soulbound tokens: Enabler for privacy-aware and decentralized authentication mechanism in medical data storage,” Blockchain in Healthcare Today, vol. 7, 2024, doi: 10.30953/bhty.v7.334.