applied sciences

MDPI

Article

Securing Construction Workers' Data Security and Privacy with Blockchain Technology

Alvina Ekua Ntefua Saah [1], **Jurng-Jae Yee** [2] **and Jae-Ho Choi** [2,*]

[1] Department of Civil Engineering, Dong-A University, Busan 49315, Republic of Korea; alvinasaah@donga.ac.kr
[2] ICT Integrated Safety Ocean Smart Cities Engineering Department, Dong-A University, Busan 49315, Republic of Korea; jjyee@dau.ac.kr
* Correspondence: jaehochoi@dau.ac.kr

Abstract: The construction industry, characterized by its intricate network of stakeholders and diverse workforce, grapples with the challenge of managing information effectively. This study delves into this issue, recognizing the universal importance of safeguarding data, particularly amid rising concerns around unauthorized access and breaches. Aiming to harness the potential of blockchain technology to address these challenges, this study used hypothetical biographical and safety data of construction workers securely stored on a Hyperledger Fabric blockchain. Developed within the Amazon Web Services (AWS) cloud platform, this blockchain infrastructure emerged as a robust solution for enhancing data security and privacy. Anchored in the core principles of data security, the model emerges as a potent defender against the vulnerabilities of traditional data management systems. Beyond its immediate implications, this study exemplifies the marriage of blockchain technology and the construction sector, and its potential for reshaping workforce management, especially in high-risk projects and optimizing risk assessment, resource allocation, and safety measures to mitigate work-related injuries. Practical validation through transaction testing using Hyperledger Explorer validates the model's feasibility and operational effectiveness, thus serving as a blueprint for the industry's data management. Ultimately, this research not only showcases the promise of blockchain technology in addressing construction data security challenges but also underscores its practical applicability through comprehensive testing, thus heralding a new era of data management that harmonizes security and efficiency for stakeholders' benefit.

Keywords: blockchain technology; Hyperledger Fabric; Amazon Web Services (AWS); construction workers; privacy; safety

check for updates

Citation: Saah, A.E.N.; Yee, J.-J.; Choi, J.-H. Securing Construction Workers' Data Security and Privacy with Blockchain Technology. *Appl. Sci.* **2023**, *13*, 13339. https://doi.org/10.3390/app132413339

Academic Editor: Roberto Saia

Received: 17 October 2023
Revised: 29 November 2023
Accepted: 7 December 2023
Published: 18 December 2023

1. Introduction

The construction industry is known for its complex dynamics involving numerous stakeholders and a diverse workforce. With projects ranging from small-scale renovations to large infrastructure development, it becomes crucial to address the challenges associated with managing information in such an environment [1,2]. As construction projects involve multiple entities, including workers, clients, contractors, engineers, managers, regulatory bodies, and certification bodies, ensuring the confidentiality and security of data becomes a critical concern. One significant aspect that requires attention is the privacy and safety of construction workers' personal information.

The privacy and safety of construction workers' information pose unique challenges due to the sensitive nature of the data involved. Personal details, such as names, ages, addresses, identification numbers, qualifications, certifications, and work history, are essential for various administrative and operational purposes, including employment, compliance, and safety [3,4]. However, the exposure of this information to unauthorized individuals can lead to identity theft, misuse, fraud, exploitation, and potential harm to the workers [5–7]. Safeguarding the privacy and security of workers' personal information is not only a legal and ethical obligation but also essential for maintaining trust and protecting their rights [8]. This aligns with the work of Xu et al. [9], which highlights that privacy protection is of utmost importance as it forms a key element in societal norms and law; nevertheless, it is often traded away in favor of "good causes," like security, safety, efficiency, or productivity.

Furthermore, the construction industry has long grappled with the persistent challenge of a shortage of skilled labor, and the workforce is rapidly aging [10–13]. These factors further emphasize the importance of effectively managing construction workers' personal information. With a limited pool of skilled workers, prioritizing the protection of their personal data becomes crucial to attract and retain talent. Construction workers invest their time and expertise in projects and deserve the assurance that their sensitive information is handled with the utmost care [14].

Additionally, ensuring the efficient handling of safety-related data concerning construction workers is crucial for establishing a healthy work environment. This significance arises from the fact that the construction industry, recognized for its job-related safety risks, involves constantly changing and physically strenuous tasks of an unpredictable nature. These tasks compel workers to execute actions in precarious and uncomfortable stances over extended periods, leading to instances of non-lethal injuries [15–17]. These injuries can have long-lasting consequences, leading to permanent disabilities for construction workers. One specific type of injury is musculoskeletal disorders (WMSDs), which are often caused by external factors, such as repetitive movements, overexertion, and awkward postures in occupational settings. WMSDs can affect different areas of the body, such as the lower back, upper limbs, and lower limbs, and they are associated with impairments in physical tissues, like the joints, bones, muscles, and tendons [16,18]. By effectively managing data on high-risk construction activities in a secure and reliable system, construction stakeholders can make informed decisions that prioritize the safety and well-being of their workforce.

Data manipulation presents a significant risk within the construction industry due to the intricate network of stakeholders involved in data exchange. Unsanctioned alterations or tampering with information regarding workers' credentials, certifications, employment history, and safety records can lead to grave consequences. These include jeopardizing the credibility of projects, compromising the safety of workers, and undermining trust among stakeholders [19]. Addressing this issue is vital, as highlighted by Perera et al. [20], who emphasize that identity theft is a widespread concern across various sectors, including construction. Malicious individuals might exploit the personal details of construction personnel, such as ID numbers and addresses, for fraudulent purposes. Thus, safeguarding workers' personal data from identity theft emerges as a critical need. Doing so not only protects their well-being but also upholds the integrity of the construction field and fosters a secure work environment.

While traditional data management approaches, such as centralized databases, physical safeguards, and the need-to-know principle, have had some level of efficiency, critical challenges, including lack of transparency, susceptibility to unauthorized access, breaches, and theft [21], necessitate a shift towards more advanced privacy management practices and the adoption of secure and efficient digital solutions. Moreover, the increase in digitization and data-driven processes in the construction industry have further amplified the importance of protecting workers' personal information [22–24]. By implementing these digital solutions, the construction industry can streamline privacy-related processes, including consent management [25,26], handling data subject requests [27], and conducting privacy impact assessments [28], thus resulting in improved efficiency and compliance. However, it is vital for the construction industry to carefully select and implement these digital solutions by considering various factors, such as data security, scalability, interoperability, and alignment with privacy regulations.

Recognizing these challenges, this study aimed to address the problem of effectively managing construction workers' personal information while prioritizing their privacy and safety. To achieve this, this study focused on leveraging the Hyperledger Fabric blockchain framework, which offers a permissioned and modular architecture tailored for business networks, to develop an information management model that provides secure storage and controlled access to workers' data. The adoption of a private blockchain specifically built on the Hyperledger Fabric framework was a strategic choice driven by the unique needs and considerations of the construction industry [29]. Unlike public blockchains, private blockchains restrict access to authorized participants, thus offering a heightened level of control and privacy, which is imperative when dealing with sensitive information [30], such as construction workers' personal and safety data. The permissioned nature of the blockchain ensures that only designated stakeholders, including project managers, engineers, and regulatory bodies, have access to the stored information. This enhanced control mitigates the risks associated with unauthorized access, a critical aspect when prioritizing the privacy and security of construction workers' data.

The integration of blockchain technology within the construction industry marks a significant scientific advancement. The application of blockchain principles, including decentralization, immutability, and transparency, offers a novel approach to address the intricate challenges associated with information management in construction projects. According to Politou et al. [31], the scientific underpinning of blockchain ensures a tamper-resistant and decentralized data storage system, thus fundamentally altering the conventional landscape of information management. The scientific principles of data security and privacy are integral to this study. By leveraging cryptographic techniques and a decentralized structure, blockchain enhances the security of sensitive data in the construction sector. As noted by Pan et al. [32], the immutable nature of blockchain ensures that once data are recorded, they cannot be altered or manipulated, thus providing a robust foundation for securing construction workers' personal information. This consequently fosters trust and collaboration among the various stakeholders in the construction industry.

1.1. Problem Statement

The construction industry is characterized by its intricate dynamics, which involve a multitude of participants and a varied labor force. The industry encompasses a spectrum of projects, spanning from minor renovations to major infrastructure projects. Consequently, it becomes crucial to address the complexities and hurdles associated with information management within this dynamic setting. Traditional approaches to information management in construction often rely on manual processes, paper-based documentation, and centralized record-keeping systems. However, these methods are prone to inefficiencies, data inconsistencies, and security vulnerabilities. Such shortcomings pose a threat to the privacy and safety of workers' personal information, leaving them susceptible to risks like identity theft.

Furthermore, due to the inherent risks associated with construction activities, workers are frequently exposed to non-fatal injuries, including work-related musculoskeletal disorders (WMSDs). WMSDs are functional disorders caused by external factors, such as repetitive movements, overexertion, awkward postures, and vibrations in the occupational setting [33]. These disorders can have a significant impact on workers' health and well-being, leading to increased sick leave and decreased productivity. For instance, a study by Dong et al. [34] reported that the prevalence of WMSDs in the construction industry was found to be 31.2%. This highlights the urgent need for the construction industry to effectively manage information (i.e., risk assessment data) associated with such high-risk construction activities that threaten the safety of its workforce.

In response to these challenges, this study seeks to improve information management practices—specifically, the privacy and safety of construction workers. This study leverages advanced technologies, particularly blockchain, to establish a secure, efficient, and decentralized system for managing workers' information. The integration of Hyperledger Fabric on the robust AWS cloud platform forms the backbone of this approach. This study uniquely contributes to the field by conducting a comprehensive case study on tiling activities within a renovation project to generate worker safety data, practical implementation of GDPR-compliant biodata, and relevant safety data assessment techniques. Through phases of experimental design, including blockchain infrastructure creation, chaincode development, and real-world deployment on AWS, this research establishes a fundamental change in information management practices, thereby emphasizing worker safety, privacy, and the overall success of construction endeavors.

1.2. Research Motivation and Significance

This study is driven by the objective of transforming data management practices in the construction industry through the development of a resilient digital system. The paramount concern for the welfare of construction workers arises from the sensitive nature of their personal information, which encompasses details vital for administrative and operational purposes, such as employment, compliance, and safety. However, the conventional approaches leave a yawning gap, thus rendering these valuable data susceptible to breaches, identity theft, and misuse. The consequences, which extend beyond legal and ethical dimensions, manifest in compromised worker safety, eroded trust, and potential harm to individuals. Through the implementation of a blockchain-based solution, the authors seek to introduce a solution that significantly improves the efficiency, trustworthiness, and security of information management within the construction industry.

This study holds paramount significance for the construction workforce. The protection of personal information directly contributes to the well-being and trust of construction workers. In a sector known for its physically demanding tasks and safety risks, the social implications of ensuring privacy resonate deeply. According to Khando et al. [35], addressing the social dynamics involved in safeguarding worker information fosters a positive work environment, which ultimately impacts the morale and productivity of the workforce. Moreover, the proposed blockchain model facilitates collaboration among diverse stakeholders in the construction industry. This collaboration extends to workers, project managers, and regulatory bodies, thus emphasizing the social dynamics of trust and transparency within the construction ecosystem. As discussed by Tapscott and Tapscott [36], the collaborative nature of blockchain is transforming industries by providing shared, secure, and transparent information, thereby fostering a sense of shared responsibility and accountability among stakeholders.

1.3. Research Aim and Objectives

The aim of this study was to develop a private blockchain solution on Hyperledger Fabric to serve as an information management platform to enhance the privacy and safety of construction workers' personal information. The following objectives served as a guide for achieving the above-stated aim:

(1) To develop a Hyperledger fabric blockchain for privacy protection of personal information and safety among construction workers.
(2) To optimize Amazon Web Services (AWS) as the cloud provider and storage service to deploy the blockchain solution.
(3) To test and evaluate the effectiveness of the blockchain for ensuring privacy protection and the security of construction workers' personal information.
(4) To develop a conceptual blockchain model to enhance the privacy and safety of construction workers' personal information, and to illustrate the practical implementation of the proposed model to validate its usability and benefits for the construction industry.

2. Literature Review

2.1. Traditional Methods of Data Management

Traditional methods of data management for construction workers have long been utilized to safeguard their personal information even before the emergence of advanced technologies. These methods involve a combination of organizational policies, physical safeguards, and administrative practices aimed at safeguarding workers' privacy.

One of the primary aspects of privacy management in the construction industry is the establishment of strict organizational policies and procedures. Employers typically develop privacy policies that outline the collection, use, and disclosure of workers' personal information [37]. These policies specify the purposes for which the information is collected and how it will be protected. By clearly communicating these policies to workers, employers ensure transparency and foster a culture of privacy protection [38]. Physical safeguards are another important component of privacy management. Construction companies implement measures to secure physical spaces where workers' personal information is stored. This can include locked filing cabinets, restricted access areas, and the use of secure storage systems. By limiting physical access to personal information, employers reduce the risk of unauthorized disclosure or theft [39].

Administrative practices also play a crucial role in privacy management for construction workers. These practices involve processes and procedures for handling and managing personal information. Employers may designate specific individuals or departments responsible for collecting, storing, and handling personal data [40,41]. The principle of "need-to-know" is commonly applied, where access to workers' personal information is granted only to individuals who require it for legitimate purposes related to employment or regulatory compliance. By limiting access to such information, construction companies minimize the risk of unauthorized disclosure or misuse [21].

However, while traditional methods of privacy management for construction workers have been implemented over the years, they are not without their challenges. One significant challenge is the reliance on manual processes and paper-based documentation. This approach can be time consuming, prone to human error, and less secure compared to digital systems. Physical safeguards, such as locked filing cabinets, may provide some level of protection, but they can still be vulnerable to unauthorized access or theft [42].

Additionally, Heilig and Voß [21] affirm that the need-to-know principle, while essential for privacy management, can create difficulties in ensuring that only authorized individuals have access to personal information, especially in large construction projects with multiple stakeholders. The lack of standardized practices across the industry also poses challenges in terms of consistency and accountability in privacy management [43]. With the rise of digitization and data-centric processes in construction, ensuring the privacy and security of workers' personal information has become a crucial issue [22–24]. While traditional methods have provided some level of effectiveness, addressing these challenges requires a shift towards more advanced privacy management practices and the adoption of secure and efficient digital solutions.

