Multi-MedChain: Multi-Party Multi-Blockchain Medical Supply Chain Management System

***Abstract*—The challenges of healthcare supply chain management systems during the COVID-19 pandemic highlighted the need for an innovative and robust medical supply chain. The healthcare supply chain involves various stakeholders who must share information securely and actively. Regulatory and compliance reporting is also another crucial requirement for perishable products (e.g., pharmaceuticals) within a medical supply chain management system. Here, we propose Multi-MedChain as a three-layer multi-party, multi-blockchain (MPMB) framework utilizing smart contracts as a practical solution to address challenges in existing medical supply chain management systems. Multi-MedChain is a scalable supply chain management system for the healthcare domain that addresses end-to-end traceability, transparency, and collaborative access control to restrict access to private data. We have implemented our proposed system and report on our evaluation to highlight the practicality of the solution. The proposed solution is made publicly available.**

Keywords: Medical Supply Chain, Multi-Party Multi-Blockchain, End-to-End Traceability, Access Control.

I. Introduction

The healthcare supply chain comprises interconnected systems, components, and processes that collaboratively function to manufacture, distribute, and deliver medications and other healthcare supplies. A typical supply chain includes several organisations, resources, and interdependent operations. Fig. 1 represents the workflow of the medical supply chain during COVID-19. With the outbreak of the COVID-19 pandemic, there was a sudden surge in demand for drugs, masks, and PPE kits, overwhelming the healthcare supply chain. The scarcity of personal protective equipment (PPE) and masks during the initial stages of the pandemic is a prime example of the consequences of an inadequate healthcare supply chain management system (SCM) [1]. The holding and black marketing of lifesaving drugs and equipment by some distributors for higher profits have further induced the Bullwhip effect in the supply chain, leading to mismatches between demand and production and decreased efficiency of the supply chain [2].

Effective SCM is essential for efficient delivery of medical supplies and equipment, especially during crises. The current healthcare SCM oversees the transportation of medical supplies from the manufacturer to the final recipient, the patient. SCMs are known to be hampered by the lack of information exchange between partners [3] attributed to the absence of direct contact, reluctance to share competitive and private information, and the presence of multiple supply chains with varying trading partners over time [3]. Managing the SCM involves multiple stakeholders with different objectives and interests, making it a complex and fragmented process. Therefore, the healthcare industry requires a smarter, more decentralised, and more effective supply chain [4].

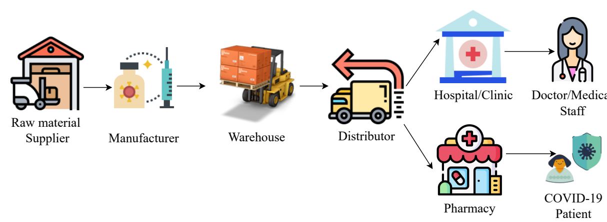


Fig. 1. The workflow of medical supply chain during COVID-19.

In addition to the issues mentioned above, the complexity of healthcare SCM is exacerbated by factors such as poor product standardization, insufficient reporting of data, a lack of automation in the process, and increasing regulatory requirements. These challenges result in higher supply costs that healthcare providers and hospitals find difficult to manage. Although the necessity for proper PPE has long been recognised, obtaining and distributing the appropriate equipment for each clinical setting has proven to be a global challenge [5]. Oftentimes, hospitals face the hoarding of certain products, such as COVID-19 vaccines by providers. Therefore, the discrepancy between incentives and independent goals can disrupt the supply chain flow of many healthcare organisations.

There has been a growing interest among industry leaders and managers in adopting blockchain technology in healthcare supply chains [6], [7]. With the rapid development of blockchain technology in healthcare, several blockchain-based mechanisms have been proposed to ensure traceability from one end to another across the supply chain [8]. However, the question of sharing accurate information and maintaining data privacy to ensure competitiveness in the market is a research challenge that has not been adequately addressed. In this paper, we propose Multi-MedChain as a novel and robust three-layer multi-party, multi-blockchain (MPMB) healthcare supply chain management system. Our proposed solution enables secure cross-chain communication to establish digital trust while keeping sensitive information private on local blockchains. For instance, trading secrets of supply chain stakeholders, such as capacities and prices, must be kept private in such a system. To further limit and impose control over the sharing of private information for different parties involved in the SCM, we have devised a dynamic access control mechanism that leverages smart contracts. This allows supply chain stakeholders to collaboratively manage user authorisations and achieve end-to-end traceability. We have implemented our solution, and the evaluation results prove the scalability of Multi-MedChain. The project source code has been made publicly accessible for replication and extensions.

II. Literature Review

Medical and pharmaceutical companies are actively exploring blockchain-enabled solutions to provide a secure and reliable method of tracking their products throughout the supply chain. Modum [9] operates on the Ethereum blockchain, powered by smart contracts, and checks the state of the drug at strategic stages to ensure that it meets the required standard. Chronicled [10], Blockpharma [11], and Tierion [12] are some of the ongoing projects that use blockchain to redefine the medical supply chain.

