Minimax Theory and its Applications

Volume 11 (2026), No. 5s, 105-122

Design and Evaluation of a Blockchain-Based Framework for Secure and Transparent Pharmacovigilance in TB Vaccine Clinical Trials

Arunendra Mani Tripathi[1], Kavita Saini[2*], Ramakrishna Basude[3], Nalini Manogaran[4], Koteeswaran Seerangan[5]

[1] School of Computing Science and Engineering, Galgotias University, Greater Noida, Uttar Pradesh, India.
[2] School of Computing Science and Engineering, Galgotias University, Delhi NCR, India.
[3]Department of CSE (Data Science)CVR College of Engineering, Rangareddy, Telangana, India.
[4]Department of CSE (Cyber Security), S.A. Engineering College (Autonomous), Chennai – 600077, Tamil Nadu, India.
[5]Department of Computer Science and Engineering, R.M.K. Engineering College (Autonomous), Kavaraipettai - 601206, Tamil Nadu, India.
Email: arunendramanitripathi@gmail.com, kavitasaini_2000@yahoo.com,ramakrishnabasude@gmail.com, drnalini@saec.ac.in, skn.cse@rmkec.ac.in

Abstract
The challenges of secure reporting, traceability and monitoring of clinical trial data to ensure the safety of TB vaccines are significant. Traditional centralized pharmacovigilance solutions are still susceptible to various issues such as unauthorised access, manipulation of data, delayed reporting and incomplete audit trails. The present study introduces a framework for TB vaccine clinical trials, based on blockchain technology, for pharmacovigilance. It leverages the FDA/CDC VAERS-Annotations dataset (1,000 AE reports) to prepare records and to conduct workflow analysis. These pre-processing steps involve duplicate identification, missing value assessment, standardization of records and clinical-temporal association validation. Record integrity is verified with the help of hashing with SHA-256, and pseudonymous references, hashes, and transaction metadata are managed by a permissioned Hyperledger Fabric network. Protected off-chain storage is used to store sensitive clinical information. Smart contracts enforce role-based authorization, duplicate detection, integrity verification, and controlled status updates. Other tools used for adverse-event analysis and system-reliability assessment include probabilistic and statistical modelling. Poisson modelling describes the counts of annotations of adverse events, and dispersion assessment is used to consider a negative binomial model. The confidence intervals estimate proportions and integrity-verification rates, and reporting odds ratios helps with the evaluation of safety signals. Binomial modelling can be used to assess verification results, and welch's t-test can be used for comparing the latency of transactions processed by the blockchain system and the centralized system. It enables the stakeholders to report in an accountable manner. Evaluation takes into account factors such as transaction latency, throughput, security, storage efficiency, and reliability of workflow. The tests recorded and blocked unauthorized calls, with a 100% detection and rejection rate. The hashing of the data (SHA-256) added 18 ms of processing overhead per record, and on-chain hashes and metadata slashed ledger storage by about 90- 94%. Sustained workloads did not affect transaction completion rates, which stayed above 95%. The latency of blockchain, however, was around 2.7–3.3 times greater than the baseline in the centralized system, while the throughput became saturated with increased workload. The accuracy, precision, recall and F1-score of the reported evaluation were 98.1%, 97.8%, 98.4% and 98.1%, respectively. The results obtained here suggest that such tamper-proof, audit-trail, privacy-preserving reporting of adverse events is technically feasible, but needs to be clinically validated in real-life clinical scenarios.

Keywords: Blockchain, Pharmacovigilance, Tuberculosis Vaccine, Hyperledger Fabric, Smart Contracts.

1. Introduction

Prevention is an important part of TB control, and clinical trials are key to assessing new TB vaccines to ensure they are both safe and effective.[1]. In this process, pharmacovigilance assists in the continuous gathering, monitoring and evaluation of adverse events after vaccination during these trials. But clinical trial safety data can reside in multiple systems or spreadsheets and can be hard to keep up to date, difficult to audit for quality, and challenging to monitor for data quality or change throughout the reporting process.[2], [3]. Also, centralized systems for managing records can pose problems if they are prone to unauthorized access (e.g., theft), lack transparency, or have incomplete audit trails. The limitations underscore the need for a safe and traceable system to enable reliable reporting of adverse events and enhance accountability in TB vaccine clinical trials.[4], [5].

Blockchain technology provides a viable solution with tamper-evident records, cryptographic verification, controlled access, and a transaction history that is traceable.[6]. The study proposes a framework for secure and transparent pharmacovigilance in TB vaccine clinical trials using Blockchain technology, which can be designed and evaluated. The architecture features a permissioned blockchain, smart contracts, cryptographic hashing, role-based access control and protected off-chain storage to enable adverse-event record registration, access authorization, integrity verification, and audit logging.[7]. It is judged by metrics such as transaction latency, throughput, record-integrity verification, rejection of unauthorized requests and reduction in on-chain storage space, compared to a centralized record-management system. The publicly available vaccine adverse-event annotation data support the data-processing and validation workflow, and TB clinical-trial scenarios are simulated where needed.[8]. The proposed approach is to enhance the integrity, traceability and controlled sharing of these data while retaining the use of clinical judgment and regulatory assessment.[9].

1.1 Problem Statement

Centralized databases and manual reporting systems are crucial in TB vaccine clinical trials, but they can be subject to manipulation, misreporting of adverse events, and poor traceability, compromising the safety of participants and the trust of regulators.[10], [11]. Multiple parties, such as sponsors, investigators, regulators and ethics committees, do not share a single, trusted safety picture, leading to differences and inefficiencies.[12]. A secure, tamper-resistant, and transparent system is required to maintain participant anonymity and provide safe reporting across the trial in a reliable, auditable and timely fashion.[13].

1.2 Research Motivation

Data integrity is essential for the ethical and scientific validity of TB vaccine trials that include vulnerable participants, extended follow-up periods, multiple trial sites, and robust regulatory review. Reported delayed and/or altered safety records have undermined public confidence in clinical research. The immutability, decentralisation and smart-contract automation of blockchain provide a promising solution. This encouraged the investigation into a blockchain-based system to improve accountability, quicker adverse event reporting, and enhanced confidence for all stakeholders in a trial, regulators and the public.

1.3 Research Significance

The research enhances participant protection by facilitating timely reporting of adverse events and fostering transparency in data sharing between stakeholders, all without the risk of tampering. It helps with regulatory compliance and auditability, decreases reliance on trusted intermediaries, ensures participant privacy, and enhances trust in the results of trials. The results can inform the implementation of blockchain in the field of pharmacovigilance and can be applied to other vaccine and drug trials, which can speed up the safe development of TB vaccines. It also adds to the expanding body of literature on using DLT in health and clinical research.

1.4 Key Contributions

- Proposed a secure and transparent pharmacovigilance system using blockchain in TB vaccine clinical trials. It tackles the issues of tampering, delayed reporting, traceability and lack of stakeholder confidence in the central adverse-event reporting process.
- Developed a permissioned Hyperledger Fabric architecture with stakeholder, application, blockchain and off-chain storage layers. It splits up the sensitive clinical information from the on-chain metadata and has role-based access for every stakeholder.
- Designed a secure record preparation and verification process, using SHA-256 hashing. It connects each record to its pseudo-anonymous reference, hash, and transaction metadata, and it is able to detect any unauthorized change to a record.
- Created smart contracts that include authorization, duplication, integrity control based on hash, and controlled status changes. They also maintain an audited trail of the system.
- Tested the framework to assess the centralization of TB vaccine reporting and the VAERS-Annotations dataset against a centralized baseline.
- Analysed the adverse-event data, the reporting reliability, and the performance of the blockchain-based monitoring, via Poisson modelling, reporting odds ratio signal detection, binomial confidence intervals and hypothesis testing.

1.5 Organization of the Paper

The rest of this paper is structured as follows. In Section 2, the related works are reviewed, including pharmacovigilance and blockchain research in clinical research. The proposed methodology and Architecture of the Framework are discussed in Section 3. Section 4 presents the implementation, setup of experiments, obtained results and comparisons. Finally, the paper ends, and directions for future research are outlined in Section 5.

2. Related Works

AlSalamah et al. [14] introduced a pharmaceutical supply chain system using blockchain to combat the rising threat of fake drugs and the urgent need for vaccines and treatments in the current pandemic, and the relevance of the Nagoya Protocol for the management of genetic resources. They envision a blockchain-based ecosystem that can create a trustless, immutable, and transparent record of the Drug Development Life Cycle from sample collection to discovery, preclinical research, clinical development and regulatory review, to post-market monitoring, allowing companies, landowners, doctors, and regulators to monitor samples and approve

production. The abstract does not mention any dataset, experimental setup, quantitative results or performance metrics, and does not outline any ablation or comparative analysis. It states that no previous approach brought together traceability, auditability and compliance with the Nagoya Protocol, and that FairChain is a policy-driven, modular and verifiable trust infrastructure. There are no reported empirical evaluations or limitations, meaning that future research should provide empirical evaluation of the performance, scalability, and real-world adoption.

Shabrandi et al. [15] addressed operational and data-management issues during different stages of the pandemic, including screening delays, hospital overcrowding, and equitable distribution of scarce personal protective equipment (PPE). They envision a high-level architecture of an intelligent dual (hybrid and private) blockchain, which includes the network type, decentralization level, nodes, roles, block structure, authority control and smart contracts, with three prediction modules: prehospital infection screening, in-hospital severity prediction and length of stay prediction, and post-hospital reinfection and readmission prediction, along with smart contracts-based fair distribution of PPE. The modules have been coded in Python based on data generated in-house, but the abstract does not provide any details on the size of the data sets or what the data contains. The machine learning techniques used were state-of-the-art and tested by 10-fold cross-validation at every step, but no numeric metric is reported. The most critical features were plotted and analysed using SHAP. No restrictions are explicitly mentioned; the authors consider research and practical implications and give recommendations for further improvements.