2.2. Advanced Privacy Management Practices and the Adoption of Secure and Efficient Digital Solutions

In response to the limitations of traditional data management methods, the construction industry is increasingly turning to advanced management practices and adopting secure and efficient digital solutions [3,44,45]. These practices leverage technological advancements to enhance privacy protection, data security, and compliance with privacy regulations. One key aspect is the implementation of privacy-enhancing technologies [46,47], such as encryption [48], tokenization [49], and data anonymization [50]. These techniques ensure that personal information is protected both during storage and transmission, thus reducing the risk of unauthorized access or breaches.

Additionally, the use of secure digital platforms and cloud-based solutions enables companies to centralize and manage workers' data more efficiently and securely. This includes various features, such as access controls, audit trails, fire walls, and user authentication mechanisms, to ensure that only authorized individuals have access to personal information [51]. Furthermore, construction companies are implementing strict data governance and data retention policies to ensure that personal information is retained only for as long as necessary and securely disposed of when no longer required [52]. By adhering to these policies, companies can minimize the potential risks associated with retaining personal information beyond its intended purpose [53].

The adoption of such digital solutions enables the construction industry to streamline privacy-related processes, such as consent management [25,26], data subject requests [27], and privacy impact assessments [28], thus leading to increased efficiency and compliance. However, it is essential for construction companies to carefully select and implement these digital solutions by considering certain factors, such as data security, scalability, interoperability, and alignment with privacy regulations.

Thus, utilizing advanced technologies, such as blockchain, can offer potential solutions to enhance privacy in the construction industry [3,20,54]. For example, in the realm of securing construction workers' data, the adoption of blockchain technology over classical encryption methods is driven by its inherent features that address specific challenges in data management. Blockchain, as a decentralized and distributed ledger, ensures enhanced security through its consensus mechanisms and cryptographic hashing. Classical encryption methods, while effective, lack the transparency and immutability that blockchain provides. The construction industry demands a system where data integrity is guaranteed and any alteration is immediately noticeable. Blockchain's decentralized nature ensures that there is no single point of failure, thus reducing vulnerability to attacks [55]. Furthermore, the transparency of the blockchain allows for secure and traceable transactions, which fosters trust among stakeholders [56]. Classical encryption methods, although capable of securing data, may not offer the same level of transparency and resistance to tampering [57].

Blockchain technology, with its decentralized and immutable nature [31,58,59], provides a secure and transparent platform for storing and managing data. This decentralized approach minimizes the risks associated with centralized databases, as it requires consensus among network participants (in the case of the construction industry, stakeholders) to validate and record transactions, thus ensuring data integrity and security. Implementing blockchain-based systems in the construction industry can foster a climate of trust and transparency [60]. Construction workers can have confidence that their personal information is securely stored and accessed only by authorized parties, thereby enhancing accountability and reducing the likelihood of privacy breaches [14].

2.3. Evolution of Blockchain Technology: From Bitcoin to Blockchain 3.0

Blockchain technology is recognized as a critical enabler of progress and innovation within several domains, including the construction industry. In 2008, Satoshi Nakamoto introduced a white paper that unveiled the concept of blockchain as a technology for validating cryptocurrency transactions [61]. This groundbreaking publication brought the term "blockchain" into mainstream recognition and paved the way for its subsequent evolution. The evolution of blockchain can be categorized into different phases: Blockchain 1.0, which primarily revolves around cryptocurrencies; Blockchain 2.0, which incorporates "smart contracts"; and Blockchain 3.0, the current and final stage that focuses on diverse applications and encompasses widespread adoption of blockchain technology in global institutions and entrepreneurial ventures [62].

Since its inception, the concept of blockchain has been shaped and defined by researchers and professionals in various ways. For instance, Casino et al. [63] described blockchain as a distributed append-only data structure with timestamps, while Lee et al. [64] emphasized its decentralized peer-to-peer network for transparently sharing real-time updates. Penzes et al. [65] defined blockchain as a type of distributed ledger technology that allows data to be shared across multiple locations without intermediaries. Gupta [66] highlighted the direct peer-to-peer interactions enabled by blockchain, which are facilitated by a consensus mechanism and cryptographic security. In the construction industry, stakeholders join a blockchain network where governance is based on consensus and consent [62]. The integration of smart contracts into blockchain technology has opened possibilities for diverse industries, including the construction sector [67]. Smart contracts stored on the blockchain are self-executing digital contracts that automatically fulfill predetermined conditions [65]. By eliminating the need for traditional intermediaries, such as banks, smart contracts enable efficient and cost-effective transactions on the blockchain [68].

2.4. Blockchain Technology as an Information Management System

Blockchain technology has emerged as a transformative solution for information and data management, and it offers unparalleled security, transparency, and efficiency. With its decentralized and distributed nature, blockchain ensures data integrity and authenticity through consensus mechanisms, thus eliminating the need for intermediaries [65]. The immutability of blockchain records provides a tamper-proof system that is particularly valuable for industries like construction, where maintaining an accurate and tamper-proof record of information is critical [69]. Enhanced data privacy and control are achieved through cryptographic keys, thus allowing individuals to manage access permissions [70].

Blockchain also streamlines data management by eliminating the need for reconciling multiple copies of data across different systems [71]. Its distributed nature ensures synchronized data for all participants, thereby reducing errors and duplication [72,73]. And, its decentralization enhances security by preventing single points of failure and promoting trust and transparency among stakeholders. Overall, blockchain technology offers unparalleled security, transparency, and efficiency in information management [60,74,75].

2.5. Blockchain Types

Blockchain technology consists of various types: public, private, and consortium blockchains. Public blockchains, like Bitcoin and Ethereum, are open to everyone, thus enabling participation, transaction validation, and ledger upkeep. They emphasize transparency and security, but their consensus mechanisms can lead to scalability and transaction speed issues [76]. Private blockchains are restricted networks that only allow certain entities or individuals to participate [77]. Examples include Hyperledger Fabric and Quorum [78,79]. These are often used by businesses to ensure data privacy and control. They offer efficiency, scalability, and faster transactions compared to public blockchains, as they do not face the same computational limitations [79].

Consortium blockchains are networks where a group of organizations jointly governs the system. Notable examples are R3 Corda [80] and Hyperledger Besu [81]. In these setups, participating entities hold partial control, and consensus is achieved through predefined mechanisms. These blockchains offer a middle ground between fully open public blockchains and tightly controlled private ones. They are ideal for industries needing collaborative information sharing while upholding trust among participants [82]. The choice of blockchain type depends on specific requirements, such as desired levels of transparency, privacy, scalability, governance, and the nature of participating entities.

2.6. Key Concepts of Blockchain Technology

The data structure of a blockchain consists of two main components: the block header and the block. The block header contains parameters, such as the index, previous block hash, timestamp, nonce, and Merkle root. These parameters play crucial roles in ensuring the integrity, security, and chronological order of the blockchain [83]. The index, also known as the block height, indicates the position of the block within the blockchain. The first block, called the genesis block, has an index of zero, and subsequent blocks increment the index [84]. The previous block hash establishes a link between blocks, thus ensuring the continuity and integrity of the blockchain, because altering a block would require recalculating the hash value for all subsequent blocks [85]. The timestamp indicates the time at which the block is created. It helps to order the blocks chronologically, which facilitates the sequence of events in the blockchain [86].

In the process of blockchain mining, miners use a random value called a nonce to fulfill specific criteria in the consensus algorithm, thereby enhancing network security and resource requirements [87]. The Merkle root ensures transaction integrity through cryptographic hashing and creates a hierarchical structure called a Merkle tree [88]. A block's body contains validated transactions, which can vary based on the application; for construction workers' information management, these transactions might include registration, updates, access permissions, verification, authentication, and termination. These transactions are stored within the block and are extremely difficult to modify due to blockchain's immutability, thus ensuring data integrity and security [89].

Figure 1 illustrates the data structure of a block, referred to as "Block w," which includes four transactions: Tx 1, Tx 2, Tx 3, and Tx 4. In the blockchain, each block has a distinct hash, and it references the previous block, thus forming an unchangeable chain of data. A hash function is applied to the information within each transaction, resulting in unique cryptographic hash values, such as Hash1, Hash2, Hash3, and Hash4. These hash values serve as digital fingerprints for the transaction data, enabling efficient detection of any unauthorized modifications. Consequently, the blockchain ensures the prevention of unauthorized changes by facilitating efficient verification and validation processes.

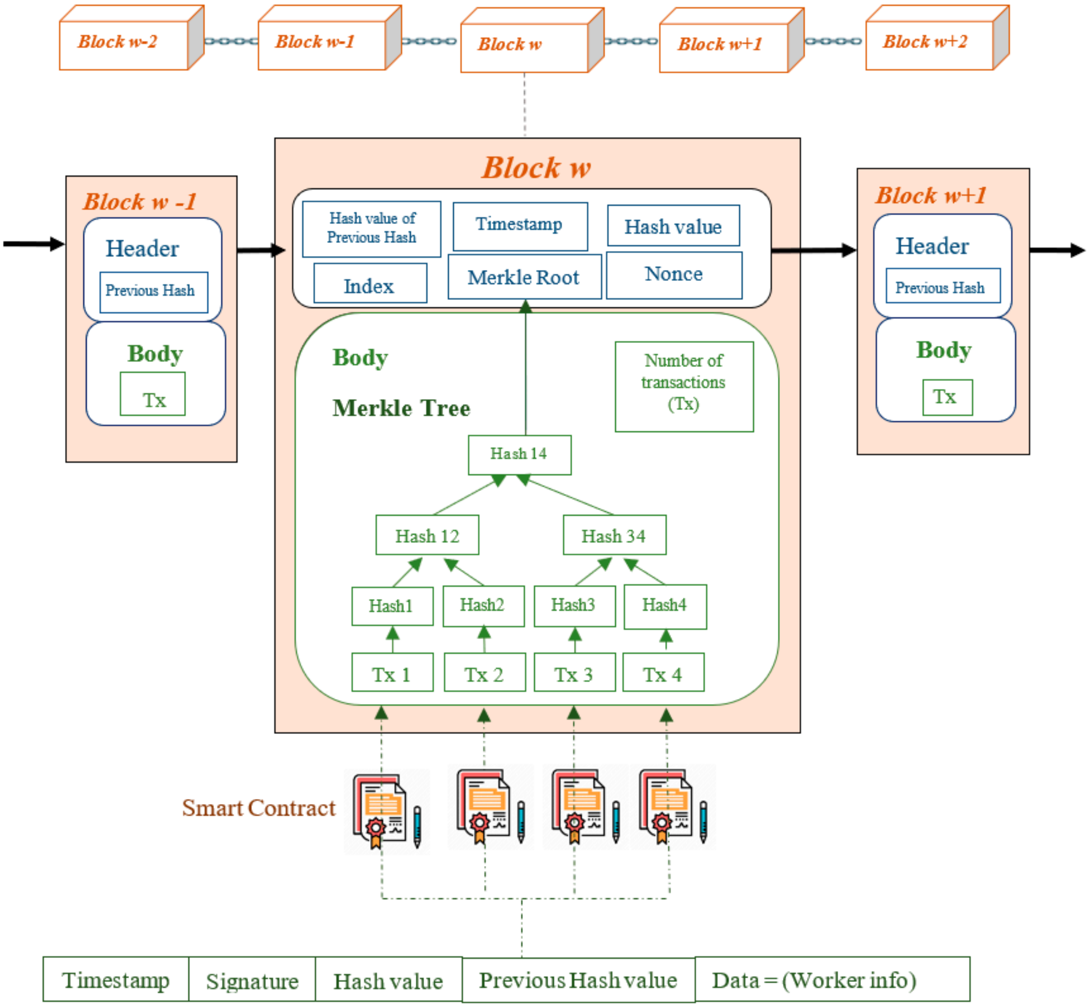


Figure 1. Data structure of a block in a blockchain.

3. Methodology

This study proposed a blockchain system architecture designed to safeguard the privacy and security of personal information for construction workers, particularly their biographic and safety data. The approach involved securely storing hypothetical biodata and safety data and managing this information using the proposed blockchain system. The biodata of workers adhere to the European Union's General Data Protection Regulation

(GDPR), including certain details, such as names, ages, addresses, identification numbers, qualifications, certifications, and employment records. The safety data include scores of the risk level based on the joint angle information from the image process using image-based motion capture technology and occupational assessments using the Rapid Entire Body Assessment (REBA) observational tool [90,91] to evaluate the risk of musculoskeletal disorders.

This system utilized the Hyperledger Fabric blockchain on the AWS cloud platform, thus ensuring decentralization and immutability. The outcome was a robust information management model that enhances the privacy and safety of construction workers' data. This model permits authorized construction stakeholders to access trustworthy and verified data, thereby enabling informed decision making that prioritizes the well-being of the workers. The overall framework of this approach is depicted in Figure 2.