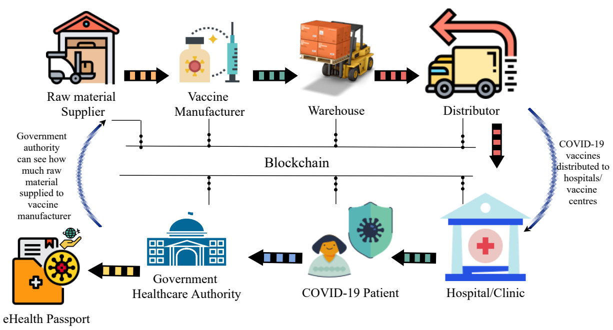


Fig. 2. Circular blockchain-based healthcare SCM.

Blockchain technology in healthcare promotes efficiency and provides better control over supply chains. It also improves overall patient safety, solves the problem of drug authenticity and traceability, and enables secure interoperability among healthcare institutions [13]. In [14] a blockchain-based drug SCM has been proposed using Hyperledger fabric to enhance the functionality of the supply chain and ensure the management of drug records. Similarly, blockchain can create a transparent and traceable vaccine supply chain, building trust between institutions and patients. [15]. In [16], the authors list crucial challenges facing the COVID-19 vaccine supply chain, such as a) accurate prediction of vaccine demand, b) proper planning and scheduling, c) coordination with local organisations, and d) correspondence among SCM vaccine entities. A smart contract-based solution for safe vaccine distribution and tracking has been proposed in [17]. In [18], a double-level blockchain structure has been designed to supervise vaccine production. Furthermore, a smart contract-based drug traceability mechanism has been proposed in [19]. [20] has devised a distributed privacy-preserving application to maintain medical certificates.

All existing healthcare SCM systems work in a circular manner, where multiple parties share the same blockchain network, as shown in Fig. 2. In such systems, consensus is governed by a single party or multiple parties involved in the network. However, this approach has potential drawbacks, including disagreement between participants, exposed intellectual property (IP) or proprietary details (demands, capacities, orders, prices, margins) and bias for privacy in open access [21]. They also have conflicts about the choice of platform and data to be shared.

None of the above-mentioned works has considered systems consisting of multiple independent blockchains for each stakeholder. In real-time applications, single blockchain models in the healthcare supply chain ecosystem limit stakeholders from sharing information in a direct, secure, and transparent manner. To overcome the limitations of existing frameworks, our scheme comprises multiple independent blockchains and facilitates cross-chain solutions among them. Multi-MedChain, our proposed solution, enables the SCM to establish digital trust and secure customer relationships. At the same time, these systems help multiple businesses and governments form digital trust, providing more control by providing direct access to sensitive information for improved, highly customised services with enhanced security and privacy. Here, each party manages its blockchain network, eliminating disagreements over consensus mechanisms, membership, or technology stack.

The comprehensive comparison of related work in the blockchain-based healthcare supply chain [8], [22]–[27] is summarised in Table I. The comparison is conducted in terms of various key features that are enumerated in the first column of the table.

III. Proposed Solution: Multi-MedChain

To facilitate demand-supply coordination, compliance certification, and improve information sharing in the healthcare supply chain management system, we propose an end-to-end solution using a multi-party multi-blockchain model illustrated in Fig. 3. For simplicity, we focus on the vaccine supply chain. However, the proposed approach is adaptable to the supply chain of other medical supplies.

TABLE I
SUMMARY OF KEY FEATURES OF THE EXISTING WORKS IN HEALTHCARE SUPPLY CHAIN.

Features	[8]	[22]	[23]	[24]	[25]	[26]	[27]
Anonymity	X	X	✓	✓	X	X	X
Access control	X	X	✓	✓	X	✓	✓
Authentication	X	X	X	✓	✓	✓	X
Data privacy	X	X	X	X	✓	X	✓
Information asymmetry	X	X	X	X	X	X	X
Information sharing	X	X	✓	✓	✓	✓	✓
Multi-chain	X	X	X	✓	X	X	X
Multi-layer	✓	✓	X	✓	✓	X	X
Traceability	X	X	X	X	✓	✓	✓
Governance	X	✓	X	X	✓	X	X
Cross-chain/Interoperability	X	X	X	✓	X	X	X
Sustainability	✓	✓	X	X	X	X	X

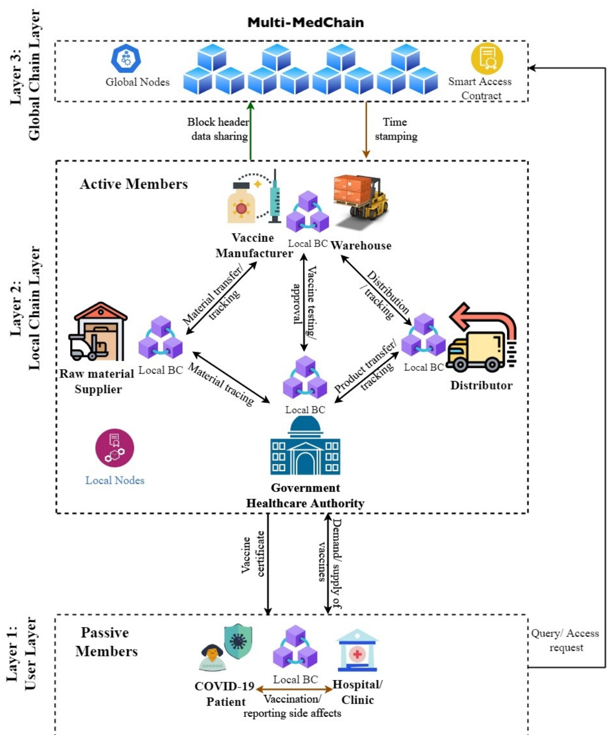


Fig. 3. Multi-MedChain framework.

