

Article

Two-Layered Mechanism of Blockchain System for Sustainable Worldwide Control and Management of Highly Contagious Diseases

Yuan-Cheng Lin ^{1,2} , Cooper Cheng-Yuan Ku ^{1,*} and Humble Po-Ching Hwang ¹¹ Institute of Information Management, National Yang Ming Chiao Tung University, Hsinchu 300093, Taiwan; yc@nari.org.tw (Y.-C.L.); samuelhwang0304@gmail.com (H.P.-C.H.)² National Atomic Research Institute, Taoyuan 325207, Taiwan

* Correspondence: cooperku@nycu.edu.tw

Abstract

The COVID-19 outbreak significantly impacted global health, resulting in widespread infections and fatalities. In response, the World Health Organization (WHO) launched the Preparedness and Resilience for Emerging Threats (PRET) program, focusing on respiratory pathogens, to prepare for future pandemics and achieve sustainable well-being around the world. Moreover, the WHO also encouraged countries to establish a National Action Plan for Health Security (NAPHS) to address various disasters and threats. Therefore, governments should develop the necessary systems aligned with NAPHS while maintaining compliance with PRET. Thus, to maintain global health and wellness, a platform for sharing medical data on highly contagious diseases worldwide, free from interference from individual countries, is critical for effective border control. In this paper, we introduce an efficient approach, i.e., a two-layer decentralized blockchain architecture. Our mechanism streamlines integration between national sovereignty and the WHO, enabling the secure and supervised exchange of pandemic data via a single global blockchain and multiple local blockchains. This blockchain framework has strong potential to enhance nations' ability to prepare for and respond to future pandemics, ensuring the safety and health of their citizens. The bottom-layer local chains facilitate the collection of pandemic immunity data within their own countries, and the upper-layer global chain, with the assistance of the WHO, facilitates the worldwide exchange of these data if needed. Given the characteristics of decentralization and transparency in blockchain technology, and the WHO's oversight, no government should worry that sensitive medical data will be manipulated or abused by superpowers on the global blockchain. It also highlights the importance of global collaboration in preventing and controlling contagious diseases. Furthermore, the performance of this system is assessed based on several sets of real-world data and requirements. We demonstrate that this global information-sharing mechanism can improve international health safety, provided it is supported by feasible and reasonable resources to handle transactional demands around the world.

Keywords: containment of contagious diseases; border control; two-layered blockchain system; smart contract; global sharing of pandemic data



Academic Editor: Harris Wu

Received: 6 December 2025

Revised: 1 February 2026

Accepted: 2 February 2026

Published: 3 February 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

1. Introduction

During the first two decades of the 21st century, the world grappled with multiple global pandemics, including SARS-CoV in 2003, H1N1 in 2009, Ebola in 2014, and

COVID-19 in 2020 [1]. Notably, the COVID-19 pandemic had a significant global impact, infecting around 61 million people worldwide and severely affecting human health and well-being. The World Health Organization (WHO) declared the global COVID-19 outbreak on 11 March 2020, which significantly impacted daily life, including education, transportation, travel, the economy, politics, human health, life expectancy, and work [2]. With vaccines and effective medicines in short supply, many countries resorted to facial masks and social distancing measures to contain the spread of the virus. To curb transmission, some governments also imposed restrictions on immigration and access to public spaces, such as schools, offices, hospitals, restaurants, and transportation. In some regions, individuals are required to present immunity certificates to enter certain public areas, with proof of immunity often requested upon arrival. To effectively address infectious disease threats and prepare for future pandemics, countries must comply with global epidemic prevention plans and tailor sustainable disaster preparedness plans, with particular attention to respiratory pathogens.

With this goal in mind, the WHO launched the Preparedness and Resilience for Emerging Threats (PRET) initiative on 26 April 2023, prioritizing respiratory pathogens as a critical measure to prepare for and prevent future pandemics [3–5]. Additionally, the WHO urged countries to establish their own National Action Plan for Health Security (NAPHS) to address diverse disasters and threats [6,7]. Regional, national, and global investments should align with PRET and NAPHS to ensure comprehensive preparedness. Therefore, countries should develop a system to implement their respective NAPHS while maintaining close ties with WHO's PRET. This collaborative approach should enhance global health security and bolster countries' capacity to prevent and respond to future pandemics and health threats.

This study proposes a two-layer decentralized architecture based on blockchain technology to address various issues, using COVID-19 as a case. We aim to develop a solution that integrates national autonomy with global protection by utilizing global and local blockchains. Leveraging blockchain technology, which provides distributed storage when needed and ensures data immutability, integrity, and consistency, is central to our approach. The local chain records vaccination records and individual testing results, while the global chain facilitates data sharing for international travelers. Instead of storing complete medical records in the blockchain, only summaries of pandemic data for border crossings are uploaded. Automation through smart contracts reduces human involvement. This framework can assist governments, healthcare providers, and research institutions worldwide in preventing and studying major pandemics, thereby contributing to global sustainable health security and pandemic preparedness. Furthermore, due to the characteristics of decentralization and transparency in blockchain technology, and the WHO's oversight, no government should worry that sensitive pandemic data will be manipulated or abused by superpowers on the global blockchain. The contributions of this study are briefly summarized as follows: (I) We propose a two-layer decentralized framework for sharing pandemic-related medical information, with a particular focus on pandemic testing history and vaccination records. (II) To the best of our knowledge, very few studies have reported using the hierarchical structure of global and local chains to address issues in exchanging pandemic data worldwide and to enable customs/ports to obtain quick access to them. In alignment with each country's NAPHS, local chains store pandemic-related metadata. The InterPlanetary File System (IPFS) is used to keep extensive electronic medical records (EMRs) of pandemic tests and vaccinations off-chain. If needed, it can be used to save pandemic testing history and vaccination records in advance, further speeding up real-time access for customs and ports. Meanwhile, the global chain complies with the WHO's PRET initiative by sharing these data for international travel and movement. This collaboration

can enhance sustainable global wellness and strengthen countries' abilities to prevent and respond to future pandemics and health threats. (III) We adopt smart contracts to automate the exchange of pandemic data and minimize human intervention. (IV) Only the necessary data, such as pandemic testing history and vaccination records from medical records, are uploaded to the blockchain to enhance the proposed system's access performance.

The remainder of this paper is organized as follows: Section 2 introduces the domain background, and Section 3 presents the literature review. In Section 4, we describe the framework and workflows of this two-layered blockchain system. Section 5 provides a critical discussion of the security and performance analysis. Finally, Section 6 concludes the paper and outlines directions for future work.

2. Domain Background

In this section, we provide the background knowledge and foundational technologies underlying the proposed system. It first introduces WHO's pandemic preparedness strategies, followed by an overview of blockchain technology, smart contracts, and IPFS. Together, these components form the technical and institutional basis for the cross-border pandemic data exchange framework.

2.1. WHO's Strategy

The PRET initiative was launched by the WHO, and the call to action was released at the Global Meeting for Future Respiratory Pathogen Pandemics held on 24–26 April 2023 in Geneva, Switzerland. PRET aims to provide comprehensive planning guidance for addressing any respiratory pathogen, including influenza and coronaviruses such as COVID-19. It focuses on strengthening and maintaining the resilience of response and healthcare systems, enhancing global pandemic preparedness, and promoting a whole-of-government and whole-of-society approach to pandemic planning. The COVID-19 pandemic and other health emergencies have underscored the need for countries to be well prepared for infectious disease threats, with tailored disaster preparedness plans and enhanced coordination and collaboration across sectors. Therefore, the WHO encourages governments to develop the NAPHS to strengthen cross-cutting core capacities applicable to all/multi-hazard situations. The NAPHS is a multi-year planning process designed by each country that outlines national health security priorities, brings together various sectors to identify potential partners for cooperation, and allocates resources to develop health security capabilities. PRET, with a disease-focused preparedness approach, is synergistic with NAPHS. Together, PRET and NAPHS should be reflected in investments at the national, regional, and global levels to enhance preparedness.

