Enhancing privacy and traceability of public health insurance claim system using blockchain technology

Andry Alamsyah* and I. Putu Sadhu Setiawan

School of Economics and Business, Telkom University, Bandung, Indonesia

Introduction: The insurance industry has evolved into a global multi-billion-dollar sector, with health insurance gaining prominence due to escalating healthcare costs. This rapid expansion brings heightened risks, including data breaches, fraud, and difficulties in safeguarding sensitive policyholder information. Indonesia's National Health Insurance (NHI)—one of the largest national insurance programs worldwide—covers over 200 million citizens, aiming to provide universal healthcare. However, this extensive coverage raises substantial concerns about data privacy and traceability, particularly during the claim process, as policyholders currently have limited control over and insight into how their data is accessed and used.

Methods: To address these challenges, we propose a blockchain-based model designed to enhance policyholders' private control over data access and improve traceability throughout the NHI claim process. Our approach employs three complementary architectures—functional, logical, and physical—to guide system implementation. The functional architecture is illustrated via a use case diagram that outlines the roles and actions of each participant. The logical architecture employs Business Process Model and Notation (BPMN) diagrams to depict the revised process flow and data movement, while also incorporating a layered design concept. The physical data architecture provides a class diagram detailing data structures and actor relationships. A proof-of-concept prototype was developed to demonstrate the core functionalities of the new system.

Results: By integrating blockchain technology, our prototype ensures authorized access, bolsters data privacy, and maintains data integrity in the NHI claim workflow. The system's layered design and use of smart contracts guarantee transparent, tamper-proof record-keeping, while parallelized processes in the logical architecture streamline claims handling. Initial tests of the prototype confirm the feasibility and robustness of the proposed solution, illustrating how blockchain can facilitate traceability and preserve confidentiality.

Discussion: The blockchain-based design addresses pressing concerns surrounding data security and accountability in large-scale health insurance systems. It allows policyholders to monitor and control their personal information, reducing the likelihood of unauthorized use. Furthermore, the transparent and immutable ledger enables stakeholders to verify data provenance and transactions, enhancing trust. Future work will focus on

scalability, regulatory compliance, and integration with existing healthcare IT infrastructures to fully realize the benefits of blockchain in national health insurance programs.

1 Introduction

Over the last decade, the insurance industry has rapidly transformed into a global multi-billion-dollar sector, providing financial protection to policyholders during accidents with expenses beyond their financial capability (Amponsah et al., 2022). Technological advancements have further improved the industry, reducing transaction times, enhancing verification and payment processes, and minimizing fraud risks (Loukil et al., 2021). Health insurance has become a critical component due to increasing healthcare costs. For example, the average healthcare spending in the USA in 2021 is $12,914, almost equal to the minimum total annual earnings using federal minimum wage law (U.S. Centers for Medicare and Medicaid Services, 2024). A KFF survey revealed that many individuals resort to sacrificing basic needs, depleting savings, or declaring bankruptcy to cover their medical expenses (Amponsah et al., 2022; Levey, 2024). Consequently, numerous nations have implemented national healthcare protection programs to safeguard vulnerable citizens and assist with medical costs.

Indonesia's National Health Insurance (NHI), managed by Badan Penyelenggara Jaminan Sosial Kesehatan (BPJS Kesehatan, 2024), was established to achieve universal healthcare for the entire community. The NHI covers around 89% of Indonesian citizens as policyholders with assets worth IDR 98.76 trillion in 2022 (Kesehatan, 2022; BPJS Kesehatan, 2024). Since its establishment, the NHI has managed more than 200 million policyholders and cooperated with more than 27 thousand healthcare facilities to provide medical assistance to citizens (BPJS Kesehatan, 2024). The growth of NHI's extensive user base, significant financial assets, and cooperation with external organizations now brings a new challenge. Even though the NHI is using a standardized data management system, a data leak by a user in an online forum exposed 100,000 data samples, including ID numbers, addresses, phone numbers, and emails, potentially costing IDR 600 trillion (Septi Jayanti, 2022; Dimas, 2024). When this issue occurred, policyholders faced difficulties in monitoring whether their data was involved in the leak because there was no official monitoring assistance from the NHI. In the current NHI claim business process, the policyholders are vulnerable to privacy risks, as they cannot control access to their data. The NHI predefined access to policyholder's data at the beginning of their cooperation with the healthcare facility, so only authorized divisions can access the data. This risk can lead to unauthorized access and misuse of policyholder data because the NHI cannot control the data access in healthcare facilities in real-time. Another issue that may occur is data traceability because the policyholders do not have real-time access to their data activity during the NHI claim process. The NHI company must establish a private and traceable system for the NHI claim process to address these issues, given that policyholders

are not directly involved (Kurnia, 2017; Maharani, 2017; Kesehatan, 2014).

Despite being a non-profit institution focused on services and the interests of Indonesian citizens, the NHI company still needs to manage public trust and the organization's reputation. This is crucial because public trust positively influences citizens' willingness to pay premiums, even though NHI membership and premium payment are mandatory (Musdalifah, 2020; Humas BPJS Kesehatan, 2023). Therefore, the NHI company must be able to assure the policyholders of their data privacy and traceability throughout and after the NHI claim process. In this context, blockchain technology emerges as a promising solution. Known for its capabilities in enhancing privacy, security, and traceability, blockchain has demonstrated significant potential in healthcare applications. However, its adoption in large-scale public health insurance systems, especially in developing countries, remains limited. Current implementations often focus on isolated technical aspects without addressing the complexities of multi-stakeholder workflows or regulatory compliance requirements.

This research addresses two key gaps in the existing literature:

1. Limited Integration of Blockchain Technology in National Health Insurance Systems in Developing Countries: While blockchain has been applied in healthcare, its implementation in large-scale government-managed insurance systems like Indonesia's NHI remains underexplored.
2. Lack of Comprehensive Architectural Framework for Privacy and Traceability in NHI Claims: Previous studies often focus on isolated blockchain features, but limited research has been done on developing a unified functional, logical, and physical architectural framework tailored for NHI claim processes.

This study proposes a blockchain-based model that enhances privacy, data ownership, and traceability. It addresses these gaps while aligning with Indonesia's NHI regulatory and operational ecosystem. Various solutions exist to these issues, such as standardized health information exchange portals and distributed cloud databases, which allow policyholders to manage, control, and monitor their data. Nevertheless, blockchain technology offers a more comprehensive solution. Using a decentralized system and cryptography, blockchain forms a secure, transparent, and tamper-proof database that enables robust data access control and traceability (Alamsyah et al., 2023).

Blockchain technology in health insurance shows promising advantages for enhancing security, privacy, and transparency within the industry. It offers a decentralized and tamper-proof record-keeping system to store sensitive data, securely ensuring its integrity and privacy. The traceability feature allows tracking data activity provenance, increasing transparency and auditability. While

FIGURE 1
Existing healthcare treatment and NHI claim process.
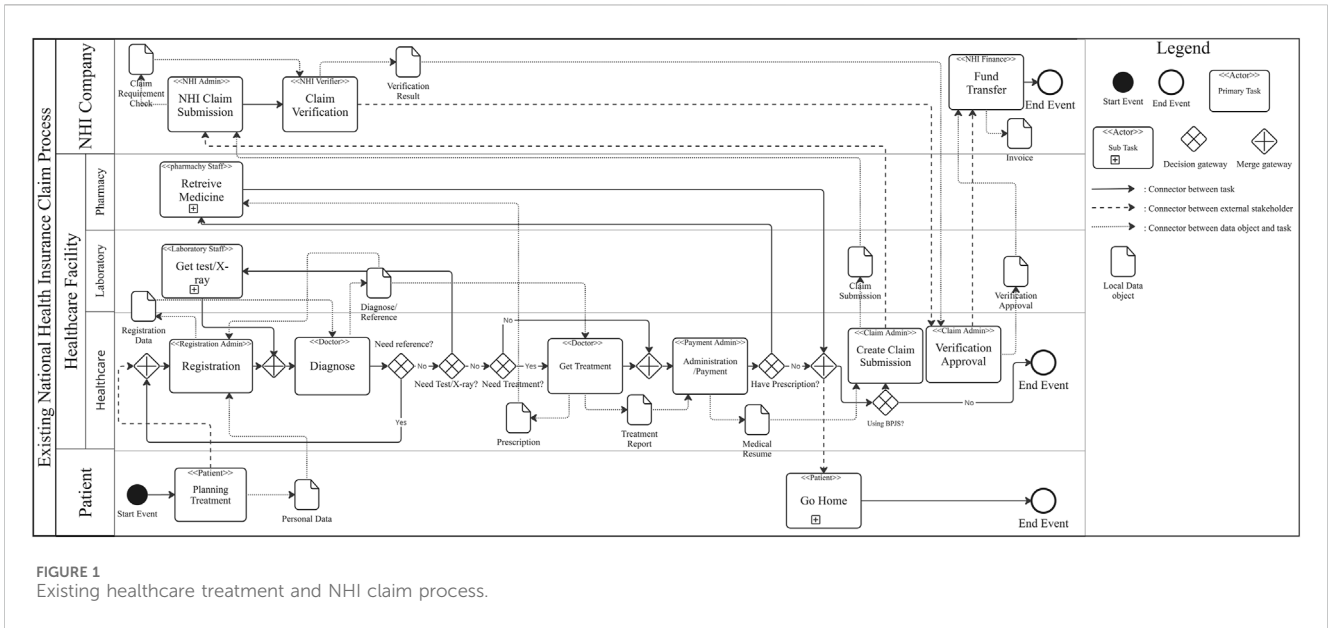
blockchain offers advantageous features and potential benefits in healthcare applications, it is crucial to recognize its limitations as technology develops. Challenges during blockchain implementation, like interoperability with existing systems, may arise (Agbo and Mahmoud, 2020). Hence, a proper protocol is essential for seamless integration between the existing system and blockchain technology. Another issue is scalability and speed when processing high data volumes, such as healthcare data, which may cause severe performance degradation. One solution for this issue involves using blockchain solely as an indexed reference for healthcare data, storing condensed data and access information, while the comprehensive healthcare data resides off-blockchain. The first application of blockchain is in the finance industry, such as cryptocurrencies facilitating peer-to-peer transactions, and throughout its development, the application becomes broader. For example, blockchain applications in the human resource industry allow employers to verify talent reputations through a decentralized autonomous organization (DAO) (Sulaiman et al., 2022). Blockchain technology implementation using smart contracts also helps to shorten health insurance transaction time by cutting the lengthy bureaucratic process (Sutanto et al., 2022). Additionally, one study shows that the blockchain application can adapt to data protection regulations such as the General Data Protection Regulation in Europe (GDPR) (Zheng et al., 2018).