In the specific use case that we consider to present Multi-MedChain, we focus on the vaccine supply chain. Here, Multi-MedChain establishes connections among suppliers, vaccine manufacturers, warehouses, and distributors with government authorities and integrates hospitals, vaccine centres, and patients.

A. Entities and Components

We describe the role of each stakeholder and component involved in each layer of our proposed system.

- *Passive Members.* Passive members mainly include patients, hospitals, and clinics. These members only have the right to access the blockchain ledger in the global chain by sending a query or access request.
- *Active Members.* The active members include the supplier, vaccine manufacturer, warehouse, distributor, and government health authorities. These members communicate with each other through their local blockchains and also have the right to access and update the blockchain ledger in the global chain.
- *Decentralised Ledger.* We use distributed and decentralised blockchain networks that are private to active members. Another blockchain network connects all nodes in the global chain layer. Only authorised and verified supply chain entities in the network can store the vaccine data in the main ledger and create immutable links in the form of blockchain transactions, which are time-stamped and secured using lightweight cryptographic technology. An entity's local blockchain network is where it stores its private and sensitive data. Users no longer need to keep all their data on the global chain, providing an advantage. Consequently, the combination of local and global chains is beneficial, as nodes in the network only retain indexed data, making it easier to locate where the data are stored.
- *Smart contracts.* Our proposed framework consists of five smart contracts, namely, the classification contract (CC), consortium contract (CTC), validation contract (VLC), the access contract (ACC) and the revoke contract (REC), each of which implements the access control policies for a pair of entities in the vaccine supply chain.

B. Multi-layer Architecture

To facilitate smooth and effective distribution of goods across the chain, Multi-MedChain adopts a multi-layer and multi-blockchain model. It allows the combination of different local blockchain platforms, where they keep their IP private and facilitate atomic data sharing. It is a permissioned blockchain-based solution, mainly consisting of three layers. Each layer is introduced in a bottom-up approach as follows.

- *User Layer.* The bottom layer consists of passive members who neither take part nor have the right to modify or alter the global chain. However, these members can query the blockchain for specific vaccine information and submit reports. For example, the patient can query the vaccine manufacturing date or other related data on vaccination and report the side effects after vaccination. In the user layer, passive members mainly include government hospitals, clinics, and vaccine centres that generate patients' EMRs and store them in their local blockchain (BC) network. They also establish cross-chain communication with the local BC owned by the government health authority (GHA). Multi-

MedChain establishes secure multi-party communication across the layers through multi-party computation (MPC) nodes [28]. The GHA issues a digital COVID-19 vaccine certificate to patients in the user layer, which can later be provided as proof to the respective authorities. Passive members in the user layer can also send queries or access requests to the main global chain through the smart contract.

- *Local Chain Layer.* The middle layer in our proposed system forms a consortium among the active members, which includes mainly raw material suppliers, vaccine manufacturers with warehouses, distributors, and GHA. This layer comprises the local BCs of each member, securely communicating with each other through local MPC nodes. These members keep their sensitive IP on their respective local BCs and share only the data related to vaccine order placement and shipment tracking with each other. These members maintain their access control lists (ACLs) based on mutual agreements. In our proposed scheme, GHA controls the registration and verification process of all entities and is responsible for setting up the ACL for passive members in the user layer. Due to multiple entities in this layer, each commodity transfer between them is coupled with a transaction on either local BC or global BC. Each entity can only write a specific type of transaction to the local BC depending on the sensitivity of the data and their role in the proposed system. When entities need to share their data with other entities' local BC or global BC, transactions and data are multi-signed. For example, when a raw material supplier sends the material to the vaccine manufacturer, it internalises the transaction containing basic information such as the batch number and the certificate of authenticity (CoA) in its local BC. Simultaneously, it shares this with the local BC of the vaccine manufacturer and global chain using multi-signature. The same process is repeated when other entities communicate or receive the shipment of the product (vaccine or raw material).
- *Global Chain Layer.* The topmost layer in our proposed scheme facilitates the sharing protocol among the user and the local layer. Members in the local chain layer can read and write transactions and share the corresponding block header with the global chain layer, which can later be used for verification purposes. These block headers are managed by the global nodes. When an access request or query is raised to a member in the local chain layer to know about product tracing or tracking, it is referred to the global chain. Afterward, the request is verified and a timestamp is generated by the global BC concerning the owner of the block header. Finally, the requested data are shared with the requester.

