A Cyber Secure Medical Management System by Using Blockchain

Muhammad Rehman, Ibrahim Tariq Javed, Kashif Naseer Qureshi, Tiziana Margaria, *Member, IEEE*, and Gwanggil Jeon, *Senior Member, IEEE*

***Abstract*— In the pharmaceutical industry, problems like counterfeit drugs, including vaccines, and their supply chain management problems like transparency, immutability, and traceability exist. In the case of vaccines, it becomes more difficult to standardize and detect fake vaccines because the public has less awareness and knowledge about vaccines. Moreover, the increase in online pharmacies gives more opportunities for counterfeiting vaccines to enter the authentic supply chain management system. We present transparent, immutable and secure vaccine supply chain (TISVSchain), a framework based on blockchain to handle the issues of counterfeited vaccines and vaccine supply chain problems like transparency, immutability, and traceability. Our proposed framework can run both on the private and public blockchain. We have implemented the framework on public blockchain by using remix ide and the smart contracts designed by solidity language run on very low gas cost. We also carried out several experiments by changing the number of nodes and their block time to evaluate the performance of our framework in terms of transaction per second (TPS), gas cost, and propagation delay. Our proposed framework improves the security by using offline unique account addresses in blockchain-based frameworks and improves the overall efficiency of the framework by keeping the gas cost low, finding a way to decrease the number of lost blocks to keep low propagation delay, and keeping high TPS value. TISVSchain shows us promising results to improve vaccine supply chain management's overall performance, security, and efficiency.**

***Index Terms*— Blockchain, data management, secure data, supply chain, vaccine.**

I. Introduction

VACCINE supply chain management faces significant obstacles in terms of transparency, vaccine record fraud like expiration dates, counterfeit vaccines, and overall security problems of vaccine supply chain management. These obstacles have a deep impact on overall human health and life as the vaccine is a biomedical product and a fake vaccine can have a fatal impact on human health. The other problem like the transparency of data and record tempering lowers the efficiency of vaccine supply chain management. Considering the traditional vaccine supply chain, the government's supervision departments have monitored the entire vaccine journey. However, this method does not guarantee effectiveness in addressing, for example, the vaccine expiration problem as someone can temper with vaccine information [1]. In the Covid-19 pandemic, pharmaceutical companies have concentrated their efforts from day one to develop a vaccine [2]. For a successful and safe vaccine supply chain, an effective logistics system of the end-to-end supply chain is required [3], [4]. Worldwide, a lot of poor-quality drugs make their way to the market, with dire consequences: according to the World Health Organization (WHO), thousands of deaths occurred in developing countries due to fake drugs [5]. According to an estimate, the annual business loss of U.S. pharmaceutical industries due to counterfeiting is U.S. $200 billion [6]. According to WHO, around 30% of the total medicine sold in Latin America, Africa, and Asia is counterfeit. In Pakistan, around 40%–50% of drugs are fake. Drugs are moved across different complex distributed networks, making it difficult to detect counterfeiting and creating opportunities for fake drugs to enter the authentic supply chain. There are successful initiatives against such practices, like the identification of medicinal products (IDMP) standards in the European Union, but this is not the practice on a global scale. To detect the origin of fake drugs and how they reach the consumer, an immutable and well-maintained supply chain is required [7]. The traditional drug supply chain process is long and diverse, including raw material suppliers, manufacturers, warehouse owners, retailers, pharmacists, and the consumer or the patient, as shown in Fig. 1 [8].

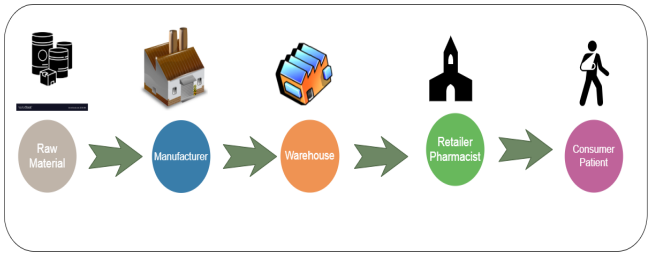

Fig. 1. Traditional drugs supply chain.