The blockchain application in public health demonstrates promising outcomes for safeguarding patient data privacy and security, particularly in emergencies (Rajput et al., 2019). With smart contracts, authorized access to patient medical records is enabled, with predetermined and time-limited authorization during emergencies. The experiment demonstrates that blockchain application ensures the security of sensitive patient Personal Health Record (PHR) data, offering time efficiency, privacy, accessibility, and granular access control management. In the national health insurance industry, blockchain technology improves stability by mitigating fraud risk, enhancing communication efficiency, and ensuring transparency, privacy,

and security (Amponsah et al., 2022). Integrated with cloud-based data storage and management, the blockchain model optimizes claims processing, controls data access, and potentially shortens processing and payment periods. However, other influential factors, such as information quality, service quality, and user satisfaction, are crucial for successfully implementing the cloud blockchain-based solution. This study uses blockchain technology to propose a data-sharing model between stakeholders involved in the NHI claim process. These stakeholders are the patient or policyholders, the healthcare facility or clinic, the pharmacy, and the NHI.

Overall, we proposed a blockchain adaptation model to answer the privacy and traceability vulnerability issues during the NHI claim process conducted by the healthcare facility and the NHI company. We developed the new model by conducting interviews with stakeholders involved in the NHI claim process and reviewing related literature and research. This research contributes to the industry and company by providing an approach to enhance data privacy and traceability in public health insurance systems through the adaptation of blockchain technology. The proposed blockchain adaptation in the NHI system must ensure the stakeholders' data security, privacy, and traceability while providing a seamless performance with the existing system integration and compiling with the local data protection regulation. We organized the paper into literature review in Section 2, research methodology in Section 3, research result in Section 4, discussion in Section 5, and conclusion and suggestion in Section 6.

2 Existing NHI claim process and related research

2.1 Existing NHI claim process

The NHI claim process reimburses the healthcare facility for the treatment policyholders have received (Kesehatan, 2014). After the

policyholders receive the medical treatment, the healthcare facility must submit the NHI claim within a specific time limit. Once the NHI company verifies the claim, it must pay the healthcare facility based on the agreed amount. Figure 1 illustrates the current NHI claim and healthcare treatment processes, including the actor managing the task. The process also includes the optional treatment without insurance, which requires the patient to pay fully for the medical treatment. We categorize the stakeholders into three based on their affiliation: the patient or policyholders, the healthcare facility, and the NHI company. The healthcare facility also stores physical and digital data in the health facility database archive. After treatment, healthcare providers must upload the medical records to the National Ministry of Health central database, and upon completion of the NHI claim process, they must upload the claim to both the National Ministry of Health central database and the integrated NHI company application (Kementerian Kesehatan Republik Indonesia, 2019; Kesehatan, 2018). The healthcare facility also stored the hardware and software data in the health facility database archive. Figure 1 shows the data output of each step during the healthcare treatment and NHI claim process. We explain the detailed process of healthcare treatment, and NHI claims in non-emergency conditions as follows (Kurnia, 2017; Maharani, 2017; Kesehatan, 2014):

1. The patient plans treatment and prepares the required documents, such as identity, NHI card, and reference.
2. To use the NHI, the patient must register their treatment at a first-level healthcare provider cooperating with the NHI company.
3. The doctor then diagnoses the patient, and they can get treatment directly or a reference to a laboratory or an advanced healthcare facility. If the doctor references the patient to an advanced healthcare facility, they must repeat the first two steps. The patient must be re-diagnosed when recommended to the laboratory to determine the appropriate treatment.
4. In the treatment process, patients can skip the treatment and only get a prescription.
5. The patient finishes the treatment's final administration process, which the payment admin manages. In this process, the patients only pay when they do not use the NHI or have non-covered treatment.
6. After the final administration, the patient can claim the medicine if given a prescription or go home directly.
7. The healthcare facility will submit the NHI claims on behalf of the patient to get reimbursed for the treatment. Only the healthcare facility and the NHI company can track the claim status during this process. In this process, the healthcare facility uploads the required documents via the integrated application and sends supporting physical documents.
8. The NHI admin will verify the required document's completeness. If the required documents are complete, the NHI admin will notify the healthcare to complete them.
9. After completing the required document, the NHI verifier will verify the document content and determine the covered amount. The NHI then notifies the healthcare and requests their agreement on the covered amount.
10. If the healthcare company agrees with the covered amount, the NHI finances will send the reimbursement directly to the healthcare bank account and send them proof of delivery.

2.2 Literature review

2.2.1 Blockchain technology

Blockchain is a decentralized ledger technology distributed across connected nodes in a peer-to-peer network (Bashir, 2018; Chilamkurti and Balamurugan, 2021). The term "blockchain" originated from storing public transaction data in a growing list of blocks linked together through mathematical procedures. The blockchain has several attributes (Alamsyah et al., 2023; Tanwar, 2018). First is the stored information in the block, and second is the hash function, which is a function that remains in each block while identifying that the information contained in the block has not been changed. There is also block information, such as block version number and timestamp. Furthermore, the last is the consensus, which will verify each block on the network through a specific mechanism, i.e., proof-of-work or proof-of-stake. The attributes establish the blockchain characteristics: immutable data recorded on the block, transparency between the network members, and privacy through anonymity or pseudonymity (Alamsyah et al., 2023; Chilamkurti and Balamurugan, 2021; Alamsyah et al., 2022). The decentralized system on the blockchain network allows stakeholders to reduce costs on the central authority. The blockchain technology has drawn researchers across various domains in recent years. Studies affirm its applicability in multiple industries, such as health insurance (Amponsah et al., 2022), healthcare system (Rajput et al., 2021), education (Sulaiman et al., 2022), and food supply chain (Alamsyah et al., 2023; Alamsyah et al., 2022). Blockchain technology can give several advantages to the insurance claim process. First, the permissioned blockchain allows the system to enable an access control feature so the data owner can control the data access (Zheng et al., 2018). This system can protect the policyholder's private information from unauthorized access, for example, outside the insurance claim process or the specified division. Second, blockchain allows the data to use pseudonyms, allowing data identification without exposing private information (Chilamkurti and Balamurugan, 2021). Third, the traceability feature can help the stakeholders trace the insurance claim process and the data activity along the treatment and insurance claim process to verify its integrity (Sulaiman et al., 2022; Rajput et al., 2021).

Blockchain applications in the insurance industry can also help with fraud prevention, efficient data management, expedited claims, transparent audits, data privacy protection, and traceable data activity (Amponsah et al., 2022; Sutanto et al., 2022). Sutanto et al. provide a blockchain model to shorten the insurance claim authentication time and cut the bureaucracy's long steps using smart contracts (Sutanto et al., 2022). They employ a Unified Modeling Language (UML) diagram to depict the model design, subsequently implementing it within the Vexanium blockchain ecosystem. The new model allows patients to control their electronic medical records and share them with doctors and insurance companies. The research shows cost reduction using an efficient and standardized automated system. Amponsah et al., on the other

hand, proposed an access control system between the patients, healthcare providers, and other stakeholders to prevent the National Health Insurance Schemes (NHIS) from falling financially due to fraud and other significant threats (Amponsah et al., 2022). They implement the model using the DeLone and McLean Information Systems Success Model, allowing the patient to control the access to their data. The researchers showed that the proposed model would protect the NHI's financial stability, guaranteeing that beneficiaries receive the benefits of universal health coverage. Based on the mentioned blockchain application, blockchain technology can also solve the NHI's privacy and traceability issues by allowing access control, pseudonymity, and data traceability to maintain the policyholder's trust in the company.

Blockchain technology has witnessed remarkable advancements, expanding its applications across various domains, including IoT networks, privacy-preserving architectures, and robust security frameworks. These developments have demonstrated blockchain's potential to address critical issues such as data integrity, transparency, and trustless operations. For instance, integrating blockchain with Internet of Things (IoT) devices has shown promise in enabling secure device-to-device communication, minimizing vulnerabilities caused by single points of failure, and enhancing overall system resilience (Yun et al., 2022). Similarly, combining fog computing with blockchain has enabled low-latency data processing and privacy-preserving mechanisms in environments requiring real-time data validation and secure storage (Dave et al., 2022). Furthermore, extensive research into blockchain security protocols has strengthened mechanisms to counter vulnerabilities like Sybil attacks, double-spending risks, and consensus failures (Sharma et al., 2021). Despite these notable advancements, the practical application of blockchain technology in large-scale healthcare systems, particularly health insurance claim processes, remains underexplored. While existing studies provide valuable insights into blockchain's potential in securing data exchanges, enhancing privacy, and ensuring trust across decentralized systems, they often focus on isolated use cases or sector-specific challenges. Healthcare insurance systems, such as Indonesia's NHI claim process, pose unique challenges, including multi-stakeholder coordination, regulatory compliance, and scalability in managing vast datasets across distributed networks. This study seeks to bridge these gaps by integrating blockchain's proven capabilities—such as off-chain storage (IPFS) for handling large datasets, Attribute-Based Access Control (ABAC) for ensuring secure and role-specific data access, and stakeholder traceability mechanisms to maintain accountability across the claim lifecycle. By leveraging these advancements, the proposed blockchain-based model aims to address scalability, privacy preservation, and real-time synchronization requirements, positioning itself as a tailored solution for managing healthcare claims efficiently in a complex, multi-stakeholder ecosystem.

Blockchain technology offers significant benefits, but its scalability remains a key limitation, particularly when handling real-time transactions involving large volumes of data (Alamsyah et al., 2023). A solution to blockchain scalability has been developed through the integration of blockchain technology with hybrid databases, which combine elements of centralized and distributed storage systems (Alamsyah et al., 2022; Safak et al., 2019; Ge et al., 2022). For example, A study shows the implementation of the

FIGURE 2
Research workflow.
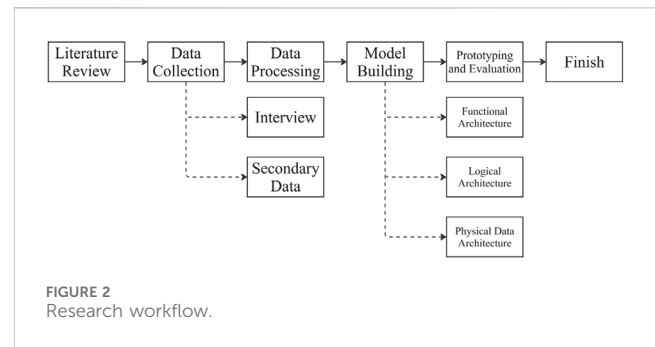
Hyperledger Fabric blockchain with a NoSQL database called MongoDB (Yun et al., 2022). They combine them by synchronizing the blockchain block data with the central database, increasing speed and performance. Another example is the research to solve blockchain scalability issues by combining blockchain technology with a distributed database (Alamsyah et al., 2022). They integrate blockchain with a distributed file system, InterPlanetary File System (IPFS), for data storage. They linked the IPFS address to the blockchain for seamless data referencing. The model can avoid scalability issues in heavy network traffic. The hybrid database comparison with the blockchain database model also shows that the hybrid database can provide higher transactions per second (TPS) (Dave et al., 2022).