The cross-chain communication from source local BC to destination local BC among the local chain layer; and across the user layer and local chain layer happens through a Polkadot bridge. The bridge is a smart contract in a destination blockchain that contains verified block headers from a source blockchain. While the external workers/agents relay block headers from source to destination, track events act accordingly, and have access to the source and destination blockchains. An off-chain database has been used to provide adequate large data storage.

C. Transaction Management

The proposed model consists mainly of three types of transactions: *access*, *send*, and *query*. It facilitates physical trade among supply chain entities. Each entity in our scheme can write specific types of transaction to the user, local, and global chain layer, depending on its role, as shown in Figs. 4 and 5. Passive members in the user layer are only allowed to write *query* and *access* transactions. These transactions are either single-signed (*unisig*) or multi-signed (*multisig*) depending on the communication among entities in the Vaccine Chain.

All transactions involved in the manufacturing, distribution, transfer, and tracking of a vaccine are chained together, i.e. every product gets stored on the main global vaccine chain, also called the Multi-MedChain.

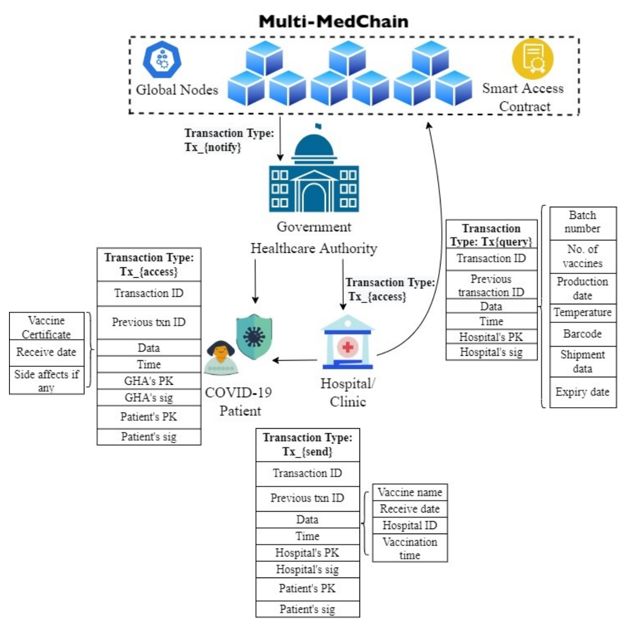


Fig. 4. Transactional asset flow in user chain layer.

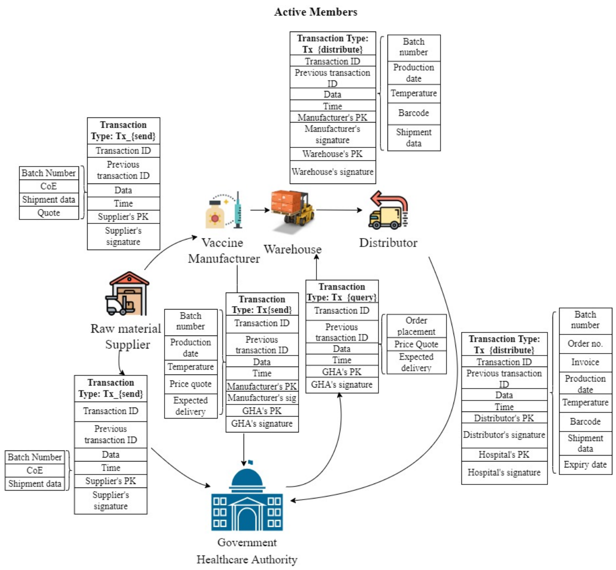


Fig. 5. Transactional asset flow in local chain layer.

D. Smart Contract-based Access Control

In our proposed scheme, access control is implemented through smart contracts [29]. The identity of the members is verified and their access rights are defined using ACL [30]. It ensures that only authorised parties can communicate and perform access control on the incoming query or access request, as depicted in Fig. 6. Our proposed framework consists primarily of five smart contracts, namely, classification contract (CC), consortium contract (CTC), validation contract (VLC), access contract (ACC), and revoke contract (REC), providing fine-grained access control. CC maintains a list to store and classify the entries for each entity in the vaccine chain system. CTC keeps a record of the agreements between stakeholders, providing and sharing access as per the consortium agreement. VLC in global BC checks the validity of the query requester and block header owner, whereas it checks the validity of the data sender and receiver in the local BC. In both layers, ACC and REC grant and revoke access to the data requester, respectively. These ACLs can be modified, and new conditions or agreement policies can be added at any point through the consortium among the involved entities.

To implement the register functionality, the classification steps are designed and implemented as shown in Algorithm 1. The *delivery()* function is used to store on-chain shipping information for deliveries, as shown in Algorithm 2. The from address and to address are recorded at the creation of the delivery. Then, the product information including product quantity and type is added at the preparing state of the delivery. The shipping time and receiving time are recorded when the delivery is shipped or received, respectively. Unlike most applications that require manual completion of each delivery, our system aims to automatically update the status of the delivery after the inventory change.