2.2. Blockchain

With the introduction of Bitcoin in 2008 by Satoshi Nakamoto [8], the blockchain began to be applied worldwide. The blockchain, i.e., a distributed ledger, develops a trust mechanism in a trustless environment. Blockchain technology provides immutability, transparency, integrity, and consistency for data storage. According to the consensus mechanism, access rights, and permission management, blockchains can be categorized into four types [9]: public, private, consortium, and hybrid. In the past, the consensus algorithms of consortium blockchains have primarily been based on the Practical Byzantine Fault Tolerance (PBFT) algorithm. Given system issues such as network attacks, performance, and scalability, most have adopted the BFT-DPoS [10] consensus algorithm, which combines Byzantine Fault Tolerance (BFT) and Delegated Proof of Stake (DPoS). In BFT-DPoS, nodes can vote for any of n block producers (BPs) in each round, with votes proportional to their stake. The more tokens a stakeholder holds, the greater their voting power. BP nodes receive rewards by producing blocks on the

blockchain. To become BP nodes, nodes in the system must demonstrate their security, stability, and fairness, including the ability to resist distributed denial-of-service (DDoS) attacks. The number of blockchain stakes can also reflect a node's security and stability. If a BP node continually misses its blocks or uploads invalid transactions, the other nodes will replace it with a better BP node. A BP node can propose and broadcast a block to all other BP nodes. A new block becomes irreversible once a BP node has received more than two-thirds of node confirmations. In the BFT-DPoS mechanism, having fewer delegates and BFT broadcasting allows BP nodes to create blocks efficiently.

Stanescu et al. [11] introduced a Converging Technologies for Sustainable Agri-Food Chains (CTSAF) conceptual framework that systematically analyzes blockchain's pivotal role as a secure, immutable infrastructure that enables converging digital technologies. This enhances transparency, traceability, trust, accountability, and resilience in sustainable agri-food chains. Sasirega and Prakash [12] proposed an efficient vehicle-to-grid (V2G) framework that addresses key challenges, including energy management and robust security. They planned the optimal electrical vehicle (EV) charging and discharging schedule using game theory and ensured authentication with the Elliptic Curve Cryptography (ECC) algorithm and hash functions. In this framework, blockchain technology is adopted for transparent and tamper-proof data management. Han et al. [13] presented a method to secure federated learning in the 5G environment. To facilitate the verification and comparison of data features across clients, they used blockchain technology to ensure immutable, transparent data exchange.

2.3. Smart Contract

Nick Szabo first proposed the concept of the smart contract in 1994 and then presented a more comprehensive version in 1996 [14]. A smart contract enables trusted and irreversible transactions without the need for intervention from any third party. Users can develop desired logic applications using smart contracts with predefined rules embedded. Once a rule is triggered, the smart contract can be automatically executed, thereby reducing the impact of human factors. Therefore, the most important objective is for the smart contract to ensure transaction fairness. Kanagi et al. [15] proposed a framework for an Ethereum-based permissioned blockchain that uses smart contracts to secure and facilitate the exchange of clinical data among healthcare facilities and medical entities. Hathaliya and Tanwar [16] integrated role-based access control (RBAC) and fine-grained attribute-based access control (ABAC) through smart contracts in a consortium blockchain to prevent unauthorized access in the medicine supply chain (MSC). Kistaubayev et al. [17] presented a multi-layered blockchain framework, i.e., the Ethereum consortium, for Kazakhstan's higher education institutions (HEIs) to address limitations of centralized systems. It employs smart contracts to ensure immutable data sovereignty, integrity, and verifiable academic credential management.

2.4. IPFS

Benet proposed the IPFS, a peer-to-peer distributed file system designed to provide a content-addressed storage and communication architecture without relying on centralized servers [18]. In IPFS, data objects are identified by cryptographic hash values, which ensure data integrity and strong tamper resistance. IPFS objects are also immutable by design. Any modification produces a new hash and results in a new version of the object. Through decentralized storage and distributed access across multiple peers, IPFS can significantly reduce the risk of a single point of failure, mitigate dependence on centralized infrastructure, and provide large-scale storage with a high peer count. Owing to these properties, IPFS

could be effectively leveraged as an off-chain storage solution for a large-scale EMR system, supporting long-term data preservation and version traceability.

Building on these characteristics, several studies have explored integrating blockchain and IPFS into healthcare applications. Nguyen et al. [19] designed an electronic health record (EHR) sharing framework that combines blockchain and IPFS and deployed it on a mobile cloud platform to address data privacy and cybersecurity concerns. Guo et al. [20] investigated privacy protection, data security, and query efficiency in blockchain-based EMR-sharing scenarios and presented a secure storage and sharing scheme that integrates Hyperledger Fabric with IPFS, where encrypted medical data are stored in IPFS to enable distributed access. Furthermore, Patel et al. [21] combined artificial intelligence (AI) and blockchain technology to identify malicious healthcare data and employed smart contracts to verify data integrity, allowing only validated medical data to be stored in IPFS under blockchain control, thereby mitigating the risk of data tampering.

3. Literature Review

Budd et al. [22] discussed the digital technologies that can aid humans during the COVID-19 pandemic, including computer vision, smartphone apps, machine learning, natural language processing, digital diagnostics, wearables, and visualization. They also already emphasized the importance of targeted public health messaging and privacy-preserving technologies. Khurshid [23] argued that blockchain technology can help mitigate the crisis of trust during the COVID-19 pandemic. The supply chains for household items such as toilet paper and hand soap are often out of stock at that time. Furthermore, the hospital's materials supply chain has also failed. Therefore, IBM has developed a system to help operate medical supply chains. The blockchain can also track medications, as there have been reports of counterfeit medicines during the COVID-19 pandemic. Chang and Park [24] indicated how blockchain technology supports from several perspectives. Blockchain technology can enhance the transparent and secure sharing of diagnostic information and clinical presentations, thereby motivating countries to develop infectious disease reporting systems based on it. Additionally, blockchain technology can help prevent the spread of COVID-19-related fake news. Thanks to the blockchain's Merkle tree and digital signatures, the information stored on the blockchain remains unaltered and tamper-proof, protected from unauthorized access. Therefore, the decentralized and shared features of blockchain are widely used in securing medical data. In [25–28], the authors also applied blockchain technology in other domains, including green electricity trading models, anonymous roaming authentication schemes for vehicular ad hoc networks (VANETs), product authenticity with carbon footprint tracing, and private parking space allocation. They sought to leverage the robust, immutable, and distributed nature of blockchain systems to safeguard sensitive and critical information against tampering. Furthermore, some studies achieved privacy-preserving authentication and secure data management by integrating cryptographic techniques and blockchain technology to enable privacy, efficient verification, and traceability. Sutrala et al. [29] developed an ECC-based Internet of Vehicles (IoV) authentication protocol that integrates batch verification to minimize computational costs. This design guarantees conditional privacy while ensuring seamless and efficient message transmission. Tan et al. [30] proposed a blockchain-enabled authentication and key agreement scheme for VANETs that employs a self-balancing tree architecture, achieving conditional vehicle privacy while enabling authorized entities to trace and remove malicious participants.

During the COVID-19 pandemic, antibody/vaccination certification and test results were essential for governments to prevent the spread of the disease and to quickly recover the economy. Eisenstadt et al. [31] developed a blockchain-based mobile app prototype

for COVID-19 antibody/vaccination certification. Bansal et al. [32] proposed a blockchain-based immunity certificate system to verify that individuals are not infected. Blockchain can reduce the falsification of test results, and an individual's biometrics are used to sign the data using a private key, preventing others from using their own certificate. Large countries, such as India, have classified the nation into various areas and reopened some lower-risk regions. A blockchain-based system that promotes social distancing by allowing a limited number of individuals to remain in a given location at a given time was proposed in [33]. Each individual signs up in the proposed system using biometrics as a private key. The blockchain is tamper-proof, preventing tampering with the movement passes issued by the proposed system. Kabashkin et al. [34] designed a comprehensive framework integrating advanced health monitoring systems (AHMSs) and life cycle management (LCM). The utilization of blockchain technology ensures the integrity, security, and traceability of maintenance and operational data, significantly enhancing aviation sustainability and cost efficiency. Resiere et al. [35] described the implementation of healthcare cooperation using blockchain to combat COVID-19 in the Caribbean. The system includes a database of medical records for healthcare service providers, facilitating data sharing and collaborative research. Tan et al. [36] proposed a blockchain-empowered framework for secure sharing and privacy protection of COVID-19 electronic medical records (CEMRs) on semi-trusted medical cloud platforms. Their approach integrates ciphertext-policy attribute-based encryption (CP-ABE) to support fine-grained access control, traceability, and direct revocation while leveraging a blockchain for identity authentication and for managing public keys and revocation lists. Security analysis shows that the scheme is provably secure under the Decision Bilinear Diffie–Hellman (DBDH) assumption and resistant to various malicious attacks. Dar et al. [37] addressed the security, privacy, and trust issues inherent in centralized COVID-19 pandemic data management systems by designing a blockchain-based framework for secure handling and protection of pandemic data. The framework adopts a layered architecture, including data collection, data access and privacy, and data storage layers. It leverages decentralized ledgers and smart contracts to enhance data integrity, real-time sharing, and privacy preservation. The results indicate that the proposed framework can effectively mitigate risks such as data tampering, single points of failure, and lack of transparency, demonstrating the feasibility and potential benefits of blockchain technology for applications such as contact tracing, outbreak monitoring, and healthcare data sharing. To address the technical challenges of exchanging pandemic medical records worldwide, Biswas et al. [38] outlined a global blockchain network (GBN) called GlobeChain that bridges national peer networks to enable secure cross-border sharing of healthcare data.