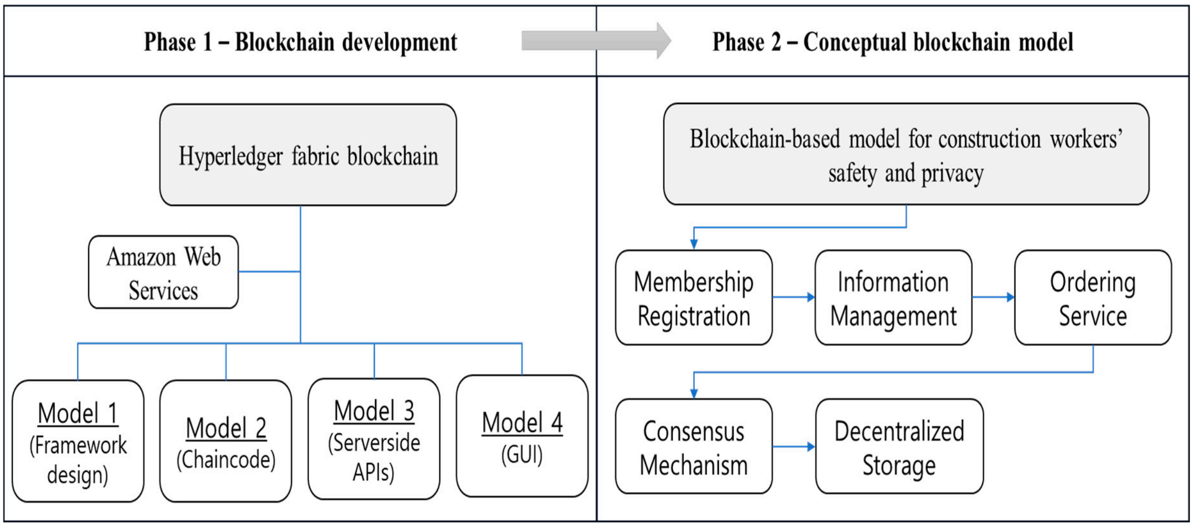

Phase 1 – Blockchain development
Phase 2 – Conceptual blockchain model
Hyperledger fabric blockchain
Amazon Web Services
Model 1 (Framework design)
Model 2 (Chaincode)
Model 3 (Serverside APIs)
Model 4 (GUI)
Blockchain-based model for construction workers' safety and privacy
Membership Registration
Information Management
Ordering Service
Consensus Mechanism
Decentralized Storage

Figure 2. Overall framework of this study.

This study was conducted in two phases. Phase 1 involved the experimental design of the proposed blockchain system and the storage of the workers' hypothetical biodata and safety data. Phase 1 was carried out in 4 modules. These included the implementation of Module 1, which focused on developing the blockchain using the Hyperledger Fabric platform on the AWS cloud provider. Module 2 encompassed the development of the chaincode. Module 3 involved the creation of a server-side Application Programming Interface (API), which allows client applications to send requests to the server and receive responses. Finally, Module 4 entailed integrating the blockchain system onto a third-party graphic user interface (GUI), thus enabling easy visualization of the data. In phase 2, the results from the experimental design and management of the blockchain led to the development of a conceptual information management model for enhancing the privacy and safety of construction workers' personal information and its practical implementation to validate its usability and benefits for the construction industry.

3.1. Experimental Design of the Proposed Blockchain

3.1.1. Blockchain System Architecture of the Case Study

In this architecture, the biodata and safety data of the tilers are stored in a decentralized manner on the blockchain network. Each worker's information is encrypted and stored in blocks, thus forming an immutable and tamper-proof ledger. Data encryption aids in preventing unauthorized users from accessing data stored within a blockchain network and its data storage system [92]. Access to the data is strictly controlled through cryptographic keys, thus ensuring confidentiality and privacy. Unlike traditional centralized systems, where a single point of failure can compromise the privacy of workers, the distributed nature of the proposed blockchain provided an added layer of protection against data breaches and unauthorized access and allowed for real-time updates and synchronized data [93] across all relevant stakeholders, including employers, regulatory bodies, and project managers. Smart contracts or chaincodes are implemented to automate key processes related to construction workers' management, such as verifying trade type or skills, certifications, high-risk-level workers, and tracking training programs.

3.1.2. System Structure of Proposed Blockchain

Figure 3 below shows the system structure for the proposed Hyperledger Fabric blockchain developed on AWS. The system structure was organized into five (5) layers to facilitate the functioning of the blockchain network. The layered structure can be described from bottom to top as follows:

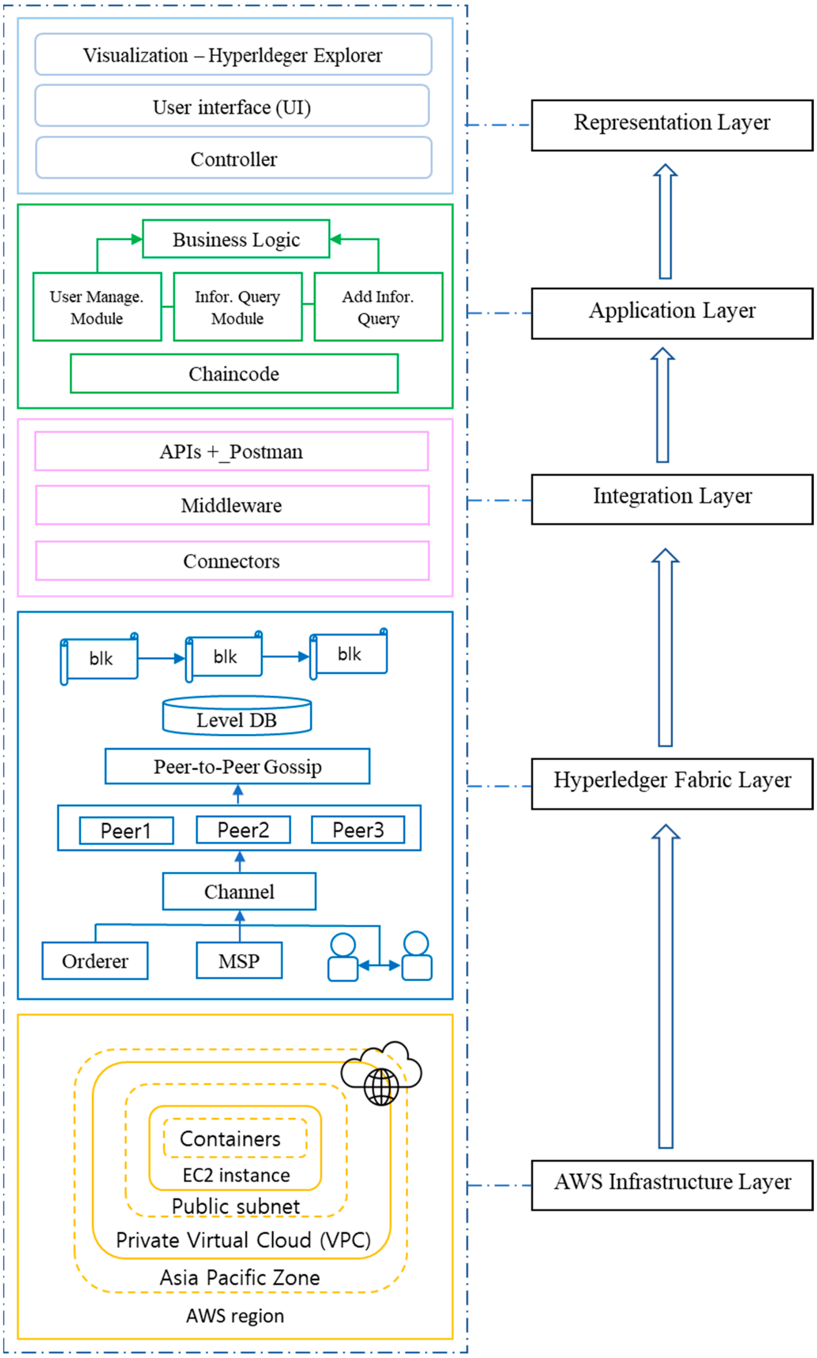


Figure 3. System structure for proposed Hyperledger Fabric blockchain.

AWS Infrastructure Layer: This layer served as the foundational layer for the proposed blockchain system, and it was built using Amazon Web Services (AWS). It established a cloud computing platform for setting up and managing the network. This layer utilized various AWS components, like virtual machines, storage services, and networking resources. To ensure scalability, Auto Scaling was implemented, which dynamically adjusted resources as per demand. AWS's Elastic Cloud Compute (EC2) provided virtual servers for running applications. This infrastructure was created in the Asia Sydney AWS region on a Virtual Private Cloud (VPC) network to ensure network isolation and security for the blockchain network. An EC2 instance on the Ubuntu platform was set up within this network to establish a secure environment. This infrastructure configuration was designed to support the secure and efficient functioning of the blockchain system.

Hyperledger Fabric Layer: This layer implemented the Hyperledger Fabric protocol, which is designed for secure and efficient permissioned networks. This layer consisted of various components, including 2 organizations, 1 Orderer node, 2 Peer nodes, 1 Certificate Authority (CA), a Membership service provider (MSP), the Channel, a Gossip, a LevelDB storage library, and blocks. In this blockchain framework, organizations represented stakeholders with authorized access, such as project managers, engineers, regulators, etc. Peer nodes were crucial for network maintenance, storing copies of the blockchain, participating in consensus, validating and sharing transactions, and upholding decentralization. These peers communicated to verify and synchronize data, thus ensuring the reliability of the distributed ledger.

The Orderer node maintained transaction sequencing and consistency. It organized transactions into blocks, thus maintaining their chronological order and integrity. By broadcasting these blocks to peers, the Orderer enabled consensus on transaction validity and ensured a synchronized view of the blockchain across the network. Certificate Authorities (CAs) played a crucial role in establishing trust and verifying the identities of network participants. They issued digital certificates that linked public keys to specific identities, thus enabling authentication and secure communication. CAs managed certificates, verified identities, and ensured secure interactions and transactions, thereby enhancing network security and trust. Channels enabled secure and confidential communication and transactions between specific stakeholders. Private channels ensured data privacy and compliance with regulations, thus facilitating secure information exchange among relevant parties. The Gossip protocol facilitated peer-to-peer communication and data synchronization in the network. It efficiently disseminated information through interconnected peers, thus ensuring scalability and efficient communication.

LevelDB, an open-source key-value storage library, was used to store and retrieve blockchain data efficiently. It provided a simple key-value data model, allowing users to insert, retrieve, and delete data based on unique keys. Blocks represented collections of transactions organized sequentially and added to the blockchain. They formed the fundamental units of the blockchain, encapsulating multiple transactions within a single entity.

Integration Layer: The integration layer facilitated the integration of the blockchain network with external systems and services. It included APIs, which were tested successfully in Postman (an API platform), a middleware, and connectors that enabled communication and data exchange between the blockchain network and other external applications. This layer ensured seamless integration and interoperability between the blockchain network and existing infrastructure.

Application Layer: The application layer was made up of business-specific applications and chaincode developed with Java version 11.10.18. Java was chosen for its broad adoption and versatility, thus streamlining the implementation process and ensuring the flexibility of the chaincode. The chaincode was built to be highly secure, deterministic, and transactional. It served as the foundation for the construction workers' information management system, offering various functions. These included adding workers' biodata and safety information, retrieving data, and making updates to details like qualifications, certifications, and work history. These features were customized to cater to the construction industry's specific requirements.

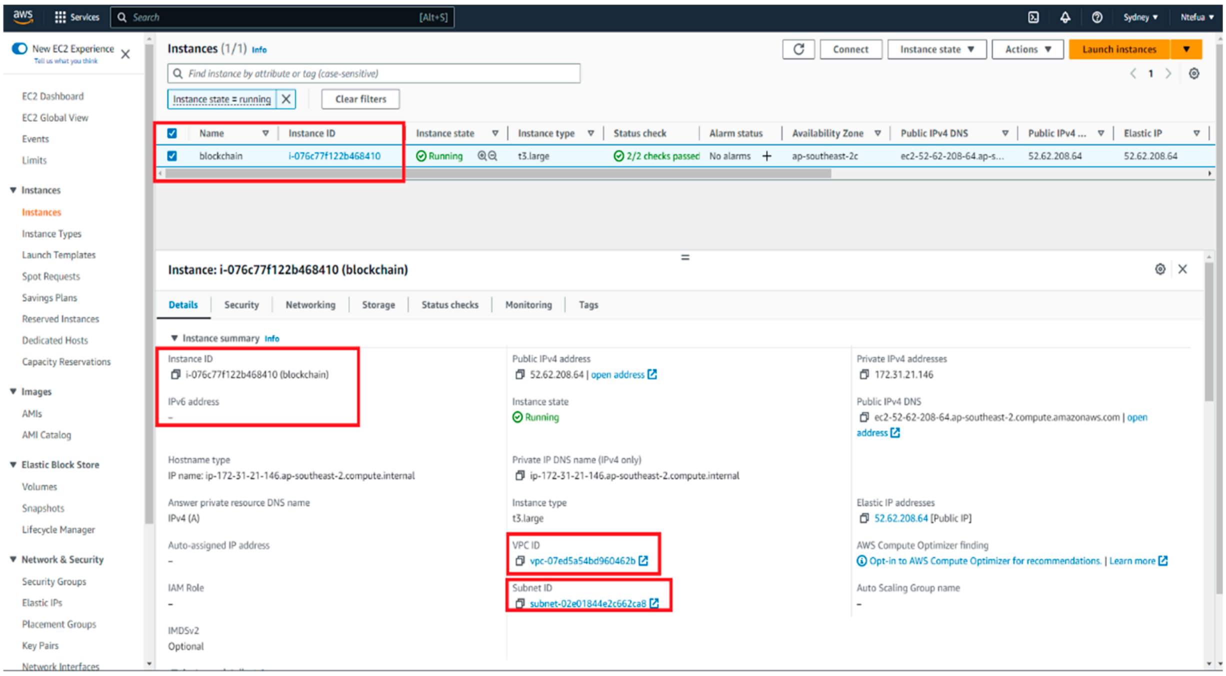
Representation layer: The representation layer was a vital part of the proposed blockchain application's user interface. It included the Controller, User Interface (UI), and Hyperledger Explorer. The Controller acted as a link between the UI and the application's logic, facilitating communication and coordination. The UI offered a graphical or command-line way for users to engage with the blockchain app, such as submitting transactions and accessing ledger data. The Hyperledger Explorer, a visualization tool, gave a comprehensive overview of the blockchain network, displaying block, transaction, and participant details. This layer was crucial for stakeholders to interact with the blockchain effectively while ensuring user-friendliness and transparency.

3.1.3. Deployment of Proposed Blockchain

The deployment of the proposed blockchain utilized a systematic approach, as outlined below in steps 1 to 5.

