

# A Blockchain-based Governance Framework for AIBOM Integrity and Automated Regulatory Compliance

Minchae Kim\*, Heemin Choi\*\*, Heeyoul Kim\*

\* Department of computer Science and engineering, Kyonggi University, Korea

\*\* Department of Software Safety and Security, Kyonggi University, Korea

kmc12291@kyonggi.ac.kr, minco777@kyonggi.ac.kr, heeyoul.kim@kyonggi.ac.kr

**Abstract**— As Artificial Intelligence (AI) advances, ensuring security and compliance is critical. While the AI Bill of Materials (AIBOM) is used for security management, guaranteeing its data integrity remains a challenge. Furthermore, the manual regulatory approval process for Medical AI is a significant barrier due to excessive time and cost. This paper proposes a blockchain-based governance system integrating Decentralized Identifiers (DID) and the InterPlanetary File System (IPFS) to address these issues. The system uses DID for authentication and stores AIBOMs on IPFS, recording their transactions and Content Identifiers (CIDs) on-chain to ensure integrity. A key feature is an automation module that generates regulatory submission documents based on the verified AIBOM and official guidelines. These documents, final regulatory approvals, and post-market vulnerability reports are also immutably recorded on the blockchain. The proposed framework enhances AI supply chain security via AIBOM integrity and streamlines the complex regulatory process, providing a transparent, efficient, and auditable governance solution.

**Keywords**— Blockchain, AI Bill of Materials (AIBOM), Decentralized Identifier (DID)

## I. INTRODUCTION

The recent explosive proliferation of generative artificial intelligence (AI) systems such as ChatGPT has accelerated AI adoption across virtually all industries. However, this rapid integration has simultaneously raised critical challenges concerning the safety, reliability, and transparency of AI systems including the *black-box* nature of AI models, ambiguous data provenance and licensing issues, and emerging security threats such as adversarial attacks.

In response, the paradigm of the Software Bill of Materials (SBOM) in traditional software supply chains is now expanding into the AI Bill of Materials (AIBOM), which has emerged as a key mechanism for ensuring AI transparency. Regulatory authorities such as the U.S. National Institute of Standards and Technology (NIST)[1], the Food and Drug Administration (FDA)[2], and the European Union (EU) under its AI Act[3] have begun to mandate AIBOM adoption. Yet, guaranteeing the integrity of AIBOM data itself remains a major challenge. If AIBOM repositories are centralized or susceptible to tampering, their trustworthiness cannot be assured thus drawing attention to blockchain technology as a promising solution that ensures data immutability and traceability[4].

However, securing AIBOM integrity alone does not resolve the bottlenecks in AI governance. In high-risk domains such as medical AI, where human safety is directly involved, regulatory approval from authorities like the Ministry of Food and Drug Safety (KMFDS) is mandatory. These approval processes typically require extensive documentation that is manually prepared, resulting in significant time and cost burdens that hinder innovation and market entry. Moreover, there is a lack of systematic post-market surveillance frameworks after product deployment.

Accordingly, this study proposes the iSBOMB framework, which integrates Decentralized Identifiers (DID), the InterPlanetary File System (IPFS), and blockchain technology to comprehensively address these challenges. Specifically, we introduce a trust-based document automation mechanism that combines verified AIBOM data with Large Language Models (LLMs) to streamline the generation of complex regulatory documents. Furthermore, to guarantee system-wide integrity, the framework employs DID-based identity verification and blockchain logging, ensuring that the entire AI lifecycle from creation to post-market supervision is immutably recorded and fully traceable. Finally, we present a real-time monitoring dashboard that provides stakeholders with continuous visibility into model status and vulnerabilities, offering a transparent and efficient blueprint for next-generation AI governance.

## II. BACKGROUND

### A. Blockchain and Smart Contracts

Blockchain is a Distributed Ledger Technology (DLT) that stores data by replicating it across multiple nodes in a Peer-to-Peer (P2P) network. Every transaction is stored in cryptographically linked 'blocks,' providing immutability, which makes recorded data virtually tamper-proof, and transparency, which allows anyone to verify it.

Ethereum is a representative platform that advanced blockchain technology to its second generation, offering the Smart Contract feature. A smart contract is program code, often written in languages like Solidity, that automatically executes when predefined rules and conditions are met. In this research, we utilize Ethereum smart contracts to design a structure that automatically records and verifies key events throughout the AI governance lifecycle such as

AIBOM creation, regulatory document submission, and approval by authorities onto the ledger.