In summary, using blockchain technology should be an effective way to prevent the spread of COVID-19 or future highly contagious diseases. However, there are still some unsolved problems:

- Prevention-related data about pandemics are not directly collected and exchanged worldwide to facilitate the rapid clearance, fast track, e-Gate, priority access, or global entry at customs or ports.
- Accessing the necessary data on international tourists regarding pandemic-related matters for cross-border purposes has been challenging until now.
- Real-time access to a vast amount of pandemic testing history and vaccination records by customs or ports is still unsettled.

Hence, we propose a two-layer blockchain to handle these issues. The local chains in the proposed system are decentralized with minimal impact from any entities. It could be adjusted somewhat in accordance with national regulations and technical capabilities. However, customs and ports must be involved to accelerate clearance. The global chain, embedded with smart contracts, can facilitate the cross-border exchange of pandemic-

related information without human involvement. Moreover, it should be free of political interference from any country under the WHO's supervision.

4. Materials and Methods

This paper presents a two-layer decentralized system based on consortium blockchains, with consensus algorithms primarily relying on BFT-DPoS. With a permission mechanism, consortium blockchains share pandemic medical information and guarantee its immutability and integrity. Notably, only pandemic data summaries necessary for border crossings, i.e., testing results and vaccination records, are uploaded to the country's local blockchain to enhance overall performance, with detailed transaction data stored and distributed across off-chain IPFS. However, IPFS serves as optional off-chain storage for preserving detailed EMRs of pandemic testing history and vaccination records for internal use within one's own country and can be adopted flexibly depending on national policies, regulations, and the level of healthcare digitalization. This is because, as is well known, some least developed countries (LDCs) may lack the infrastructure to support EMRs or IPFS. We also advocate incentivizing research institutes, universities, hospitals, and companies to serve as participating nodes, providing computing resources and maintaining the decentralized local chains. The medical data, which can be utilized for data mining, machine learning, big data analysis, or tax relief purposes, could be provided to these nodes as a reward after the identification information is removed. This incentive mechanism can avoid the shortcomings of wasting substantial computing resources on mining, as earlier blockchain systems did.

The necessary pandemic-related data are forwarded to the global chain via a smart contract when cross-border travel is underway. However, in the global chain, we believe IPFS is not required, as Customs only needs on-chain testing results and vaccination records to determine whether access is permitted, and blockchain technology can ensure the integrity and availability of this information. Therefore, we do not need to store detailed EMRs in IPFS for the global chain. The upload of pandemic summaries from the local chain to its private node on the global chain, the international exchange of these data within the global chain, and their download to the local chain are all triggered by smart contracts. Next, we describe the detailed structure of the local and global chains and smart contracts.

4.1. Local Chain

Figure 1 illustrates the architecture of the local chain in a country. The local chain operates on a consortium blockchain with a permission mechanism, which may or may not be directly managed by its government in accordance with national regulations or policies. Acting as a fair third party, the government or an authorized organization serves as the certificate authority (CA) for healthcare centers and all participants in this chain, and assists with inquiries about pandemic information. Healthcare service providers upload summaries of pandemic-related data, including testing results and vaccination records, to the local chain as they become available. At the same time, detailed EMRs could be uploaded to IPFS for backup, double-checking, dispute handling, and future use. Individual countries can define the format of EMRs stored in IPFS, but they must be converted to the Health Level Seven (HL7) or Fast Healthcare Interoperability Resources (FHIR) standards [39] to be exchanged across institutions or internationally. This IPFS supplement can be customized to each country's specific needs, circumstances, and related regulations. As emphasized earlier, the infrastructure for detailed EMR and IPFS may not yet be ready in some LDCs.

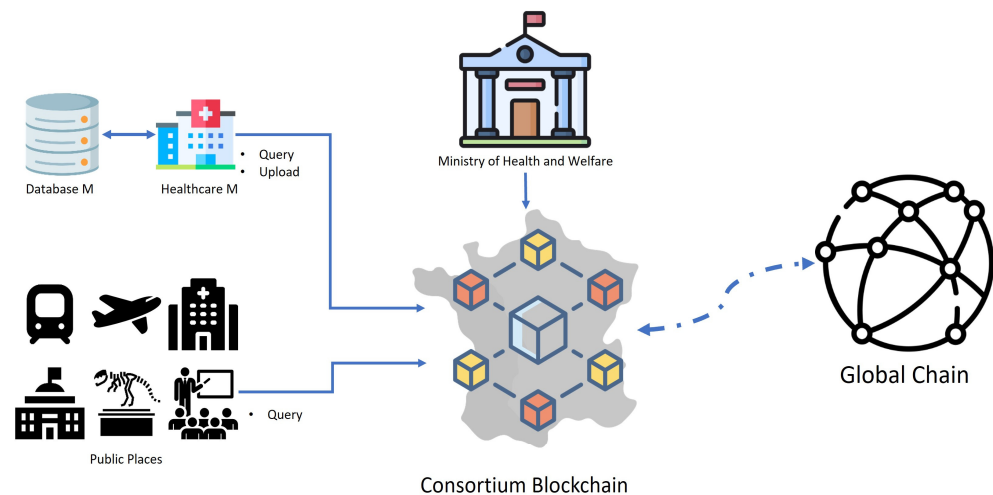


Figure 1. Architecture of a local chain.

Customs and Border Protection activates a smart contract to automatically upload pandemic-related data to the country's private node on the global chain for cross-border travelers as they leave the country, and another smart contract to automatically download the above-mentioned data from its private node to the local chain for visiting tourists. In addition, involving Customs/ports in the operation of the proposed two-layered blockchain system helps them quickly access the necessary pandemic-related data.

4.2. Global Chain

The global chain, overseen by the WHO, is built on a consortium blockchain with a permission mechanism, and each country has its own private node within it. Figure 2 illustrates the overview of the global chain system, which includes embedded private country nodes associated with their own local chains.



Figure 2. Architecture of the global chain.

To monitor and assist in the operation of the proposed structure, the WHO serves as the CA for governments worldwide, and the Customs and Border Protection agencies of all countries provide storage and computing resources as full private nodes in this chain. The pandemic data transmitted from the local chain are first validated, and then forwarded to the private node in the global chain. After the uploaded data are verified and packaged into a block by a BP node, the global chain enables the sharing of pandemic testing results and vaccination records between multiple private nodes across different countries for trips with multiple destination points. Private nodes are used to accelerate downloading when

tourists visit the Customs agency. The border control department of any government can retrieve exchanged pandemic data from its own private node without having to search the entire global chain ledger. Then, Customs checks whether a specific visitor's record complies with its immigration regulations and decides whether to admit the traveler into its territory. Furthermore, we believe that the private nodes of each country in the global chain could be extended into full private chains if stringent immutability and integrity requirements for pandemic testing results and vaccination records, as well as much higher computational capacity, are required. In this way, the global chain could adopt a hybrid consortium blockchain structure, where a consortium chain stores the content and logs of the exchange processes, and multiple private chains enable efficient and secure access to and download of pandemic-related data for individual countries.

4.3. Smart Contracts

The proposed blockchain framework deploys three types of smart contracts: local record contracts (LRCs), global record contracts (GRCs), and travel record contracts (TRCs). Before introducing the exchange procedures, Table 1 provides the definitions of essential symbols used in the detailed flowcharts.

Table 1. Symbol definition.

Symbol	Definition
H	Hash function
ID _c	The ID of a person
ID _h	The ID of the healthcare institute
Timestamp	The timestamp of the medical record
VR	Vaccination record
TR	Testing report
EMR	The detailed EMR
D _{EMR}	The saved document in IPFS
D _H	The transmitted document to a local chain of country A
D _{LCA}	The transmitted document from a local chain of country A
D _{GC}	The transmitted document within the global chain
D _{LCB}	The transmitted document to a local chain of country B
S _{HSEmr}	The signature of the healthcare institute for H (Timestamp H(ID _c) ID _h VR TR EMR)
S _{HS}	The signature of the healthcare institute for H (Timestamp H(ID _c) ID _h VR TR)
S _{LA}	The signature of the Customs of country A for H (Timestamp H(ID _c) ID _h VR TR S _{HS})
S _W	The signature of the WHO for H (Timestamp H(ID _c) ID _h VR TR S _{HS} S _{LA})
S _{LB}	The signature of the Customs of country B for H (Timestamp H(ID _c) ID _h VR TR S _{HS} S _{LA} S _W)

The symbol || denotes the concatenation of data.