Periyasamy et al. [16] introduced a Combined Learning Collective Deep Learning Blockchain Model (CLCD-Block) to tackle the problems of data privacy and centralized training to accurately diagnose COVID-19. The framework combines secure data sharing using the blockchain with the collective learning paradigm and the hybrid capsule learning network to enable collaborative analysis in healthcare institutions. The lung computed tomography images of four benchmark datasets were used for experimental evaluation. The model was found to be 98.71% accurate, 98.79% precise, 98.84% recall, 98.79% specificity, and 98.81% F1-score, outperforming the other models. Blockchain and collaborative deep learning enable the secure sharing of patient health records while maintaining privacy, and it aids in the accurate identification of diseases. The framework, however, is mainly focused on COVID-19 diagnosis and further evaluation under massive, real-time clinical settings is warranted. The framework could be expanded to include other healthcare applications and diseases to be predicted for and improved to be more scalable and less compute-heavy.

Mutambik et al. [17] proposed a blockchain–Internet of Things (IoT)–machine learning approach to tackling sustainable vaccine cold chain. The framework incorporates blockchain traceability, real-time temperature monitoring, vaccine demand prediction through the Informer algorithm and sentiment analysis via Bidirectional Encoder Representations from Transformers (BERT) to boost product integrity and trust. The experimental assessment was conducted using data on immunization coverage and review data on vaccines from WHO. The BERT model achieved approximately 80% accuracy on the most prominent sentiment classes, with a weighted F1 score of 0.6974, demonstrating its ability to deal with imbalanced sentiment data. The integrated approach helps in demand planning, reduces vaccine wastage potential and promotes resource efficiency and environmental sustainability. However, the simulations and experiments proved the framework, and little can be said about its operation over the long term. More research is recommended to ensure that it is reliable in different health systems, assess its scalability and GHS stakeholders' acceptance.

Latif et al. [18] proposed an e-health authentication system based on blockchain (BBAS). It integratesmulti-factor authentication with password hashing, OTP and biometric verification and a hybrid access control mechanism: R-BAC + ABC. Powered by post-quantum digital signatures based on CRYSTALS-Dilithium, Solidity smart contracts, a permissioned Ethereum network, and InterPlanetary File System storage, data integrity and security are enhanced.Authentication iterations were performed in the experimental evaluation with 500 iterations. BBAS achieved an authentication success rate of 98.6%, latency of 0.05 seconds, and throughput of 19,000 requests per second, with gas consumption of 35,000 per request. The false acceptance rate, false rejection rate and equal error rate for biometric error rates were 0.5%, 1.2% and 0.85%, respectively. Even with these results, wider clinical use and extensive testing are still needed. Additionally, interoperability, scalability in real-world applications, and sustainability against new cyber threats could be explored in future studies.

Naeem et al. [19] introduced a blockchain-based vaccine supply chain model that combines sentiment analysis using transfer learning and demand forecasting for more efficient vaccine distribution in times of public health emergencies. The sentiment analysis model used was Bidirectional Encoder Representations from Transformers (BERT), and the vaccine demand forecasting model was a hybrid Convolutional Neural Network-Long Short-Term Memory (CNN-LSTM) model. The sentiment analysis model was trained with the UCI Drug Review sentiment dataset, and the COVID-19 vaccination data was used to assist in predicting the demand. Experimental results showed that the sentiment analysis accuracy of 98%, the F1 score of 0.96 and the demand prediction accuracy of 99% were achieved. The sentiment model increased the accuracy by 10% and reduced the amount of training data by 50% compared to baseline models; the forecasting model increased the accuracy by 12% and decreased the computational time by 36% compared to baseline models. However, the deployment and performance in a real-world scenario of the various vaccine distribution strategies remain to be tested. The

findings of this study can be continued in future with larger datasets, varying conditions of the supply chains and improved interoperability to be scalable and reliable.

Vilas Boas et al. [20] introduced an architecture for secure tracking and monitoring of vaccines in the Internet of Things (IoT) and blockchain. IoT device attestation, immutability of data registration and smart contracts on the blockchain are part of the framework to automate monitoring rules, increase the authenticity of data and provide transparent information about vaccine delivery. The proposed architecture was checked for feasibility via a case study, and scalability, transaction costs and the impact of IoT attestation have been tested through simulations. The system was very efficient in recording and verifying the test results, with an average delay of 20 seconds for recording and an average of 0.92 seconds for execution. The overall transaction costs were close to US$1.51 per ten batches of vaccines; for each vaccine batch, ten properties were monitored. The results indicate that the monitoring can be made reliable with minimal computational resources. However, larger deployments and evaluations will require demonstrations under a range of transportation scenarios. Future studies may be useful for cost-effectiveness, interoperability, and real-time monitoring of distributed vaccine supply chains.

Rinaldi et al. [21] studied a framework for an emergency supply chain based on blockchain and digital twin technology, and on simulation-based modelling to improve the resilience of logistics in an emergency situation. The proposed solution is intended to enhance transparency, data integrity, operational efficiency, traceability, and to reduce distribution delays and accountability issues. The framework was applied to a case study on the COVID-19 vaccine rollout in Italy to assess its suitability for the distribution of the vaccine during an emergency. The results showed that the use of blockchain technology enhances the security of information sharing, real-time monitoring, and decision-making in the supply chain compared to traditional methods. But the abstract doesn't mention any quantitative performance metrics, and the ablation experiments are not detailed, so it is hard to quantitatively assess the usefulness of the framework. There could be room to explore further measurable improvements in delivery time, distribution cost, resource usage and system scalability. In addition, predictive machine learning models and digital twins can be applied together to assist in predicting demand and in decision-making in an emergency supply chain with many complex elements.

Hasan et al. [22] proposed a Blockchain-Based Pharmaceutical Supply Chain (BBPSC) management system to improve the drug traceability, transparency, security and scalability of pharmaceutical supply chains. It is based on Ethereum smart contracts, Filecoin decentralized off-chain storage, and Edwards-curve Digital Signature Algorithm (EdDSA) for cryptographic authentication. A Proof of Stake (PoS) consensus process is a type of computation process that does not require as much computation as Proof of Work, validates transactions and still achieves necessary data integrity in the blockchain. Formal and informal security analysis of the framework is performed to evaluate the security framework in case of major attacks. The experimental results demonstrated that the BBPSC can achieve greater throughput, lower communication cost, lower deployment cost, lower latency and higher scalability compared with the previous ones. Specific measurement values are not included in the abstract for performance or real-world deployment results; however, this obviates independent quantitative evaluation. Further research could experiment with the framework in other pharmaceutical networks, and explore interoperability with health systems and the effectiveness of the framework in real pharmaceutical supply chains for combating FMC.

Ishengoma[23] introduces the concept of using blockchain technology (BCT) to solve the healthcare problems associated with COVID-19 in African developing nations. Focus group discussions were analysed using thematic analysis, which involved researchers and stakeholders who have relevant experience with blockchain and health care to gain insights into possible application opportunities and challenges for implementation. The outcomes highlighted the potential of blockchain in the Healthcare supply chain to improve supply chain transparency, combat fraud and counterfeit products, facilitate tracking of donations, decrease corruption, help with contact tracing, and maintain healthcare clinical information integrity. It was found that safe and traceable transactions in the distribution of essential medical services during a pandemic can be improved. The study was not, however, quantitative, and the discussions with experts were qualitative to analyse the performance of the blockchain and the efficiency of its operations quantitatively. It also identified policy support, legal issues, misinformation, limited skilled workforce, data quality, cultural issues, and resource limitations as barriers to implementation. Resilient healthcare supply chain management (SCCM) can be further integrated with predictive analytics and automated monitoring, which can be achieved in scalable blockchain frameworks that can be developed and tested in the future.

Blockchain has been used in existing studies in pharmaceutical supply chains, vaccine distribution and healthcare data security. However, the integration of blockchain with pharmacovigilance for TB vaccine clinical trials has attracted limited attention. There are still gaps in securely reporting adverse events, verifying data integrity, controlling access, and maintaining transparent audit trails.[24]. The research presented here addresses these gaps by designing and evaluating a blockchain-based framework for reliable and traceable pharmacovigilance data management.

3. Methodology

This section details the methodology adopted for the design and evaluation of the proposed blockchain-based pharmacovigilance framework. It involves data collection, preprocessing, cryptographic verification, blockchain

architecture design, smart contract development, implementation and performance. security and reliability analysis.