### B. Decentralized Identifier (DID)

Traditional centralized identity (ID) systems grant specific service providers (e.g., governments, corporations) exclusive control over user authentication and personal data. This creates risks of data breaches and a lack of interoperability between services. Decentralized Identifier (DID), a W3C standard[5], is a technology that enables individuals to manage their own identities autonomously (Self Sovereign Identity, SSI), free from the control of such central authorities.

Hyperledger Indy is a distributed ledger specifically designed for DID management, while Hyperledger Aries is a framework that provides interoperable protocols and agents for wallets operating on DID ledgers like Indy[6]. Using Indy/Aries, users can create their own DID, store Verifiable Credentials (VCs) received from an Issuer in their wallet, and selectively submit only the necessary information to a Verifier.

### C. InterPlanetary File System (IPFS)

While blockchain guarantees data integrity, it was not designed to store large scale data on the ledger itself. Storing large files on Ethereum would incur prohibitive gas fees, making it inefficient. IPFS is a P2P based distributed file system that solves this problem[7].

Unlike the traditional HTTP protocol, IPFS uses content-based addressing (determining the address based on the content's hash) rather than location based addressing. When a file is uploaded to IPFS, a unique CID (Content Identifier) is generated based on the file's contents. If the file content changes by even a single bit, the CID changes completely.

In this study, large original files such as AIBOMs and regulatory documents are stored on IPFS. Then, only the CID the unique fingerprint proving the file's immutability is extracted and recorded onto the Ethereum smart contract described in Section A. This allows the system to minimize gas fees (efficiency) while strongly guaranteeing the integrity of the original data via the blockchain (trust).

## III. PROPOSAL MODEL

This study proposes the iSBOMB (Integrity-assured Software Bill of Materials using Blockchain) framework to address the dual challenges of AIBOM data reliability and inefficiency of manual regulatory processes raised in the Introduction. iSBOMB aims to ensure the integrity of all deliverables and actions throughout the AI lifecycle and to automate regulatory compliance procedures.

### A. System Architecture

[Figure 1] illustrates the overall architecture of the proposed iSBOMB framework. The platform consists of three distinct layers, the Application & Authentication Layer, the Data Processing & Storage Layer, and the Blockchain Layer. Each layer operates cohesively to

manage everything from user interaction to data integrity assurance.

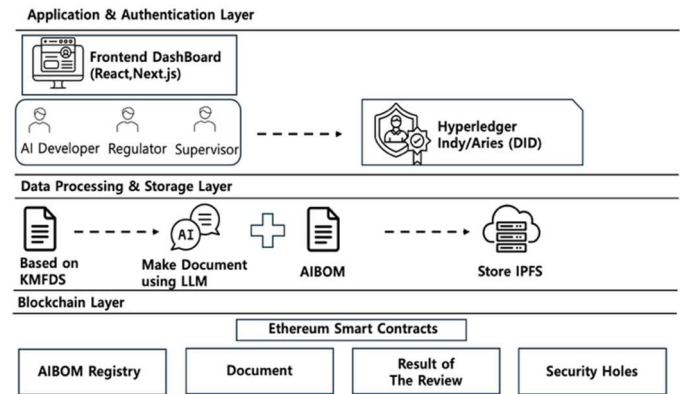


Figure 1. Overall Architecture of the iSBOMB Framework

#### 1. Application & Authentication Layer

This layer serves as the tier for user interaction and decentralized identity management. The Frontend Dashboard (React) operates as a web-based interface, providing role-specific functions to each participant (Developer, Regulator, Supervisor), while Hyperledger Indy/Aries authenticates users via DID wallets without a centralized server, ensuring that all blockchain transactions include verified signatures.

#### 2. Data Processing & Storage Layer

This layer is dedicated to the secure management of large-scale data and automated document generation. IPFS stores original AIBOM files and AI-generated documents in a distributed manner, generating unique content-based CIDs to prevent tampering, while the LLM Module uses Retrieval-Augmented Generation (RAG) to reference KMFDS guidelines and analyze developer inputs to automatically draft regulatory documents.

#### 3. Blockchain Layer (On-Chain)

This layer functions as the core tier for ensuring system trust and immutable record-keeping. Operating through Ethereum Smart Contracts, it manages the entire governance history—including AIBOM registration, document CID storage, regulatory approval results, and supervisor reports—thereby providing a transparent Single Source of Truth for all stakeholders.