2.2.2 Blockchain privacy and traceability

Blockchain technology ensures data privacy by allowing a secure sharing system between the stakeholders (Rajput et al., 2021; Pawar et al., 2022). Research shows the implementation of blockchain technology in a data-sharing system in emergency healthcare treatment (Rajput et al., 2021). They use an access control system, allowing the predefined authorized actor to access the patient's personal health record in case of an emergency condition. The research utilizes a Hyperledger Composer blockchain, allowing the data owner to set access rules for authorized staff members and specifying time-limited permissions to retrieve current information from the PHR. The proposed system improves the security and accessibility of PHR data while ensuring enhanced privacy and traceability. However, the model still needs a standardized data-sharing regulation like HL7 FHIR to guarantee data-sharing security because the PHR is shared among different agencies. Blockchain technology can also ensure data traceability, maintaining data activity integrity. Omar et al. combine blockchain and cloud storage to provide a privacy-friendly healthcare data platform. Their research proposes a secure, private, accountable, and pseudonymous system (Al Omar et al., 2019). The proposed model employed the *Medibloc* blockchain, allowing only authorized parties to access the data while protecting the patient's real identity by exchanging them as a dynamic key. Blockchain can also safeguard privacy and security when combined with modern devices (Pawar et al., 2022). The model integrates with medical IoT services such as smartwatches, pill bottles, and activity trackers to gather real-time patient data. They implement the model using Hyperledger Fabric as a blockchain platform to store personal health data obtained from devices like the *Qardioarm* blood pressure monitor, RENPHO digital weighing scale, and the Google Fit application.

TABLE 1 Literature review source and categories.

Source	Categories		
	Health and insurance	Supply chain	Others (blockchain, data management, human resources, education)
Elsevier	Al Omar et al. (2019), Amponsah et al. (2022), Zhu et al. (2021)	Alamsyah et al., 2023	
IEEE	Zheng et al. (2018), Rajput et al. (2019)		Besancon et al. (2019), Sulaiman et al. (2022), Zhu et al. (2023), Harris (2023)
MDPI	Rajput et al. (2021), Sutanto et al. (2022), Ghosh et al. (2023)	Alamsyah et al. (2022)	Safak et al. (2019), Khan et al. (2021)
ACM Digital Library			Ge et al. (2022), Androulaki et al. (2018)
Springer	Pawar et al. (2022)		Alamsyah and Syahrir (2023)
Others	Kurnia (2017), Musdalifah (2020), Agbo and Mahmoud (2020)		Baliga et al. (2018), Brophy (2020), Mardiansyah and Sari (2022)

Nevertheless, the model still needs more development to add an interoperability layer for sharing personal health data with external electronic health record systems.

Blockchain technology also ensures data transparency across various data activities by enabling traceability mechanisms. The traceable data encompasses a wide range, from tangible items like coffee and meat (Alamsyah et al., 2023; Alamsyah et al., 2022) to intangible information such as personal health records and education certificates (Sulaiman et al., 2022; Rajput et al., 2021). A research from Alamsyah et al. proposed a traceability model for the coffee industry supply chain using blockchain technology (Alamsyah et al., 2023). The system allows the stakeholders to trace the coffee production information from sensors or data collection procedures only by scanning a QR code to access the tracker. Using smart contracts and the Polygon blockchain, the proposed system allows the stakeholders to trace back the product's originality, components, or locations in the supply chain.

On the other hand, Zhu et al. offer insights into using blockchain for tracing intangible objects such as infectious diseases (Zhu et al., 2021). The proposed model shares disease-related details like case information, checkup reports, and abnormal reports on the blockchain network. Subsequently, it triggers an early warning across the network via smart contracts. The simulation shows that the proposed model can work efficiently while greatly enhancing infectious disease information security, storage, query efficiencies, authenticating authorized nodes for diverse data operations, alleviating central database issues, and enabling more coordinated management of infectious disease information across all levels.

3 Methodology

This research employs a qualitative method, combining a literature review from reputable publications and interviews with stakeholders involved in the NHI claim process to explore the adaptation of blockchain technology in NHI's claim system. The research methodology is divided into several stages, as shown in

Figure 2: literature review, data collection, data processing, model building, prototyping, and evaluation.

3.1 Literature review

We examined previous studies on the NHI claim process and blockchain technology in the literature review stage. We sourced articles from reputable publishers like Elsevier, Springer, IEEE, MDPI, Scopus, Google Scholar, and Semantic Scholar. We used keywords related to blockchain adaptation in insurance and other industries, data exchange, security, privacy, and traceability. Additionally, we explored the potential of blockchain technology in the industry, including its integration with modern devices and hybrid database systems. The data collection stage involved gathering insights from interviews with stakeholders directly involved in the NHI claim process. Finally, in the model-building stage, we synthesized the collected data to design a blockchain-based system that addresses the identified challenges in the NHI claim process.

We categorized the gathered articles based on their source and industries, as shown in Table 1. The articles include blockchain applications in healthcare, insurance, supply chain, data management, human resources, and education. We also focused on articles related to data privacy, traceability, and blockchain integration with modern technologies. We applied several research questions to filter the literature review that was fitted for the model construction. We listed the question as follows:

1. How does blockchain implementation work in public health, health insurance, and the public health insurance industry?
2. What blockchain features support personal health data privacy and traceability protection?
3. How do the blockchain features protect personal health data privacy and traceability?
4. What are the essential requirements of a blockchain platform compatible with the new model?

TABLE 2 Design system criteria.

Criteria	Description
Security	Authorized users and policyholders exclusively control access to policyholder data and authorization
Privacy	The system ensures policyholder privacy by anonymizing information during unauthorized data exchanges
Traceability	Users can track data activity details, including origin time, source, previous activities, involved actors, and data modifications

What are the challenges and issues that may arise in the blockchain implementation?

3.2 Data collection

In the data collection stage, we conducted interviews with stakeholders involved in the NHI claim process to gain insights into the business process. The interviewees were selected from three key divisions: first-tier healthcare data verifiers, advanced-tier data verifiers, and claim payment administration staff. First-tier healthcare data verifiers, for instance, handle claim verification at facilities such as clinics, public health centers, and small hospitals.

Interview questions were designed to address critical aspects of the NHI claim process, including the following:

1. What is the overall process for insurance claims through healthcare at facilities that collaborate with the NHI company in detail?
2. Which stakeholders and data are involved in the NHI claim process?
3. How do the stakeholders determine whether the policyholders are secure and have their privacy protected during the healthcare and insurance claim process?
4. Does the current system allow policyholders to control their data access, know the authorized actors, and trace their data activities?

The interview data were analyzed using thematic analysis to identify recurring patterns and insights. Transcripts were imported into NVivo software for systematic coding and theme identification. An inductive coding approach was applied, involving: 1) open coding to capture meaningful segments of text, 2) grouping similar codes into categories, and 3) refining categories into broader themes. Key issues identified included data privacy, traceability, and operational challenges. Themes were further categorized into: 1) stakeholders' concerns about unauthorized data access, (2) inefficiencies in the current claim process, and 3) requirements for a transparent and secure data system. This approach ensured a comprehensive analysis of diverse perspectives to inform the design of the proposed blockchain-based model.

In addition to interviews, secondary data was gathered from official NHI business publications and previous research studies. These sources included administrative guides, application manuals, and reviews of hospital medical records for NHI claims. The combination of interview findings and secondary data provided a detailed understanding of the NHI claim business process, aiding in the construction of the adapted model depicted in Figure 1.

3.3 Model building

In the model building stage, we build the blockchain version of the NHI claim system model. We adopt Model-Based System Engineering (MBSE) and divide it into functional, logical, and physical data architectures based on the existing business process (Fernandez and Hernandez, 2019). We use a use case diagram to depict the functional architecture and show the actor's behavior. The logical layer bridges the functional and physical data architectures, indicating the abstract interaction of the actors, application, database, and blockchain network using a Business Process Model and Notation (BPMN) and custom process design. Using a UML class diagram, the physical data architecture will show detailed interaction between actors.

Table 2 shows that we designed a model to facilitate secure, private, and traceable data exchange among NHI claim stakeholders during healthcare treatment and the NHI claim process. We achieve data security by employing a permissioned blockchain with access controls, allowing policyholders to manage data access. The new model also ensures that the policyholders own their data so only they can access and control it. Policyholders can preset the authorizations for the entire process to ensure convenience, rendering data inaccessible once it concludes. Users must request permission from the policyholder to access data outside the authorized process. This system enhances data security and privacy by preventing unauthorized access to the data. The new system also enhances policyholder privacy by enabling data owner's unique "userIDs." This system allows the authorized actor to access the data pseudonymously. We also proposed a data traceability feature, allowing the stakeholders to evaluate whether the data activity is authorized by tracing them along the process.

3.4 Blockchain platform selection, prototyping and evaluation

The selection of an appropriate blockchain platform is a critical step in developing a robust system for enhancing privacy and traceability in the National Health Insurance (NHI) claim process. In this study, we establish a set of criteria to guide the selection process, ensuring alignment with the unique requirements of Indonesia's NHI system. These criteria include transaction speed, which must support high transaction throughput to accommodate the large volume of daily claims; privacy and access control, ensuring sensitive policyholder data is protected through permissioned access; cost efficiency, minimizing operational expenses such as gas fees; scalability, allowing the system to handle future growth in both data volume and user participation; and ecosystem maturity,
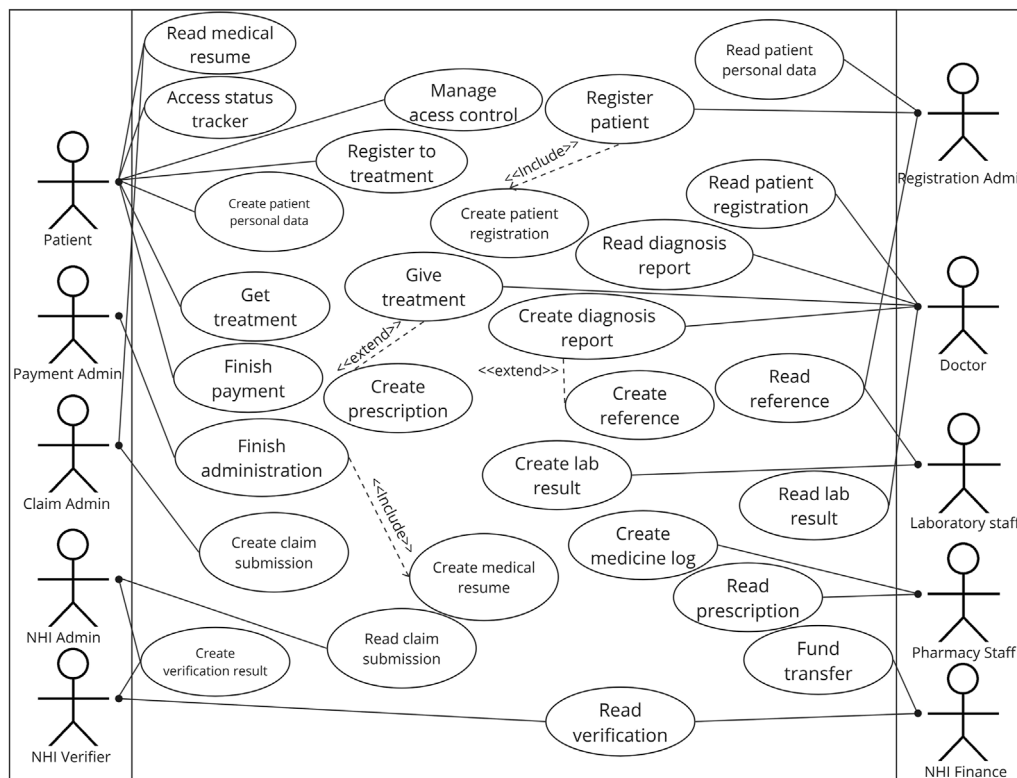
FIGURE 3
Proposed healthcare and NHI claim functional architecture in A use case diagram.

emphasizing platforms with a strong developer community and proven industry adoption.