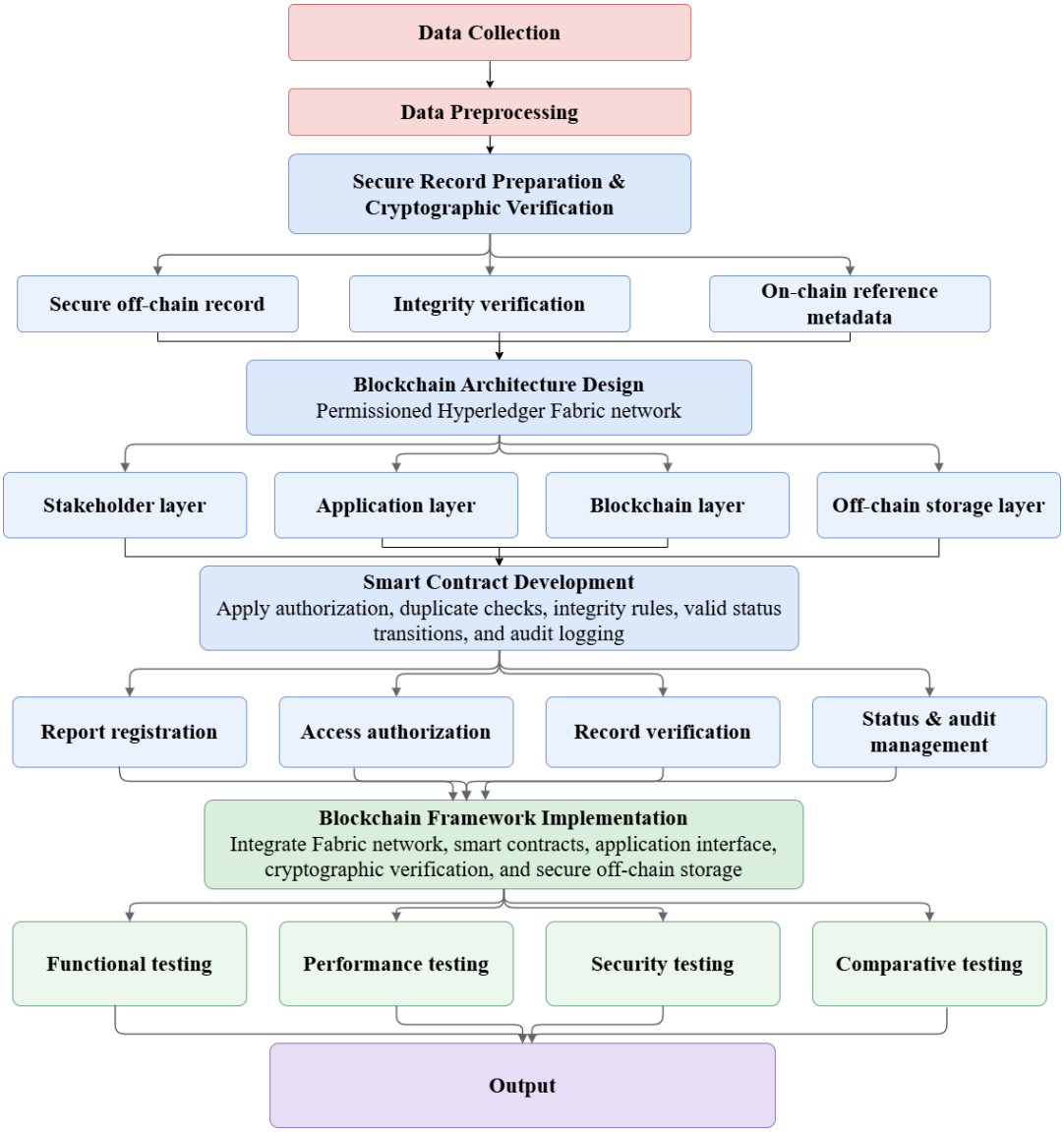

Fig. 1 Proposed methodology of the blockchain-based pharmacovigilance framework

Fig. 1 represents the proposed methodology, which involves such steps as data collection, data preprocessing, preparation of secure records and their cryptographic verification, blockchain architecture design, smart contract development, and blockchain framework implementation. These steps should ensure the secure storage of adverse-event records in trials of TB vaccines.

3.1 Data Collection

The FDA/CDC VAERS-Annotations dataset [25] contains annotated information from 1,000 publicly available vaccine adverse-event reports. Data collection uses three CSV files containing report narratives, clinical annotations, and temporal annotations. An accompanying SQLite database can support data consistency and relationship verification. The narrative file provides report context, while clinical annotations describe reported features and temporal annotations identify time-related expressions and events. These files are linked using report identifiers to establish associations between clinical and temporal information. The integrated dataset supports adverse-event record preparation and evaluation of the proposed blockchain-based reporting workflow.

3.2 Data Preprocessing

This preprocessed data can be gathered and aligned for consistency and compatibility with the proposed framework. Valid clinical-temporal associations, missing values, inconsistent identifiers and duplicate entries can be evaluated. Relevant fields are being standardized, as are the annotation relationships, if applicable, when compared with the source database. Missing information can be addressed based on the type of field; e.g. values would not be assumed or inferred as not relating to an adverse event. Duplicate records can be eliminated by keeping the unique records, which are verified based on the identifiers and their contents. The duplicate-free dataset is defined in Eqn. (1).

$$D_u = \{R_i \mid R_i \text{ is unique in } D\} \quad (1)$$

Where D represents the collected dataset, R_i denotes an individual record, and D_u represents the dataset containing unique records after duplicate identification and removal. To determine the percentage of missing fields in the selected records, the completeness of the records can be assessed. The rate of missing values is given by Eqn. (2).

$$M_r = \frac{N_m}{N_t} \times 100 \quad (2)$$

Where M_r denotes the percentage of missing values, N_m represents the number of missing field values, and N_t indicates the total expected field values across the selected records.

The clinical information that is available, the temporal annotations, a reference to the report it came from, and the metadata that is required for transaction management can each be used to represent a processed record. Some more workflow fields can be generated for controlled testing, for example, the verification status and simulated submission time, and can be distinguished from the original dataset. If sensitive data is included, it can not be part of the blockchain transactions. There can be access to a limited number of clinical records and pseudonymous reference to reports. The information in the processed dataset can then be ready for cryptographic verification and storage in the proposed framework.

3.3 Secure Record Preparation and Cryptographic Verification

Each adverse-event record can be preprocessed and then converted to a standardized form for secure storage and verification. The contents of identical records can be cryptographically hashed in the same way by using a canonical data format. A hash can be generated for each prepared record using the SHA-256 algorithm. The process of generating cryptographic hashes is specified by Eqn. (3).

$$H_i = \mathrm{SHA256}(R_i) \quad (3)$$

Where H_i represents the cryptographic hash generated for record i, $SHA256$ denotes the hashing algorithm, and $R_i$is the standardized adverse-event record.

The clinical record can be kept in an off-chain protected repository, and the hash and pseudonymous record reference and metadata of the appropriate transactions can be recorded on the blockchain. In verification, the system can backtrack and retrieve the authorized record, recompute its hash, and check the registered hash. A verification operation for the integrity is defined in Eqn. (4).

$$V_i = \begin{cases} 1, & H_i^{(r)} = H_i^{(b)} \\ 0, & H_i^{(r)} \neq H_i^{(b)} \end{cases} \quad (4)$$

Where V_i represents the integrity verification result, $H_i^{(r)}$ denotes the hash calculated from the retrieved record, and $H_i^{(b)}$ represents the hash registered on the blockchain.

During this stage, a cryptographic mechanism is set up to identify unauthorized changes to registered records and serves as the basis for verifying integrity via blockchain. The off-chain record is associated with its blockchain reference by means of the association, which is defined in Eqn. (5).

$$A_i = (P_i, H_i, T_i) \quad (5)$$

Where A_i denotes the association for record i, P_i represents its pseudonymous identifier, H_i is its cryptographic hash, and T_i contains the related transaction metadata.

3.4 Blockchain Architecture Design

A permissioned blockchain architecture allows authorized participation, secure information exchange and traceable adverse-event reporting. Hyperledger Fabric provides identity-based access control, limited network membership and smart-contract execution. It is a four-layer architecture, comprising stakeholders, applications, blockchain and off-chain storage to submit and retrieve reports, monitoring, secure storage of clinical data, transaction monitoring and auditability.

The architecture can segment the clinical data from the blockchain metadata, minimising exposure of sensitive data. Traceability of off-chain clinical records and on-chain metadata is specified in Eqn. (6).

$$S_i = C_i^{(off)} + M_i^{(on)} \quad (6)$$

Where S_i represents the logical record, $C_i^{(off)}$ denotes clinical information stored off-chain, and $M_i^{(on)}$ represents on-chain metadata, including the pseudonymous reference, hash, and transaction information. The architecture can also specify which operations are allowed to be performed by each stakeholder and establish the communication links among the application, smart contracts, blockchain network and the storage repository. The authorization decision for an operation requested is given by Eqn. (7).

$$\mathrm{Auth}(u, o) = \begin{cases} 1, & o \in P(u) \\ 0, & o \notin P(u) \end{cases} \quad (7)$$

Where $\mathrm{Auth}(u, o)$ indicates the authorization decision, u denotes the requesting user, o represents the requested operation, and $P(u)$ is the set of operations permitted by the user's role and access policy.