Algorithm 1 accountRegister & Deployment ABI

Input: *credential details for registeration*
Output: *contract address, confirmation status of the registered method.*
Required: *name, unique email ID, identity of user, password, abi.*

1) Select(*entity*←*users*) **then**
2) *Info*← *entity*[*unique email ID*]
3) **If** (info == True) **then**
   Registration failed (Account already exists)
   Confirmation← **false**
4) **Else**
   Check identity **then**
   Compile corresponding contract **then**
   Deploy contract
   Entity←*[name], [unique email ID], [identity], [password], [contract address]*
   Create (users← entity)
   Info ← contract address
   Confirmation ← **true**
5) **End**

Algorithm 2 Delivery contract deployment

Input: *address of both receiver and sender, product info*
Output: *contract address, confirmation status.*
Required: *address_from, address_to, product_id, product_quantity, producer_address, time.*

1) Compile corresponding contract **then**
2) *Deploy contract*← *address_from*, *address_to*
3) *Info*← *address_delivery*
4) *addProduct*← *product_id*, *product_quantity*, *producer_address*
5) *shipping*← *time*
6) *Entity*← [*name*, *address_delivery*, *address_from*, *address_to*, *time*]
7) *Create* (Delivery← Entity)
8) *Confirmation* ← **true**
9) **End**

To trace the product back to the source, the whole supply chain should be searched for possible records as outlined in Algorithm 3. To simplify this process, all deliveries are stored under particular batches of product, ensuring that each batch contains all the deliveries it has experienced and is traceable throughout the supply chain.

As a result of tracking, the patient will have access to all delivery information from the manufacturer to the hospital, including departure and receiving time. All records are compared with the data on-chain to provide tamper-proof confirmation when they are recorded, ensuring that the records are trustworthy and reliable.

Algorithm 3 Trace delivery record for patients

Input: *product info*
Output: *delivery records*
Required: *product name, product production date, product batch number*

1) Select(*entity*←*items*) **then**
2) *Info*← *entity*[*product name, product date, product batch number*]
3) **If** (info == False) **then**
   Tracking failed (Could not find item)
   Confirmation← **false**
4) **Else**
5) *Delivery detail* ← Info **then**
   Select (Entity ← Delivery) **then**
6) *Entity* ← [deliveryIds]
   Result ← Entity
   Confirmation ← **true**
7) **End**

Members			Consortium Agreements	Access Control List	Query Management (Local Chain)	Query Management (Global Chain)
	Active	Raw material Supplier	Modify	Read	✓	✓
			Add	Write		
		Vaccine Manufacturer	Modify	Read	✓	✓
			Add	Write		
		Distributor	Modify	Read	✓	✓
			Add	Write		
		Government Health Authority	Modify	Read	✓	✓
			Add	Write		
	Passive	Hospitals	×	Read	✓ (only to GHA)	✓
		COVID-19 Patient	×	Read	×	✓

Fig. 6. Access control list management.

IV. Implementation & Results

A. Implementation

The implementation is done using the web3 Python library that facilitates interaction with the Ethereum blockchain, allowing us to build decentralised application (DApp) by providing a simple interface to interact with smart contracts and access blockchain data.

1) Ethereum and Ganache: Ethereum, a decentralised and open source blockchain platform, empowers the creation and execution of smart contracts and decentralised applications (DApps). Our implementation of smart contracts focuses on storing supply chain data on-chain, thereby enabling the functionalities of inventory management and delivery tracking. Ganache, a personal blockchain emulator, establishes a local environment, allowing for the simulation of Ethereum network behaviour on individual machines. The rationale behind our utilisation of Ganache lies in its capacity to provide a convenient and efficient means for testing and debugging interactions between the back-end and smart contracts within a controlled local environment.

2) React and Database: We use React for front-end development due to its efficiency, flexibility, and developer-friendly features. Additionally, we have employed an SQLite database, where all shipment data has been recorded off-chain. For the overall view of the system architecture, both the off-chain database and the blockchain would interact with the server. During the data storage and verification process, a comparison between the off-chain and on-chain contents is conducted to ensure that the data are tamper-free.

B. Results

In the proposed approach, the government assumes ownership of the global vaccine supply chain. To facilitate the registration of relevant stakeholders, the GHA has implemented a smart contract called the VLC. Upon successful registration, VLC updates the list of entities and categorises them accordingly. The entities subsequently execute access control contracts in accordance with the mutual agreement defined in the CTC, allowing the establishment of permissions for data access and information dissemination regarding various supply chain processes. Once the registration and access permissions have been established, the government can place vaccine orders. The GHA can specify the required quantity and delivery date, and the transaction is signed by a GHA signature. Based on this order request, the vaccine manufacturer dispatches the vaccine to the warehouse, with a corresponding transaction being uploaded to the global chain and signed by the manufacturer. Access to this information is contingent upon established access policies. The warehouse then sends the vaccines to the distributor, with the transaction being uploaded to the global chain and signed by the warehouse. The distributor allocates the vaccines to various hospitals and clinics, following the guidance provided by the GHA. To track vaccine distribution, the distributor creates a transaction that includes information about the vaccine and its recipient hospitals/clinics. Upon receipt of the vaccines, hospitals administer them to the general public and subsequently generate vaccine certificates. The hospital uploads the information about the citizen, the corresponding vaccine data, and its registration ID, in a signed transaction, and sends it to the local chain of GHA. Finally, the GHA verifies the data, approves the vaccine certificate with its digital signature, and issues the certificate to the citizens.