We conduct a comparative analysis using these predefined criteria to systematically evaluate potential blockchain platforms. Platforms like *Hyperledger Fabric, Ethereum,* and *Corda* are examples of enterprise-grade blockchain solutions commonly used in the healthcare and financial sectors. However, at this stage, no specific platform is selected. Instead, the focus remains on identifying how each platform aligns with the system requirements and assessing its potential advantages and limitations. After evaluating each platform's performance against these criteria, the final selection will be justified in the Discussion section (Chapter 5).

Following establishing these criteria, the prototyping phase focuses on developing a prototype to simulate the functionality and performance of the proposed blockchain model. The prototype includes a mobile application interface designed to demonstrate the practical implementation of the system's core capabilities. The development process ensures that the prototype meets functional and usability requirements. The design draws inspiration from existing applications to simulate real-world scenarios, allowing stakeholders to interact with the system realistically. Key features such as data access control, traceability mechanisms, and privacy protection are integrated into the prototype to address the primary objectives of the system.

In the evaluation phase, we gather stakeholder feedback through interviews and usability tests involving representatives from healthcare providers, NHI administrators, and technical staff.

This phase evaluates key performance indicators such as transaction speed, latency, and data traceability accuracy while assessing the system's overall usability and user experience. Feedback collected during this phase helps identify usability challenges and provides insights for further prototype refinement to ensure alignment with the stakeholders' needs and expectations. The results from the prototyping and evaluation phases will serve as the foundation for the final blockchain platform selection, presented in the Discussion section (Chapter 5). This approach ensures a structured, transparent, and evidence-based methodology for selecting and evaluating Indonesia's NHI system's most suitable blockchain platform.

4 Result and analysis

In this section and the following subsections, we introduce our proposed blockchain-based NHI claim model and lay the foundation for its discussion. The section is structured into four key parts: 1) the criteria for the new model, 2) its architectures (functional, logical, and physical data architectures) along with their properties, 3) the prototyping phase showcasing the system's key features, and 4) the evaluation phase presenting feedback from stakeholders.

The functional architecture, illustrated in Figure 3, uses a use-case diagram to depict the behavior of each actor involved in the treatment and NHI claim process. The system involves 10 primary actors, including patients, registration admins, doctors, payment

TABLE 3 Stakeholder roles and responsibilities.

| Actor/Stakeholder	Role	Blockchain interaction
Patient (Policyholder)	Data owner	Controls access permissions and monitors traceability
Registration Admin	Data Registrar	Inputs initial patient registration data securely
Doctor	Data Contributor	Uploads treatment details, diagnosis reports, and referrals
Laboratory Staff	Data Input Specialist	Uploads lab results securely to the blockchain
Pharmacy Staff	Data Contributor	Logs prescription details and medication usage securely
Payment Admin	Financial Executor	Executes smart contract-based payments for reimbursements
Claim Admin	Claim Validator	Cross-verifies claims and supporting documents
NHI Admin	Compliance Auditor	Monitors claim compliance, ensures regulatory alignment
NHI Verifier	Claim Approver	Grant final claim approval after review
NHI Finance	Financial Oversight	Oversees financial transactions, audits reimbursement logs
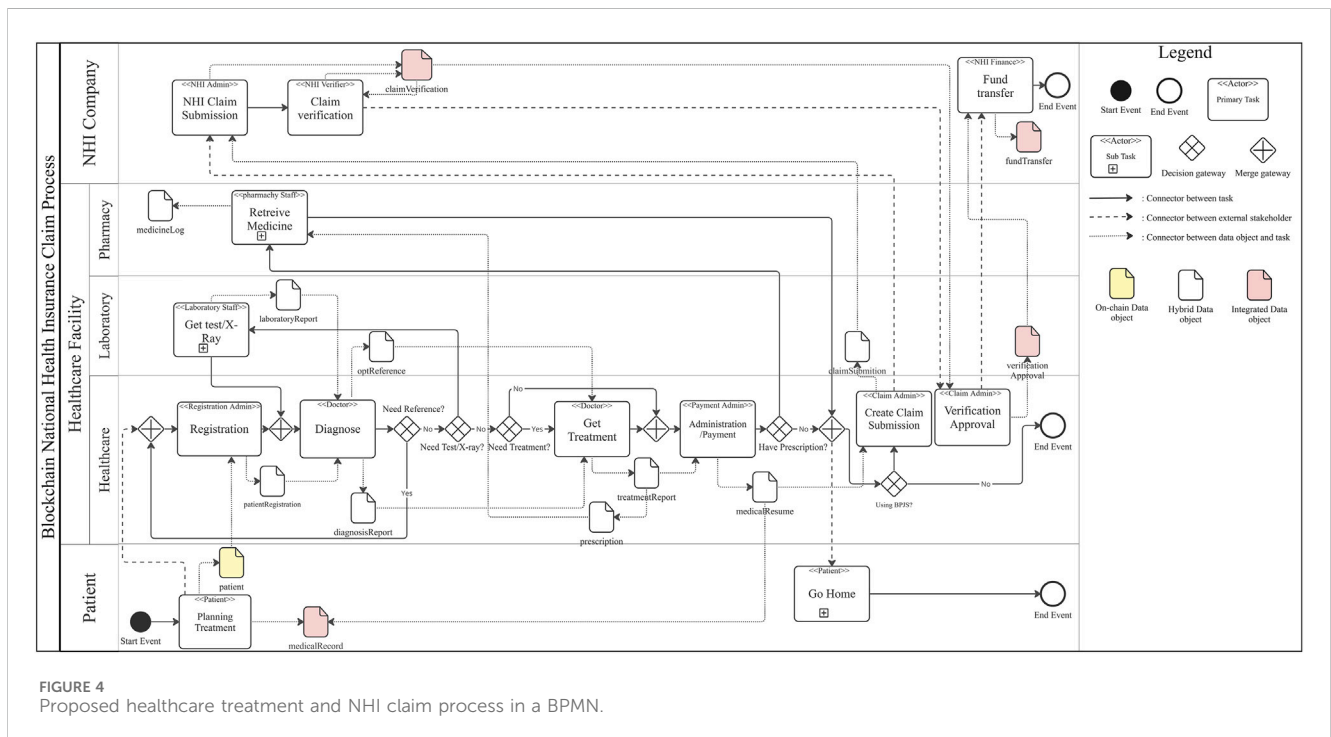
FIGURE 4
Proposed healthcare treatment and NHI claim process in a BPMN.

admins, claim admins, laboratory staff, pharmacy staff, NHI admins, NHI verifiers, and NHI finance teams. Each actor plays a specific role in handling data entry, transactions, verification, and auditing, ensuring seamless coordination across the system. While their responsibilities align closely with the existing NHI claim process, the blockchain integration introduces new functionalities, such as managing access control and tracking patient or policyholder data activities.

For instance, patients can now control who accesses their data and monitor real-time activities on their records. Certain actions in the workflow are mandatory, while others are conditional, depending on specific scenarios. This is visually represented by the <<include>> and <<extend>> dotted-line arrows in the diagram. For example, after the payment admin completes the

patient registration, they must create a medical resume <<include>>, whereas a doctor can create a reference report <<extend>> if deemed necessary following a diagnosis.

It is essential to clearly define each actor's roles and responsibilities to ensure seamless integration and efficient operations within this ecosystem. Each actor interacts with the blockchain system via dedicated interfaces, such as dashboards or mobile applications, and performs specific tasks to ensure data integrity, traceability, and transparency across the claim lifecycle. Table 3 outlines each actor's roles, responsibilities, and blockchain interactions in the NHI claim process.

To demonstrate the practical application of the proposed blockchain-based NHI claim system, we present specific real-world use cases that cover the interactions of stakeholders across
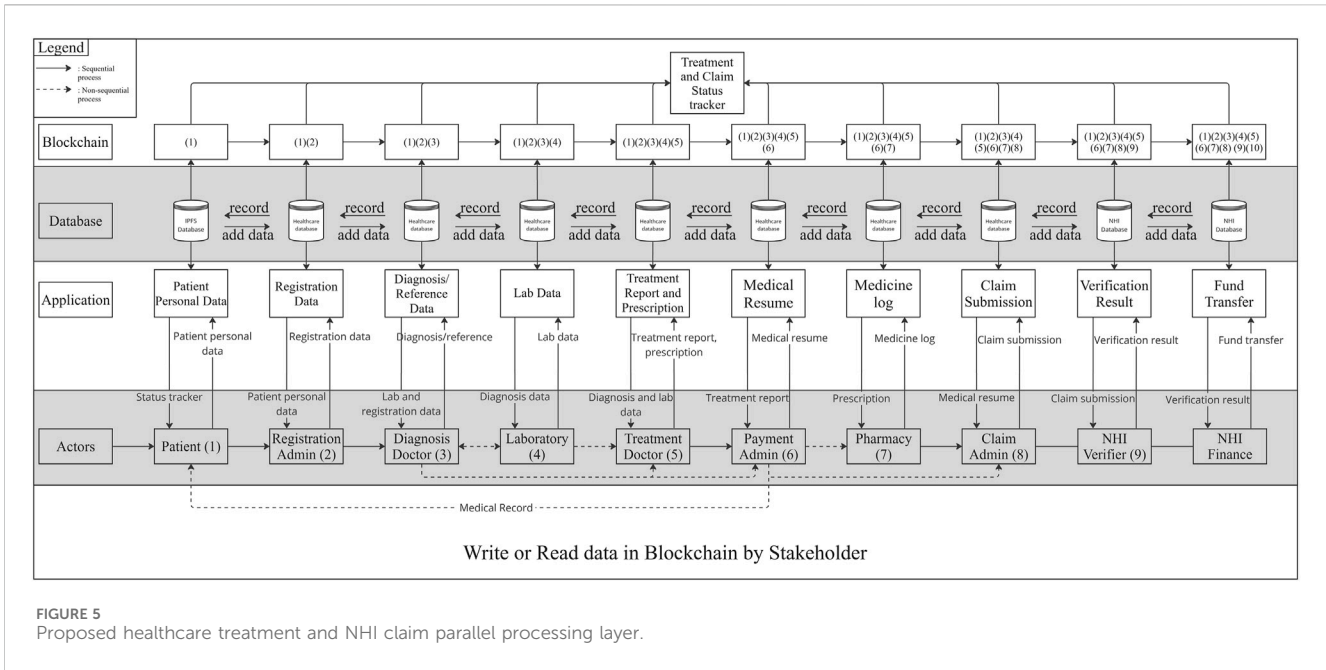
FIGURE 5
Proposed healthcare treatment and NHI claim parallel processing layer.