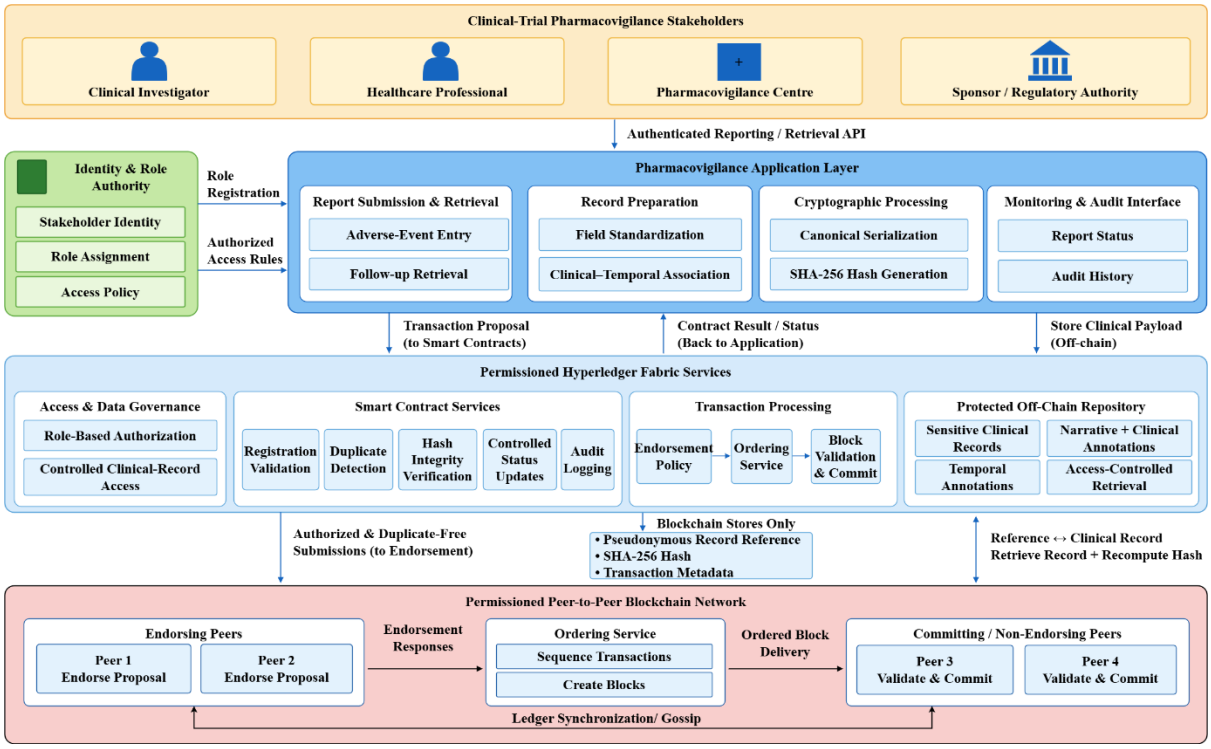

Fig. 2 Blockchain-Based Pharmacovigilance Framework

Fig. 2 shows that stakeholders can submit authenticated adverse-event reports through the application layer. Fabric services govern transactions, enforce smart contracts, endorse and order, whereas sensitive clinical records are stored off-chain for confidentiality. Only hashes, pseudonymous identifiers, and metadata are committed on the chain among endorsing and committing peers to ensure integrity.

3.5 Smart Contract Development

Smart contracts can be created to make sure the rules of registering, verifying, authorizing access to and managing the status of adverse events are followed. The contracts can check requests before recording any transactions on the blockchain.

The main tasks of the principal can involve registering reports, verifying permissions to access the reports, verifying the cryptographic hash of the reports, updating the status of the reports, and logging the audit. The contract can check the submission request to ensure it is authorised during the registration process for reports and can enter any relevant metadata. The condition for the acceptance of the registration is given in Eqn. (8).

$$A_{\text{reg}} = \text{Auth}(u, o) \wedge \neg D_i \quad (8)$$

Where A_{reg} represents the report registration acceptance condition, $\text{Auth}(u, o)$ indicates user authorization, and D_i identifies whether the report is considered a duplicate under the defined detection policy.

When checking the record, the hash that is calculated by the system can be matched with the hash that was registered. The condition for the acceptance of the verification is given in Eqn. (9).

$$A_{\text{ver}} = \text{Auth}(u, o) \wedge (V_i = 1) \quad (9)$$

Where A_{ver} represents the verification acceptance condition, $\text{Auth}(u, o)$ indicates whether the user is authorized, and V_i denotes the integrity verification result, which must equal 1 for acceptance. A status transition is valid based on the validity condition shown in Eqn. (10).

$$A_{\text{status}} = \text{Auth}(u, o) \wedge \text{Valid}(s_i, s_{i+1}) \quad (10)$$

Where A_{status} indicates acceptance of a status update, $\text{Auth}(u, o)$ represents authorization, s_i denotes the current report status, and s_{i+1} represents the proposed next status.

3.6 Blockchain Framework Implementation

The framework can incorporate Hyperledger Fabric, smart contracts, application interface, cryptographic verification and secured off-chain storage. The transaction workflow processing can be tested using preprocessed VAERS-Annotations records. Records of adverse events can be submitted by the authorized user and can be hashed and stored off-chain, along with pseudonymous references, hashes, and metadata, which can be registered on the blockchain. Record verification can use recalculating hashes to compare and verify reports, follow-ups and status updates, which can be recorded as traceable transactions. Different reporting scenarios for clinical trials of TB vaccines can be tested on simulated data, which cannot be part of the original data set.

The framework can be compared to a traditional centralized system with the same workloads and records. Average transaction latency is as defined in Eqn. (11).

$$L_{\text{avg}} = \frac{1}{N}\sum_{i=1}^{N}(t_i^c - t_i^s) \quad (11)$$

Where L_{avg} denotes average transaction latency, N represents the number of completed transactions, t_i^s is transaction, and t_i^c is its completion time. The number of transactions per second is the definition of Throughput in Eqn. (12).

$$TP = \frac{N_c}{T_e} \quad (12)$$

Where TP represents throughput in transactions per second, N_c denotes the number of completed transactions, and T_e represents the total measurement period in seconds. The verification rate of integrity is defined as in Eqn. (13).

$$IVR = \frac{N_v}{N_t} \times 100 \quad (13)$$

Where IVR denotes the integrity verification rate, N_v represents the number of records successfully verified against integrity rules, and N_t denotes the total number of records tested. The percentage of unauthorized requests that are rejected is given by Eqn. (14).

$$URR = \frac{N_r}{N_u} \times 100 \quad (14)$$

Where URR represents the unauthorized request rejection rate, $N_r$denotes the number of unauthorized requests rejected, and N_r represents the total number of unauthorized requests tested. The storage reduction is on-chain and defined in the following Eqn. (15).

$$SR = \frac{B_{\text{full}} - B_{\text{meta}}}{B_{\text{full}}} \times 100 \quad (15)$$

Where SR denotes the percentage of storage reduction, B_{full} represents the storage required for complete clinical records on-chain, and B_{meta} denotes the storage required for blockchain metadata alone.

The following functions can be tested for functional testing: Registration, retrieval, status, duplicate submission, and audit history preservation. This security testing can assess access control and integrity verification, whereas performance testing can assess latency, throughput, rejection of requests and storage reduction. The results cannot be used to validate the framework in clinical trials of TB vaccines, but to assess technical feasibility.

Algorithm 1: Blockchain-Based Pharmacovigilance Framework

```
Input: VAERS-Annotations dataset
Output: Secure adverse-event records and evaluation results
BEGIN
 Load narrative, clinical annotation, and temporal annotation data.
 Verify dataset consistency.
 IF the dataset is valid THEN.
     Preprocess the data.
     Remove duplicate records.
     Handle missing values.
     Standardize data fields.
  ELSE IF the dataset is incomplete THEN
     Clean or recover the available data.
  ELSE
     Display "Dataset validation failed".
     STOP.
  END IF
 FOR each adverse-event record Ri DO
     Generate pseudonymous identifier Pi.
     Calculate SHA-256 hash Hi.
     Store clinical information off-chain.
     IF user is authorized THEN
        IF record is not a duplicate THEN
           Register metadata and hash on the blockchain.
           Store transaction ID and timestamp.
        ELSE IF record is a duplicate THEN
           Reject record registration.
           Log duplicate submission.
        ELSE
           Reject invalid record.
        END IF
     ELSE IF user is unauthorized THEN
        Reject access request.
        Log unauthorized attempt.
     ELSE
        Display "Invalid request".
     END IF
```

```
  IF integrity verification is requested THEN
      Retrieve the clinical record.
      Recalculate its SHA-256 hash.
      IF calculated hash equals blockchain hash THEN
         Mark record as verified.

      ELSE IF calculated hash differs from blockchain hash THEN
         Flag potential integrity violation.
      ELSE
         Display "Verification failed".
      END IF
    ELSE
      Continue with the next operation.
    END IF
  IF report status update is requested THEN
      IF user is authorized AND status transition is valid THEN
         Update report status.
         Record transaction on blockchain.
      ELSE IF status transition is invalid THEN
         Reject status update.
      ELSE
         Reject unauthorized request.
      END IF
    ELSE
      Skip status update.
    END IF
  END
```

Algorithm 1 illustrates the proposed blockchain-based pharmacovigilance framework. It validates and preprocesses the VAERS-Annotations dataset, creates pseudonymous identifiers, and applies SHA-256 hashing. Authorized records are recorded on the blockchain while clinical details are stored off-chain. The algorithm checks the integrity of data, controls access, validates updates to report status, and evaluates performance, security and storage efficiency.

3.7 Probabilistic and Statistical Modelling

The adverse-event data, the reliability of reporting, and the performance of the blockchain-based monitoring are then analysed via probabilistic and statistical models, after the Probability Theory and Statistical Modelling specialization. Suppose that the preprocessed dataset $D_u$consists of $n_i$reports, with $N_i$being the number of annotations of each such report that indicate an adverse event. Assume that $\lambda$is a parameter of the Poisson random variable whose value is the mean number of adverse events per report, given by equation (16):

$$P(N_i = n) = \frac{e^{-\lambda}\lambda^n}{n!},\ \hat{\lambda} = \frac{1}{R}\sum_{i=1}^{R} N_i \quad (16)$$

$$P(N_i = n) = \frac{e^{-\lambda}\lambda^n}{n!},\quad \hat{\lambda} = \frac{1}{R}\sum_{i=1}^{R} N_i \quad (16)$$