In the traditional drug supply chain, manufacturers source the raw materials needed to manufacture a product. A considerable amount of time and investment is required for the research and the proper synthesis of drugs. Once a product is developed, the manufacturer sends it to the warehouse, from where it is shipped to retailers or pharmacists, who receive the product and sell it to the consumers. There are many challenges in the traditional drug supply chain. Some of them

Manuscript received 3 April 2022; revised 20 July 2022; accepted 18 September 2022. Date of publication 24 November 2022; date of current version 2 August 2023. *(Corresponding author: Gwanggil Jeon.)*

Muhammad Rehman is with the Technology Risk Department, Ey ford Rhodes, Islamabad 44000, Pakistan (e-mail: muhammd.rehman@pk.ey.com).

Ibrahim Tariq Javed is with the Blockchain Department, The University of British Columbia, Vancouver, BC V6T 1Z4, Canada (e-mail: ijaved02@mail.ubc.ca).

Kashif Naseer Qureshi is with the Department of Electronic and Computer Engineering, University of Limerick, Limerick V94 T9PX, Ireland (e-mail: KashifNaseer.Qureshi@ul.ie).

Tiziana Margaria is with the Health Research Institute (HRI), University of Limerick, V94 T9PX Limerick, Ireland (e-mail: tiziana.margaria@ul.ie).

Gwanggil Jeon is with the Department of Embedded Systems Engineering, Incheon National University, Incheon 22012, South Korea (e-mail: gjeon@inu.ac.kr).

Digital Object Identifier 10.1109/TCSS.2022.3215455

are listed below [9], [10]. Fig. 1 shows the traditional supply chain management process, in which raw material is given to the manufacturer and the manufacturer produces the required material and sends it to the warehouse, from where the retailer and pharmacist purchase and provide it to the consumer. It is the traditional way which includes a lack of transparency, traceability, and immutability.

Lack of Transparency: Millions of dollars have been invested to create transparent drug supply chain management, but little success has been achieved so far. Lack of visibility of the vaccine supply chain is the main issue in the pharmaceutical industry.

Lack of Traceability: Predictive monitoring and traceability of products are very challenging because, in traditional drug supply chain management systems, stakeholders maintain their database. Maintaining a manual record of every product delays the process and requires more time. This problem can be fixed by using smart contracts and adopting a blockchain-based framework for drug supply chain management.

Trust Issue: As shown in Fig. 1, supply chain management is a complex process that involves many participants until the product is received by a consumer. Consistently maintaining trust across all these stakeholders is one of the major challenges in drug supply chain management, and it can also affect the smoothness of the whole process.

Cold-Chain Shipping: Temperature-controlled drugs like vaccines or blood require extra care and equipment to guarantee proper refrigeration transport. Not all supply chain entities provide cold facilities, and the pharmacy industry is currently facing the production and distribution of vaccines which need a proper cold chain system to be managed.

Fake Drugs: A lot of fake drugs make their way into the market because of lacking transparency and outdated information-sharing mechanisms in the pharma products supply chain system. Counterfeited products are delivered to the consumers, affecting thousands of lives and the economy.

Single Point of Failure: The current system of drug supply chain management uses centralized cloud-based systems to store the data. If somehow this centralized server is compromised, the whole system can collapse. Another problem with this system is that users have less control over their data because the cloud provider for data storage is a third party to the supply chain management.

Unreliable Reputation Systems: Feedback and user comments are crucial to determine the effectiveness of drug quality management. By centralizing systems, third parties manage the storing of data which introduces a risk of tampering with the user feedback or comments, e.g., hiding the bad comments. Hence, an immutable and transparent reputation system is required, which can be achieved by using blockchain.

Contracts and Documentation: Traditional drug supply chain management involves paperwork for different transactions, a change of ownership, and a letter of credit, which makes it complicated and outdated. These problems can be resolved by a smart contract system that does all these transactions automatically and records them in an immutable way.

Blockchain networks can be used to cover all the phases of the supply chain. To keep the record of specific products, every transaction is stored in immutable and time-stamped blocks which link together to form a chain of blocks [11], and the blockchain system inherently assures that the details present in the chain are not tampered with [12] and [13]. To verify the authenticity and manufacturing and distribution history of any drug, all the entities of the network can log in to the network [8].