TABLE 4 Data type based on location.

Categories	Location
On-chain	IPFS database
Hybrid	Local database (NHI company or healthcare facility database)
Integrated	IPFS, local database (NHI company or healthcare facility database)

various phases of the NHI claim process, from claim submission to reimbursement. Use Case 1: Policyholder Claim Submission and Transparency. A policyholder visits a healthcare facility for medical treatment. The healthcare provider securely uploads medical records and claim details to the blockchain during registration through a decentralized application (DApp). The policyholder can access a traceability dashboard via their mobile application, allowing them to track data access points, view transaction logs, and ensure transparency throughout the claim lifecycle. Blockchain immutability ensures that no data can be altered retroactively. Use Case 2: Claim Verification and Approval by NHI Administrators. Once healthcare providers upload claim details, NHI administrators review and verify the claims via their blockchain interface. The immutable audit trails allow administrators to efficiently cross-verify medical records and treatment details. Smart contracts automate claim validation, significantly reducing manual intervention and processing delays. Use Case 3: Claim Reimbursement and Auditing. After claims are approved, smart contracts execute automated reimbursement processes, transferring funds from NHI accounts to the healthcare provider. Every financial transaction is securely logged on the blockchain, including timestamps, transaction amounts, and involved parties. Auditors can later verify these records for compliance and fraud prevention through the blockchain's transparent architecture.

The logical architecture is shown in Figures 4, 5. The BPMN shown in Figure 4 represents the complex blockchain NHI claim process, which mirrors the existing effective and legally compliant process. The key difference is that the new model stores policyholder data in three separate databases, as shown in Table 4. The layers of parallel processing between actors, decentralized applications (DApps), local databases, and blockchain networks are shown in Figure 5. The layer shows the process sequence indicated by the arrow between the actor and the non-sequential process shown by the dotted arrow. In the new model, the policyholders provide their public key during treatment, and NHI claims to ensure data ownership and control. The authorized actor then encrypts the public key so only the data owner or authorized actor can decrypt the data. The new model allows the actors to create, write, or read the data based on their authorization through an intermediary web/ mobile application. After authorization verification, the application will forward commands from the actor to write or read data from or to the target database via the blockchain network. The custom design also shows the level of actor authorization that is the same as an existing business process, which is indicated by the type of data entering and leaving the actor. The traceability feature in the new model will allow the policyholders and the other stakeholders in the existing business process to trace their data activity.

We present the physical data architecture shown in Figure 6, explaining the data flow recorded in the NHI claim process. Before implementing the new model, the existing system relied on centralized local or cloud databases varying by health facility,

FIGURE 6
Proposed NHI claim physical data architecture in A class diagram.
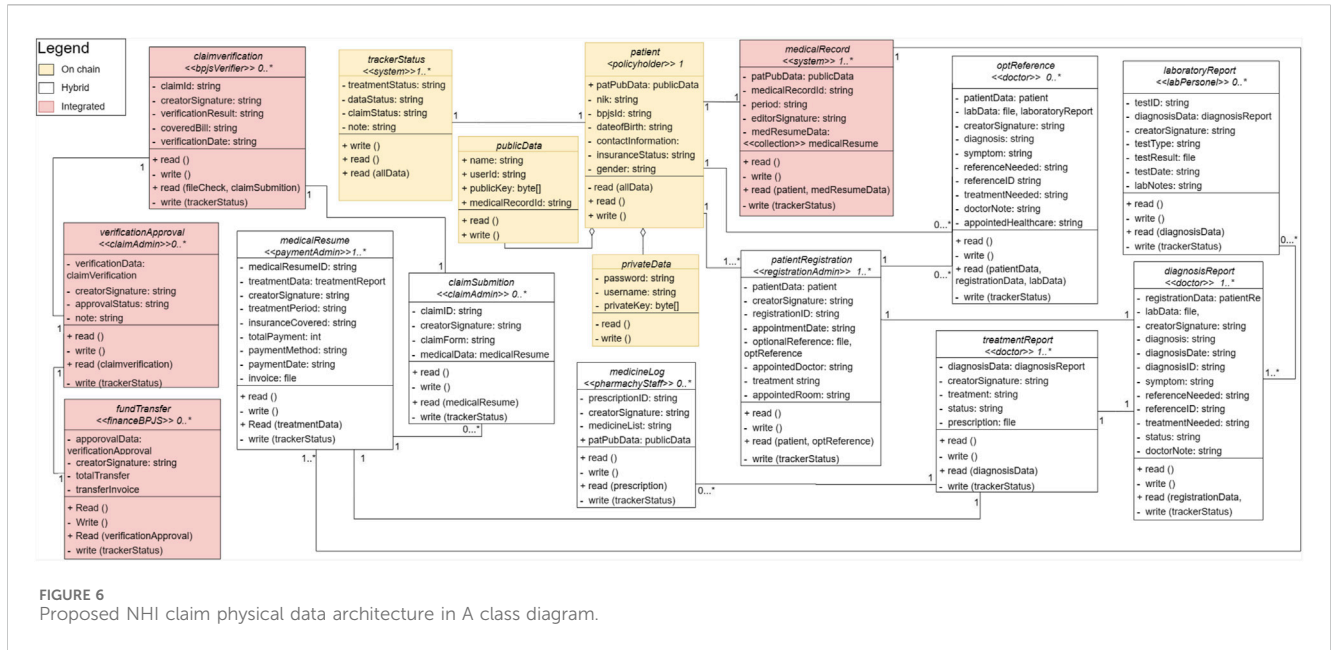
posing security risks like data breaches due to non-standardized data management. The new model categorizes the data type into on-chain, hybrid, and integrated, as shown in Table 3. The system stores on-chain data solely in the IPFS database for integrity assurance. It also utilizes hybrid data types stored in the local BPJS Kesehatan or healthcare facility database. Moreover, the new model stores an integrated data type in IPFS and a local database. The figure also shows the authorized actor managing the data class indicated by the stereotype (<<actor>>) below the class title. The data class attribute shows the information managed in the healthcare treatment and NHI claim process. The attributes also contain compressed information from the other classes differentiated by their data type and signify information as public (+) or private (−). Public information permits access by different classes at any process stage, while private data requires data owner authorization. This categorization ensures policyholder privacy by displaying public information anytime and revealing private details when necessary. The figure shows multiplication to indicate the number of data classes managed per actor and their relationships. Each data class specified the actor's authorization, represented as the write or read method. The actors involved in the medical treatment and NHI claim process can write the data activity on the *trackerStatus* data class through the intermediary application, allowing the stakeholders to monitor and evaluate the data validity. Only the data owner or policyholder has the authorization to read all the data through the tracker status. We explain detailed process and data class managed in the healthcare treatment and NHI claim process as follows:

1. The policyholders manage the patient class, which has an aggregation relationship with *publicData* and *privateData* classes. They can also access the data activity through the *trackerStatus* class. The patient data class includes information about the policyholder's identity. The *publicData* will be visible to anyone in the process as it keeps the policyholder's pseudonymity, and the *privateData* will only be accessible

by the policyholder as the data owner. The *patient*, *privateData*, *publicData*, and *trackerStatus* data will be stored in the IPFS distributed database to ensure data security and integrity.

2. In the registration process, the registration administrator will manage the *patientRegistration* data class, which includes the necessary information regarding the upcoming healthcare treatment process. The *patientRegistration* class also specifies the registration admin's authorization to read the compressed information from the patient and *optReference* class. The one-on-one multiplication indicates the relationship between classes, in which policyholders can only have one *patientRegistration* data at a time and *vice versa*.

3. After the registration, the doctor will conduct a diagnosis, allowing them to create the *diagnosisReport* and *optReference* data class. The *optReference* allows the patient to get the recommended treatment at a better healthcare facility. At the same time, the *diagnosisReport* will guide doctors in treatment or aid laboratory personnel in conducting required tests. The doctor also can read the *laboratoryReport* resulting from the previous laboratory test. The multiplication between the *patientRegistration* and the diagnosis is one-on-one, while with *optReference* and *laboratoryReport* is one-on-zero-or-many, showing that they are optional if needed. The doctor may require further information via lab tests for treatment determination based on the diagnosis result. The lab personnel will manage the test procedure and the *laboratoryReport* data class, allowing them to read the *diagnosisReport* class. The one-on-zero-or-many multiplications signifies that the laboratory test is optional.

4. The doctor conducts the required treatment based on the *diagnosisReport*, *laboratoryReport*, and *optReference* included in the *patientRegistration*. The data output of this process is the *treatmentReport*, which includes a prescription file if required. The *treatmentReport* and *diagnosisReport* have a one-to-one multiplication, limiting one data entry per class.
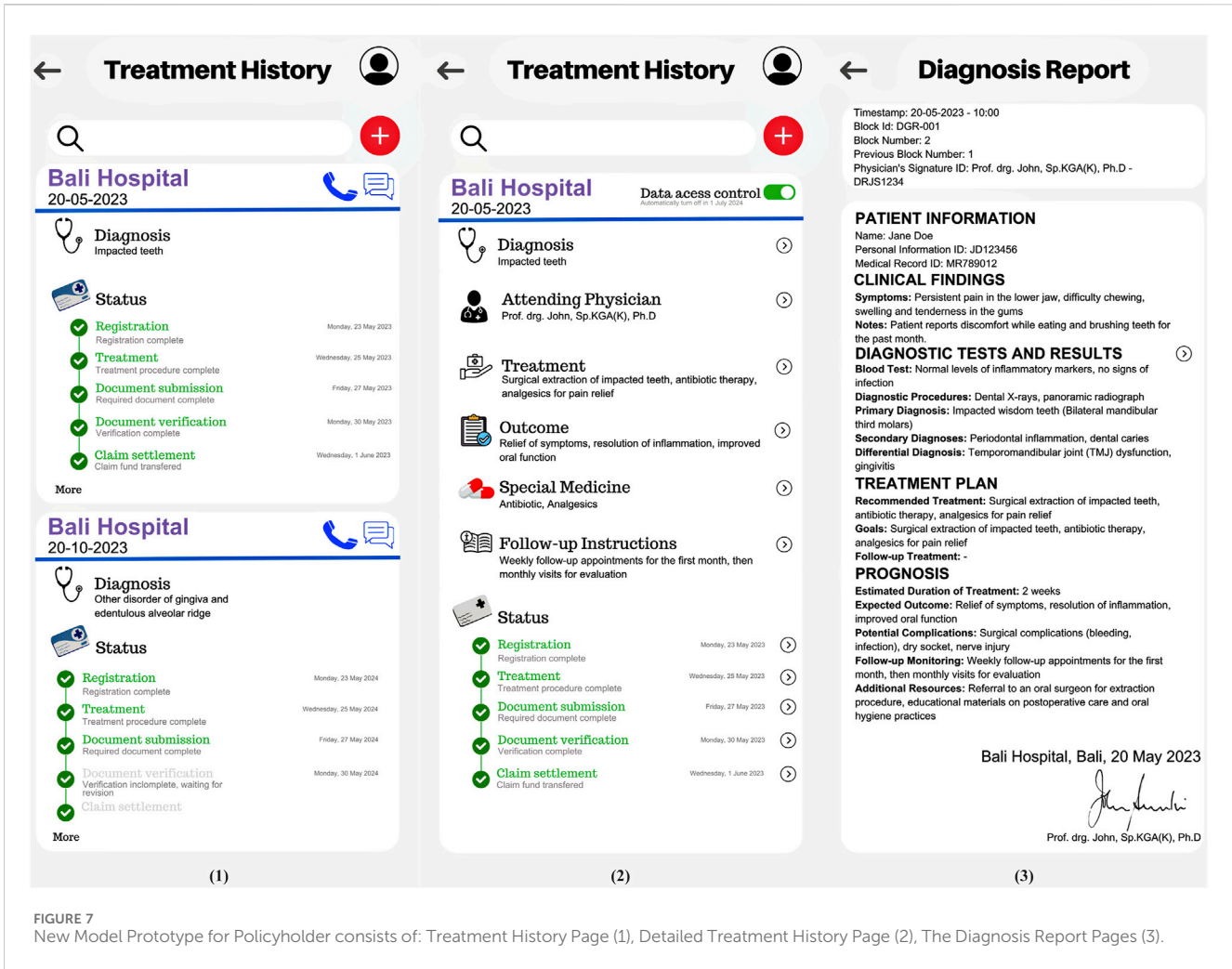
FIGURE 7
New Model Prototype for Policyholder consists of: Treatment History Page (1), Detailed Treatment History Page (2), The Diagnosis Report Pages (3).