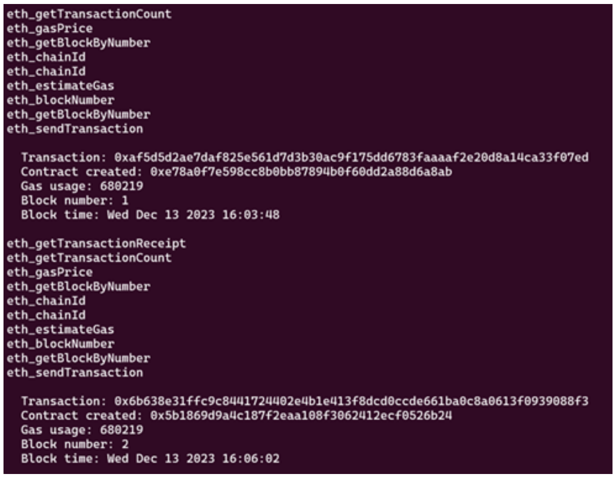


Fig. 7. Transaction details and gas usage.

TABLE II
GAS DEPLOYMENT COST.

Functions	Manufacturer	Wholesaler/Hospital	Distributor
Deployment	680219	680219	1029634
Inbound inventory	95956	73411	N/A
Send Delivery/Outbound	1160363	1153747	N/A
Add Product	N/A	N/A	50636
Set Shipment	N/A	N/A	51413
Receive	N/A	N/A	51347

Ethereum blockchain platform denotes the amount of work done in the form of a unit called gas. Since we have used the test Ethereum network, these gas values are only test values. In our case study, as depicted in Fig. 7, the gas required to deploy various functions such as *deployment()*, *inbound inventory()*, *send delivery()*, *add product()*, *set shipment()* and *receive()* in regards to manufacturer, wholesaler/hospital and distributor is given in Table II.

1) Latency Analysis: Latency heavily depends on the blockchain interaction. For normal requests or functionalities accomplishment, latency generally remains below 20 ms (e.g., Login/Logout function, manufacturer new item/check item function, and tracking functions). Despite the low latency of these simple functionalities, differences arise depending on the number of queries to the local off-chain database. For example, hospital/wholesaler tracking performs only one query to the database, while Login/Logout requests perform two queries per call. Specifically, for patient tracking, the function requires four queries, resulting in roughly four times the latency of a one-time query. However, functionalities that involve interaction with the smart contract experience a dramatic increase in processing time. The smart contract interaction includes the deployment and other function calls inside or cross-contract. The deployment time incurs the most significant cost, leading to considerable latency for the Register function, as shown in Fig. 8(a). Additionally, the inbound functions for manufacturers (Fig. 8(b)) and the outbound functions for hospitals or wholesalers (Fig. 8(c)) are not as large due to a single function call inside the contract. However, latency is high for manufacturer outbound inventory functions and hospital or wholesaler inbound functions due to cross-contract function calls. As connecting to the blockchain server results in large latency, we optimised tracking to minimise interaction with the blockchain, thus significantly reducing the latency of tracking functionalities. Furthermore, we simplified the interaction with the blockchain to reduce both gas fees and runtime latency. Only data including shipment status, shipment quantity, and inventory details are recorded on-chain to optimise system performance.

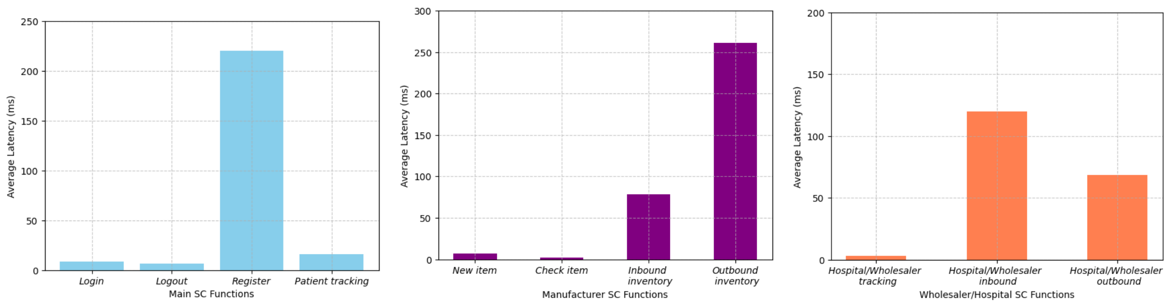
TABLE III
PERFORMANCE COMPARISON BETWEEN OUR PROPOSED SOLUTION AND RELATED WORK.