Step 1: Establishing AWS infrastructure

An AWS infrastructure was created to establish a secure and isolated environment for the blockchain network. This involved setting up an IAM account for access control and provisioning EC2 instances with the necessary computing power and storage. Security measures, including firewalls, access controls, and a VPC (Figure 4), were implemented to prevent unauthorized access and ensure data privacy. Subnets, route tables, and network ACLs were configured within the VPC for traffic control. Network and security groups were employed to manage communication rules, thus adding an extra layer of security. Data protection was ensured through encryption methods like AWS Key Management Service (KMS). Overall, this setup laid a strong foundation for the blockchain system, guaranteeing both network security and efficient operation.



Instances (1/1) Info

Instance state = running

☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
☑	blockchain	i-076c77f122b468410	Running	t3.large	2/2 checks passed	No alarms +	ap-southeast-2c	ec2-52-62-208-64.ap-s...	52.62.208.64	52.62.208.64

Instance: i-076c77f122b468410 (blockchain)

▼ Instance summary Info

Instance ID
i-076c77f122b468410 (blockchain)

IPv6 address
–

Hostname type
IP name: ip-172-31-21-146.ap-southeast-2.compute.internal

Answer private resource DNS name
IPv4 (A)

Auto-assigned IP address
–

IAM Role
–

IMDSv2
Optional

Public IPv4 address
52.62.208.64 | open address

Instance state
Running

Private IP DNS name (IPv4 only)
ip-172-31-21-146.ap-southeast-2.compute.internal

Instance type
t3.large

VPC ID
vpc-07ed5a54bd960462b

Subnet ID
subnet-02e01844e2c662ca8

Private IPv4 addresses
172.31.21.146

Public IPv4 DNS
ec2-52-62-208-64.ap-southeast-2.compute.amazonaws.com | open address

Elastic IP addresses
52.62.208.64 [Public IP]

AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations. | Learn more

Auto Scaling Group name
–

Figure 4. AWS infrastructure showing EC2, VPC, and Subnet.

Step 2: Installing and configuring the Hyperledger Fabric components

The AWS infrastructure was set up, followed by the installation and configuration of Hyperledger Fabric components. This involved deploying peers, orderers, and certificate authorities on AWS, each with specific configurations. The network's structure, peer roles, orderer nodes, MSP, and CA infrastructure were established meticulously to meet the network's needs. These components facilitated decentralized consensus, secure transactions, and identity management, thus ensuring the privacy and security of worker data. The proper deployment and configuration led to the creation of a robust and efficient Hyperledger Fabric blockchain system, with detailed information provided in Table 1.

Table 1. Hyperledger Fabric components.

Container ID	Names
76f609623b6e	dev-peer0.org2.example.com-construction-chaincode
5fcc2dcfae2c	dev-peer0.org1.example.com-construction-chaincode
2b0446d09f92	dev-peer0.org2.example.com-basic
89cadb858e55	dev-peer0.org1.example.com-basic
e7a5f020a84f	cli
3fc7a199eaa1	Peer0.org2.example.com
859c95e237d8	Peer0.org.example.com
442b5b213879	couchdb0
d1d9090efa1f	couchdb1
66abe5c9301c	orderer.example.com
d453f4b69751	ca_orderer
c8b1ea1a7c9b	ca_org2
817296bd5f4a	ca_org1

dev = fabric-dev-servers; org = organization; cli = fabric-tools; ca = certificate authority.

Step 3: Storing and managing construction workers' data

To ensure secure storage and management of blockchain data, the LevelDB storage library was integrated with Amazon Web Services (AWS), specifically utilizing Amazon Relational Database Service (RDS). This integration provided a reliable solution for storing and organizing construction worker information, thus ensuring data integrity and confidentiality. RDS, a scalable relational database service, handled essential database management tasks, such as provisioning, scaling, backups, and recovery. By leveraging RDS, construction workers' biodata and safety data were securely stored, while also benefiting from RDS's built-in security capabilities to comply with industry regulations, such as the General Data Protection Regulation (GDPR).

Step 4: Enabling communication and integration among network components

The deployment utilized AWS networking features, including a Virtual Private Network (VPN) and security groups, to enable secure and private communication among the network components. VPN technology established encrypted tunnels for data transmission, thus ensuring data privacy and protection against unauthorized access. Security groups acted as virtual firewalls, regulating traffic flow and enforcing access control policies within the network. AWS's comprehensive suite of services, including data encryption and IAM, further enhanced data confidentiality and security. The deployment met stringent data privacy requirements and upheld the confidentiality of sensitive information stored on the blockchain by adhering to industry best practices and leveraging AWS's robust networking capabilities.

Step 5: Configuration and deployment of chaincode

The proposed blockchain included one chaincode with five algorithm classes (namely, User, SpreadingMortar, TransactionHistory, Keys, and ConstructionChaincode), which were implemented in Java. For example, Algorithm 1 described a Java class called "User" that managed and organized the biodata of the workers into a block. The class defined the structure and properties of a user entity, including various fields, such as user_id, user_name, user_address, user_email, and account_type. Getter and setter methods were provided for each field, thus enabling access and modification of user information.

Algorithm 1 Biodata of construction workers in case study

```
// Define a User class
class User {
    // Define private member variables
    String user_id
    String user_name
    String user_address
    String user_email
    String account_type
    // Define getters and setters for the member variables
    method getUser_id() : String
    method setUser_id(user_id : String) : void
    method getUser_name() : String
```

Algorithm 2 described the safety data of the workers. The algorithm represented a Java class called "SpreadingMortar", which served as a data structure to store information related to risk assessments of the tilers during mortar spreading. The class contained various properties, such as "id", "numberOfFrames", "neckAngle", etc., which represented different aspects of the worker's posture and movements when spreading the mortar, and properties like "rebaScore" and "levelOfMSDRisk" to indicate the calculated risk score and the level of work-related musculoskeletal disorder risk associated with the worker's activities. The class also provided getter and setter methods for accessing and modifying these properties.

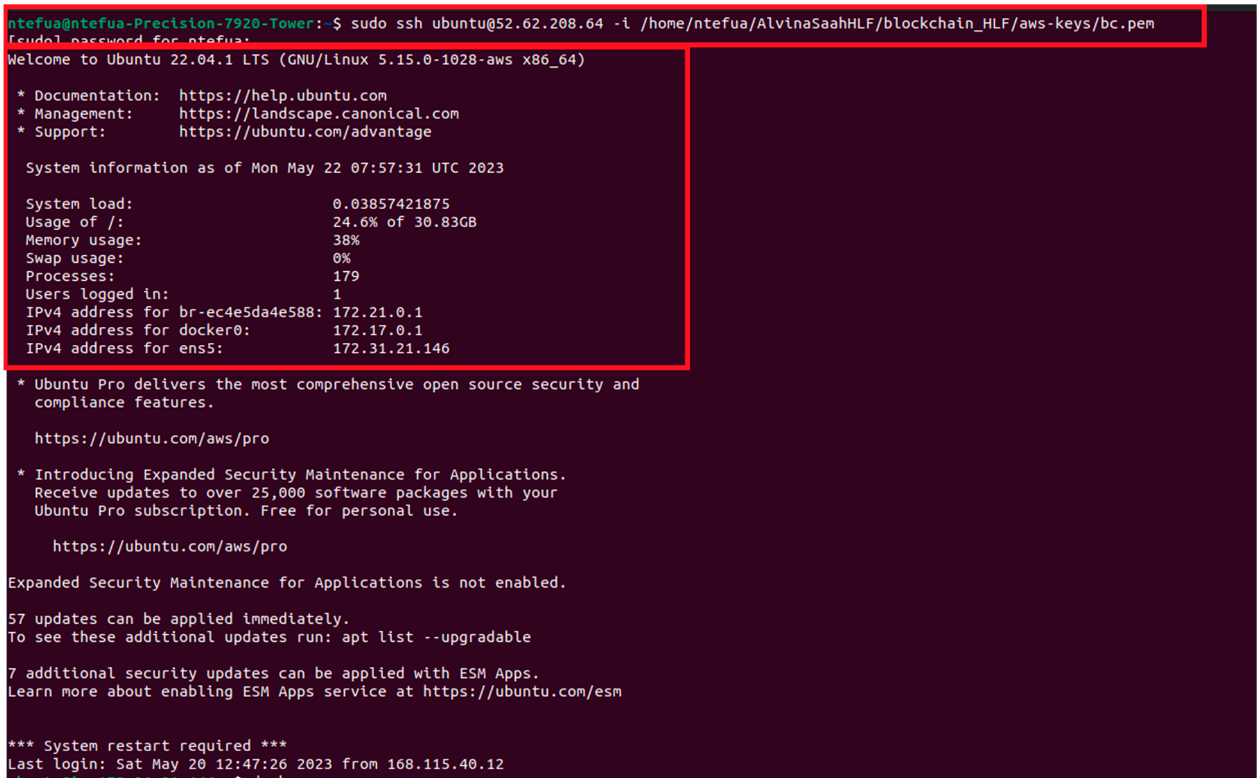
Algorithm 2 Safety data of construction workers

```
// Define a SpreadingMortar class
class SpreadingMortar {
    // Declare private member variables
    String id
    String numberOfFrames
    String neckAngle
    String rightElbow
    String leftElbow
    String rightwrist
    String lefttwrist
    String rightSoulder
    String leftSoulder
    String rightHip
    String leftHip
    String rightKnee
    String leftKnee
    String rebaScore
    String levelOfMSDRisk
    // Define a parameterized constructor
    method SpreadingMotor(id : String, numberOfFrames : String, neckAngle : String,
rightElbow : String, leftElbow : String, rightwrist : String, lefttwrist : String, rightSoulder : String,
leftSoulder : String,
```

4. Results and Discussions

4.1. Results

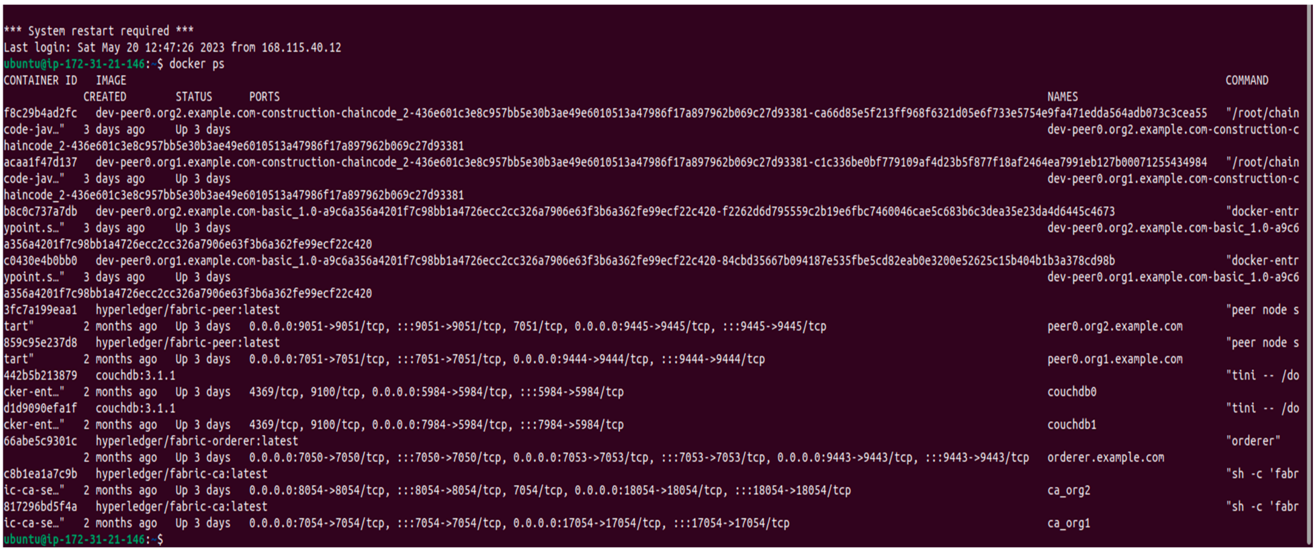
The proposed Hyperledger Fabric blockchain designed on AWS was integrated into an Ubuntu 22.04.1 (64 bit) computer @ LTS (GNU/Linux). The integration was successfully performed using an SSH connection with IP address 52.62.208.64, a private key, and a Username, AlvinaSaahHLF, as shown in Figure 5. This was possible after running Hyperledger Fabric version 2.4.9 on the Ubuntu computer.



```
ntefua@ntefua-Precision-7920-Tower:~$ sudo ssh ubuntu@52.62.208.64 -i /home/ntefua/AlvinaSaahHLF/blockchain_HLF/aws-keys/bc.pem
[sudo] password for ntefua:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-1028-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon May 22 07:57:31 UTC 2023

  System load:                      0.03857421875
  Usage of /:                       24.6% of 30.83GB
  Memory usage:                     38%
  Swap usage:                       0%
  Processes:                        179
  Users logged in:                  1
  IPv4 address for br-ec4e5da4e588: 172.21.0.1
  IPv4 address for docker0:         172.17.0.1
  IPv4 address for ens5:            172.31.21.146

 * Ubuntu Pro delivers the most comprehensive open source security and
   compliance features.

   https://ubuntu.com/aws/pro

 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.

     https://ubuntu.com/aws/pro

Expanded Security Maintenance for Applications is not enabled.

57 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

7 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm


*** System restart required ***
Last login: Sat May 20 12:47:26 2023 from 168.115.40.12
```

Figure 5. AWS-based blockchain integration on Ubuntu computer.