5. The patient needs to finish the administration for the treatment, which the payment admin manages. In this process, the patient also determines whether they use NHI. The payment admin then creates the *medicalResume* data class, allowing them to read the *treatmentReport*. Based on their multiplication, each *treatmentReport* can only have one *medicalResume* at a time. After the administration or payment is finished, the patient can go home, and the healthcare facility will carry out any NHI claim process.

6. The system will update the patient's *medicalRecord* data using the *medicalResume* collection of each treatment. The system will store the medicalRecord data in IPFS and a local database as an integrated data type, allowing the healthcare facility to have archives while ensuring data integrity. Each patient can only have one *medicalRecord*, while the *medicalRecord* can consist of at least one-to-many *medicalResume* collection.

7. If the patient gets a prescription during the treatment, they must claim the prescribed medication in the affiliated pharmacy. The pharmacy staff then manages the *medicineLog* data class. Their multiplication indicates that each *treatmentReport* can have a zero-to-one prescription and *medicineLog* data class at a time.

8. The healthcare facility will submit the NHI claim periodically every specific period on behalf of the patient. The claim admin will need to recap the treatment document required for the claim and create *claimSubmission* data through the intermediary application. The claim admin can create zero-to-one *claimSubmission* for each medical resume.

9. The submitted claim needs document verification by the NHI verifier to ensure the policyholder's identity, the required treatment document, and the total claim funds that will be paid. The verifier then creates the *claimVerification* data, which has one-on-one multiplication with the *claimSubmission*. After receiving the verification result, the healthcare facility needs to approve the *claimVerification* data, allowing NHI Finance to transfer the reimbursement treatment payment to the healthcare facility. During the insurance claim process, we categorize the *claimVerification*, *verificationApproval*, and the *fundTransfer* data class as the integrated data type.

Figure 7 shows the new model user interface of the mobile application for policyholders. The application provides access to trace and monitor the policyholder's treatment and insurance claim history. On the treatment history page 1), users can access the

TABLE 5 Blockchain platform recommendation comparison.

Criteria	Blockchain platform		
	Hyperledger fabric	Quorum	Corda
Industry Focus	Cross-industry	Cross-industry	Mainly financial services
Transaction Rate	More than 2000 TPS	Approximately 600 TPS	Approximately 550 TPS
Ecosystem Size	>2000 companies	>400 companies	>900 companies
Scalability	Yes	Yes	Yes
Type	Private	Private	Private
Enterprise Level	Yes	Yes	Yes
Smart Contracts	Programmed in Go Language	Programmed in Solidity	Programmed in Kotlin

comprehensive overview of their currently active and past medical treatments. The detailed treatment history page 2) shows deeper information regarding the specific treatment record. It offers detailed information about the user's medical treatment, including access to documents of each stage of treatment to ensure transparency and integrity. Additionally, the detailed treatment history page allows an access control mechanism, allowing the stakeholders to access the user's personal information, such as medical records, within a limited period of time to safeguard the user's privacy. The diagnosis report pages 3) serve as example documents accessible to users, showing the overview of block information such as timestamps, block identity, and the writer's digital signatures, further enhancing transparency and trust in the system.

We evaluate the system prototype by conducting interviews with stakeholders involved in the NHI claims process: the first-tier verifier, advanced verifier, and finance administration staff. The evaluation shows supportive feedback towards the prototype, particularly highlighting the improvement in data access control and traceability. However, the interviewees raised some concerns regarding the level of detail in the traceability and data access features. Specifically, the possibility of over-detailed traceability and data access control at the individual level is viewed as potentially overwhelming and unnecessary for day-to-day operations. Even though granular transparency is beneficial, there should be an option to aggregate the data to avoid information overload and make the system more user-friendly. Overall, the evaluation shows positive feedback to the prototype but still needs refinement to ensure accessibility and a user-friendly environment.

5 Discussion

5.1 Blockchain platform recommendations

When implementing the new model, the right blockchain platform must be considered so the model can work seamlessly with the existing system. Factors such as cost, speed, scalability, and the existing ecosystem must be evaluated to ensure optimal performance and integration. Considering the existing NHI claim conditions, the blockchain platform has to meet a few requirements.

First, the platform needs to have a low gas fee, enabling cost-effective operations within the blockchain network and still allowing the NHI to provide the service at a low cost. Second, the network must be able to carry out transactions at a high rate since the NHI claim process involves a large amount of data. Third, it must have a scalable option, allowing it to manage increasing transactions while maintaining network performance, as the NHI goal is to cover all Indonesian citizens. Last, the blockchain platform must have a proven and large ecosystem as it will be implemented in an NHI involving citizens' data. Based on the criteria, we recommend several popular enterprise-grade permissioned blockchain platforms, as shown in Table 5.

Currently, numerous blockchain platforms are available with various specializations and focus on industries. We recommend enterprise-grade permissioned blockchain platforms, specifically *Hyperledger Fabric, Quorum,* and *Corda* as shown in Table 5, over popular public blockchains like *Ethereum, Polkadot,* and *Solana*, considering their alignment with industry needs and research goals. These platforms prioritize data privacy and traceability, offering low-cost private transactions with controlled access features. Furthermore, these enterprise-focused blockchain platforms solve industry needs and offer tailored solutions for handling high-rate transactions. They are well-known for their enterprise-level support for big organizations.

The first recommendation is *Hyperledger Fabric*, a blockchain platform established by the Linux Foundation. The platform offers a permissioned network with high transaction output, low latency confirmation, and private transactions without gas fees (Androulaki et al., 2018; Hyperledger, 2023). The blockchain platform works on a peer-to-peer distributed network, with each peer replicating and consistently copying each block data structure (Rajput et al., 2021). The platform uses an Attribute-based access control (ABAC), enabling data owners, acting as admins, to authorize data access based on attributes such as division, job title, license, or certifications. For example, a healthcare provider may require access to a patient's treatment history to verify claims in the NHI workflow. ABAC policies ensure that only authorized personnel, such as certified healthcare administrators with specific roles and permissions, can access this sensitive data. Similarly, policyholders can monitor who accessed their data and when, reinforcing transparency and trust within the system. Governed by a diverse technical steering committee and maintained by contributors from

various organizations, *Hyperledger Fabric* has expanded its development community to over 35 companies and 200 developers since it was established.

The second suitable platform for the proposed model is *Quorum*, a blockchain platform based on the *Ethereum blockchain* designed for enterprises and businesses by JP Morgan Chase. It offers a confidential, private, and permissioned consortium platform using smart contracts with crash and Byzantine fault-tolerant consensus algorithms using RAFT and IBFT, which enable faster consensus and transaction finality (Baliga et al., 2018). The platform client varies from various industries, including big enterprises such as JP Morgan, Amazon Web Services, and the South African Reserve Bank.

The last recommended platform is *Corda*, developed by R3, offering a permissioned and private transaction using a mechanism called contracts (Gendal Brown, 2018). These contracts integrate logic, business data, and the judicial process, anchoring them within the existing legal system. The consensus mechanism increases *Corda's* scalability and security by not routinely grouping the transactions into the network. Initially built to solve the need to regulate financial organizations, the *Corda* application became broader and included clients from various industries.

The recommended blockchain platforms share similarities in scalability, validators, and gas fees. Based on the technical specifications such as essential features, cost, gas fees, transaction rate, and ecosystem size, *Hyperledger Fabric* emerges as the most suitable option for implementing the proposed model. The comparison indicates that *Hyperledger Fabric* has no transaction fees, supports more than 2000 transactions per second (TPS), and offers modular design, private transactions, and advanced traceability features. Additionally, its ecosystem, supported by over 2000 organizations, highlights widespread industry adoption and trust.

To support the development and deployment of the prototype, a set of supporting tools and technologies have been identified to ensure efficient implementation. The system utilizes the *Hyperledger Fabric* SDK for Node.js to manage interactions between the application layer and the blockchain network, enabling efficient deployment and management of smart contracts. Docker containers isolate each node in the blockchain network, ensuring modular scalability and secure execution environments. For off-chain data storage, IPFS (InterPlanetary File System) securely and efficiently manages large datasets, while the hashes of off-chain data are stored on-chain to maintain integrity and verifiability. These components interact seamlessly through API gateways, which act as bridges facilitating communication between the blockchain network and existing NHI databases, ensuring secure and real-time data exchange across systems.

The integration of blockchain technology into the NHI system is supported by middleware solutions that manage interactions between the blockchain network and NHI's existing databases. Middleware ensures real-time synchronization of claim data between healthcare providers, administrators, and policyholders, minimizing latency and data inconsistencies. Middleware solutions act as an interface layer between the Hyperledger Fabric blockchain and the existing NHI databases. These middleware components handle API communication, ensuring seamless data synchronization across distributed systems. They also translate data formats between legacy systems and blockchain nodes, ensuring compatibility and reducing latency in data exchanges. This approach guarantees minimal disruption to existing NHI workflows while enabling enhanced traceability and privacy through blockchain technology. Data access is securely managed through Attribute-Based Access Control (ABAC), ensuring that only authorized stakeholders can access specific claim data. Furthermore, a traceability dashboard allows stakeholders to monitor claim transactions across different stages, enhancing transparency and accountability.

While *Hyperledger Fabric* aligns well with Indonesia's NHI system's technical and operational requirements, there are still challenges and future considerations to address. These include human resource readiness across multiple branches, hidden operational costs, and compliance with national data protection laws. Future development will focus on evaluating middleware compatibility, optimizing scalability, and conducting extensive real-world performance testing to ensure the seamless deployment of the proposed system across Indonesia's healthcare infrastructure.