After a person in country A completes a pandemic test or receives a vaccine injection, the healthcare center scrambles their ID using a hash function and generates a summarized report. The medical center then forwards the detailed EMR to IPFS and transmits the aforementioned summarized document, D_H, to the local blockchain. The process of adding a new report D_H to the local chain is depicted in Figure 3.

When this traveler plans to leave country A and visit country B, Customs A completes the outbound procedures and then requests initiation of the LRC, uploading the pandemic test and vaccination data to the global chain. This smart contract primarily validates the healthcare provider's signatures, attaches the signature S_{LA} of Customs A if the S_{HS} is validated, and uploads the summarized report and the traveler's destination(s) to its private node on the global chain. While the testing results and vaccination reports are

then packaged as a new block in the global chain, the GRC is initiated. This smart contract primarily performs the following functions: validating the summarized reports, attaching the WHO's signature S_W , and then transmitting these documents to the private nodes of destination countries for tourists. Figure 4 outlines the processes for transmitting the summarized report of an international traveler to the private node of the source country in the global chain, then forwarding it to the private node of the destination country or to several private nodes for a multi-destination trip.

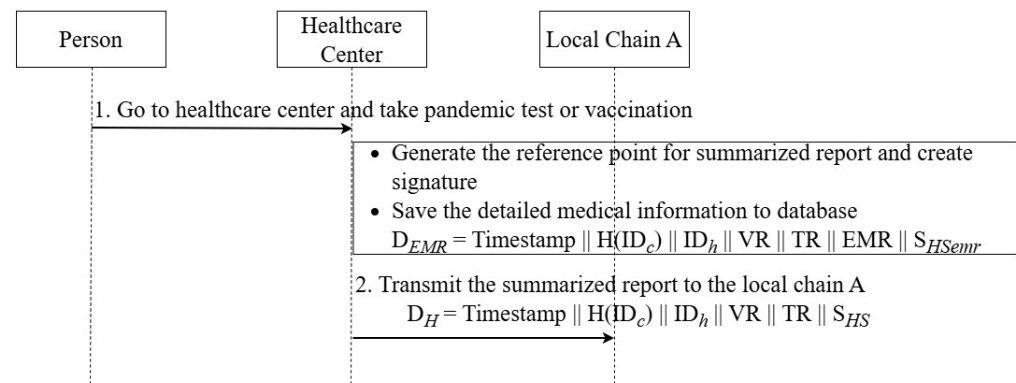


Figure 3. Flowchart of adding a summarized report to a local chain.

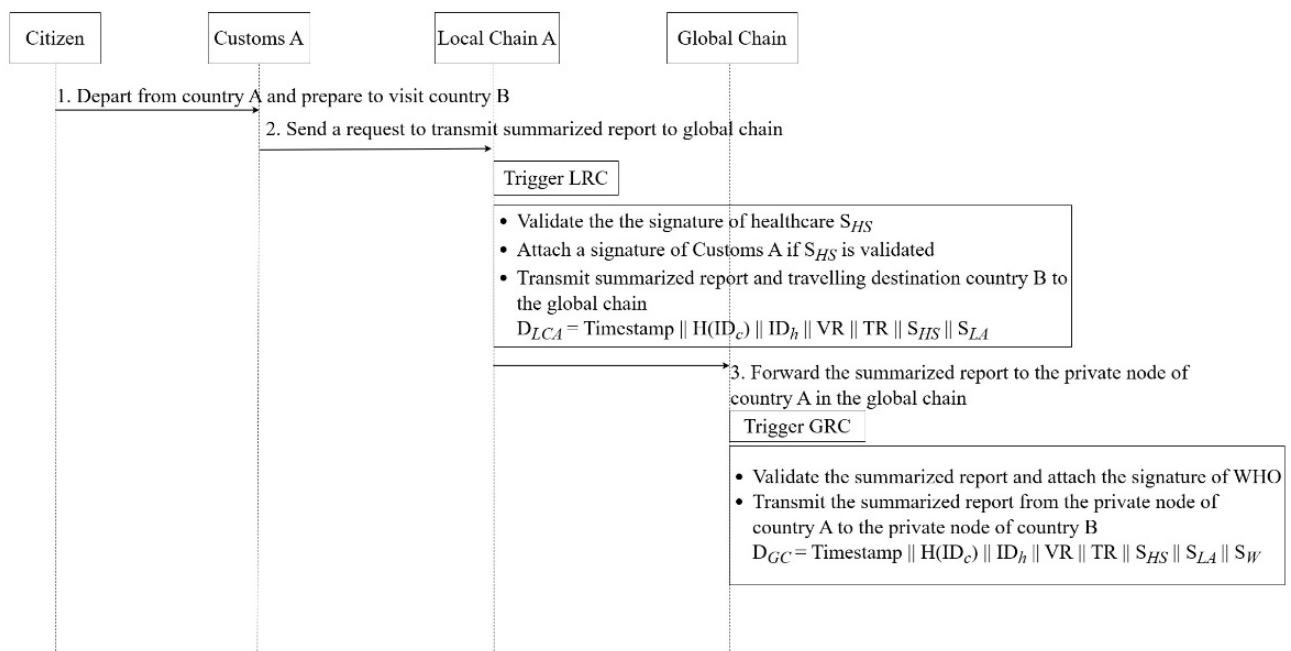


Figure 4. Flowchart of custom clearance and moving a record within the global chain.

When the traveler arrives in country B, Customs B initiates the TRC to download the summarized pandemic-related report from its private node to the local chain. Additionally, this smart contract validates the WHO signature and, upon verification, attaches a signature from Customs B. While the summarized report meets the customs entry regulations of country B, the tourist is allowed to enter the country. Figure 5 illustrates the personnel clearance process for a cross-border traveler. However, in very busy customs offices in some countries, the TRC could be programmed to periodically download summarized pandemic-related reports from the global chain in advance and store them in a separate distributed IPFS, in addition to data blocks in the local chain, to provide quick access for Customs.

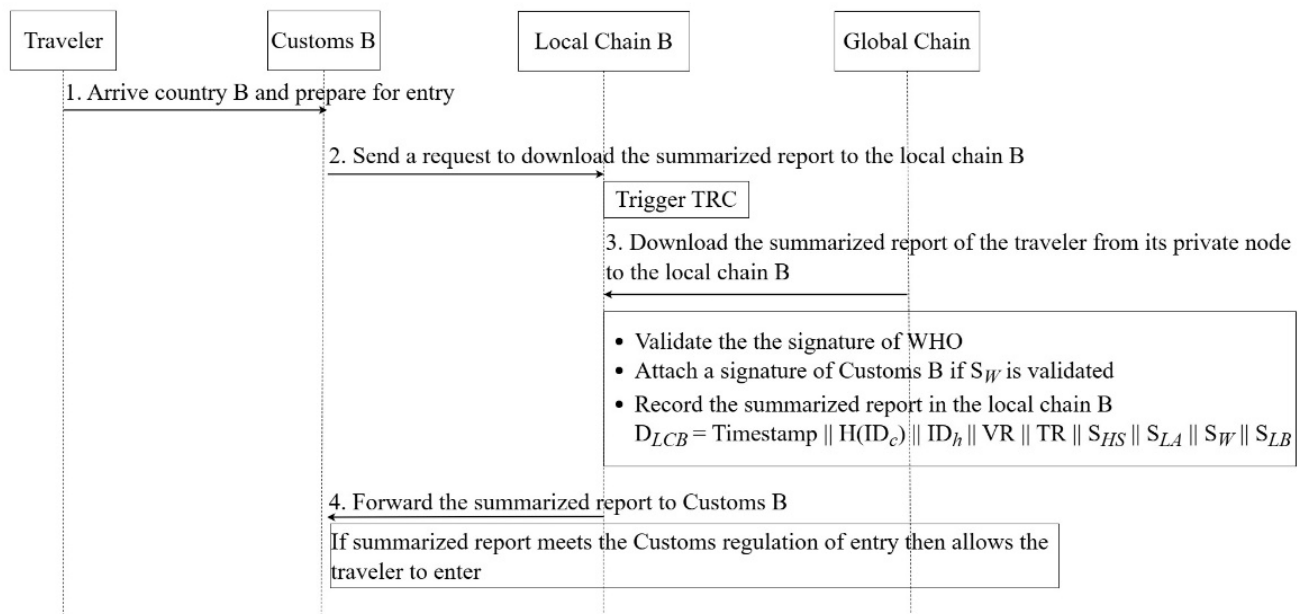


Figure 5. Flowchart of international traveler clearance at arrival customs.