### B. Participants and Roles

The iSBOMB framework defines three main stakeholders involved in the AI governance lifecycle.

- 1) AI Developer:** This entity is responsible for creating the AI model and the corresponding AIBOM. They also utilize the LLM module to generate regulatory documents and submit them to the regulatory body.
- 2) Regulator:** This entity reviews and verifies the submitted AIBOM and regulatory documents. They are responsible for recording the final audit results (e.g., approval or rejection) on the blockchain.

- 3) **Supervisor:** This entity accesses the AIBOMs of approved, in market AI models to conduct security audits and post market surveillance. If a security issue is discovered, they are responsible for reporting the findings on the blockchain.

### C. Operating Process

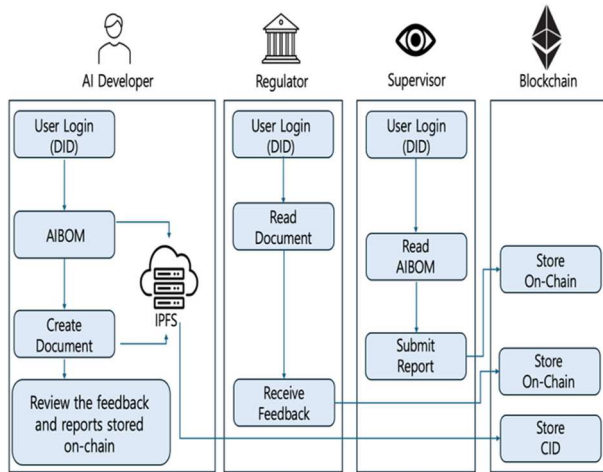


Figure 2. iSBOMB-based AI Governance Workflow

As illustrated in [Figure 2], the AI governance process of the proposed framework proceeds in the following 7 stages.

1) **DID Authentication:** All participants (Developer, Regulator, Supervisor) log into the system using their DID wallets. This process corresponds to the flow in the User Layer on the left of [Figure 2], where each user is authenticated via the DID Auth module before accessing the core system.

2) **AIBOM Registration:** The AI Developer stores the original AIBOM file in the IPFS Storage (depicted at the bottom of [Figure 2]) and registers the resulting CID and metadata via a Smart Contract. This illustrates the data flow where the hash generated from IPFS is recorded into the central **Blockchain Layer**.

3) **Automated Regulatory Document Generation:** The LLM Engine analyzes inputs such as clinical results and references the Guideline DB to draft a regulatory document. The document is stored on IPFS, and its CID is automatically linked to the corresponding Model Block in the Blockchain, as shown in the upper section of [Figure 2].

4) **Regulatory Review and Approval:** The Regulator verifies the integrity of the AIBOM by querying the blockchain and records the final approval result on-chain. This is represented by the bidirectional interaction in [Figure 2], where the Regulator reads verification data from the Blockchain and writes the Approval transaction back to the ledger.

5) **Post-Market Surveillance and Audit:** The Supervisor accesses the approved model's data to inspect vulnerabilities and perform audits. This corresponds to the Post-Market phase on the right side of [Figure 2], where the

Supervisor retrieves original data anchored in the Blockchain for verification.

6) **Vulnerability Reporting:** The Supervisor generates a Vulnerability Report containing risk levels and descriptions, which is then recorded via a transaction. This aligns with the input flow in [Figure 2], where the report data is sent to and immutably stored within the specific Model Block on the Blockchain.

7) **Feedback and Improvement:** The AI Developer receives real-time **Feedback** triggered by blockchain events and registers a resolution plan (Patch) on-chain. This completes the cycle structure shown in [Figure 2], where the feedback loop facilitates continuous improvement and transparent lifecycle tracking.

## IV. IMPLEMENTATION

This section details the development environment used to implement the proposed iSBOMB framework and validates its core functionalities through scenario based experiments.

### A. Development environment

The development environment for the system implementation is shown in [Table 1].

Table 1. System Development Environment

| Category       | Technology Stack    | Details                           |
|----------------|---------------------|-----------------------------------|
| Frontend       | Web Application     | React, Next.js, Tailwind CSS      |
| Backend        | API Server          | FastAPI (Python)                  |
| Blockchain     | Smart Contract      | Solidity, Hardhat                 |
|                | Network             | Polygon Testnet                   |
|                | Wallet              | Metamask                          |
| Infrastructure | DID Framework       | Hyperledger Indy + Aries          |
|                | Distributed Storage | IPFS (InterPlanetary File System) |
|                | Utility             | Docker, Docker-compose            |

### B. Scenario based Experiments and Results

To verify the core functions of the proposed framework, a 5stage scenario was conducted based on the 'Operating Process' from the 'Proposed Model' section.