5.2 Scalability and feasibility discussion

Scalability remains a significant concern for blockchain implementations in large-scale, data-intensive environments like Indonesia's National Health Insurance (NHI) system. With millions of daily transactions and extensive data records from healthcare providers, ensuring the system remains efficient, responsive, and scalable is critical. Our proposed blockchain-based NHI claim system incorporates several strategies to address scalability challenges. First, off-chain storage solutions using IPFS (InterPlanetary File System) are employed to reduce on-chain congestion. IPFS efficiently handles large datasets, such as medical records and claim attachments, while only immutable hashes are stored on the blockchain. This approach optimizes storage use and improves transaction processing speeds. Second, the system explores data sharding mechanisms to distribute data processing across multiple blockchain nodes. Sharding breaks data into smaller, manageable pieces, enabling parallel processing and reducing the computational load on individual nodes. This strategy enhances the overall throughput and scalability of the system without compromising data integrity. Additionally, the system leverages a hybrid blockchain approach, combining permissioned on-chain transactions with off-chain computation where appropriate. Critical data, such as transaction validation and audit trails, remain on the blockchain, while less sensitive, larger datasets are handled off-chain.

During the Proof of Concept (PoC) phase, a prototype system was deployed in a controlled testing environment to simulate the operational conditions of Indonesia's NHI system. The initial tests focused on evaluating transaction throughput, latency, and data synchronization across distributed nodes. Results demonstrated that the system could handle over 2000 transactions per second (TPS) with an average latency of less than 1 s, even under simulated peak loads. The integration of off-chain storage via IPFS showed significant improvements in managing large datasets while maintaining on-chain data integrity. Stakeholder feedback

gathered during this phase highlighted improvements in transaction transparency and reduced processing times for claims verification, addressing long-standing challenges in the current centralized system. However, certain scalability challenges in real-world deployment were identified, including data synchronization delays across regional branches, bandwidth limitations in remote areas, and compatibility with legacy systems. These challenges are planned for further analysis in subsequent phases.

Moving forward, the system will undergo a phased testing approach to validate scalability and feasibility under real-world conditions. The initial phase, Alpha Testing, will be conducted internally using selected NHI claim scenarios within a sandboxed environment. This phase will focus on evaluating technical performance benchmarks, including transaction speed, latency, and resource utilization. Following this, Beta Testing will involve rolling out the system in selected regional NHI branches to assess its real-world performance, focusing on database integration, user adoption rates, and resilience under variable network conditions. In the Pilot Deployment phase, the system will be expanded to multiple regions, incorporating a larger dataset and diverse claim scenarios to evaluate system robustness, long-term performance stability, and error recovery mechanisms. Finally, the system will enter the Nationwide Rollout phase, marking its full-scale implementation across Indonesia's NHI infrastructure. Insights from the beta and pilot phases will inform iterative refinements to address any identified bottlenecks.

Each testing phase is designed to produce performance benchmarks, uncover potential bottlenecks, and collect valuable stakeholder feedback to guide further optimizations. By integrating off-chain solutions, sharding mechanisms, and hybrid blockchain architecture, the proposed system is strategically designed to efficiently manage the large volume and complexity of Indonesia's NHI claim data. Ongoing evaluations, stress testing, and iterative optimizations will ensure that scalability concerns are proactively addressed throughout each deployment phase, laying a strong foundation for the system's long-term sustainability and success.

5.3 Challenges and issues in implementation

While blockchain technology holds numerous advantages, its implementation presents challenges and issues, necessitating careful consideration and strategic approaches to overcome. Improperly addressing these challenges and issues can lead to organizational losses from technology. Hence, we outline various challenges and issues associated with implementing blockchain technology at the NHI company.

5.3.1 Regulatory compliance

Ensuring regulatory compliance during blockchain implementation for NHI claims presents significant challenges. It is important to note that the challenges occur due to the different regulation levels among countries regarding blockchain and its components, especially if the blockchain project involves several parties subject to other regulations. Therefore, all stakeholders must collaborate to comply with local regulations, while regulators are crucial in enacting preventive measures (Brophy, 2020). The failure

to regulate blockchain activities can lead to various negative adverse consequences. The anonymity of blockchain can facilitate criminal money laundering activity where the user executing the transaction cannot always lead to real individual identity (Yeoh, 2017; Alamsyah and Syahrir, 2023). The complexity of blockchain technology may expose the customer to blockchain scams, and it will be hard to proceed with the investigation without appropriate regulations to safeguard the citizens. The lack of regulation regarding operational blockchain leads to conflict with the regulator; for example, Indonesia has different data protection regulations from the EU, which has GDPR. To prevent conflicts between different country regulations, extensive research and collaboration with relevant authorities is needed to develop an appropriate framework for blockchain implementation. Failure to effectively address these challenges could result in legal risks, financial penalties, and reputational damage for organizations implementing blockchain solutions and regulators. Therefore, researching regulatory requirements and ensuring compliance with regulations such as taxation and data security is an important aspect of successful blockchain implementation initiatives in various countries.

5.3.2 Interoperability

Interoperability is a challenge that needs to be overcome when implementing blockchain technology in existing systems, such as the NHI claim process. The term interoperability can refer to a cross-communication system that enables the ability to data sharing, transfer assets, payments, or information between different blockchain networks, decentralized applications (DApps) that use the same blockchain, or non-blockchain network (Besancon et al., 2019; Zhu et al., 2023). The Interoperability challenge can appear in developing countries because of unstandardized healthcare systems. The conventional healthcare system tends to rely on centralized, local, or offline databases, which can have proprietary data formats and protocols (Ghosh et al., 2023). The discrepancy between existing healthcare systems and the blockchain system can obstruct seamless data exchange, creating complex and time-consuming services. There are various approaches and technologies to achieve interoperability in blockchain implementation, such as notary schemes, sidechains/relays, atomic swaps, bridge protocols, and standardized protocols (Harris, 2023). Reorienting the existing healthcare system to newly standardized protocols adapted to blockchain implementation will need coordination, collaboration, and advanced research from involved stakeholders since it can be disruptive and resource-intensive, further complicating interoperability efforts.

5.3.3 Cost

Although blockchain implementation can reduce the operational cost of the transaction, restructuring the system to be suitable for blockchain can be a challenge in the process. The main costs in implementing blockchain are related to the system's initial setup, which affects the organization and regulators, who require specialized experts and resources. The possible costly stages in the implementation include restructuring the existing system, research and development plans, establishing regulations, specialized staff training, maintenance costs, and routine future updates to ensure a smooth functioning system. Building a seamless functioning blockchain network will require proper resources, such as

specialized hardware and energy-intensive computing resources, leading to rising costs because of the high upfront and ongoing costs for organizations, especially for the national-scale blockchain system with multiple organization branches. Using a fee-based incentive for the miners is also a factor in a rising cost, especially with high transaction volumes, which leads to increasing fees (Alamsyah et al., 2024). Failure to mitigate the cost challenges can harm the organization, such as over budget, financial and resource allocation issues, and diverting funds from critical projects. Ultimately, the organization may struggle to maintain competitiveness as the decrease in operational and innovation capability lowers the stakeholder trust in the organization. To address this challenge, organizations need to create proper preparation for blockchain implementation. This requires careful budgeting and strategic planning while considering the long-term improvement of the system as blockchain innovation evolves and new platforms with lower costs are emerging.

5.3.4 Human resource and user readiness

Implementing blockchain technology into an existing system can present notable challenges to human resources and user readiness. Although blockchain has many advantages, its adaptation requires the user's knowledge to develop and operate the new model. To create a seamlessly functional system, the developer will need specialized knowledge of blockchain technology, which may require hiring or training programs. The need to restructure the existing system to accommodate blockchain technology may also trigger resistance from the employees used to conventional systems. The lack of mitigation to overcome these challenges can lead to low acceptance rates, user error, and operational inefficiencies, hindering the successful integration of blockchain technology and its advantages. Addressing these challenges requires an organization to educate, socialize, and train the stakeholders to familiarize them with blockchain technology. Organizations must invest in user-centric design approaches to create a user-friendly system and promote a collaborative culture that can stimulate user participation and support the transition of blockchain-enabled processes.

6 Conclusion

We proposed a blockchain adaptation model and developed a prototype for the NHI claim system to enhance stakeholders' data privacy and traceability, minimizing the risks of unauthorized data access, misuse, privacy breaches, and untraceable activities. The new model involves key stakeholders, including policyholders, administration administrators, doctors, laboratory staff, payment administrators, pharmacists, claim administrators, claim verifiers, and NHI finance staff. Policyholders can now control data access, access their sensitive information pseudonymously, and monitor data activities throughout the healthcare and claim process. This research introduced a detailed model, divided into three architectural layers—functional, logical, and physical architectures—and utilized UML diagrams to illustrate these layers. Using use-case diagrams, the functional layer highlights actor behavior, while the logical architecture depicts interactions among actors, stakeholders, and data flow outputs. The physical data

architecture outlines data entities and relationships using class diagrams, ensuring clarity and alignment across processes. Covering the general NHI claim process under non-emergency conditions in Indonesia's healthcare industry, this study establishes a strong foundation for future research and testing phases.

Future research will focus on structured phased testing, including Alpha Testing, Beta Testing, and Pilot Deployment. Alpha Testing will evaluate the system's performance metrics, such as transaction speed, latency, and resource utilization, in a controlled environment with internal stakeholders. Beta Testing will validate system integration, resilience, and user adoption across selected healthcare facilities, while Pilot Deployment will assess scalability, regional variations, and system stability under diverse claim scenarios. These phases aim to refine the system before a Nationwide Rollout, which will validate long-term performance, compliance with healthcare regulations, and operational efficiency. Additionally, emerging challenges such as standardizing healthcare databases, managing legacy system integration, and addressing diverse insurance claim scenarios, including emergency cases, will require further investigation. Future research could also explore advanced techniques like machine learning for fraud detection, predictive analytics for claim optimization, and improving system resilience in low-connectivity regions.

We suggest adopting a lightweight blockchain framework to address computational demands associated with large-scale insurance claims, which is crucial given the data-intensive insurance claim process (Mardiansyah and Sari, 2022). The findings from this study offer valuable insights for NHI policymakers and service providers to build a more transparent, efficient, and secure claim system. From a managerial perspective, the implementation of this model is expected to enhance policyholders' trust by ensuring robust privacy and traceability measures. This study also serves as a reference for system designers, developers, and researchers, offering applicable insights for improving data privacy and traceability. Beyond academia, the research aims to raise public awareness of blockchain adoption and promote its integration into broader healthcare and insurance ecosystems. In summary, this research contributes to the ongoing dialogue on blockchain adoption in healthcare systems, offering a scalable, privacy-centric model tailored to Indonesia's healthcare infrastructure.

Data availability statement

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

Ethics statement

The studies involving humans were approved by BPJS Kesehatan (Indonesia National Health Insurance). The studies were conducted in accordance with the local legislation and institutional requirements. The participants provided their written informed consent to participate in this study.