	[17]	[18]	[19]	[20]	Proposed system
Decentralised	Yes	Yes	No	Yes	Yes
Blockchain	Fabric	Fabric	Ethereum	Ethereum	Ethereum
Off-chain storage	No	Yes	No	Yes	Yes
Latency	Medium	High	High	High	Low
Scalability	Low	Low	Medium	Medium	Higher

The performance comparison of the proposed work with the related works [28]-[31] is summarized in Table III. Our system is more scalable than [17] and [18], storing most of the data off-chain, while simultaneously meeting security requirements. By opting for off-chain storage for the majority of data, our system achieves low latency for a wide range of operations. Compared to the system by [20], our system incurs lower gas fees by reducing on-chain data storage and optimising the data structure of smart contracts. To optimise the data structure, mapping is generally used across all smart contracts to avoid potential loops in querying the data. Our system offers more functionalities, including tracking each stage of the supply chain, and inventory control irrespective of [19]. Furthermore, we ensure that the gas fees of our system remain acceptable, aligning with or even surpassing the cost-effectiveness of the system proposed by [19] for certain functionalities.

2) Features of Proposed System: The proposed project, in which the government takes ownership of the global vaccine supply chain and uses smart contracts for various processes, has several results and business implications.

- *Efficiency in Supply Chain Management:* By assuming ownership and control of the vaccine supply chain, the government can potentially streamline and optimise the distribution process. The use of smart contracts automates and accelerates various aspects of SCM, including registration, allocation, and tracking.



(a) (b) (c)

Fig. 8. Latency during the execution of (a) main SC functions, (b) manufacturer SC functions, and (c) wholesaler/hospital SC functions.

- *Transparency and Accountability:* The utilisation of blockchain technology and smart contracts ensures transparency at various stages of the supply chain. All transactions and interactions are recorded on an immutable ledger, providing a clear audit trail and enhancing accountability among stakeholders.
- *Enhanced Data Security:* Blockchain's decentralised nature and cryptographic security protect sensitive data related to vaccine orders, shipments, and recipients, making the information tamper-resistant and protected from unauthorised access.
- *Improved Access Control:* Smart contracts enable precise control over who can access specific data and at what stages of the supply chain. Access permissions are established based on mutual agreements, enhancing data privacy and reducing the risk of data breaches.
- *Faster Order Placement and Fulfillment:* With streamlined processes facilitated by smart contracts, the government can place vaccine orders more efficiently. Manufacturers can respond quickly to orders and the entire fulfilment process can be accelerated.
- *Efficient Allocation:* The distributor's ability to allocate vaccines based on the guidance of the Global Health Authority (GHA) ensures that vaccines are distributed according to predefined priorities. This helps ensure that high-priority recipients receive vaccines promptly.
- *Accurate Tracking and Reporting:* The use of transactions recorded on the blockchain allows accurate tracking of vaccine distribution. These data are used to generate reports and insights on the movement of vaccines, which can aid in decision-making and resource allocation.

In summary, the project leads to an efficient, transparent, and accountable vaccine supply chain management system. It has the potential to positively impact public health efforts by ensuring timely and equitable distribution of vaccines while maintaining data security and privacy.

V. Discussion and Conclusion

Multi-MedChain facilitates the integration of multiple blockchain platforms within a three-layer multi-party, multi-blockchain framework. It establishes a scalable and distributed SCM system for healthcare, addressing crucial gaps in existing solutions such as end-to-end traceability and collaborative access control to restrict access to private data, which are essential for regulatory and compliance reporting. Stakeholders can securely store sensitive data on their private or local blockchains, meeting practical requirements in a typical medical supply chain. Multi-MedChain promotes transparency among stakeholders and facilitates secure communication to ensure trust. We leverage smart contracts to devise an access control mechanism that supports custom-designed access authorizations. This results in verifiable automation and reduced information asymmetries within the supply chain. The source code for Multi-MedChain is made publicly available and we believe our proposed solution can lead to a more robust healthcare supply chain system by minimizing redundancies and combating counterfeit medical supplies during pandemics.

Our performance results demonstrate the scalability of the proposed solution. However, incorporating blockchain and decentralised access control still encounters some performance challenges compared to traditional centralised supply chain systems. To minimize latency in processing and retrieving supply chain data, the integration of technologies like edge computing and the Internet of Things may prove beneficial. We plan to extend Multi-MedChain and integrate such technologies into our architecture to further improve the practicality of the proposed solution for real-world adoption.

VI. Source Code & Implementation

GitHub link to the project source code is omitted due to the double-blind policy requirements of ICBC 2024.

REFERENCES

[1] C.-Y. Park, K. Kim, and S. Roth, *Global shortage of personal protective equipment amid COVID-19: supply chains, bottlenecks, and policy implications*. Asian Development Bank, 2020, no. 130.

[2] R. L. Bray and H. Mendelson, "Information transmission and the bullwhip effect: An empirical investigation," *Management Science*, vol. 58, no. 5, pp. 860–875, 2012.

[3] M. Nakasumi, "Information sharing for supply chain management based on block chain technology," in *2017 IEEE 19th conference on business informatics (CBI)*, vol. 1. IEEE, 2017, pp. 140–149.

[4] P. Dutta, T.-M. Choi, S. Somani, and R. Butala, "Blockchain technology in supply chain operations: Applications, challenges and research opportunities," *Transportation research part e: Logistics and transportation review*, vol. 142, p. 102067, 2020.