#### 1. DID based Authentication and Role Assignment

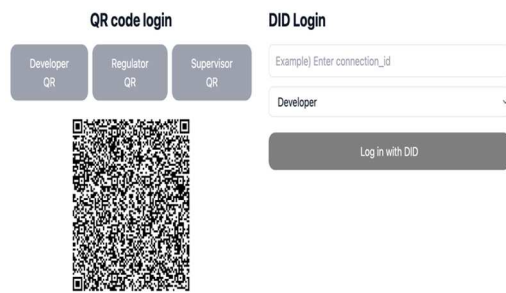


Figure 3. DID-based Authentication Process

As shown in [Figure 3], the user establishes a secure connection with the system agent by scanning a QR code generated by the Hyperledger Aries framework. This process creates a unique Connection ID (DID), granting the user role-based access (Developer, Regulator, Supervisor) without relying on a centralized identity provider.

## 2. AIBOM Registration on IPFS and Blockchain



Figure 4. AIBOM Registration (IPFS and On-Chain)

The developer uploads the AIBOM file via the dashboard interface. The system first stores the file on IPFS, generating a unique CID. Subsequently, the developer records this CID and model metadata onto the blockchain smart contract, as shown in [Figure 4], confirming the successful registration via the displayed transaction hash.

## 3. LLM-based Regulatory Document Generation

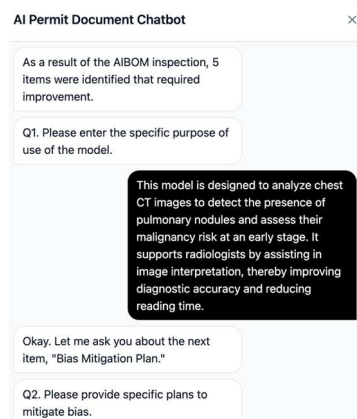


Figure 5. Automated Regulatory Document Generation using LLM

[Figure 5] illustrates the interaction workflow of the LLM-based Chatbot designed for automated regulatory document generation. Upon analyzing the AIBOM inspection results, the system first identifies the number of items requiring improvement and then initiates a structured questionnaire aligned with KMFDS regulatory guidelines. As depicted in the example, the chatbot queries essential details, such as the

intended use of the model (Q1) and bias mitigation strategies (Q2). The developer's real-time responses are synthesized by the LLM module to populate the draft regulatory submission document.

## 4. Regulatory Review and On-Chain Approval

### Review Request Queue

Confirm the submission request received.

| Request ID | Model ID | Developer                                 | CID                                        | Status    | Actions                            |
|------------|----------|-------------------------------------------|--------------------------------------------|-----------|------------------------------------|
| REQ-2025-1 | 1        | 0xf39fd6e51aad88f6f4ce6ab8827279cfff92266 | QmbVdCUCKXZohYkLn5nZ5GcQkVbUMfjYceCjshx8d  | Submitted | Open Dossier<br>Compare CID ↔ IPFS |
| REQ-2025-0 | 0        | 0xf39fd6e51aad88f6f4ce6ab8827279cfff92266 | QmYxHSGFMPmjuKBrvKypv1uYb9p4Lp5mX0nGJa3903 | Submitted | Open Dossier<br>Compare CID ↔ IPFS |

Figure 6. Regulatory Review Dashboard

As shown in [Figure 6], the Regulator's dashboard displays a list of models submitted for review. The interface explicitly presents the Developer's DID and the AIBOM's CID, enabling the regulator to cross-verify the submitter's identity and data integrity. Upon validation, the regulator records the approval decision on the blockchain via the 'Actions' panel.

## 5. Post-Market Surveillance and Vulnerability Reporting

### Vulnerability Analysis and Reporting

After analyzing the AIBOM document, vulnerabilities and recommendations are registered on-chain.