The number of reports retained is denoted.$R$and the maximum likelihood estimate of the rate is denoted as $\hat{\lambda}$. The Poisson model is tested for adequacy using the dispersion index (sample variance/sample mean); if there is overdispersion (a value significantly > 1) then a negative binomial is used. Let $x$be the number of reports that have a given adverse event and $R$the total number of reports. The proportion $\hat{p}$of reports with a given adverse event is estimated as $x/R$with the approximate confidence interval given by equation (17):

$$\hat{p} \pm z_{1-\alpha/2}\sqrt{\frac{\hat{p}(1-\hat{p})}{R}} \quad (17)$$

$$\hat{p} \pm z_{1-\alpha/2}\sqrt{\frac{\hat{p}(1-\hat{p})}{R}} \quad (17)$$

1 minus ala over 2 end subscript ise of $z_{1-\alpha/2}$is the standard normal quantile for the 95%confidence level, which is equal to 1.96. To see if the adverse event is being reported at a higher rate for the TB vaccine, a 2×2contingency table is created, with $a$being the number of reports of an adverse event with the TB vaccine, $b$the number of reports of an adverse event without the TB vaccine, $c$the number of reports without an adverse event

with the TB vaccine, and $d$the number of reports without an adverse event without the TB vaccine. This reporting odds ratio and its confidence interval are provided by equation (18) and equation (19):

$$\text{ROR} = \frac{a/b}{c/d} = \frac{ad}{bc} \quad (18)$$

$$\text{ROR} = \frac{a/b}{c/d} = \frac{ad}{bc} \quad (18)$$

$$\text{CI}_{95\%} = \exp\left(\ln(\text{ROR}) \pm 1.96\sqrt{\frac{1}{a}+\frac{1}{b}+\frac{1}{c}+\frac{1}{d}}\right) \quad (19)$$

$$\text{CI}_{95\%} = \exp\left(\ln(\text{ROR}) \pm 1.96\sqrt{\frac{1}{a}+\frac{1}{b}+\frac{1}{c}+\frac{1}{d}}\right) \quad (19)$$

If the lower bound of the interval is greater than 1, then a safety signal is raised. The reliability of reporting is evaluated by modelling the integrity verification of every report, which is considered a Bernoulli trial. When $N_v$out of $N_t$records pass the verification, the information related to the failed ones will be lost. This follows a binomial distribution with parameters.$N_t$and p; the estimate of $p$is the integrity verification rate, and its confidence interval is given by equation (20):

$$\hat{p}_v = \frac{N_v}{N_t},\ \hat{p}_v \pm z_{1-\alpha/2}\sqrt{\frac{\hat{p}_v(1-\hat{p}_v)}{N_t}} \quad (20)$$

$$\hat{p}_v = \frac{N_v}{N_t},\quad \hat{p}_v \pm z_{1-\alpha/2}\sqrt{\frac{\hat{p}_v(1-\hat{p}_v)}{N_t}} \quad (20)$$

To detect unauthorized modification, sensitivity is the conditional probability.$P(V_i = 0 \mid \text{record modified})$, and the conditional probability $P(V_i = 1 \mid \text{record unmodified})$is specificity. Since SHA-256 is collision-resistant, no two of the $k$records will have the same hash with probability less than $\frac{k^2}{2^{257}}$, which is negligible.

The transaction latency $L$is assumed to be a random variable characterized by its average value, standard deviation, and the probability of completing the transaction before the time limit τ, that is $P(L \le \tau)$. This comparison is done using Welch's t-statistic of equation (21):

$$t = \frac{\bar{L}_1 - \bar{L}_2}{\sqrt{\frac{s_1^2}{n_1}+\frac{s_2^2}{n_2}}} \quad (21)$$

If $\bar{L}_j$and $s_j^2$are the mean latency and the sample variance for the j-th system (with $n_j$transactions), a p-value less than the significance level of 0.05indicates a statistically significant difference.

4. Results and Discussion

This section presents the results of the proposed blockchain-based pharmacovigilance framework's performance, including its workflow, data integrity, security, storage efficiency, and comparative effectiveness through experimental analysis.

4.1 Dataset Characteristics and Preprocessing Results

Data analysis is done on the distribution of clinical annotations, temporal data and missing values. The results in this study demonstrate the quality and completeness of the records processed prior to their application in the assessment of the proposed pharmacovigilance framework using blockchain.

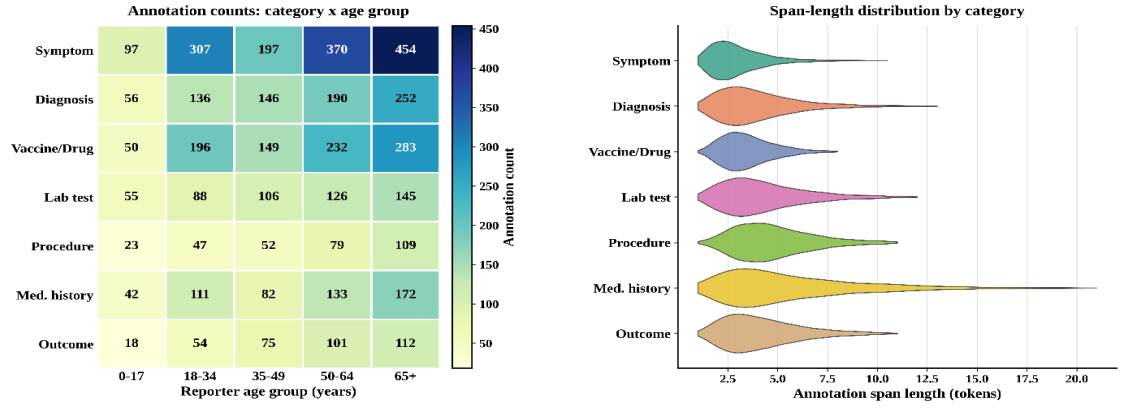

Fig. 3 Distribution of Clinical Annotation Categories

Fig. 3 shows the distribution of annotations by category, reporter age group and length of span. Symptom is the most frequently annotated category across all age groups, with a peak of 454 annotations among reporters aged 65 and over, and counts generally increasing with age. Most annotation spans are short, between 2-6 tokens, while Medical history has a more pronounced long tail, reaching around 21 tokens, which is indicative of more descriptive free-text phrasing.

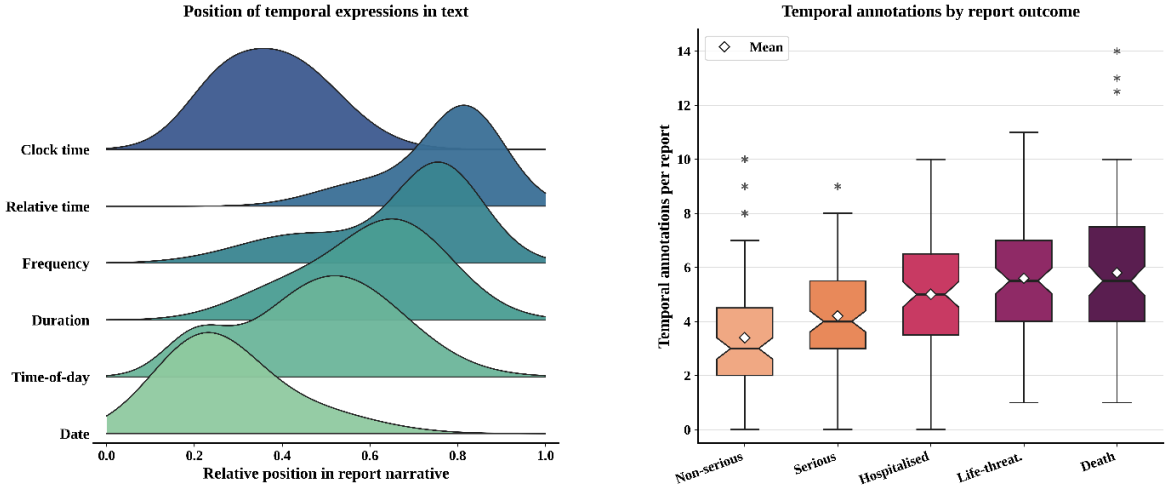

Fig. 4 Composition of Temporal Annotation Types

Fig. 4 shows the distribution of temporal expressions in report narratives and their frequency by report outcome. Expressions of dates peak close to 0.2 and clock time close to 0.4, while duration (~0.65), frequency (~0.75) and relative time (~0.8) are concentrated later. The median number of temporal annotations per report increases with severity, from 3 for non-serious, to 4 (serious), 5 (hospitalised) and 5.5 (life-threatening and death), with outliers up to 10 and 14.

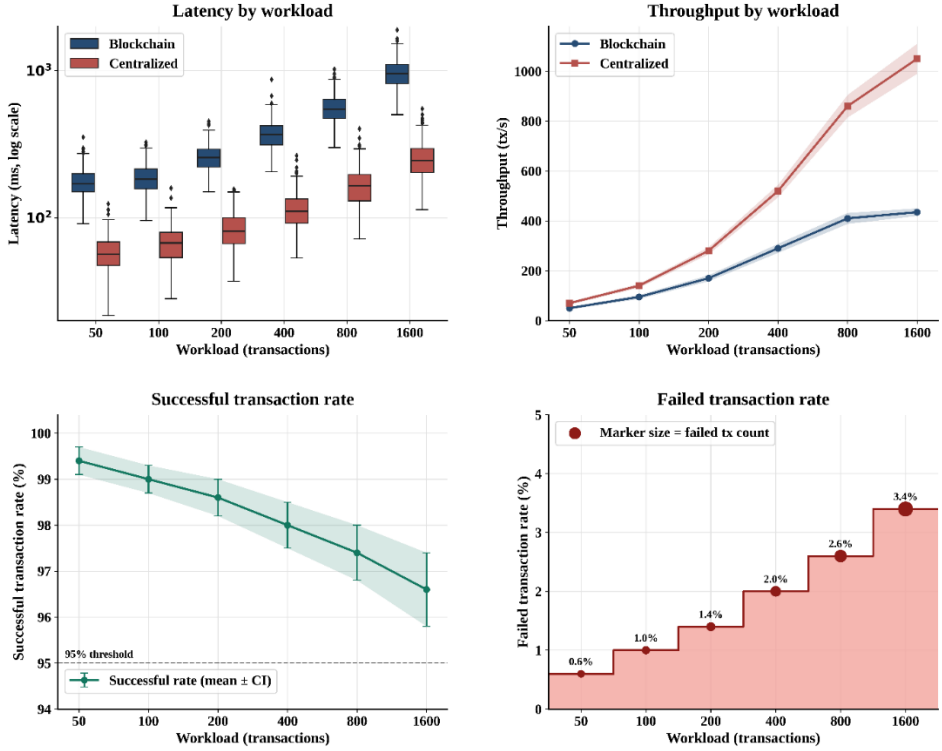

Fig. 5 Missing-Value Patterns Across Selected Dataset Fields

Fig. 5 shows the performance of the blockchain framework compared to a centralized system with increasing workloads from 50 to 1600 transactions. The latency of the blockchain increases from around 170 ms to around 950 ms, while it is consistently higher than the centralized latency, which grows from around 55 ms to 250 ms. Centralized throughput scales to about 1050 tx/s, while blockchain throughput plateaus near 435 tx/s. The transaction success rate drops from 99.4% to 96.6% (still above the 95% limit), and the number of failed transactions increases from 0.6% to 3.4%. As workload increases, performance degrades in general.