[5] Y. Yue and X. Fu, "Research on medical equipment supply chain management method based on blockchain technology," in *2020 International Conference on Service Science (ICSS)*. IEEE, 2020, pp. 143–148.

[6] L. Pawczuk, R. Massey, and D. Schatsky, "Breaking blockchain open deloitte's 2018 global blockchain survey. deloitte," 2018.

[7] M. Pournader, Y. Shi, S. Seuring, and S. L. Koh, "Blockchain applications in supply chains, transport and logistics: a systematic review of the literature," *International Journal of Production Research*, vol. 58, no. 7, pp. 2063–2081, 2020.

[8] N. Kshetri, "1 blockchain's roles in meeting key supply chain management objectives," *International Journal of Information Management*, vol. 39, pp. 80–89, 2018.

[9] "Modum: A seamless and trusted block data exchange," https://www.modum.io/, [Online].

[10] "Chronicled," https://www.chronicled.com/, [Online].

[11] "Blockpharma," https://www.blockpharma.com/, [Online].

[12] "Blockpharma," https://tierion.com/, [Online].

[13] M. Reda, D. B. Kanga, T. Fatima, and M. Azouazi, "Blockchain in health supply chain management: State of art challenges and opportunities," *Procedia Computer Science*, vol. 175, pp. 706–709, 2020.

[14] F. Jamil, L. Hang, K. Kim, and D. Kim, "A novel medical blockchain model for drug supply chain integrity management in a smart hospital," *Electronics*, vol. 8, no. 5, p. 505, 2019.

[15] B. Yong, J. Shen, X. Liu, F. Li, H. Chen, and Q. Zhou, "An intelligent blockchain-based system for safe vaccine supply and supervision," *International Journal of Information Management*, vol. 52, p. 102024, 2020.

[16] S. T. Alam, S. Ahmed, S. M. Ali, S. Sarker, G. Kabir *et al.*, "Challenges to covid-19 vaccine supply chain: Implications for sustainable development goals," *International Journal of Production Economics*, vol. 239, p. 108193, 2021.

[17] J. Li, D. Han, Z. Wu, J. Wang, K.-C. Li, and A. Castiglione, "A novel system for medical equipment supply chain traceability based on alliance chain and attribute and role access control," *Future Generation Computer Systems*, vol. 142, pp. 195–211, 2023.

[18] S. Peng, X. Hu, J. Zhang, X. Xie, C. Long, Z. Tian, and H. Jiang, "An efficient double-layer blockchain method for vaccine production supervision," *IEEE transactions on nanobioscience*, vol. 19, no. 3, pp. 579–587, 2020.

[19] A. Musamih, K. Salah, R. Jayaraman, J. Arshad, M. Debe, Y. Al-Hammadi, and S. Ellahham, "A blockchain-based approach for drug traceability in healthcare supply chain," *IEEE access*, vol. 9, pp. 9728–9743, 2021.

[20] P. Sharma, S. Namasudra, N. Chilamkurti, B.-G. Kim, and R. Gonzalez Crespo, "Blockchain-based privacy preservation for iot-enabled healthcare system," *ACM Transactions on Sensor Networks*, vol. 19, no. 3, pp. 1–17, 2023.

[21] Y. Yang, J. Lin, G. Liu, and L. Zhou, "The behavioural causes of bullwhip effect in supply chains: A systematic literature review," *International Journal of Production Economics*, vol. 236, p. 108120, 2021.

[22] M. Xu, X. Chen, and G. Kou, "A systematic review of blockchain," *Financial Innovation*, vol. 5, no. 1, pp. 1–14, 2019.

[23] A. A. Monrat, O. Schelén, and K. Andersson, "A survey of blockchain from the perspectives of applications, challenges, and opportunities," *IEEE Access*, vol. 7, pp. 117 134–117 151, 2019.

[24] Y. Gong, Y. Jiang, and F. Jia, "Multiple multi-tier sustainable supply chain management: a social system theory perspective," *International Journal of Production Research*, pp. 1–18, 2021.

[25] Z. A. Collier and J. Sarkis, "The zero trust supply chain: Managing supply chain risk in the absence of trust," *International Journal of Production Research*, pp. 1–16, 2021.

[26] S. Xu and K. H. Tan, "Data-driven inventory management in the healthcare supply chain," in *Supply Chain and Logistics Management: Concepts, Methodologies, Tools, and Applications*. IGI Global, 2020, pp. 1390–1403.

[27] K. A. Clauson, E. A. Breeden, C. Davidson, and T. K. Mackey, "Leveraging blockchain technology to enhance supply chain management in healthcare:: An exploration of challenges and opportunities in the health supply chain," *Blockchain in healthcare today*, 2018.

[28] O. Goldreich, "Secure multi-party computation," *Manuscript. Preliminary version*, vol. 78, no. 110, 1998.

[29] "Introduction to smart contracts," https://docs.soliditylang.org/en/v0.8.6/introduction-to-smart-contracts.html, [Online].

[30] A. Saini, Q. Zhu, N. Singh, Y. Xiang, L. Gao, and Y. Zhang, "A smart-contract-based access control framework for cloud smart healthcare system," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5914–5925, 2021.