Model ID
Vulnerability CID or Description
HIGH

On-chain vulnerability reporting

Security Advisory (Supervisor)

Recommendation Document CID or Summary

Scope (e.g. v1.3.x)

Action (e.g., patch recommendation)

Save Advisory (On-chain) Broadcast Advisory (mock)

Recommendations recorded on-chain

No recommendations

Vulnerabilities recorded on-chain

No record

Figure 7. On-Chain Confirmation of Vulnerability Report

As shown in [Figure 7], the Supervisor audits an approved model and submits a vulnerability report. The system confirms the successful on-chain recording of the report, displaying the transaction hash and the new IPFS CID for the report artifact. This demonstrates that the entire post-market lifecycle is transparently tracked and immutable.

## V. CONCLUSIONS

As Artificial Intelligence (AI) advances, the opacity of models and inefficient manual regulatory processes create significant barriers to safe adoption. This study proposed the iSBOMB framework to address these dual challenges by integrating Decentralized Identifiers (DID) for identity verification, IPFS for AIBOM integrity, and Large Language

Models (LLMs) for automated regulatory document generation. We demonstrated the feasibility of recording the entire AI lifecycle—from creation and approval to post-market supervision—on the Polygon testnet, ensuring a transparent and auditable governance process.

The proposed framework offers distinct advantages for next-generation AI governance. First, it achieves both reliability and efficiency by employing Trust-based Document Automation, which significantly reduces the time and cost of compliance compared to manual methods. Second, the integration of DID and blockchain technology establishes clear accountability and transparent history management, ensuring that all actions within the system are immutable and traceable. Third, the inclusion of a Real-time Monitoring Dashboard enables stakeholders to proactively manage risks by providing immediate visibility into the status and vulnerabilities of AI models.

Future work will focus on three key areas. First, we plan to incorporate Zero-Knowledge Proofs (ZKP) to enhance privacy for sensitive AIBOM data. Second, we aim to migrate to advanced Layer 2 solutions like Polygon zkEVM to improve scalability and reduce transaction costs. Finally, we will ensure interoperability with international AI SBOM standards such as SPDX, CycloneDX, and NIST to broaden the framework's practical applicability.

#### ACKNOWLEDGMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(RS-2020-NR049579)

#### REFERENCES

- [1] NIST, "The NIST AI Risk Management Framework (AI RMF 1.0)," National Institute of Standards and Technology, Gaithersburg, MD, USA, NIST AI 100-1, Jan. 2023. [Online]. Available: <https://doi.org/10.6028/NIST.AI.100-1>
- [2] U.S. Food and Drug Administration (FDA), "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions," FDA, Silver Spring, MD, USA, Guidance for Industry and FDA Staff, Sep. 2023. [Online]. Available: <https://www.fda.gov/media/119933/download>
- [3] European Parliament and Council of the European Union, "Regulation (EU) 2024/1689... laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)," Official Journal of the European Union, L 1689, Jun. 2024. [Online]. Available: <https://eur-lex.europa.eu/eli/reg/2024/1689>
- [4] A. B. M. M. R. Khan, et al., "Blockchain-Integrated Software Bill of Materials (SBOM) for Real-Time Vulnerability Detection in Decentralized Package Repositories," arXiv preprint arXiv:2305.10980, May 2023. [Online]. Available: <https://arxiv.org/abs/2305.10980>
- [5] W3C, "Decentralized Identifiers (DIDs) v1.0," W3C Recommendation, Jul. 2022. [Online]. Available: <https://www.w3.org/TR/did-core/>
- [6] Hyperledger Foundation, "Hyperledger Aries," Hyperledger Foundation Projects, 2024. [Online]. Available: <https://www.hyperledger.org/projects/aries>
- [7] J. Benet, "IPFS - Content Addressed, Versioned, P2P File System," arXiv preprint arXiv:1407.3561, Jul. 2014. [Online]. Available: <https://arxiv.org/abs/1407.3561>



**Minchae Kim** is an undergraduate student in the Department of computer Science and engineering, Kyonggi University, Korea. Her major research interests include blockchain and security.



**Heemin Choi** is in the master's course of the Department of Software Safety and Security, Kyonggi University, Korea. Her major research interests include blockchain and security.



**Heeyoul Kim** received the B.E. degree in Computer Science from KAIST, Korea, in 2000, the M.S. degree in Computer Science from KAIST in 2002, and the Ph.D. degree in computer science from KAIST in 2007. From 2007 to 2008, with the Samsung Electronics as a senior engineer. Since 2009 he has been a faculty member of Department of Computer Science at Kyonggi University. His major research interests include cryptography, security and blockchain.