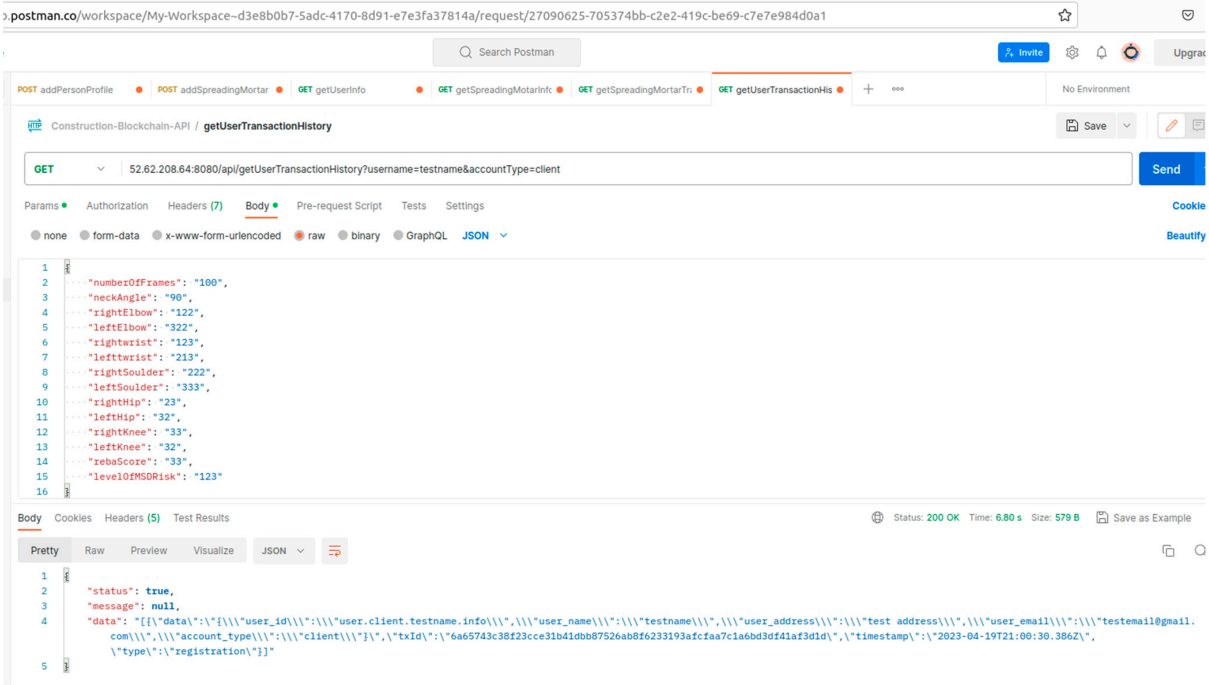
The integration, as shown in Figure 5, confirms that the Hyperledger components were successfully running. Furthermore, the results shown in Figure 6 display the fabric components, including the container IDs, status, ports, names, and commands, which suggest that the Hyperledger Fabric blockchain developed was running successfully.



```
*** System restart required ***
Last login: Sat May 20 12:47:26 2023 from 168.115.40.12
ubuntu@ip-172-31-21-146:~$ docker ps
CONTAINER ID   IMAGE                                                                                                                                                                  COMMAND
               CREATED        STATUS      PORTS                                                                                                                       NAMES
f8c29b4ad2fc   dev-peer0.org2.example.com-construction-chaincode_2-436e601c3e8c957bb5e30b3ae49e6010513a47986f17a897962b069c27d93381-ca66d85e5f213ff968f6321d05e6f733e5754e9fa471edda564adb073c3cea55   "/root/chain
code-jav…"   3 days ago     Up 3 days                                                                                                                               dev-peer0.org2.example.com-construction-c
haincode_2-436e601c3e8c957bb5e30b3ae49e6010513a47986f17a897962b069c27d93381
acaa1f47d137   dev-peer0.org1.example.com-construction-chaincode_2-436e601c3e8c957bb5e30b3ae49e6010513a47986f17a897962b069c27d93381-c1c336be0bf779109af4d23b5f877f18af2464ea7991eb127b00071255434984   "/root/chain
code-jav…"   3 days ago     Up 3 days                                                                                                                               dev-peer0.org1.example.com-construction-c
haincode_2-436e601c3e8c957bb5e30b3ae49e6010513a47986f17a897962b069c27d93381
b8c0c737a7db   dev-peer0.org2.example.com-basic_1.0-a9c6a356a4201f7c98bb1a4726ecc2cc326a7906e63f3b6a362fe99ecf22c420-f2262d6d795559c2b19e6fbc7460046cae5c683b6c3dea35e23da4d6445c4673          "docker-entr
ypoint.s…"   3 days ago     Up 3 days                                                                                                                               dev-peer0.org2.example.com-basic_1.0-a9c6
a356a4201f7c98bb1a4726ecc2cc326a7906e63f3b6a362fe99ecf22c420
c0430e4b0bb0   dev-peer0.org1.example.com-basic_1.0-a9c6a356a4201f7c98bb1a4726ecc2cc326a7906e63f3b6a362fe99ecf22c420-84cbd35667b094187e535fbe5cd82eab0e3200e52625c15b404b1b3a378cd98b          "docker-entr
ypoint.s…"   3 days ago     Up 3 days                                                                                                                               dev-peer0.org1.example.com-basic_1.0-a9c6
a356a4201f7c98bb1a4726ecc2cc326a7906e63f3b6a362fe99ecf22c420
3fc7a199eaa1   hyperledger/fabric-peer:latest                                                                                                                                         "peer node s
tart"        2 months ago   Up 3 days   0.0.0.0:9051->9051/tcp, :::9051->9051/tcp, 7051/tcp, 0.0.0.0:9445->9445/tcp, :::9445->9445/tcp                              peer0.org2.example.com
859c95e237d8   hyperledger/fabric-peer:latest                                                                                                                                         "peer node s
tart"        2 months ago   Up 3 days   0.0.0.0:7051->7051/tcp, :::7051->7051/tcp, 0.0.0.0:9444->9444/tcp, :::9444->9444/tcp                                        peer0.org1.example.com
442b5b213879   couchdb:3.1.1                                                                                                                                                          "tini -- /do
cker-ent…"   2 months ago   Up 3 days   4369/tcp, 9100/tcp, 0.0.0.0:5984->5984/tcp, :::5984->5984/tcp                                                               couchdb0
d1d9090efa1f   couchdb:3.1.1                                                                                                                                                          "tini -- /do
cker-ent…"   2 months ago   Up 3 days   4369/tcp, 9100/tcp, 0.0.0.0:7984->5984/tcp, :::7984->5984/tcp                                                               couchdb1
66abe5c9301c   hyperledger/fabric-orderer:latest                                                                                                                                      "orderer"
             2 months ago   Up 3 days   0.0.0.0:7050->7050/tcp, :::7050->7050/tcp, 0.0.0.0:7053->7053/tcp, :::7053->7053/tcp, 0.0.0.0:9443->9443/tcp, :::9443->9443/tcp   orderer.example.com
c8b1ea1a7c9b   hyperledger/fabric-ca:latest                                                                                                                                           "sh -c 'fabr
ic-ca-se…"   2 months ago   Up 3 days   0.0.0.0:8054->8054/tcp, :::8054->8054/tcp, 7054/tcp, 0.0.0.0:18054->18054/tcp, :::18054->18054/tcp                          ca_org2
817296bd5f4a   hyperledger/fabric-ca:latest                                                                                                                                           "sh -c 'fabr
ic-ca-se…"   2 months ago   Up 3 days   0.0.0.0:7054->7054/tcp, :::7054->7054/tcp, 0.0.0.0:17054->17054/tcp, :::17054->17054/tcp                                    ca_org1
ubuntu@ip-172-31-21-146:~$
```

Figure 6. Fabric components of the proposed blockchain.

In Figure 7, the APIs tested on POSTMAN revealed the transaction status to be true, as the transactions for construction workers' personal information and risk assessment data were carried out and added to the blockchain successfully.



```
.postman.co/workspace/My-Workspace~d3e8b0b7-5adc-4170-8d91-e7e3fa37814a/request/27090625-705374bb-c2e2-419c-be69-c7e7e984d0a1
```

```
GET 52.62.208.64:8080/api/getUserTransactionHistory?username=testname&accountType=client
```

○ none ○ form-data ○ x-www-form-urlencoded ● raw ○ binary ○ GraphQL JSON

```
{
    "numberOfFrames": "100",
    "neckAngle": "90",
    "rightElbow": "122",
    "leftElbow": "322",
    "rightwrist": "123",
    "lefttwrist": "213",
    "rightSoulder": "222",
    "leftSoulder": "333",
    "rightHip": "23",
    "leftHip": "32",
    "rightKnee": "33",
    "leftKnee": "32",
    "rebaScore": "33",
    "levelOfMSDRisk": "123"
}
```

Status: 200 OK Time: 6.80 s Size: 579 B

JSON

```
{
    "status": true,
    "message": null,
    "data": "[{\"data\":\"{\\\"user_id\\\":\\\"user.client.testname.info\\\",\\\"user_name\\\":\\\"testname\\\",\\\"user_address\\\":\\\"test address\\\",\\\"user_email\\\":\\\"testemail@gmail.
        com\\\",\\\"account_type\\\":\\\"client\\\"}\",\"txId\":\"6a65743c38f23cce31b41dbb87526ab8f6233193afcfaa7c1a6bd3df41af3d1d\",\"timestamp\":\"2023-04-19T21:00:30.386Z\",
        \"type\":\"registration\"}]"
}
```

Figure 7. Screenshot of part of the Transaction History API tested in POSTMAN.

4.1.1. A Conceptual Blockchain-Based Model for Enhancing the Privacy and Safety of Construction Workers' Personal Information

The results from the experimental design led to the development of a robust information management blockchain model aimed at enhancing the privacy and safety of construction workers (Figure 8). The model functions because (i) it allows pertinent stakeholders, such as the Human resource manager, project manager, contractor, health and safety officer, regulatory bodies, inspector, and certification body, to register as members of the network to endorse the construction workers' data; (ii) construction workers' biodata and safety data are stored and require the participants in (i) to sign and endorse the information digitally, and the governance of the network is established based on the consensus and consent of all of the stakeholders; (iii) every time information is requested by a permitted stakeholder, the smart contract (chaincode) converts it into a transaction and sends it to the ordering service through which transactions are packed into blocks; in this way, the transactions are then secured cryptographically before being added to a blockchain system to create an immutable chain of records; (iv) to further enhance the security of the information during the endorsement process, the proposed model uses a consensus algorithm to ensure complete protection of the privacy of the data; and (v) each participant (stakeholder) on the blockchain sets up a copy of the ledger to keep track of the endorsed transaction information, and the smart contract can retrieve the stored transactions from the ledgers whenever requested by the stakeholders.

4.1.2. Testing of Conceptual Blockchain-Based System Using the Transaction Testing Approach

To validate the functionality and effectiveness of the Hyperledger Fabric blockchain system developed for the tiling activity case study, comprehensive testing was conducted, with a significant focus on transaction verification. The primary objective was to ensure the system's reliability, data accuracy, and its ability to securely manage and store construction workers' biographic and safety data related to work-related musculoskeletal disorder (WMSD) risk assessments. Transaction testing played a crucial role in validating the blockchain's functionality and data integrity. Hyperledger Explorer, a powerful visualization tool, was employed to facilitate the monitoring and analysis of transactions, shown in Figure 9.

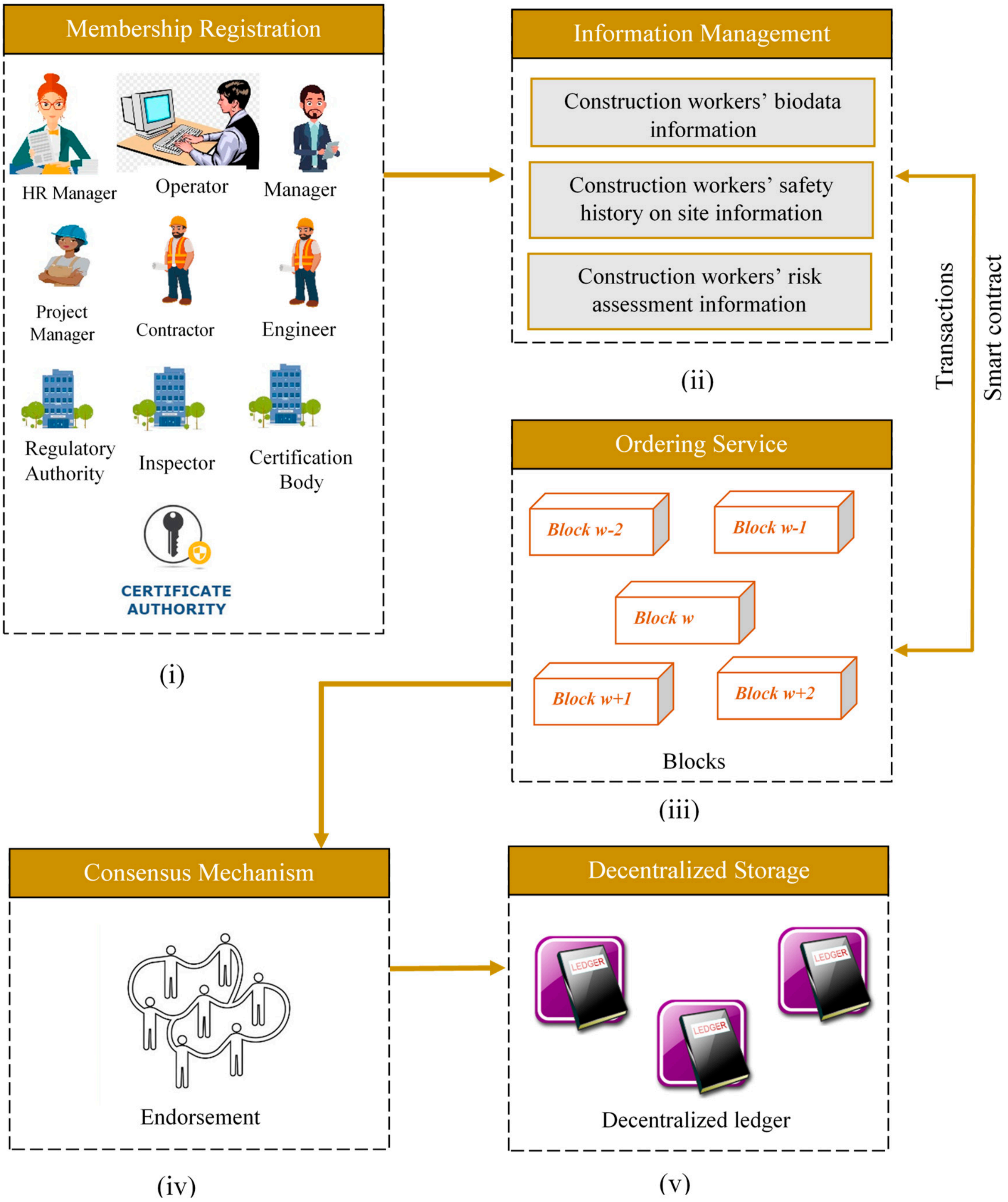
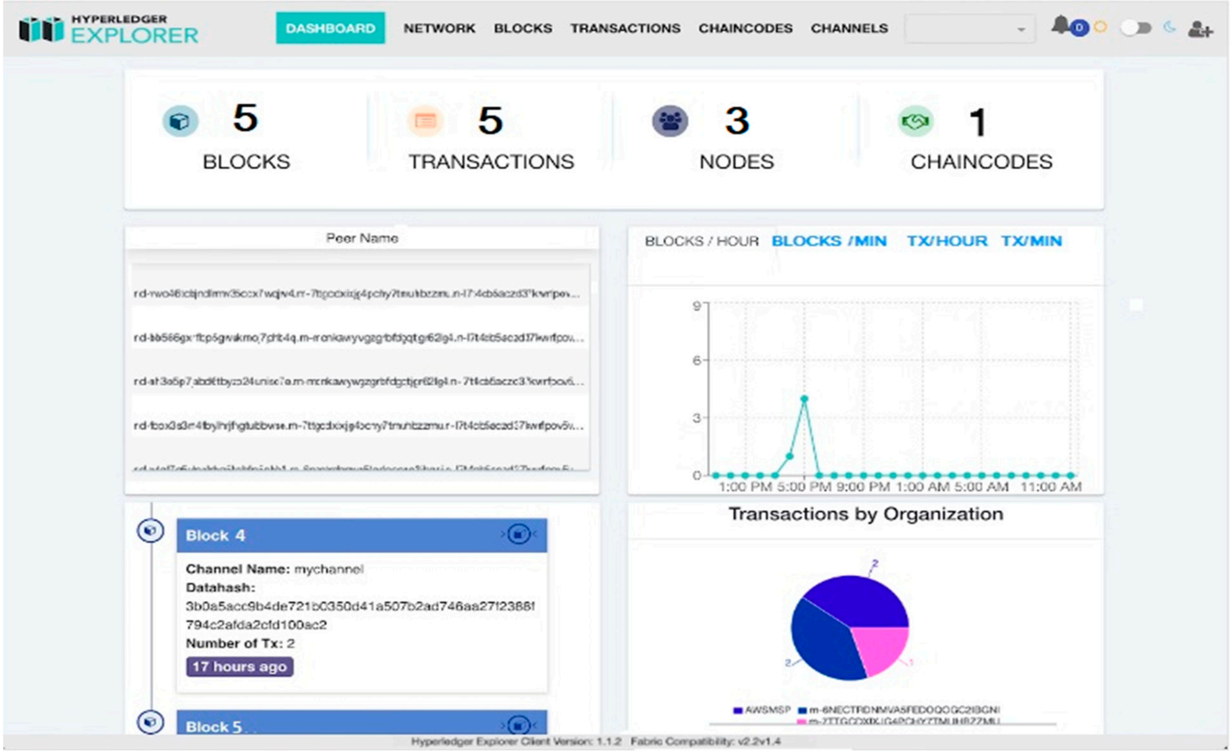