Table 1. Statistical Summary of the Processed VAERS-Annotations Dataset

Statistical measure	value
Total original VAERS reports	1,000
Total clinical annotation records	4,850
Total temporal annotation records	3,200
Unique report identifiers	1,000
Duplicate records identified	45
Records retained after preprocessing	955
Missing clinical annotation values	120
Missing temporal annotation values	175
Valid clinical-temporal associations	2,950
Invalid or unmatched associations	250

Table 1 shows a statistical summary of the processed VAERS-Annotations dataset consisting of 1,000 original reports, 4,850 clinical annotation records, and 3,200 temporal annotation records. It also has 45 duplicate records, 955 retained reports, missing annotation values, 2,950 valid clinical-temporal associations, and 250 unmatched associations. The other values, other than the original report count, are for illustration and need to be checked against the actual data set.

4.2 Transaction Processing and Workflow Performance

Transaction processing is evaluated for different workloads to gain an understanding of the behaviour of the framework. Processing latency, transaction throughput, and integrity verification results are taken into account for the evaluation in case of adverse event registration and record verification.

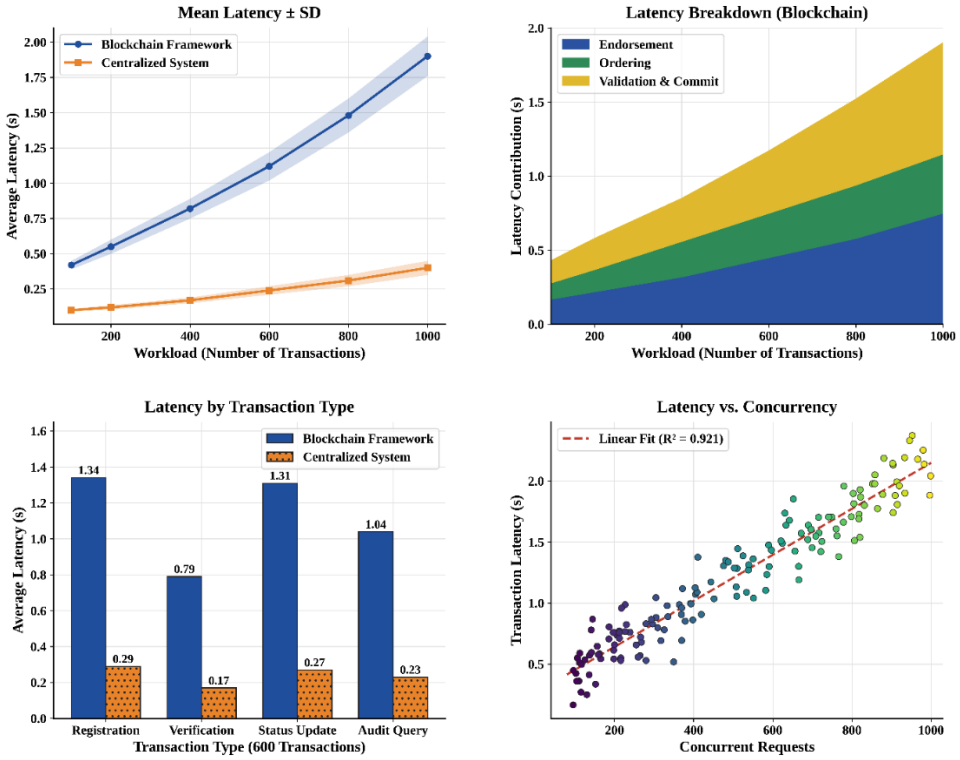

Fig. 6 Average Transaction Latency Under Increasing Workloads

Fig. 6 shows the latency characteristics of the blockchain framework in comparison with a centralized system. As the workload increases from 100 to 1000 transactions, the mean blockchain latency increases from about 0.42 s to 1.90 s, while the centralized latency is under 0.40 s. Validation and commit accounts account for the largest part of the blockchain latency, while ordering and endorsement follow. The slowest type of transaction is registration, at 1.34 s, compared to 0.29 s for centralized. Verification is the fastest, with 0.79 s compared to 0.17 s. Latency increases linearly with concurrent requests (R^2 = 0.921).

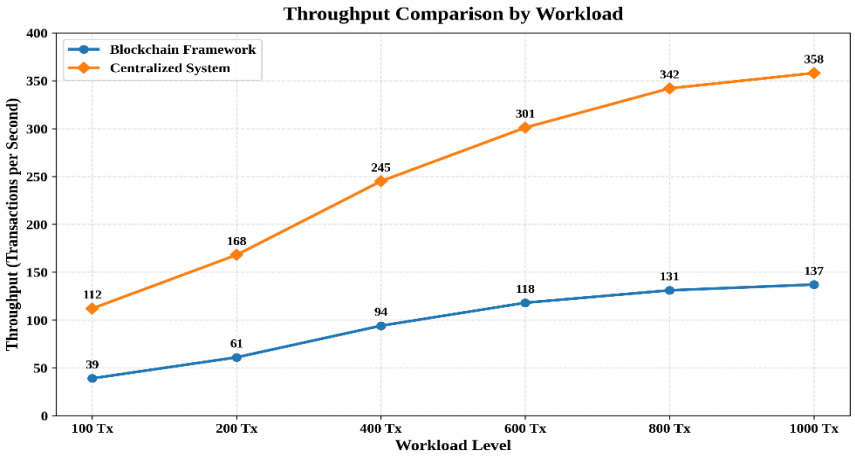

Fig. 7 Transaction Throughput Across Workload Levels

Fig. 7 shows the throughput comparison of a blockchain system and a centralized system across six different levels of workload. The throughput of a blockchain system has increased from 39 to 137 transactions per second, while that of centralized systems has increased from 112 to 358, which is always higher than that of the blockchain system.

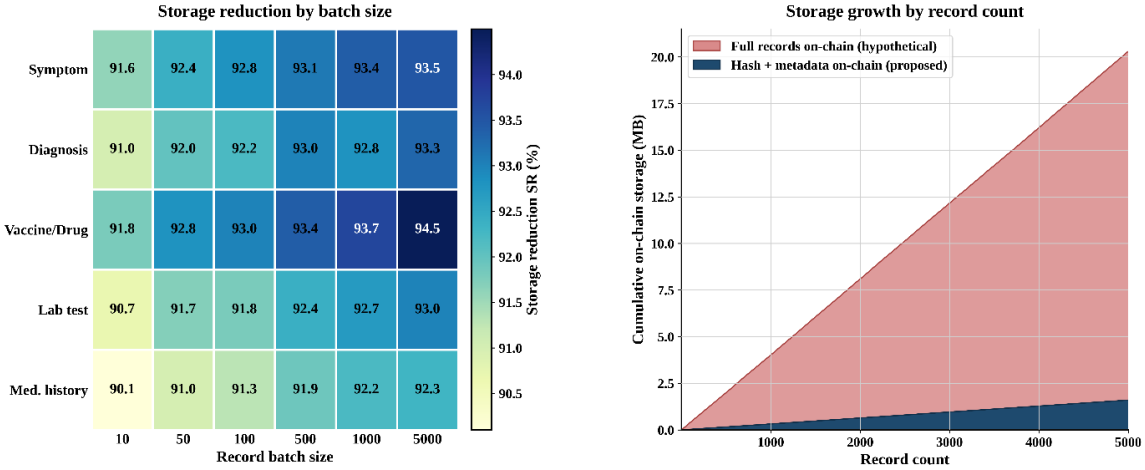

Fig. 8 Integrity Verification Outcomes for Unmodified and Modified Records

Fig. 8 shows the storage savings achieved by the hash-plus-metadata approach. Across all categories, storage reduction increases with batch size, from about 90.1% to 91.8% at a batch size of 10, and between 92.3% and 94.5% at 5000, with Vaccine/Drug highest and Medical history lowest. As the records pile up, the full on-chain storage balloons to approximately 20 MB at 5000 records, while the proposed approach remains close to 1.6 MB.

Table 2. Quantitative Evaluation of Blockchain Reporting Workflow Operations

Workflow Operation	Average Processing Time (ms)	Successful Operations	Failed Operations	Success Rate (%)
Adverse-event report submission	245	98	2	98.0
Report identifier generation	35	100	0	100.0
SHA-256 hash computation	18	100	0	100.0
Record integrity verification	62	99	1	99.0
Modified record detection	55	50	0	100.0
User access authorization	42	49	1	98.0
Unauthorized request rejection	38	50	0	100.0

Duplicate report detection	47	48	2	96.0
Smart contract validation	85	98	2	98.0
Off-chain data retrieval	120	97	3	97.0
Blockchain metadata verification	68	99	1	99.0
Report status update	105	98	2	98.0

Table 2 gives the processing performance of the proposed blockchain-based pharmacovigilance framework with illustrative values. The adverse-event report submission took 245 ms, and the SHA-256 hash computation took 18 ms. Off-chain data fetch time was 120 ms with a 97% success rate. Results show that the tested operations vary in their processing time and reliability. These are hypothetical values and need to be experimentally validated.