5. Evaluation Results

In this study, we present a conceptual system architecture that is not yet fully implemented or comprehensively validated. Given the global-scale information exchange scenario, implementing it at full scale and in greater detail remains challenging at this stage. Therefore, after presenting the proposed framework, we first conduct security analyses using various attack types and threats across different workflows. We then use real data and simulated system parameters to assess the theoretical practicability of our proposal. We leverage the EOS blockchain [10] to simulate and verify the maximum transaction-per-second (TPS) capacity of our blockchain system and then analyze the required TPS for various scenarios to validate the feasibility of our design. We believe that its high performance and scalability, which meet the collaborative needs of many hospitals in the consortium blockchain of a country and the similar needs of many countries in the consortium blockchain worldwide, make it an excellent choice for implementation. Moreover, EOS also adopts BFT-DPoS, as does the proposed system. Finally, we also provide evaluations of dispute handling, performance requirements, storage considerations, and cost structure in this section.

5.1. Security Analyses

The security issues in various aspects of the proposed system are discussed as follows:

- **Anti-DDoS attack:** This study adopts BFT-DPoS as a consensus mechanism. Multiple BP nodes can produce the block. If a BP node is under DDoS attack, the other BP nodes can continue to create new blocks. Moreover, the TRC could be programmed to periodically download summarized pandemic-related reports from the global chain in advance and store them in the distributed IPFS, along with data blocks in the local chain, to provide quick access for busy customs or ports. IPFS's distributed architecture thus makes it easy to counter DDoS attacks. Therefore, DDoS can have only a minor impact on the proposed system.
- **Stability of miners:** The WHO and each government can determine who can participate and act as BP nodes in the proposed system. Moreover, in the BFT-DPoS election mechanism, nodes must prove their stability, security, and fairness to be elected as BP nodes. Therefore, the BP nodes are trustworthy.

- **Tamper resistance:** In the Merkle tree mechanism of blockchain, as long as users maliciously tamper with the data, the value of the Merkle root will be different. Therefore, the Merkle tree mechanism ensures that the records on the blockchain remain unaltered.
- **Decentralized system:** The proposed system acts based on blockchain, which means it can avoid security risks caused by a centralized mechanism, such as ransomware, malicious viruses, and central server failure.
- **Anti-Sybil attack:** There is an election BP node mechanism in BFT-DPoS consensus, and the candidates are measured according to the stakes of blockchain, security, and stability. Therefore, the proposed system can prevent Sybil nodes from being elected as BP nodes, preventing Sybil attacks.
- **Cross-border policy conflicts:** Regulatory inconsistency among participating countries may result in conflicting rules or processes during cross-border data exchange. The proposed system addresses this issue by isolating country-specific policies in the local chains while enforcing only a minimal set of standard requirements in the global chain to preserve interoperability.
- **Privilege escalation across roles:** Entities may attempt to perform actions beyond their authorization or impersonate top management in the local or global chains. This risk is mitigated by explicitly binding roles to a digital certificate and by smart-contract-enforced access control, ensuring that each participant can execute only authorized operations.
- **Trust-anchor compromise:** Trusted authorities, including government agencies or WHO-side operators, may become compromised. In the proposed system, abnormal signing or verification behaviors are immutably recorded in the global chain, enabling global observability and facilitating coordinated operation. As with the implementation of general-purpose blockchains and CAs, correction and/or revocation could be used to remedy such events or incidents.
- **Malicious denial or selective acceptance at the destination:** Customs may arbitrarily deny or selectively accept valid records. This situation happens often and has nothing to do with the information system. However, the proposed system can record all verification outcomes on the global chain, ensuring auditability and enabling post hoc accountability.

5.2. Performance Analyses

TPS is widely used to evaluate the performance of blockchain systems. The higher the TPS, the better the system's performance. The TPS of Bitcoin is around seven because it uses Proof of Work (PoW) as its consensus algorithm, in which miners spend significant time competing to validate transactions [40,41]. On the other hand, the TPS of Ethereum is about 20 [40,41]. The TPS of Ethereum [42] and Bitcoin differ significantly from that of a traditional centralized system (about 1 million). In this study, we adopt a weakly centralized consensus BFT-DPoS. Because the proposed system likely has only a few delegates (BP nodes) producing blocks, it should perform better than other consensus algorithms that require much computational power. For example, the TPS of BitShares [43], which adopts DPoS, can reach 3000.

We assess the proposed chain's TPS using the `txn_test_gen_plugin` 3.1 program [44], which can create the required number of transactions per second for performance evaluation. A simulation of a prototype system was conducted on four homogeneous nodes, each equipped with an Intel i9-class multi-core CPU and 64 GB DDR4 memory. Each node ran Ubuntu Linux 21.10 in a controlled environment. All nodes were deployed within a local setup with high-speed connectivity and without injected network latency. The `txn_test_gen_plugin` was used solely for transaction load generation, without modifying the consensus or scheduling mechanisms. This setup is intended as a lightweight feasibility

study rather than a full-scale performance benchmark. Under this prototype configuration, the system generated two blocks per second, each accommodating approximately 500 transactions. This results in an estimated throughput of around 1000 TPS and demonstrates the reachability of 1000 TPS under controlled conditions. We observed that 1000 TPS is close to the sustainable processing limit in our prototype configuration; beyond this rate, transactions accumulated in memory, leading to rapidly increasing queuing delays.

Furthermore, current studies report that several modern blockchain platforms can achieve TPS ranging from thousands to one million [45,46], suggesting that about 1000 TPS falls within a realistic and reachable range and can serve as a conservative upper bound for the analysis of stable real-time responsiveness. The following performance evaluation is based on a theoretical study that does not consider wide-area network latency, cross-border synchronization overhead, heterogeneous hardware environments, or failure scenarios. Accordingly, the reported analytical results should be interpreted as indications of feasibility.

To illustrate the workability under extreme conditions, we refer to the peak of COVID-19 vaccination in China on 24 June 2021. The daily vaccination rate reached a staggering historic high of 24.7 million doses [47]. Another report indicated that China's average daily rate during a specific period of COVID-19 was approximately 20 million doses [48]. Conservatively assuming that one local chain primarily operates within an 8 h injection window, these peak and average workloads need approximately 857.6 TPS and 694.4 TPS, respectively, indicating that thousand-level TPS capacity should support large-scale vaccination operations.

According to projections by the United Nations World Tourism Organization (UNWTO), there were approximately 1.545–1.575 billion international travelers in 2025 [49]. The average number of transactions per day for the global chain is therefore $1,560,000,000/365 \cong 4,273,973$, which corresponds to the average daily number of cross-border travel worldwide. This results in a required TPS $4,273,973/(24 \times 60 \times 60) \cong 49.5$, and $49.5 \ll 1000$.

Based on the analytical results and performance evaluation, we believe the proposed framework, embedded with standard blockchains, can effectively handle the necessary transactions required to combat COVID-19 or future contagious diseases at global border controls. Moreover, as was emphasized earlier in this subsection, several modern blockchain platforms have achieved TPS ranging from thousands to one million, and the necessary computational capabilities can be easily scaled using cloud services and virtual machine (VM) infrastructure.

ChakraChain introduces two types of approaches to implement parallel VM on blockchains, i.e., state access method and optimistic parallelization, to increase the throughput (or TPS) of their full nodes [50]. The core concept is based on a well-designed parallelization mechanism. Their experiment on a 4-thread Substrate BlockSTM shows that an improvement of 5.6 times in TPS has been achieved. This result has also led to the emergence of numerous parallel VM projects for real-world blockchains, such as Aptos, Sui, Monad, and Solana [50].

5.3. Data Validity and Dispute Handling

While blockchain technology ensures the integrity and immutability of recorded data, it does not inherently guarantee the correctness of data when it is entered into the information system. In addition, erroneous data or records may arise from human neglect, system integration issues, or delayed updates, rather than from malicious intent. Since blockchains do not support direct deletion or modification of on-chain records, corrections are handled through append-only updates instead that explicitly reference and supersede previous records. The WHO may arbitrate all disputes, as it is a neutral organization representing all countries and has the appropriate authority. This system, under the WHO's

supervision, could help identify disputed or erroneous records, review them, and resolve them through procedural mechanisms. However, a major limitation of the proposed system is precisely its reliance on a globally trusted coordinating and supervisory authority, such as the WHO, to support data validation and regulatory alignment and to handle disputes between countries. As is well known, geopolitical struggles, international conflicts, security threats, resource competition, and other factors may affect or weaken the WHO's authority, leading to possible malicious intervention or disruption of the proposed system. In fact, the above issues cannot be solved using any technical methods.

5.4. Performance Requirements

In the local chain, primary transactions involve uploading vaccination or testing records generated by healthcare institutions to the blockchain and downloading them from the global chain to the local chain. However, from a border-crossing perspective, uploading these data is considered a non-real-time application. This is because immediate transmission completion or a quick response is not necessary. For similar reasons, the global chain generally does not need to operate in real time, since most international travel cases take time to clear customs in one country and then enter another country's customs. Therefore, even when transaction rates temporarily exceed processing capacity, some transactions can be queued rather than dropped. As discussed in Section 5.2, the average required TPS for international border crossings is about 49.5, which is $\ll 1000$; therefore, the global chain can handle it with much redundancy.