Figure 8. A blockchain-based model for enhancing the privacy and safety of construction workers' information. (**i**) Membership registration; (**ii**) Information management; (**iii**) Ordering Service; (**iv**) Consensus mechanism; (**v**) Decentralized ledger of construction workers' biodata and safety data.

Through this implementation, the blockchain demonstrated its capability to securely collect, store, and manage sensitive worker information. Each step of the data collection process, from capturing workers' biodata to assessing WMSD risks, was translated into transactions on the blockchain. These transactions were then visualized using Hyperledger Explorer, providing a clear and transparent overview of the entire process. In this testing scenario, a total of five blocks, each containing a set of transactions, were generated. These transactions represented various interactions related to the management of construction workers' data. The involvement of three nodes in the network underlines the decentralized nature of the Hyperledger Fabric blockchain, where multiple stakeholders collaboratively maintain the integrity of the network and validate transactions. Furthermore, the presence of one chaincode emphasized the smart contract's role in governing the rules and logic for managing data on the blockchain.



rd-nwo46icbjndimw3bccx7wqjw4.m-7tgccxisjg4pchy7tmuhbzzmu.n-l74cb6aczd3'kwfpev...

rd-bb566gx-fcp5gwakmo7chb4q.m-nonkawyvgzgrbfdgqtgr62lg4.n-l7t4cb5aczd17kwfpov...

rd-at3a6p7abd6tbyzo24unisc7a.m-mcnkawywgzgrbfdgctjgr62lg4.n-7t4cb6aczc3'kwfpov6...

rd-fcox3s3r4fbylhrjfhgtubbwse.m-7ttgcdxixjg4pcny7tmuhbzzmu.r-l7t4cb6acad17kwfpov5v...

Channel Name: mychannel
Datahash:
3b0a5acc9b4de721b0350d41a507b2ad746aa27f23881
794c2afda2cfd100ac2
Number of Tx: 2

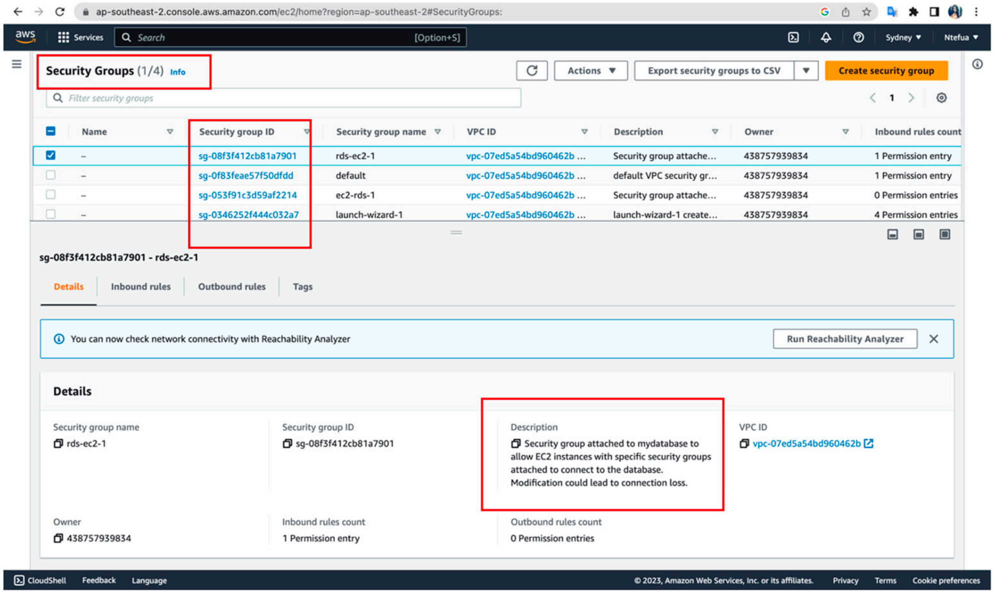
Hyperledger Explorer Client Version: 1.1.2 Fabric Compatibility: v2.2v1.4

Figure 9. Testing of conceptual blockchain system using Hyperledger Explorer.

This comprehensive testing phase not only ensured the technical robustness of the blockchain system but also demonstrated its applicability in a real-world construction context. The blockchain system exhibited its capability to securely manage and provide access to authenticated and verified construction workers' information. The successful visualization of transactions using Hyperledger Explorer showcased the transparency and tamper-resistant nature of the data stored. The outcomes of this testing contribute significantly to the advancement of blockchain technology within the construction industry, empowering stakeholders with informed decision making capabilities, enhancing safety measures, and streamlining workforce management practices.

4.1.3. Security Details of the Conceptual Blockchain Developed on AWS

This section provides a detailed overview of the rigorous security measures integrated into the conceptual blockchain hosted on the Amazon Web Services (AWS) platform. Four specialized security groups (sg-08f3f412cb81a7901, sg-0f83feae57f50dfdd, sg-053f91c3d59af2214, and sg-03462527444c032a7) were meticulously implemented to govern network access to specific instances. Functioning as virtual firewalls, these security groups offer heightened control over communication channels, as represented in Figure 10. Each security group is customized to fortify the overall resilience of the blockchain network, thus addressing stringent security requirements and mitigating the risks associated with unauthorized access.


ap-southeast-2.console.aws.amazon.com/ec2/home?region=ap-southeast-2#SecurityGroups:
aws
Services
Search
[Option+S]
Sydney ▼
Ntefua ▼
Actions ▼
Export security groups to CSV
Create security group
Filter security groups
1
Details
Inbound rules
Outbound rules
Tags
Run Reachability Analyzer
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Security Groups (1/4) Info

	Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbound rules count
☑	–	sg-08f3f412cb81a7901	rds-ec2-1	vpc-07ed5a54bd960462b ...	Security group attache...	438757939834	1 Permission entry
□	–	sg-0f83feae57f50dfdd	default	vpc-07ed5a54bd960462b ...	default VPC security gr...	438757939834	1 Permission entry
□	–	sg-053f91c3d59af2214	ec2-rds-1	vpc-07ed5a54bd960462b ...	Security group attache...	438757939834	0 Permission entries
□	–	sg-0346252f444c032a7	launch-wizard-1	vpc-07ed5a54bd960462b ...	launch-wizard-1 create...	438757939834	4 Permission entries

sg-08f3f412cb81a7901 - rds-ec2-1

You can now check network connectivity with Reachability Analyzer

Details

Security group name: rds-ec2-1

Security group ID: sg-08f3f412cb81a7901

Description: Security group attached to mydatabase to allow EC2 instances with specific security groups attached to connect to the database. Modification could lead to connection loss.

VPC ID: vpc-07ed5a54bd960462b

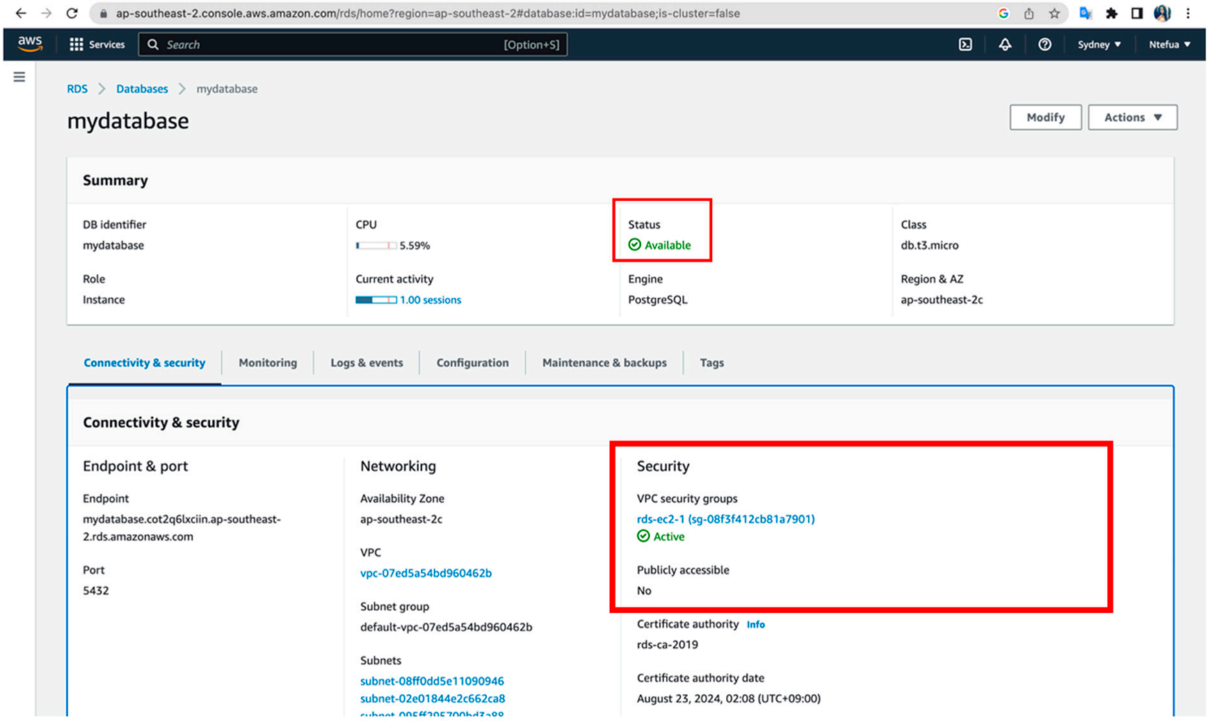
Owner: 438757939834

Inbound rules count: 1 Permission entry

Outbound rules count: 0 Permission entries

Figure 10. Security groups developed on developed blockchain.

Figure 11 provides a snapshot of the database housing the comprehensive data of construction workers securely stored on the blockchain. It confirms the database's availability status, highlighting the active integration of the security group sg-08f3f412cb81a7901 by rds-ec2-1. The "Publicly accessible" parameter status is set as "No," which signifies a secure, non-publicly-accessible blockchain environment. This configuration establishes a robust defense mechanism, thus safeguarding the blockchain against unauthorized external access and aligning with the stringent security standards embedded in the AWS ecosystem. This depiction underscores the stringent security protocols meticulously implemented within our AWS-hosted blockchain, thus ensuring the confidentiality and integrity of the stored construction worker data.



mydatabase

Summary

DB identifier: mydatabase

CPU: 5.59%

Status: Available

Class: db.t3.micro

Role: Instance

Current activity: 1.00 sessions

Engine: PostgreSQL

Region & AZ: ap-southeast-2c

Connectivity & security

Endpoint & port

Endpoint: mydatabase.cot2q6lxciin.ap-southeast-2.rds.amazonaws.com

Port: 5432

Networking

Availability Zone: ap-southeast-2c

VPC: vpc-07ed5a54bd960462b

Subnet group: default-vpc-07ed5a54bd960462b

Subnets: subnet-08ff0dd5e11090946
subnet-02e01844e2c662ca8

Security

VPC security groups: rds-ec2-1 (sg-08f3f412cb81a7901) Active

Publicly accessible: No

Certificate authority Info: rds-ca-2019

Certificate authority date: August 23, 2024, 02:08 (UTC+09:00)

Figure 11. Database snapshot and security status.