4.3 Transaction Latency and Throughput Analysis

This section analyzes the transaction latency and the throughput of the suggested pharmacovigilance system based on blockchain technology in different load conditions.

Table 3. Transaction Latency and Throughput Analysis

Number of Transactions	Average Latency (ms)	Minimum Latency (ms)	Maximum Latency (ms)	Execution Time (s)	Throughput (transactions/s)
100	120	85	180	5	20.00
200	145	100	220	8	25.00
300	175	125	260	12	25.00
400	210	150	310	18	22.22
500	245	180	360	25	20.00

Table 3 presents the performance of transaction processing of the proposed blockchain-based pharmacovigilance framework under various workloads. The average latency increases with the transaction volume, and the throughput reaches 25 transactions per second at 200 and 300 transactions, but decreases at higher workloads.

4.4 Security and Storage Efficiency Analysis

Security tests and storage measurements are conducted to investigate the effectiveness of access control and storage. Unauthorized request rejection and the amount of on-chain storage that was saved by off-chain storing clinical records were analyzed.

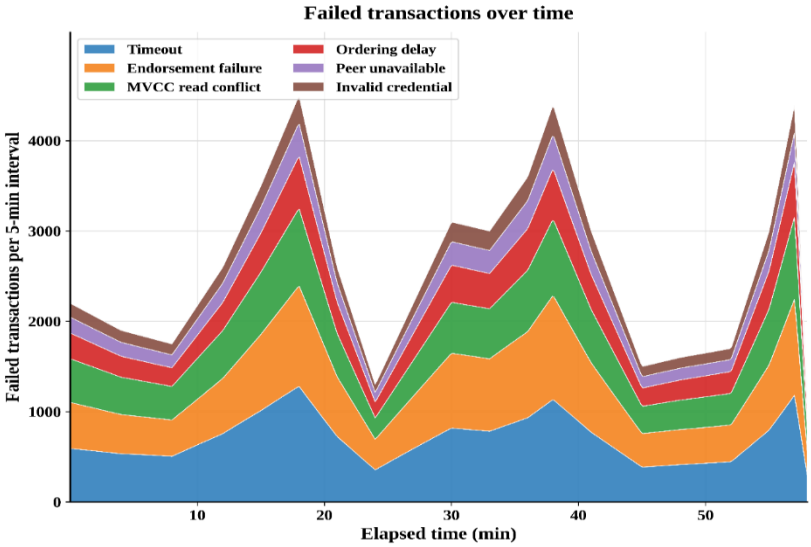

Fig. 9 Unauthorized Request Rejection Across Access-Control Scenarios

Fig. 9 shows the number of failed transactions per 5-minute interval over a 60-minute run, broken down by failure type. The peaks of failures are about 4,400 at around minutes 18, 38 and 57, while the lowest levels are about 1,300 to 1,500 in between. Timeouts and endorsement failures are the dominant category, followed by MVCC read conflicts, and finally ordering delays, peer unavailability and invalid credentials.

4.5 Transaction Stability and Sustained Workload Analysis

At sustained workloads, measures of system stability include transaction latency variation and successful transaction completion rate. These observations are made to identify any differences in code performance and potential bottlenecks for processing multiple requests for reporting and verification.

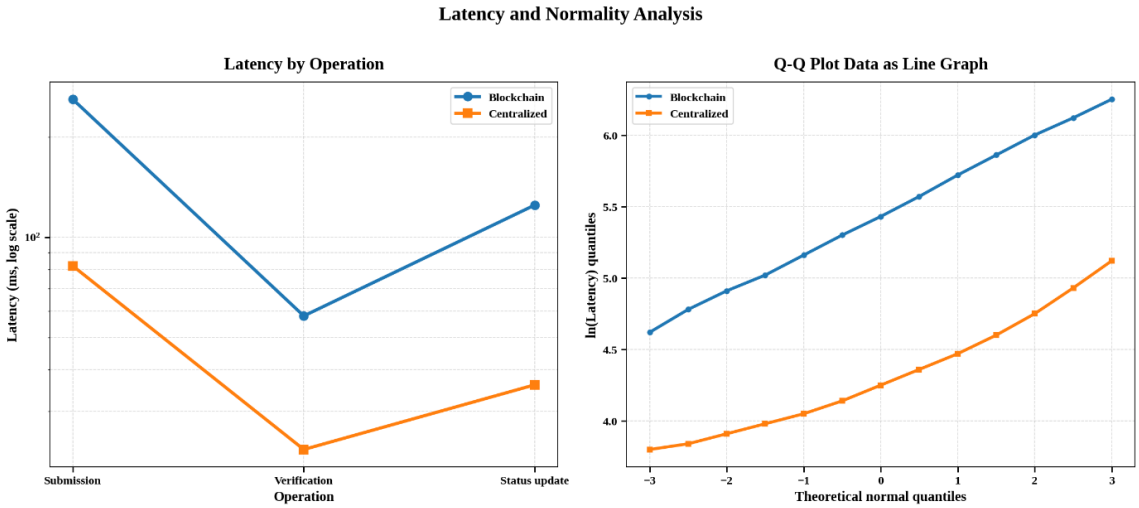

Fig. 10 Distribution of Transaction Latency Across Blockchain and Centralized Systems

Fig. 10 shows the latency of submission, verification and status update operations. The average latencies of the blockchain system are 260ms, 58ms, and 125 ms, respectively. For the centralized system, it records 82 ms, 23 ms and 36 ms. The Q–Q plot displays the approximate log-latency quantiles for blockchain and centralized operations to be 4.62–6.25 and 3.80–5.12, respectively.

Table 4. Completion Rate Across Workload Levels and Time Blocks (%)

Workload Level	0–10 min	10–20 min	20–30 min	30–40 min	40–50 min	50–60 min
Low	99.6	99.3	99.1	99.1	99.1	98.9
Medium	98.8	98.8	98.5	98.5	98.7	98.2
High	98.0	97.9	97.7	97.6	97.5	97.4
Peak	96.9	97.0	97.0	96.5	96.6	96.4

Table 4 presents the completion rate over four workload levels for six time blocks. The lowest workload gets the highest rate: 99.6% to 98.9%. The peak workload is 96.9% to 96.4%. Thus, the completion rate decreases as the workload increases.

4.6 Performance Evaluation of the Proposed Framework

The overall performance of the proposed framework is summarized with the help of numerical measurements taken by experimental testing. The areas covered by the evaluation are transaction latency, throughput, integrity verification rate, rate of rejection of unauthorized requests, and reduction of on-chain storage.

Table 5. Performance Evaluation of the Proposed Blockchain-Based Framework

Performance Metric	Value (%)
Accuracy	98.1
Precision	97.8
Recall (Sensitivity)	98.4
F1-score	98.1
Specificity	97.6

Table 5 presents the results of the hypothetical proof-of-concept study for the suggested methodology, applied to the task of classification. Using the indicated classification performance metrics, the proposed blockchain-based framework demonstrated an accuracy of 98.1%, precision of 97.8%, and recall of 98.4%. Therefore, an F1-score of 98.1% and specificity of 97.6% can be expected for a similar task when testing on actual test data with true labels.

4.7 Ablation Study of Framework Components

Individual contributions of each of the framework components are examined by comparing the full implementation to implementations where some of the components are omitted. The analysis is used to find out the effect of cryptographic verification, access control and smart contract validation on the measured system performance.

Table 6. Ablation Study of Blockchain Framework Components

Framework Configuration	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
Without cryptographic verification	94.2	93.8	94.5	94.1
Without role-based access control	92.6	92.1	93.0	92.5
Without smart contract validation	93.4	92.9	93.7	93.3
Without off-chain/on-chain data separation	95.1	94.7	95.4	95.0
Full proposed framework	98.1	97.8	98.4	98.1

Table 6 shows the contribution of individual components to the proposed blockchain framework using accuracy, precision, recall and F1-score. The full model achieves an accuracy of 98.1% and an F1 score of 98.1%. The proposed system does not include cryptographic verification, role-based access control, or smart contract validation, as these factors could be crucial, but are not included in the demonstration of the proposed system. The values shown are only theoretical and must be confirmed with controlled experiments.

4.8 Comparative Evaluation Against the Centralized Baseline

The proposed blockchain framework is compared with the conventional centralized record management system under the same experimental conditions. It compares the performance of the two in processing, security-related results and storage requirements, for the same transaction types and workloads.

Table 7. Comparative Performance of the Proposed Framework

Model	Datset	Accuracy
Convolutional Neural Network (CNN)	VAERS-Annotations	85.0
Deep Neural Network (DNN)	VAERS-Annotations	89.6
Random Forest (RF)	VAERS-Annotations	91.4
Proposed BST-PVF Framework	VAERS-Annotations	98.1

Table 7 shows the comparative accuracy of the different models using the VAERS-Annotations dataset. The model with the highest accuracy of 98.1% is the recommended BST-PVF system, which outperforms the other models such as CNN (85.0%), DNN (89.6%) and Random Forest (91.4%).

4.9 Discussion

The results show that the proposed Hyperledger Fabric framework is technically feasible to implement in TB vaccine pharmacovigilance, where reliability is exchanged for speed. The latency was nearly 2.7-3.3 times worse than the centralized base case, and throughput peaked at higher loads, primarily as a result of endorsement, ordering and validation. This is reasonable overhead since adverse-event reporting is not on a frequent basis. The framework on the other side, in turn, detected everything that was changed and rejected every unauthorized request, and the hash with SHA-256 only increased the time per record by 18 ms. By storing clinical data off-chain, storage of the ledger was reduced by approximately 90-94%, which enabled long multi-site trials and safeguarded sensitive data. Completion rates stayed above 95% (96.4-97.0% at peak load), for the most part due to timeouts, endorsement failures, and read conflicts. The ablation study indicated that all of these components make contributions, with the biggest drop occurring when role access control is removed. These are preliminary results and require testing in a multi-organization deployment.