Real-time processing is primarily required during destination-side customs verification. In France, the total number of inbound tourists reached a historic high of 217,877,000 in 2019, according to data from the UNWTO website [51]. This means an average required TPS $217,877,000 / (365 \times 24 \times 60 \times 60) \cong 6.9$, and $6.9 \ll 1000$. Recent statistical data on inbound tourists for individual countries either declined during the COVID-19 pandemic or remain outdated for unknown reasons. Dubai International Airport is used as another example; it handles about 324,000 passengers on peak days [52], which corresponds to an average of approximately 3.8 TPS. It is much under the conservative assumption of 1000. These analyses suggest that the proposed system maintains a substantial performance margin to withstand potential variations in real-world deployments. Furthermore, as emphasized above, IPFS can be used to store pre-downloaded pandemic testing history and vaccination records, or cloud services and VM infrastructure can be implemented to provide greater computational capacity, further accelerating real-time access for customs and ports.

5.5. Scalability and Storage Considerations

Only the minimum information required for cross-border verification is stored on-chain, including timestamps, hashed identifiers, healthcare institution IDs, vaccination or testing records, and a few digital signatures from different authorities. Considering transaction overhead, each on-chain transaction could be estimated at approximately several hundred to a thousand bytes. Therefore, based on the above estimates, 10 K, 1 M, 10 M, and 100 M records require approximately 10 MB, 1 GB, 10 GB, and 100 GB of storage, respectively. According to UN Tourism projections, there are 1.545–1.575 billion international travelers in 2025 [49]. Then, the annual on-chain data volume for the global chain is about 0.94–1.56 TB, which remains manageable for modern blockchain systems. From a practical perspective, similar storage requirements are observed across existing platforms, such as the Ethereum Chain, which stands at around 1.51 TB as of 18 January 2026 [53]. As is well known, this 1.51 TB of the Ethereum Chain has been accumulated over ten years, but about 0.94–1.56 TB of storage in our blockchain system is required annually. However,

the proposed two-layered framework only functions during the pandemic period and should not work forever, as assumed by all financial blockchains. The WHO activates the two-layered blockchain system during the pandemic and switches it from active to sleep mode after the pandemic ends; then, cross-border controls will no longer be needed. In fact, out-of-date or expired vaccination and testing records are not useful for border crossings; therefore, a new blockchain should be established if the next pandemic breaks out. This should reduce storage requirements, since our system will not run continuously. So, from this perspective, we believe an annual on-chain storage demand of about 0.94–1.56 TB is still acceptable.

5.6. Cost Structure of Local and Global Chains

The proposed blockchain architecture incurs different costs for local and global chains. Local chains typically operate with several to a dozen full nodes, assuming each node is provisioned with 2X Intel Xeon Gold or AMD EPYC (multiple cores), 384 GB DDR5 RAM, and several 122.88 SSD storage devices. These result in an estimated annual infrastructure cost of USD 80K–120K and an operational workforce requirement of about 2 full-time equivalents (FTEs), which will require USD 300K per year. On the other hand, the global chain is assumed to operate with around several hundred full nodes to ensure representation of all countries worldwide, each using higher-level servers than those specified above. Under conservative estimates, these result in annual infrastructure costs of USD 4.5–6.0 million and an operational workforce requirement of approximately 8–10 FTEs, costing USD 1.2–1.5 million per year. For an international-scale system, the estimated expenditures fall within a reasonable range. While the global chain serves as the primary cost center, these costs can be distributed across participating countries or organizations, thereby supporting the economic feasibility of the proposed framework.

5.7. IPFS-Based Off-Chain Storage: Volume and Cost Considerations

In this section, we estimate the storage volume and cost implications of using IPFS as an optional off-chain distributed preservation for detailed EMR of pandemic testing history and vaccination records. According to Lugo et al. [54], an HL7 CDA-based EMR has an average file size of approximately 30 KB. Since the detailed EMR for pandemic testing history and vaccination records is lightweight, we assume the EMR size for this type is 50–100 KB. According to WHO and related databases, approximately 3.52 billion vaccine doses had been injected in China by October 2023 [55]. Given that IPFS deployments commonly use redundancy to enhance data persistence and availability, the total storage requirement is approximately 528–1056 TB for three replicas. In a 50-node peer-to-peer IPFS deployment, this corresponds to an average storage requirement of about $(50 \text{ KB} \times 3,520,000,000 \times 3)/50 = 10.56 \text{ TB}$ or $(100 \text{ KB} \times 3,520,000,000 \times 3)/50 = 21.12 \text{ TB}$ per node. It is really feasible since the biggest SSD on the market now is 122.88 TB. In fact, the associated IPFS costs are primarily driven by computational power, storage capacity, and redundancy requirements. Considering an IPFS with 50 peers, as mentioned above, for a national-scale deployment scenario, each provisioned with 2X Intel Xeon Gold or AMD EPYC (multiple cores), 384 GB DDR5 RAM, and several 122.88 TB SSDs as well, the estimated annual infrastructure cost is around USD 500K. Therefore, the feasibility and scalability of IPFS within the proposed two-layered framework do not constitute fundamental bottlenecks in regular deployments.

5.8. Discussion

While consortium blockchains enable shared governance among multiple participants, a hybrid architecture that integrates a global ledger with sovereign-level private

chains is increasingly viewed as a flexible alternative that can address jurisdiction-specific requirements. This architectural approach is associated with the following advantages:

- **Operational efficiency:** Delegating transactions involving local chains to national private chains in the global chain, while reserving the global ledger for essential cross-border validations, is considered a viable means of mitigating consensus-related workload—particularly in environments characterized by high local transaction density.
- **Security and privacy alignment:** The implementation of layered access controls may assist in isolating risks across jurisdictions. Moreover, the selective transmission of only essential information closely aligns with key regulatory frameworks, such as the General Data Protection Regulation (GDPR) in the EU, particularly regarding data minimization and localized control.
- **Regulatory clarity:** By allowing each jurisdiction to retain autonomy over data governance, the two-layered and hybrid characteristics may help clarify responsibility boundaries and simplify oversight procedures, particularly in cross-border data exchange contexts.

6. Conclusions

To maintain global health and wellness, a platform for the international sharing of medical data on highly contagious diseases, free from interference from individual countries, is necessary for effective border control. Therefore, in this paper, we propose a two-layer blockchain architecture for managing pandemic-related data, incorporating a global chain and multiple local chains to ensure national autonomy and sustainable pandemic protection worldwide. The bottom-layer local chains facilitate the preparation of pandemic immunity data within their own countries, and the upper-layer global chain, with the assistance of the WHO, facilitates the worldwide exchange of these pandemic data if needed. In this endeavor, educational institutions, research organizations, businesses, and healthcare facilities can serve as blockchain nodes for maintaining local chains. Miners will be rewarded with medical data, subject to patients' permission or tax relief. This incentive model addresses the drawbacks of resource waste in previous blockchain systems, enabling medical records to be used for research. Moreover, a similar motivation could also be designed for the global chain. Due to the characteristics of decentralization and transparency of blockchain technology and the supervision of the WHO, no government should worry that sensitive medical data will be manipulated or abused by superpowers. It also highlights the importance of sustainable global collaboration in preventing and controlling contagious diseases. Furthermore, we select distributed data storage, IPFS, as an option that can effectively address security concerns such as data backup, ransomware, viruses, and central server failures commonly associated with centralized systems. Instead of transferring complete records to the blockchain, we only upload record summaries. By leveraging blockchain technology, the challenge of sharing pandemic-related data is addressed through its tamper-resistant, secure, and traceable features, which help prevent malicious tampering with records. In addition, the automated enforcement of smart contracts helps mitigate risks associated with human and/or political factors.

Even though this framework can enable efficient sharing of pandemic-related data, it still faces some limitations. As with any governance-based blockchain, the proposed system cannot technically prevent a sovereign authority from intentionally submitting false data. Instead of assuming universal honesty, the system mitigates such risks through transparency and international governance. Cross-border records linked to the global chain are observable worldwide, and detected misconduct may result in suspension or restriction of future participation. Furthermore, this framework is primarily designed to support cross-border data verification and exchange rather than full-scale EMR sharing.

Thus, it intentionally maintains a lightweight application-layer scope. Its practical deployment involves coordination among governments and international organizations; however, variations in national policies, global environments, institutional readiness, and heterogeneous healthcare data standards across countries may pose challenges to deployment and interoperability. While the current performance evaluation provides an initial feasibility assessment under controlled conditions, further empirical studies under global-scale operational settings are needed to understand system performance in the real world.