Author contributions

Funding

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

Agbo, C. C., and Mahmoud, Q. H. (2020). Blockchain in healthcare opportunities, challenges, and possible solutions. *Int. J. Healthc. Inf. Syst. Inf.* 15 (3), 82–97. doi:10.4018/IJHISI.2020070105

Alamsyah, A., Hakim, N., and Hendayani, R. (2022). Blockchain-based traceability system to support the Indonesian halal supply chain ecosystem. *Economies* 10 (6), 134. doi:10.3390/economies10060134

Alamsyah, A., and Syahrir, S. (2023). The taxonomy of blockchain-based technology in the financial industry. *F1000Res* 12 (July), 457. doi:10.12688/f1000research.133518.2

Alamsyah, A., and Syahrir, S. (2024). "A taxonomy on blockchain-based technology in the financial industry: drivers, applications, benefits, and threats," in *Blockchain and smart-contract technologies for innovative applications.* Editors N. El Madhoun, I. Dionysiou, and E. Bertin (Cham: Springer). doi:10.1007/978-3-031-50028-2_4

Alamsyah, A., Widiyanesti, S., Wulansari, P., Nurhazizah, E., Dewi, A. S., Rahadian, D., et al. (2023). Blockchain traceability model in the coffee industry. *J. Open Innovation Technol. Mark. Complex.* 9 (1), 100008. doi:10.1016/j.joitmc.2023.100008

Al Omar, A., Bhuiyan, M. Z. A., Basu, A., Kiyomoto, S., and Rahman, M. S. (2019). Privacy-friendly platform for healthcare data in cloud based on blockchain environment. *Future Gener. Comput. Syst.* 95, 511–521. doi:10.1016/j.future.2018.12.044

Amponsah, A. A., Adekoya, A. F., and Weyori, B. A. (2022). Improving the financial security of national health insurance using cloud-based blockchain technology application. *Int. J. Inf. Manag. Data Insights* 2 (1), 100081. doi:10.1016/j.jjimei.2022.100081

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., et al. (2018). "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proceedings of the 13th EuroSys conference, EuroSys 2018*, 2018-Janua. doi:10.1145/3190508.3190538

Baliga, A., Subhod, I., Kamat, P., and Chatterjee, S. (2018). "Performance evaluation of the *quorum* blockchain platform".

Bashir, I. (2018). *Mastering blockchain.* Second Edition. Birmingham: Packt Publishing.

Besancon, L., Da Silva, C. F., and Ghodous, P. (2019). "Towards blockchain interoperability: improving video games data exchange," in *ICBC 2019 - IEEE international conference on blockchain and cryptocurrency*, 81–85. doi:10.1109/BLOC.2019.8751347

BPJS Kesehatan (2024). Jumlah peserta program JKN dan fasilitas kesehatan JKN. Available at: https://faskes.bpjs-kesehatan.go.id/aplicares/#/app/peta (Accessed April 05, 2023).

Brophy, R. (2020). Blockchain and insurance: a review for operations and regulation. *J. Financial Regul. Compliance* 28 (2), 215–234. doi:10.1108/JFRC-09-2018-0127

Chilamkurti, N., and Balamurugan, B. (2021). Blockchain, Internet of Things, and artificial intelligence, vol. 1.

Dave, M., Rastogi, V., Miglani, M., Saharan, P., and Goyal, N. (2022). Smart fog-based video surveillance with privacy preservation based on blockchain. *Wirel. Pers. Commun.* 124, 1677–1694. doi:10.1007/s11277-021-09426-8

Dimas, C. (2024). BPJS kesehatan akui kebocoran data 279 juta WNI. Available at: https://www.kompas.tv/nasional/177478/bpjs-kesehatan-akui-kebocoran-data-279-juta-wni (Accessed June 27, 2023).

Fernandez, J. L., and Hernandez, C. (2019). Practical model-based system engineering.

Ge, Z., Loghin, D., Ooi, B. C., Ruan, P., and Wang, T. (2022). Hybrid blockchain database systems. *Proc. VLDB Endow.* 15 (5), 1092–1104. doi:10.14778/3510397.3510406

Gendal Brown, R. (2018). R3-Corda platform whitepaper. *Corda Platf. White Pap.*, 1–21.

Ghosh, P. K., Chakraborty, A., Hasan, M., Rashid, K., and Siddique, A. H. (2023). Blockchain application in healthcare systems: a review. *Systems* 11 (1), 38. doi:10.3390/systems11010038

Harris, C. G. (2023). "Cross-chain technologies: challenges and opportunties for blockchain interoperability," in *2023 IEEE international conference on omni-layer intelligent systems, COINS 2023*. doi:10.1109/COINS57856.2023.10189298

Humas BPJS Kesehatan, (2023). "Menjaga reputasi organisasi dengan mengedepankan kepuasan peserta JKN." Accessed: June. 26, 2023. Available at: https://www.bpjs-kesehatan.go.id/bpjs/post/read/2022/2406/Menjaga-Reputasi-Organisasi-dengan-Mengedepankan-Kepuasan-Peserta-JKN

Hyperledger, (2023). "Introduction — hyperledger-fabricdocs main documentation," *Hyperledger-Fabricdocs.* Accessed: September. 04, 2023. Available at: https://hyperledger-fabric.readthedocs.io/en/release-2.5/whatis.html.

Kementerian Kesehatan Republik Indonesia (2019). 3. Petunjuk Teknis Aplikasi E-KLAIM [Aplikasi INA-CBG] - v5. Available at: https://inacbg.kemkes.go.id/DL/Petunjuk_Teknis_E-Klaim_5.3.2_Tahun_2019.pdf (Accessed December 27, 2023).

Kesehatan, B. (2014). "Panduan praktis administrasi klaim fasilitas kesehatan BPJS kesehatan".

Kesehatan, B. (2018). *User manual aplikasi VClaim v. 1.4.0,* 0–17.

Kesehatan, B. (2022). "Loran pengelolaan program tahun 2022 dan laporan keuangan tahun 2022(auditan)".

Khan, D., Jung, L. T., and Hashmani, M. A. (2021). Systematic literature review of challenges in blockchain scalability. *Appl. Sci.* 11 (20), 9372. doi:10.3390/app11209372

Kurnia, R. (2017). Kajian Sistem Pengajuan Klaim Pasien Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan di RSD Balung Kabupaten Jember Tahun 2017".

Levey, N. N. (2024). 100 million people in America are saddled with health care debt. *DIAGNOSIS.* Available at: https://kffhealthnews.org/news/article/diagnosis-debt-investigation-100-million-americans-hidden-medical-debt/.

Loukil, F., Boukadi, K., Hussain, R., and Abed, M. (2021). Ciosy: a collaborative blockchain-based insurance system. *Electron. Switz.* 10 (11), 1343–1415. doi:10.3390/electronics10111343

Maharani, I. L. (2017). "Pengenalan Program Vedika (Verifikasi di Kantor) dan e-claim".

Mardiansyah, V., and Sari, R. F. (2022). Lightweight blockchain framework for medical record data integrity. *J. Appl. Sci. Eng.* 26 (1), 91–103. doi:10.6180/jase.202301_26(1).0010

Musdalifah, S. (2020). *Pengaruh kepercayaan masyarakat terhadap pembayaran premi bpjs kesehatan,* 1–5.

Pawar, P., Parolia, N., Shinde, S., Edoh, T. O., and Singh, M. (2022). eHealthChain—a blockchain-based personal health information management system. *Ann. des Telecommunications/Annals Telecommun.* 77 (1–2), 33–45. doi:10.1007/s12243-021-00868-6

Rajput, A. R., Li, Q., and Ahvanooey, M. T. (2021). A blockchain-based secret-data sharing framework for personal health records in emergency condition. *Healthc. Switz.* 9 (2), 206–217. doi:10.3390/healthcare9020206

Rajput, A. R., Li, Q., Taleby Ahvanooey, M., and Masood, I. (2019). EACMS: emergency access control management system for personal health record based on blockchain. *IEEE Access* 7, 84304–84317. doi:10.1109/ACCESS.2019.2917976

Safak, E., Furkan, A., and Erol, T. (2019). "Hybrid database design combination of blockchain and central database," in *3rd international symposium on multidisciplinary studies and innovative technologies, ISMSIT 2019 - proceedings*. doi:10.1109/ISMSIT.2019.8932763

Septi Jayanti, C. (2022). The issues of data protection against leaking of personal data in security health services (A comparison between Indonesia and other countries regulations). *Int. J. Bus. Econ. Law* 26 (1), 1.

Sharma, S., Kumar, A., Bhushan, M., Goyal, N., and Iyer, S. S. (2021). "Is blockchain technology secure to work on?," in *Blockchain and AI technology in the industrial Internet of Things*. Editor S. Kumar Pani, (IGI Global), 66–80. doi:10.4018/978-1-7998-6694-7.ch005

Sulaiman, R., Alamsyah, A., and Wulansari, P. (2022). "Reshaping the future of recruitment through talent reputation and verifiable credentials using blockchain technology," in *10th international conference on information and communication technology*. ICoICT, 316–321. doi:10.1109/ICoICT55009.2022.9914891

Sutanto, E., Mulyana, R., Arisgraha, F. C. S., and Escrivá-Escrivá, G. (2022). Integrating blockchain for health insurance in Indonesia with hash authentication. *J. Theor. Appl. Electron. Commer. Res.* 17 (4), 1602–1615. doi:10.3390/jtaer17040081

Tanwar, S. (2018). Blockchain technology: from theory to practice.

U.S. Centers for Medicare and Medicaid Services. (2024). The national health expenditure accounts (NHEA): historical. *Natl. Health Expend. Data*. Available at: https://www.cms.gov/research-statistics-data-and-systems/statistics-trends-and-reports/nationalhealthexpenddata/nationalhealthaccountshistorical.

Yeoh, P. (2017). Regulatory issues in blockchain technology. *J. Financial Regul. Compliance* 25 (2), 196–208. doi:10.1108/JFRC-08-2016-0068

Yun, J.-H., Jeon, Y.-J., and Kang, M.-S. (2022). Prediction of the elastic properties of ultra high molecular-weight polyethylene particle-reinforced polypropylene composite materials through homogenization. *Appl. Sci.* 12, 7699. doi:10.3390/app12157699

Zheng, X., Mukkamala, R. R., Vatrapu, R., and Ordieres-Mere, J. (2018). "Blockchain-based personal health data sharing system using cloud storage," in *2018 IEEE 20th international conference on e-health networking, applications and services, healthcom 2018*. doi:10.1109/HealthCom.2018.8531125

Zhu, P., Hu, J., Zhang, Y., and Li, X. (2021). Enhancing traceability of infectious diseases: a blockchain-based approach. *Inf. Process Manag.* 58 (4), 102570. doi:10.1016/j.ipm.2021.102570

Zhu, S., Chi, C., and Liu, Y. (2023). A study on the challenges and solutions of blockchain interoperability. *China Commun.* 20 (6), 148–165. doi:10.23919/JCC.2023.00.026