These robust security measures are pivotal in addressing concerns related to data vulnerability, identity theft, and misuse. By systematically controlling access to critical information stored on the blockchain, these security configurations act as a bulwark against unauthorized entry. This deliberate emphasis on security aligns with industry best practices, thus aiming to create a blockchain environment resilient to external threats and unauthorized access and ensuring the integrity and confidentiality of the stored data.

4.2. Discussion

The development of the conceptual blockchain model for information management presents a significant improvement in addressing the privacy and safety concerns surrounding construction workers' personal information. The model establishes a secure and transparent process for registering and endorsing construction workers' data.

The process involves the storage of construction workers' biodata and safety data, and it requires digital signatures and endorsements from authorized participants, thus restricting access to unauthorized personnels and thereby controlling the vital challenges of data manipulation and breach, as highlighted in [19–21]. The governance structure ensures that each participant's input is valued and authenticated. When information is requested, the smart contract converts it into a transaction, sending it through the ordering service to be included in blocks, which are then cryptographically secured and added to the blockchain. This creates an immutable chain of records, safeguarding the integrity and privacy of the data.

To reinforce information security during the endorsement, the model incorporates a consensus algorithm, which provides a robust layer of protection and ensures the privacy of workers' information, thus addressing the identified threats, such as identity theft. The model functions as a comprehensive information management platform and complies with the European Union's GDPR. It secures sensitive worker information, including biodata and safety data, through encryption and decentralized control. This directly responds to the identified threat of unauthorized access and breaches. The transparency achieved through blockchain ensures auditable data management, thus fostering trust and collaboration among stakeholders, which provides solutions for the shortcomings of the traditional approaches.

Furthermore, one of the key challenges emphasized is the need for digital solutions that accommodate the diverse nature of construction projects globally. The geographical applicability of the proposed blockchain model is a critical consideration. Developed within the Asia Sydney AWS region, scalability and adaptability to different regions are fundamental aspects of this study. By examining the unique regional variations in construction practices and data protection regulations, the model aims to be a global solution. Understanding the global trends in the construction industry is crucial for ensuring the applicability of innovative solutions across diverse geographical contexts. Referencing global trends in the construction industry, it becomes evident that this study aligns with the challenges faced by construction projects on a global scale. The need for standardized yet flexible solutions that can accommodate regional variations underscores the geographical relevance of this study.

5. Conclusions

The primary objective of this study was to leverage the potential of blockchain technology to fortify data security, with a focus on the biographical and safety data of construction workers. The developed solution, a robust Hyperledger Fabric blockchain deployed on the AWS platform, was successfully implemented as a feasible solution to the vulnerabilities of the traditional data management systems. Beyond addressing immediate concerns of data security, this study points towards the promise of the blockchain model in significantly optimizing risk assessment, resource allocation, and enhanced safety measures, especially in high-risk construction projects.

Practical validation through transaction testing using Hyperledger Explorer has affirmed the feasibility and operational effectiveness of the proposed model. This validation serves as a blueprint for the industry's data management practices, especially in construction workers' personal information management, thus providing a tangible pathway for stakeholders to enhance security without compromising efficiency.

This study assumes pivotal significance as it not only addresses immediate challenges of data breaches, identity theft, and misuse but also pioneers a fundamental change in how the construction industry approaches decision making, data security, privacy, and industry innovation.

1. Informed decision making for high-risk activities: By storing safety data, especially work-related musculoskeletal disorder (WMSD) risk assessments, on the blockchain, construction stakeholders gain access to verified and authenticated information. This empowers them to make informed decisions related to workforce management during high-risk construction tasks. Comprehensive safety data facilitate effective risk assessment, optimal resource allocation, and the assignment of skilled workers to specific high-risk activities. This proactive approach enhances safety measures, reduces accidents, and ensures the well-being of construction personnel.
2. Enhanced data security and privacy: Storing workers' biographic data on the blockchain enhances security and privacy compared to centralized systems. The blockchain's decentralized architecture distributes data across multiple nodes, making unauthorized manipulation challenging. Cryptographic techniques further safeguard sensitive information, ensuring its confidentiality. This heightened data security fosters trust between construction stakeholders and workers, assuring them that their information is handled with the utmost security.
3. Promotion of Industry Innovation and Trust: The successful implementation of blockchain within the construction sector sets a precedent for technological innovation. Demonstrating the practical application of blockchain in enhancing data security and privacy inspires confidence among stakeholders. This newfound trust encourages further adoption of advanced technologies to modernize construction practices, driving industry-wide innovation and fostering a culture of continuous improvement.

6. Limitations, Recommendations, and Future Research Direction

6.1. Limitations

One limitation of this study is the focus on a specific use case and the use of a single construction activity for data collection. The tiling activity chosen may not capture the full range of risks and challenges present in other construction tasks. Moreover, the use of a specific blockchain infrastructure on the AWS platform may limit the generalizability of the findings to other blockchain implementations. Furthermore, as this study is based on a case study approach, the results may not be fully representative of the broader construction industry. Future research could explore the applicability of the proposed blockchain model to various construction activities and assess its scalability and effectiveness on a larger scale.

6.2. Recommendations

To optimize the adoption and effectiveness of the Hyperledger Fabric blockchain for construction workers' data management, the following recommendations are proposed.

(1) Continuous Monitoring and Auditing: Ensuring compliance with data protection regulations and preemptively identifying vulnerabilities require consistent monitoring and auditing of the blockchain system. Regular updates and patches should be swiftly applied to mitigate potential security risks, thus creating a robust environment for data management.

(2) Real-world Testing and Iterative Enhancement: Real-world testing and pilot implementation of the blockchain platform in construction projects are essential. This approach

facilitates the identification of practical challenges and permits iterative refinements. Collecting user feedback and promptly addressing any emerging issues will optimize the system's performance and tailor its functionality to the specific requirements of the construction industry.

6.3. Future Work

One area of future research could involve exploring the extension of smart construction technology and its integration with the proposed blockchain solution. Smart construction technology refers to the use of advanced technologies, such as Internet of Things, sensors, artificial intelligence, and data analytics, in the construction industry to improve efficiency, productivity, and safety. Investigating how the proposed blockchain model can interface with smart construction technology systems and leverage their data for enhanced information management and decision making would be valuable. Another potential avenue for future research is to examine the application of the proposed blockchain model in the context of smart city initiatives. Smart cities aim to leverage technology and data to enhance the quality of life for citizens, improve resource management, and promote sustainability. Integrating the proposed blockchain solution into the broader framework of a smart city could provide additional benefits, such as secure and transparent data sharing across different stakeholders, improved interoperability between systems, and increased trust in the exchange of information.

Author Contributions: Conceptualization, A.E.N.S. and J.-H.C.; methodology, A.E.N.S.; validation, A.E.N.S.; formal analysis, A.E.N.S.; investigation, A.E.N.S., J.-J.Y. and J.-H.C.; data curation, A.E.N.S.; writing—original draft preparation, A.E.N.S.; writing—review and editing, A.E.N.S., J.-J.Y. and J.-H.C.; visualization, A.E.N.S.; supervision, J.-J.Y. and J.-H.C.; project administration, J.-H.C.; funding acquisition, J.-H.C. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the Korea Agency for Infrastructure Technology Advancement (KAIA) grant funded by the Ministry of Land, Infrastructure and Transport (National Research for Smart Construction Technology: Grant 225MIP-A156381-03).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author. The data are not publicly available due to privacy.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Alaloul, W.S.; Liew, M.S.; Zawawi, N.A.W.A.; Kennedy, I.B. Industrial Revolution 4.0 in the construction industry: Challenges and opportunities for stakeholders. *Ain Shams Eng. J.* **2020**, *11*, 225–230. [CrossRef]
2. World Economic Forum. *Shaping the Future of Construction a Breakthrough in Mindset and Technology*; World Economic Forum: Cologny, Switzerland, 2016.
3. Chen, J.; Lv, Z.; Song, H. Design of personnel big data management system based on blockchain. *Future Gener. Comput. Syst.* **2019**, *101*, 1122–1129. [CrossRef]
4. Gruschka, N.; Mavroeidis, V.; Vishi, K.; Jensen, M. Privacy issues and data protection in big data: A case study analysis under GDPR. In Proceedings of the IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 10–13 December 2018; pp. 5027–5033.
5. Monahan, T. Identity theft vulnerability: Neoliberal governance through crime construction. *Theor. Criminol.* **2009**, *13*, 155–176. [CrossRef]
6. Wang, W.; Yuan, Y.; Archer, N. A contextual framework for combating identity theft. *IEEE Secur. Priv.* **2006**, *4*, 30–38. [CrossRef]
7. Smith, A.D.; Lias, A.R. Identity theft and e-fraud as critical CRM concerns. *Int. J. Enterp. Inf. Syst. (IJEIS)* **2005**, *1*, 17–36. [CrossRef]
8. Tikkinen-Piri, C.; Rohunen, A.; Markkula, J. EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Comput. Law Secur. Rev.* **2018**, *34*, 134–153. [CrossRef]
9. Xu, J.; Lu, W.; Wu, L.; Lou, J.; Li, X. Balancing privacy and occupational safety and health in construction: A blockchain-enabled P-OSH deployment framework. *Saf. Sci.* **2022**, *154*, 105860. [CrossRef]

10. Gamil, Y.; Alhagar, A. The impact of pandemic crisis on the survival of construction industry: A case of COVID-19. *Mediterr. J. Soc. Sci.* **2020**, *11*, 122. [CrossRef]
11. Olanrewaju, A.; Tan, S.Y.; Kwan, L.F. Roles of communication on performance of the construction sector. *Procedia Eng.* **2017**, *196*, 763–770. [CrossRef]
12. Ho, P.H. Labour and skill shortages in Hong Kong's construction industry. *Eng. Constr. Archit. Manag.* **2016**, *23*, 533–550. [CrossRef]
13. Olsen, D.; Tatum, M.; Defnall, C. How industrial contractors are handling skilled labor shortages in the United States. In Proceedings of the 48th ASC Annual International Conference Proceedings, Birmingham, UK, 11–14 April 2012.
14. Kerrest, F. Commentary: How Blockchain Could Put an End to Identity Theft. Fortune. 2018. Available online: http://fortune.com/2018/04/20/blockchain-technology-identity-theft-dataprivacy-protection/ (accessed on 27 September 2018).
15. Antwi-Afari, M.F.; Li, H.; Edwards, D.J.; Pärn, E.A.; Seo, J.; Wong, A.Y.L. Biomechanical analysis of risk factors for work-related musculoskeletal disorders during repetitive lifting task in construction workers. *Autom. Constr.* **2017**, *83*, 41–47. [CrossRef]
16. Antwi-Afari, M.F.; Li, H.; Yu, Y.; Kong, L. Wearable insole pressure system for automated detection and classification of awkward working postures in construction workers. *Autom. Constr.* **2018**, *96*, 433–441. [CrossRef]
17. Boschman, J.S.; van der Molen, H.F.; Sluiter, J.K.; Frings-Dresen, M.H. Musculoskeletal disorders among construction workers: A one-year follow-up study. *BMC Musculoskelet. Disord.* **2012**, *13*, 196. [CrossRef] [PubMed]
18. Valero, E.; Sivanathan, A.; Bosché, F.; Abdel-Wahab, M. Analysis of construction trade worker body motions using a wearable and wireless motion sensor network. *Autom. Constr.* **2017**, *83*, 48–55. [CrossRef]
19. Cheng, S.; Daub, M.; Domeyer, A.; Lundqvist, M. *Using Blockchain to Improve Data Management in the Public Sector*; McKinsey Digital: Kolkata, India, 2017.
20. Perera, S.; Nanayakkara, S.; Rodrigo, M.N.N.; Senaratne, S.; Weinand, R. Blockchain technology: Is it hype or real in the construction industry? *J. Ind. Inf. Integr.* **2020**, *17*, 100125. [CrossRef]
21. Heilig, L.; Voß, S. A holistic framework for security and privacy management in cloud-based smart ports. In Proceedings of the 15th International Conference on Computer and IT Applications in the Maritime Industries-COMPIT '16, Lecce, Italy, 9–11 May 2016.
22. Nikmehr, B.; Hosseini, M.R.; Martek, I.; Zavadskas, E.K.; Antucheviciene, J. Digitalization as a strategic means of achieving sustainable efficiencies in construction management: A critical review. *Sustainability* **2021**, *13*, 5040. [CrossRef]
23. Klinc, R.; Turk, Ž. Construction 4.0–digital transformation of one of the oldest industries. *Econ. Bus. Rev.* **2019**, *21*, 4. [CrossRef]
24. Gourévitch, A.; Fæste, L.; Baltassis, E.; Marx, J. Data-Driven Transformation. *BCG Perspect.* **2017**, *5*, 8.
25. Bonnici, C.J.; Coles-Kemp, L. Principled electronic consent management: A preliminary research framework. In Proceedings of the 2010 International Conference on Emerging Security Technologies, Canterbury, UK, 6–7 September 2010; pp. 119–123.
26. Li, H.; Lu, M.; Hsu, S.C.; Gray, M.; Huang, T. Proactive behavior-based safety management for construction safety improvement. *Saf. Sci.* **2015**, *75*, 107–117. [CrossRef]
27. Boniface, C.; Fouad, I.; Bielova, N.; Lauradoux, C.; Santos, C. Security analysis of subject access request procedures: How to authenticate data subjects safely when they request for their data. In *Privacy Technologies and Policy: 7th Annual Privacy Forum, APF 2019, Rome, Italy, 13–14 June 2019*; Springer International Publishing: Berlin/Heidelberg, Germany, 2019; Proceedings 7; pp. 182–209.
28. Oetzel, M.C.; Spiekermann, S. A systematic methodology for privacy impact assessments: A design science approach. *Eur. J. Inf. Syst.* **2014**, *23*, 126–150. [CrossRef]
29. Yang, R.; Wakefield, R.; Lyu, S.; Jayasuriya, S.; Han, F.; Yi, X.; Yang, T.; Amarasinghe, G.; Chen, S. Public and private blockchain in construction business process and information integration. *Autom. Constr.* **2020**, *118*, 103276. [CrossRef]
30. Makhdoom, I.; Zhou, I.; Abolhasan, M.; Lipman, J.; Ni, W. PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. *Comput. Secur.* **2020**, *88*, 101653. [CrossRef]
31. Politou, E.; Casino, F.; Alepis, E.; Patsakis, C. Blockchain mutability: Challenges and proposed solutions. *IEEE Trans. Emerg. Top. Comput.* **2019**, *9*, 1972–1986. [CrossRef]
32. Pan, X.; Zhong, B.; Sheng, D.; Yuan, X.; Wang, Y. Blockchain and deep learning technologies for construction equipment security information management. *Autom. Constr.* **2022**, *136*, 104186. [CrossRef]
33. Kim, K.H.; Kim, K.S.; Kim, D.S.; Jang, S.J.; Hong, K.H.; Yoo, S.-W. Characteristics of Work-related Musculoskeletal Disorders in Korea and Their Work-relatedness Evaluation. *J. Korean Med. Sci.* **2010**, *25*, S77–S86. [CrossRef]
34. Dong, X.S.; Betit, E.; Dale, A.M.; Barlet, G.; Wei, Q. Trends of Musculoskeletal Disorders and Interventions in the Construction Industry. 2019. Available online: https://stacks.cdc.gov/view/cdc/86273 (accessed on 16 October 2023).
35. Khando, K.; Gao, S.; Islam, S.M.; Salman, A. Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Comput. Secur.* **2021**, *106*, 102267. [CrossRef]
36. Tapscott, D.; Tapscott, A. How blockchain will change organizations. *MIT Sloan Manag. Rev.* **2017**, *58*, 10.
37. Kobsa, A. Privacy-enhanced personalization. *Commun. ACM* **2007**, *50*, 24–33. [CrossRef]
38. Cranor, L.F. Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. *J. Telecomm. High Tech. L.* **2012**, *10*, 273.
39. Johnson, V.R. Cybersecurity, Identity Theft, and the Limits of Tort Liability. *South Carol. Law Rev.* **2005**, *57*, 255.
40. Ahmad, S. Green human resource management: Policies and practices. *Cogent Bus. Manag.* **2015**, *2*, 1030817. [CrossRef]