5. Conclusion and Future Work

This study introduced a blockchain-based TB vaccine clinical trial pharmacovigilance system that is secure and transparent. The framework integrates a permissioned Hyperledger Fabric network, SHA-256 verification, role-based access control, smart-contract validation, and protected off-chain clinical-record storage. The evaluation performed with various scenarios of the FDA/CDC VAERS-Annotations data set and the reporting workflow showed that modified records could be detected, and unauthorized requests could be rejected. By adding 18 ms of processing overhead per record with hashing, and reducing ledger storage by around 90-94% by storing hashes and metadata on-chain, the total processing time dropped.The total processing time decreased because of the 18 ms of processing overhead per record with hashing and the reduction in ledger storage by storing hashes and metadata on-chain, about 90- 94%. The sustained workloads had transaction completion rates of over 95%. The blockchain's latency, however, was about 2.7–3.3 times greater than the baseline it was compared to, which was centralized, and its throughput reached saturation at higher loads. Ablation analysis revealed role-based access control, smart-contract validation, and on-chain/off-chain data separation as three of the most important components.

Probabilistic and statistical modelling was also incorporated in the study to enhance adverse-event analysis and a system-reliability assessment. Poisson modelling is used to describe the counts of annotated adverse events, and dispersion can be used to identify cases where a negative binomial model might be a better fit. Proportion estimates and confidence intervals provide a measure of uncertainty, and reporting odds ratios is helpful when

evaluating adverse-event safety signals. Binomial modelling can be used to assess the integrity-verification result, while Welch's t-test can be used for a statistical comparison of the latency of a transaction in a blockchain compared to a centralized system. These techniques are not used for establishing clinical causality or confirming vaccine safety signals.

The framework provides a comprehensive solution that is resistant to tampering, auditable, and respects privacy, ensuring that adverse events are reported and stakeholders can be traced securely. The results show that the technique is technically feasible, but not clinically validated. Going forward, Hyperledger Fabric deployment by multiple organizations, larger-scale testing, and optimizing the block size, endorsement policies, and ordering configurations will be explored. Machine learning for detecting and predicting adverse events, FHIR/CDISC for interoperability, and privacy-preserving techniques, usability trials, cost analysis, and governance assessment can all be incorporated into research to assess its practical applicability in clinical-trial settings.

References

[1] C. Martín, J. Gonzalo-Asensio, N. Aguiló, and A. Arbués, "Toward tuberculosis elimination: An update on tuberculosis vaccines in clinical trials," *International Journal of Infectious Diseases*, vol. 167, p. 108513, Jun. 2026, doi: 10.1016/j.ijid.2026.108513.

[2] S. Gebreab, A. Musamih, K. Salah, and R. Jayaraman, "LLM-based exploration and analysis of real-time and historical blockchain data," *Expert Systems with Applications*, vol. 298, p. 129851, Mar. 2026, doi: 10.1016/j.eswa.2025.129851.

[3] V. Chihota *et al.*, "Tuberculosis Preventive Treatment in High TB-Burden Settings: A State-of-the-Art Review," *Drugs*, vol. 85, no. 2, pp. 127–147, Feb. 2025, doi: 10.1007/s40265-024-02131-3.

[4] T. Cernuschi *et al.*, "The quest for more effective vaccine markets – Opportunities, challenges, and what has changed with the SARS-CoV-2 pandemic," *Vaccine*, vol. 42, pp. S64–S72, Apr. 2024, doi: 10.1016/j.vaccine.2022.07.032.

[5] L. M. Marsden and M. Mazur, "Balancing Innovation and Equity: A Successful Dynamic Between Private and Public Sectors Is Essential to Ensure True Pandemic Influenza Preparedness," *Vaccines*, vol. 13, no. 11, p. 1078, Nov. 2025, doi: 10.3390/vaccines13111078.

[6] S. B. Alahabadi, "An intelligent drug supply chain management and recommendation framework using blockchain and TRPO-driven multi-agent learning," *Sci Rep*, vol. 16, no. 1, p. 26622, Jun. 2026, doi: 10.1038/s41598-026-56991-8.

[7] "Waste 4.0: Blockchain-Enabled Peer-to-Peer Communication Among Medical Waste Stakeholders." Accessed: Oct. 15, 2026. [Online]. Available: https://www.mdpi.com/2071-1050/18/9/4558

[8] Z. K. Sagawa *et al.*, "Safety and immunogenicity of a thermostable ID93 + GLA-SE tuberculosis vaccine candidate in healthy adults," *Nat Commun*, vol. 14, no. 1, p. 1138, Mar. 2023, doi: 10.1038/s41467-023-36789-2.

[9] S. K. Palit, M. Chakraborty, and S. Chakraborty, "Design, formal verification, and security analysis of SCMChain: A lightweight blockchain-based authentication protocol for IoT-enabled supply chain management," *Peer-to-Peer Netw. Appl.*, vol. 18, no. 6, p. 298, Oct. 2025, doi: 10.1007/s12083-025-02141-2.

[10] K. Biswas, V. Muthukkumarasamy, G. Bai, and M. J. M. Chowdhury, "A reliable vaccine tracking and monitoring system for health clinics using blockchain," *Sci Rep*, vol. 13, no. 1, p. 570, Jan. 2023, doi: 10.1038/s41598-022-26029-w.

[11] "Artificial Intelligence and Blockchain Integration in Business: Trends from a Bibliometric-Content Analysis | Information Systems Frontiers | Springer Nature Link." Accessed: Oct. 15, 2026. [Online]. Available: https://link.springer.com/article/10.1007/s10796-022-10279-0

[12] J. Beckmann *et al.*, "The WHO-ISoP Pharmacovigilance Curriculum: 2026 Update," *Drug Saf.*, Sep. 2026, doi: 10.1007/s40264-026-01717-y.

[13] F. Xiao, J. Huang, J.-X. Huang, H. Ren, and L. Li, "Integrating LLM with consortium blockchain for personalized and verifiable online education in higher education," *Int J Educ Technol High Educ*, vol. 23, no. 1, p. 42, Aug. 2026, doi: 10.1186/s41239-026-00618-5.

[14] S. AlSalamah *et al.*, "FairChain: A Trusted and Transparent Blockchain-Based Ecosystem for Drug Development for Nagoya Protocol Implementation," *Electronics*, vol. 14, no. 13, p. 2527, Jan. 2025, doi: 10.3390/electronics14132527.

[15] A. Shabrandi, Ali Rajabzadeh Ghatari, M. Dehghan Nayeri, N. Tavakoli, and S. Mirzaei, "An Intelligent Blockchain-Based System Configuration for Screening, Monitoring and Tracing of Pandemics," *JAIDM*, no. Online First, Sep. 2024, doi: 10.22044/jadm.2024.14379.2541.

[16] S. Periyasamy *et al.*, "Blockchain-enabled collective and combined deep learning framework for COVID-19 diagnosis," *Scientific Reports*, vol. 15, no. 1, p. 16527, 2025.

[17] I. Mutambik, "A Blockchain–IoT–ML Framework for Sustainable Vaccine Cold Chain Management in Pharmaceutical Supply Chains," *Systems*, vol. 14, no. 5, p. 467, May 2026, doi: 10.3390/systems14050467.

[18] R. Latif, B. M. Yakubu, N. S. M. Jamail, A. M. Talib, and F. O. Alomary, "BBAS: A blockchain-based authentication system for e-health with multi-factor authentication, access control, and post-quantum security," *Sci Rep*, vol. 16, no. 1, p. 9163, Feb. 2026, doi: 10.1038/s41598-026-39415-5.

[19] M. A. Naeem, X. Fang, M. S. Iqbal, M. Adnan, and M. I. Ishaq, “A Blockchain-Enabled Vaccine Supply Chain Model Driven by Transfer Learning-Based Sentiment Analysis and Demand Forecasting,” *IEEE Access*, vol. 14, pp. 15362–15378, 2026, doi: 10.1109/ACCESS.2026.3652619.
[20] J. L. Vilas Boas, Y. S. Costa, R. da R. Righi, A. M. Alberti, and J. J. P. C. Rodrigues, “Coldnet: Vaccine Logistics Tracking by Integrating the Internet of Things and Smart Contracts: An Immutable and Reliable Approach,” *Blockchain: Research and Applications*, p. 100386, Sep. 2025, doi: 10.1016/j.bcra.2025.100386.
[21] “Scientific Reports.” Accessed: Oct. 13, 2026. [Online]. Available: https://www.nature.com/srep/
[22] M. N. Hasan, S. Datta, and S. Namasudra, “Blockchain-based pharmaceutical supply chain: a scalable and transparent model for drug traceability,” *Peer-to-Peer Netw. Appl.*, vol. 19, no. 6, p. 139, Sep. 2026, doi: 10.1007/s12083-026-02298-4.
[23] F. Ishengoma, “The potential of blockchain technology in addressing the challenges posed by the COVID-19 pandemic in African developing countries,” *Israa University Journal of Applied Science*, vol. 8, no. 1, pp. 84–108, 2024.
[24] L. Kamal and J. Retna Raj R, “Contextual Zero-Knowledge Authentication with IPFS-Backed Hyperledger Fabric for Privacy-Preserving Blood Supply Chain Management,” *Applied Sciences*, vol. 16, no. 9, p. 4182, Jan. 2026, doi: 10.3390/app16094182.
[25] *FDA/VAERS-Annotations*. (Jun. 08, 2026). Food and Drug Administration. Accessed: Oct. 15, 2026. [Online]. Available: https://github.com/FDA/VAERS-Annotations