In summary, we have demonstrated that this global information system can enhance international health safety by providing sufficient capability to handle transactional demands worldwide during the pandemic. It also has strong potential to strengthen all nations' ability to prepare for and respond to future pandemics, thereby ensuring global human safety.

Author Contributions: Conceptualization, Y.-C.L. and C.C.-Y.K.; methodology, Y.-C.L. and C.C.-Y.K.; software, H.P.-C.H.; validation, Y.-C.L., C.C.-Y.K. and H.P.-C.H.; formal analysis, C.C.-Y.K.; investigation, H.P.-C.H.; data curation, Y.-C.L. and H.P.-C.H.; writing—original draft preparation, Y.-C.L., C.C.-Y.K. and H.P.-C.H.; writing—review and editing, C.C.-Y.K.; visualization, Y.-C.L. and H.P.-C.H.; supervision, C.C.-Y.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available in [COVID-19 vaccination program in the mainland of China: A subnational descriptive analysis on target population size and current progress] at [<https://link.springer.com/article/10.1186/s40249-021-00909-1>], reference number [47], [China is vaccinating a staggering 20 million people a day] at [<https://www.nature.com/articles/d41586-021-01545-3>], reference number [48], and [World Tourism Barometer and Statistical Annex] at [<https://doi.org/10.18111/wtobarometereng>], reference number [49]. These data were derived from the following resources available in the public domain: [World Tourism Organization (UN Tourism)/Tourism Statistics—Inbound Tourism and <https://www.untourism.int/tourism-statistics/tourism-data-inbound-tourism>], [Kenya Association of Travel Agents and <https://katakanya.org/dubai-international-dxb-hits-three-hundred-twenty-four-thousand-passengers-in-just-one-day/>], and [World Health Statistics/WHO COVID-19 Dashboard and <https://data.who.int/dashboards/covid19/vaccines?m49=156>]. All the URLs above were accessed on 5 December 2025.

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

Abbreviations

The following abbreviations are used in this manuscript:

WHO	World Health Organization
PRET	The Preparedness and Resilience for Emerging Threats
NAPHS	National Action Plan for Health Security
COVID-19	Coronavirus Disease 2019
IPFS	InterPlanetary File System
SARS-CoV	Severe Acute Respiratory Syndrome Coronavirus
H1N1	Influenza A Virus Subtype H1N1
BFT-DPoS	Byzantine Fault Tolerance Delegated Proof of Stake
PBFT	Practical Byzantine Fault Tolerance
DPoS	Delegated Proof of Stake
BFT	Byzantine Fault Tolerance
BP	Block Producer

DDoS	Distributed Denial-of-Service
CTSAF	Converging Technologies for Sustainable Agri-Food Chains
V2G	Vehicle-to-Grid
EV	Electrical Vehicle
ECC	Elliptic Curve Cryptography
RBAC	Role-based Access Control
ABAC	Attribute-based Access Control
MSC	The Medicine Supply Chain
EHR	Electronic Health Record
VANET	Vehicular Ad-Hoc Network
AHMSs	Advanced Health Monitoring Systems
LCM	Life Cycle Management
CA	Certificate Authority
LRC	Local Record Contracts
GRC	Global Record Contracts
TRC	Travel Record Contracts
VR	Vaccination Record
TR	Testing Report
EMR	Electronic Medical Record
TPS	Transactions per Second
PoW	Proof of Work

References

1. World Health Organization. Naming the Coronavirus Disease (COVID-19) and the Virus That Causes It. 2020. Available online: [https://www.who.int/emergencies/diseases/novel-coronavirus-2019/technical-guidance/naming-the-coronavirus-disease-\(covid-2019\)-and-the-virus-that-causes-it](https://www.who.int/emergencies/diseases/novel-coronavirus-2019/technical-guidance/naming-the-coronavirus-disease-(covid-2019)-and-the-virus-that-causes-it) (accessed on 17 November 2025).
2. World Health Organization. Coronavirus Disease (COVID-19) Pandemic. 2023. Available online: <https://www.who.int/europe/emergencies/situations/covid-19> (accessed on 17 November 2025).
3. World Health Organization. Preparedness and Resilience for Emerging Threats (PRET). 2023. Available online: <https://www.who.int/initiatives/preparedness-and-resilience-for-emerging-threats> (accessed on 17 November 2025).
4. World Health Organization. A Brief Overview of the Preparedness and Resilience for Emerging Threats Initiative (PRET). 2023. Available online: <https://www.who.int/news/item/14-04-2023-a-brief-overview-of-the-preparedness-and-resilience-for-emerging-threats-initiative-pret> (accessed on 17 November 2025).
5. World Health Organization. Preparedness and Resilience for Emerging Threats Module 1: Planning for Respiratory Pathogen Pandemics. 2024. Available online: <https://www.who.int/publications/i/item/9789240084674> (accessed on 17 November 2025).
6. World Health Organization. National Action Plan for Health Security (NAPHS). 2025. Available online: <https://www.who.int/emergencies/operations/international-health-regulations-monitoring-evaluation-framework/national-action-plan-for-health-security> (accessed on 17 November 2025).
7. World Health Organization. World Health Organization Strategy (2022–2026) for the National Action Plan for Health Security. 2022. Available online: <https://www.who.int/publications/i/item/9789240061545> (accessed on 17 November 2025).
8. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. *SSRN Electron. J.* 2008. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3440802 (accessed on 15 March 2023).
9. Hossain, M.R.; Nirob, F.A.; Islam, A.; Rakin, T.M.; Al-Amin, M. A comprehensive analysis of blockchain technology and consensus protocols across a multilayered framework. *IEEE Access* **2024**, *12*, 63087–63129. [CrossRef]
10. Larimer, D. DPoS BFT—Pipelined Byzantine Fault Tolerance. 2018. Available online: <https://medium.com/eosio/dpos-bft-pipelined-byzantine-fault-tolerance-8a0634a270ba> (accessed on 17 November 2025).
11. Stanescu, S.-G.; Ionescu, C.A.; Ștefan, M.C.; Ionescu, L.; Bondac, G.-T.; Cristea, A.M. Digitalization and blockchain integration in Agri-Food supply chains: Towards a resilient, circular, and sustainable future. *Sustainability* **2025**, *17*, 9276. [CrossRef]
12. Sasirega, R.; Prakash, S. Secure and incentivized V2G participation with blockchain and game theory. *J. Inf. Secur. Appl.* **2025**, *89*, 103975. [CrossRef]
13. Han, G.; Ma, W.; Zhang, Y.; Liu, Y.; Liu, S. BSFL: A blockchain-oriented secure federated learning scheme for 5G. *J. Inf. Secur. Appl.* **2025**, *89*, 103983. [CrossRef]