41. Clough, R.H.; Sears, G.A.; Sears, S.K.; Segner, R.O.; Rounds, J.L. *Construction Contracting: A Practical Guide to Company Management*; John Wiley & Sons: Hoboken, NJ, USA, 2015.
42. Siegel, K.M. Protecting the Most Valuable Corporate Asset: Electronic Data, Identity Theft, Personal Information, and the Role of Data Security in the Information Age. *Penn. St. L. Rev.* **2006**, *111*, 779.
43. Al-Zaben, N.; Onik, M.M.H.; Yang, J.; Lee, N.Y.; Kim, C.S. General data protection regulation complied blockchain architecture for personally identifiable information management. In Proceedings of the 2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE), Southend, UK, 16–17 August 2018; pp. 77–82.
44. Yi, X.; Wu, J. Research on safety management of construction engineering personnel under "big data+ artificial intelligence". *Open J. Bus. Manag.* **2020**, *8*, 1059–1075. [CrossRef]
45. Chanal, P.M.; Kakkasageri, M.S. Security and privacy in IOT: A survey. *Wirel. Pers. Commun.* **2020**, *115*, 1667–1693. [CrossRef]
46. Safa, N.S.; Mitchell, F.; Maple, C.; Azad, M.A.; Dabbagh, M. Privacy Enhancing Technologies (PETs) for connected vehicles in smart cities. *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e4173. [CrossRef]
47. Curzon, J.; Almehmadi, A.; El-Khatib, K. A survey of privacy enhancing technologies for smart cities. *Pervasive Mob. Comput.* **2019**, *55*, 76–95. [CrossRef]
48. Bhanot, R.; Hans, R. A review and comparative analysis of various encryption algorithms. *Int. J. Secur. Its Appl.* **2015**, *9*, 289–306. [CrossRef]
49. Cachin, C.; Camenisch, J.; Freire-Stögbuchner, E.; Lehmann, A. Updatable tokenization: Formal definitions and provably secure constructions. In *Financial Cryptography and Data Security: 21st International Conference, FC 2017, Sliema, Malta, 3–7 April 2017, Revised Selected Papers*; Springer International Publishing: Cham, Switzerland, 2017; pp. 59–75.
50. Murthy, S.; Bakar, A.A.; Rahim, F.A.; Ramli, R. A comparative study of data anonymization techniques. In Proceedings of the 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), Washington, DC, USA, 27–29 May 2019; pp. 306–309.
51. David, A.; Zarli, A.; Mirarchi, C.; Naville, N.; Perissich, L. DigiPLACE: Towards a reference architecture framework for digital platforms in the EU construction sector. In *ECPPM 2021–eWork and eBusiness in Architecture, Engineering and Construction*; CRC Press: Boca Raton, FL, USA, 2021; pp. 511–518.
52. Smallwood, R.F. *Information Governance: Concepts, Strategies and Best Practices*; John Wiley & Sons: Hoboken, NJ, USA, 2019.
53. Voss, W.G. Cross-border data flows, the GDPR, and data governance. *Wash. Int. Law J.* **2019**, *29*, 485. [CrossRef]
54. Kuperberg, M. Blockchain-Based Identity Management: A Survey from the enterprise and ecosystem perspective. *IEEE Trans. Eng. Manag.* **2020**, *67*, 1008–1027. [CrossRef]
55. Swan, M. *Blockchain: Blueprint for a New Economy*; O'Reilly Media, Inc.: Sebastopol, CA, USA, 2015.
56. Mougayar, W. *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*; John Wiley & Sons: Hoboken, NJ, USA, 2016.
57. Shabir, M.Y.; Iqbal, A.; Mahmood, Z.; Ghafoor, A. Analysis of classical encryption techniques in cloud computing. *Tsinghua Sci. Technol.* **2016**, *21*, 102–113. [CrossRef]
58. Wu, H.; Zhang, P.; Li, H.; Zhong, B.; Fung, I.W.; Lee, Y.Y.R. Blockchain Technology in the Construction Industry: Current Status, Challenges, and Future Directions. *J. Constr. Eng. Manag.* **2022**, *148*, 03122007. [CrossRef]
59. Monrat, A.A.; Schelén, O.; Andersson, K. A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access* **2019**, *7*, 117134–117151. [CrossRef]
60. Lu, W.; Wu, L.; Zhao, R. Rebuilding trust in the construction industry: A blockchain-based deployment framework. *Int. J. Constr. Manag.* **2023**, *23*, 1405–1416. [CrossRef]
61. Nakamoto, S. Bitcoin v0. 1 Released. The Mail Archive, 9. 2009. Available online: https://www.mail-archive.com/cryptography@metzdowd.com/msg10142.html (accessed on 15 May 2023).
62. Saah, A.E.N.; Choi, J.H. Blockchain technology in the AEC industry: Scientometric analysis of research activities. *J. Build. Eng.* **2023**, *72*, 106609. [CrossRef]
63. Casino, F.; Dasaklis, T.K.; Patsakis, C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telemat. Inform.* **2019**, *36*, 55–81. [CrossRef]
64. Lee, D.; Lee, S.H.; Masoud, N.; Krishnan, M.S.; Li, V.C. Integrated digital twin and blockchain framework to support accountable information sharing in construction projects. *Autom. Constr.* **2021**, *127*, 103688. [CrossRef]
65. Penzes, B.; KirNup, A.; Gage, C.; Dravai, T.; Colmer, M. *Blockchain Technology in the Construction Industry: Digital Transformation for High Productivity*; Institution of Civil Engineers (ICE): London, UK, 2018.
66. Gupta, M. *Blockchain for Dummies*; John Wiley & Sons, Inc.: Hoboken, NJ, USA, 2019.
67. Li, J.; Kassem, M. Applications of distributed ledger technology (DLT) and Blockchain-enabled smart contracts in construction. *Autom. Constr.* **2021**, *132*, 103955. [CrossRef]
68. Giancaspro, M. Is a 'smart contract' really a smart idea? Insights from a legal perspective. *Comput. Law Secur. Rep.* **2017**, *33*, 825–835. [CrossRef]
69. Rahardja, U.; Hidayanto, A.N.; Lutfiani, N.; Febiani, D.A.; Aini, Q. Immutability of Distributed Hash Model on Blockchain Node Storage. *Sci. J. Inform.* **2021**, *8*, 137–143. [CrossRef]

70. Nanayakkara, S.; Perera, S.; Bandara, D.; Weerasuriya, T.; Ayoub, J. Blockchain technology and its potential for the construction industry. In Proceedings of the AUBEA Conference 2019, Noosa, QLD, Australia, 6–8 November 2019; pp. 662–672.
71. Wiatt, R.G. From the mainframe to the blockchain. *Strateg. Financ.* **2019**, *100*, 26–35.
72. Yaqoob, I.; Salah, K.; Jayaraman, R.; Al-Hammadi, Y. Blockchain for healthcare data management: Opportunities, challenges, and future recommendations. *Neural Comput. Appl.* **2022**, *34*, 11475–11490. [CrossRef]
73. Shah, T.; Jani, S. *Applications of Blockchain Technology in Banking & Finance*; Parul CUniversity: Vadodara, India, 2018.
74. Liu, H.; Han, S.; Zhu, Z. Blockchain technology toward smart construction: Review and future directions. *J. Constr. Eng. Manag.* **2023**, *149*, 03123002. [CrossRef]
75. Wu, L.; Lu, W.; Zhao, R.; Xu, J.; Li, X.; Xue, F. Using blockchain to improve information sharing accuracy in the onsite assembly of modular construction. *J. Manag. Eng.* **2022**, *38*, 04022014. [CrossRef]
76. Sheth, H.; Dattani, J. Overview of blockchain technology. *Asian J. Converg. Technol. (AJCT)* **2019**. [CrossRef]
77. Guegan, D. Public Blockchain versus Private Blockhain. 2017. Available online: https://shs.hal.science/halshs-01524440/document (accessed on 16 October 2023).
78. Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C.; Christidis, K.; De Caro, A.; Yellick, J. Hyperledger fabric: A distributed operating system for permissioned blockchains. In Proceedings of the 13th EuroSys Conference 2018, Porto, Portugal, 23–26 April 2018; pp. 1–15.
79. Baliga, A.; Subhod, I.; Kamat, P.; Chatterjee, S. Performance evaluation of the quorum blockchain platform. *arXiv* **2018**, arXiv:1809.03421.
80. Mohanty, D. *R3 Corda for Architects and Developers: With Case Studies in Finance, Insurance, Healthcare, Travel, Telecom, and Agriculture*; Apress: New York, NY, USA, 2019.
81. Mostarda, L.; Pinna, A.; Sestili, D.; Tonelli, R. Performance Analysis of a BESU Permissioned Blockchain. In *International Conference on Advanced Information Networking and Applications*; Springer International Publishing: Cham, Switzerland, 2023; pp. 279–291.
82. Panda, S.K.; Daliyet, S.P.; Lokre, S.S.; Naman, V. Distributed Ledger Technology in the Construction Industry Using Corda. In *The New Advanced Society: Artificial Intelligence and Industrial Internet of Things Paradigm*; Scrivener Publishing LLC.: Austin, TX, USA, 2022; pp. 15–41.
83. Zhong, B.; Wu, H.; Ding, L.; Luo, H.; Luo, Y.; Pan, X. Hyperledger fabric-based consortium blockchain for construction quality information management. *Front. Eng. Manag.* **2020**, *7*, 512–527. [CrossRef]
84. Read, C.L. The Genesis Block. In *The Bitcoin Dilemma: Weighing the Economic and Environmental Costs and Benefits*; Springer International Publishing: Cham, Switzerland, 2022; pp. 29–36.
85. Di Pierro, M. What is the blockchain? *Comput. Sci. Eng.* **2017**, *19*, 92–95. [CrossRef]
86. Donet Donet, J.A.; Pérez-Sola, C.; Herrera-Joancomartí, J. The bitcoin P2P network. In *Financial Cryptography and Data Security: FC 2014 Workshops, BITCOIN and WAHC 2014, Christ Church, Barbados, 7 March 2014*; Revised Selected Papers 18; Springer: Berlin/Heidelberg, Germany, 2014; pp. 87–102.
87. MacKenzie, D. Pick a nonce and try a hash. *Lond. Rev. Books* **2019**, *41*, 35–38.
88. De Ocáriz Borde, H.S. An Overview of Trees in Blockchain Technology: Merkle Trees and Merkle Patricia Tries. 2022. Available online: https://www.researchgate.net/publication/358740207_An_Overview_of_Trees_in_Blockchain_Technology_Merkle_Trees_and_Merkle_Patricia_Tries (accessed on 16 October 2023).
89. Jing, N.; Liu, Q.; Sugumaran, V. A blockchain-based code copyright management system. *Inf. Process. Manag.* **2021**, *58*, 102518. [CrossRef]
90. Purnomo, H.; Apsari, A.E. REBA analysis for construction workers in Indonesia. *J. Built Environ. Technol. Eng.* **2016**, *1*, 104–110.
91. Supanich, W.; Kulkarineetham, S.; Sukphokha, P.; Wisarnsart, P. Machine Learning-Based Exercise Posture Recognition System Using MediaPipe Pose Estimation Framework. In Proceedings of the 9th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 17–18 March 2023; Volume 1, pp. 2003–2007.
92. Guo, L.; Xie, H.; Li, Y. Data encryption based blockchain and privacy preserving mechanisms towards big data. *J. Vis. Commun. Image Represent.* **2020**, *70*, 102741. [CrossRef]
93. Karia, J.; Sundararajan, M.; Raghavan, G.S. Distributed Ledger Systems to Improve Data Synchronization in Enterprise Processes. In Proceedings of the IEEE International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER), Nitte, India, 19–20 November 2021; pp. 41–45.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.