14. Szabo, N. Smart Contracts: Building Blocks for Digital Markets. 1996. Available online: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html (accessed on 17 November 2025).
15. Kanagi, K.; Ku, C.C.-Y.; Lin, L.-K.; Hsieh, W.-H. Efficient clinical data sharing framework based on blockchain technology. *Methods Inf. Med.* **2020**, *59*, 193–204. [\[CrossRef\]](#) [\[PubMed\]](#)
16. Hathaliya, J.J.; Tanwar, S. Role and attribute-based access control scheme for decentralized medicine supply chain. *J. Inf. Secur. Appl.* **2024**, *85*, 103851. [\[CrossRef\]](#)
17. Kistaubayev, Y.; Liébana-Cabanillas, F.; Shaikh, A.A.; Mutanov, G.; Ussatova, O.; Shinbayeva, A. Enhancing transparency and trust in higher education institutions via blockchain: A conceptual model utilizing the Ethereum consortium approach. *Sustainability* **2025**, *17*, 9350. [\[CrossRef\]](#)
18. Cristea, A.-G.; Alboaie, L.; Panu, A.; Radulescu, V. Offline but still connected with IPFS based communication. *Procedia Comput. Sci.* **2020**, *176*, 1606–1612. [\[CrossRef\]](#)
19. Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. Blockchain for secure EHRs sharing of mobile cloud based E-health systems. *IEEE Access* **2019**, *7*, 66792–66805. [\[CrossRef\]](#)
20. Guo, J.; Zhao, K.; Liang, Z.; Min, K. Efficient and secure EMR storage and sharing scheme based on Hyperledger fabric and IPFS. *Appl. Sci.* **2024**, *14*, 5005. [\[CrossRef\]](#)
21. Patel, N.; Patel, D.; Jadav, N.K.; Rathod, T.; Tanwar, S.; Pau, G.; Sharma, G.; Alqahtani, F.; Tolba, A. Fuzzy-enhanced secure messaging framework for smart healthcare system. *IEEE Access* **2024**, *12*, 102977–102993. [\[CrossRef\]](#)
22. Budd, J.; Miller, B.S.; Manning, E.M.; Lampos, V.; Zhuang, M.; Edelstein, M.; Rees, G.; Emery, V.C.; Stevens, M.M.; Keegan, N.; et al. Digital technologies in the public-health response to COVID-19. *Nat. Med.* **2020**, *26*, 1183–1192. [\[CrossRef\]](#) [\[PubMed\]](#)
23. Khurshid, A. Applying blockchain technology to address the crisis of trust during the COVID-19 pandemic. *JMIR Med. Inform.* **2020**, *8*, e20477. [\[CrossRef\]](#)
24. Chang, M.C.; Park, D. How can blockchain help people in the event of pandemics such as the COVID-19? *J. Med. Syst.* **2020**, *44*, 102. [\[CrossRef\]](#) [\[PubMed\]](#)
25. Shi, R.; Guo, X.; Ren, D. How to extend the photovoltaic value chain? A blockchain-based strategy for photovoltaic-storage-hydrogen integration with green electricity trading. *Energy* **2025**, *315*, 134394. [\[CrossRef\]](#)
26. Chen, X.; Cheng, Q.; Yang, W.; Luo, X. A novel blockchain-based anonymous roaming authentication scheme for VANET. *J. Inf. Secur. Appl.* **2025**, *88*, 103922. [\[CrossRef\]](#)
27. Babaei, A.; Khedmati, M.; Akbari Jokar, M.R.; Babaei Tirkolaee, E. Product tracing or component tracing? Blockchain adoption in a two-echelon supply chain management. *Comput. Ind. Eng.* **2025**, *200*, 110789. [\[CrossRef\]](#)
28. Gaurav, K.K.; Baranwal, G. A blockchain-enabled private parking space allocation with improved parking space utilization. *Comput. Ind. Eng.* **2024**, *197*, 110613. [\[CrossRef\]](#)
29. Sutrala, A.K.; Bagga, P.; Das, A.K.; Kumar, N.; Rodrigues, J.J.P.C.; Lorenz, P. On the design of conditional privacy preserving batch verification-based authentication scheme for Internet of Vehicles deployment. *IEEE Trans. Veh. Technol.* **2020**, *69*, 5535–5548. [\[CrossRef\]](#)
30. Tan, H.; Wang, M.; Shen, J.; Vijayakumar, P.; Moh, S.; Wu, Q.M.J. Blockchain-assisted conditional anonymous authentication and adaptive tree-based group key agreement for VANETs. *IEEE Trans. Dependable Secur. Comput.* **2025**; early access. [\[CrossRef\]](#)
31. Eisenstadt, M.; Ramachandran, M.; Chowdhury, N.; Third, A.; Domingue, J. COVID-19 antibody test/vaccination certification: There's an app for that. *IEEE Open J. Eng. Med. Biol.* **2020**, *1*, 148–155. [\[CrossRef\]](#)
32. Bansal, A.; Garg, C.; Padappayil, R.P. Optimizing the implementation of COVID-19 immunity certificates using blockchain. *J. Med. Syst.* **2020**, *44*, 140. [\[CrossRef\]](#)
33. Garg, C.; Bansal, A.; Padappayil, R.P. COVID-19: Prolonged social distancing implementation strategy using blockchain-based movement passes. *J. Med. Syst.* **2020**, *44*, 165. [\[CrossRef\]](#)
34. Kabashkin, I.; Perekrestov, V.; Tyncherov, T.; Shoshin, L.; Susanin, V. Framework for integration of health monitoring systems in life cycle management for aviation sustainability and cost efficiency. *Sustainability* **2024**, *16*, 6154. [\[CrossRef\]](#)
35. Resiere, D.; Resiere, D.; Kallel, H. Implementation of medical and scientific cooperation in the Caribbean using blockchain technology in coronavirus (COVID-19) pandemics. *J. Med. Syst.* **2020**, *44*, 123. [\[CrossRef\]](#) [\[PubMed\]](#)
36. Tan, L.; Yu, K.; Shi, N.; Yang, C.; Wei, W.; Lu, H. Towards secure and privacy-preserving data sharing for COVID-19 medical records: A blockchain-empowered approach. *IEEE Trans. Netw. Sci. Eng.* **2022**, *9*, 271–281. [\[CrossRef\]](#)
37. Dar, A.A.; Alam, M.Z.; Ahmad, A.; Reegu, F.A.; Rahin, S.A. Blockchain framework for secure COVID-19 pandemic data handling and protection. *Comput. Intell. Neurosci.* **2022**, *2022*, 7025485. [\[CrossRef\]](#)
38. Biswas, S.; Sharif, K.; Li, F.; Bairagi, A.K.; Latif, Z.; Mohanty, S.P. GlobeChain: An interoperable blockchain for global sharing of healthcare data—A COVID-19 perspective. *IEEE Consum. Electron. Mag.* **2021**, *10*, 64–69. [\[CrossRef\]](#)
39. ASTP. Health Level 7 (HL7) Fast Healthcare Interoperability Resources (FHIR). 2025. Available online: <https://www.healthit.gov/topic/standards-technology/standards/fhir> (accessed on 19 January 2026).

40. Tang, H.; Shi, Y.; Dong, P. Public blockchain evaluation using entropy and TOPSIS. *Expert Syst. Appl.* **2019**, *117*, 204–210. [CrossRef]
41. Sun, Y.; Zhang, L.; Feng, G.; Yang, B.; Cao, B.; Imran, M.A. Blockchain-enabled wireless Internet of Things: Performance analysis and optimal communication node deployment. *IEEE Internet Things J.* **2019**, *6*, 5791–5802. [CrossRef]
42. Ethereum. Welcome to Ethereum. 2025. Available online: <https://ethereum.org/en/> (accessed on 17 November 2025).
43. BitShares. BitShares Core 7.0.2. 2025. Available online: <https://bitshares.org/> (accessed on 17 November 2025).
44. EOS Network. txn_test_gen_plugin. 2022. Available online: https://docs.antelope.io/leap/3.2-rc1/nodeos/plugins/txn_test_gen_plugin/ (accessed on 17 November 2025).
45. Miah, S. 10 Fastest Blockchains by TPS 2025. 2025. Available online: <https://www.webopedia.com/crypto/learn/fastest-blockchains-tps/> (accessed on 3 January 2026).
46. NEAR. NEAR Hits 1 Million TPS: A Major Milestone for Blockchain Scalability. 2025. Available online: <https://www.near.org/blog/near-protocol-achieves-1-million-tps> (accessed on 7 January 2026).
47. Zheng, W.; Yan, X.; Zhao, Z.; Yang, J.; Yu, H. COVID-19 vaccination program in the mainland of China: A subnational descriptive analysis on target population size and current progress. *Infect. Dis. Poverty* **2021**, *10*, 124. [CrossRef] [PubMed]
48. Mallapaty, S. China Is Vaccinating a Staggering 20 Million People a Day. *Nature Website*. 9 June 2021. Available online: <https://www.nature.com/articles/d41586-021-01545-3> (accessed on 5 December 2025).
49. World Tourism Organization (UN Tourism). World Tourism Barometer and Statistical Annex. *World Tour. Barom.* **2025**, *23*, 1–36. [CrossRef]
50. ChakraChain. Parallel VM, Chakra’s Path to 100,000 TPS. 2024. Available online: <https://medium.com/@chakrachainbtc/parallel-vm-chakras-path-to-100-000-tps-eace1f1a6c2a> (accessed on 5 December 2025).
51. World Tourism Organization (UN Tourism). Tourism Statistics—Inbound Tourism. 2025. Available online: <https://www.untourism.int/tourism-statistics/tourism-data-inbound-tourism> (accessed on 5 December 2025).
52. Kenya Association of Travel Agents (KATA). Dubai International (DXB) Hits Three Hundred Twenty-Four Thousand Passengers in Just One Day. 2026. Available online: <https://katakkenya.org/dubai-international-dxb-hits-three-hundred-twenty-four-thousand-passengers-in-just-one-day/> (accessed on 5 December 2025).
53. YCharts. Ethereum Chain Full Sync Data Size. 2025. Available online: https://ycharts.com/indicators/ethereum_chain_full_sync_data_size (accessed on 5 December 2025).
54. Lugo, E.; Muñoz, R.; Vilachá, C.; Villegas, Á.; Pacheco, J.; Villegas, R. A digital system for managing HL7/CDA electronic medical records stored in iButtons®. *E-Health Telecommun. Syst. Netw.* **2014**, *3*, 24–32. [CrossRef]
55. World Health Statistics. WHO COVID-19 Dashboard. 2023. Available online: <https://data.who.int/dashboards/covid19/vaccines?m49=156> (accessed on 5 December 2025).

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.