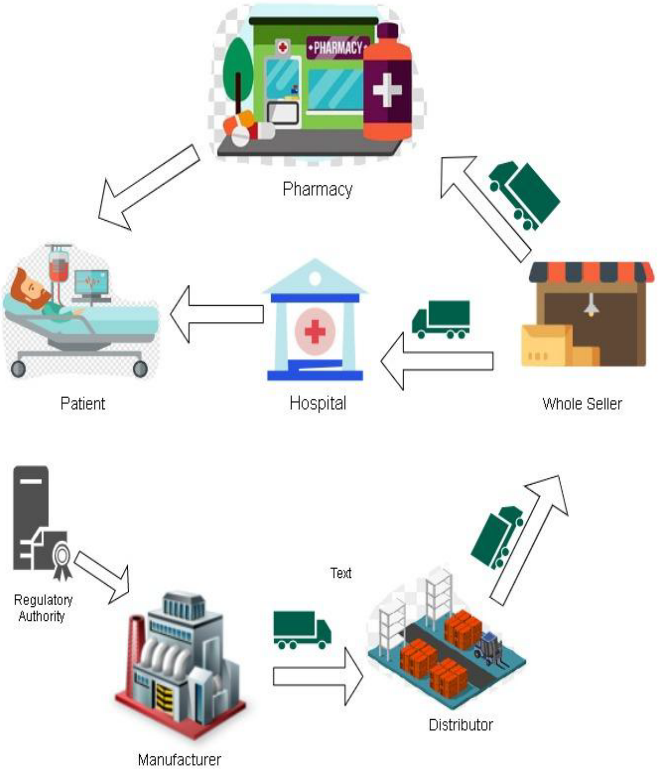

Fig. 2. General flow of vaccine supply chain management.

Vaccine supply chain management is different from other drugs' supply chain management because vaccines are biological products that need extra care to maintain a prescribed cold chain throughout all the phases and stakeholders. A vaccine cold chain is a global network of cold boxes, refrigerators, cold rooms, and freezers. The general diagram of vaccine supply chain management is shown in Fig. 2. Once a manufacturer gets vaccine approval from the regulatory authority (RA), they produce a specifically approved vaccine which they deliver to distributors and is then further delivered to the wholesaler. The wholesaler will further deliver it to pharmacies and hospitals, and finally, the vaccine will be delivered to the patient or consumer. In this whole process, the transactions at any node can be compromised. The secure and decentralized nature of blockchain will provide integrity, confidentiality, availability, traceability, and auditability.

Vaccine supply chain management is a centralized system (cloud-based) that is controlled by some specific authority, and the security of such a system can be compromised. Fake vaccine identification is the problem; consumers need to ensure that the vaccine is authentic. Because of a centralized system, there is a chance of feedback and rating tampering. No secure data management is available for Covid-19 vaccine supply chain management. To resolve the issues of data integrity, transparency, and immutability, this article proposed a secure data management framework for vaccine supply

chain management by using blockchain. Our main objectives are as follows:

1) to design a decentralized vaccine supply chain data management system by using blockchain technology;
2) to ensure authenticity, immutability, and traceability of supply chain data;
3) to compute/examine the performance of our framework by different performance metrics.

This article is organized as follows. Section II presents an overview of studies and research articles related to the proposed research work. Section III explains the proposed mechanism in detail, and Section IV presents the results and analysis. Section V concludes this article with a future direction.

II. Related Work

Blockchain technology provides transparency, faster and easy accessibility, efficiency, and security [14]. Detection and prevention of fake drugs in pharmacology are a big problem, especially because the increase of Internet-based pharmacies has made it more difficult to standardize medicine because Internet-based pharmacology involves different complex networks which provide many ways for an intruder to enter an insecure supply chain. To tackle all these problems, Jamil et al. [15] use hyper ledger fabric, which is based on blockchain, to keep a record of all the transactions and smart contracts to give limited-time access to drugs and patient health records.

To handle the drug counterfeiting problem, Sylim et al. [16] proposed a distributed application that will run on smart contracts and use swarm as a distributed file system. Swarm is a self-adapting distributed system. Blockchain will support information sharing along with the official drug distribution network. To track down the entire path of a drug from the manufacturer to the consumer, Erokhin et al. [17] proposed the distributed ledger technology based on blockchain to prevent fake drugs from reaching the market. The Covid-19 vaccine requires special care to maintain its specific, very demanding cold chain process: the Pfizer-made vaccine requires storage at -70 °C freezer temperature and can last up to 30 days after opening the freezer. The modern vaccine requires -20 °C refrigeration and lasts up to 30 days [18].

Jamil et al. [15] proposed a blockchain-based framework to handle the pharmaceutical medicine supply chain system. Specifically, it describes the design, performance, and implementation of hyper ledger fabric blockchain for smart hospitals, based on the proof-of-concept consensus-based mechanism used by hyper ledger fabric blockchain. This proposed framework will allow the staff to manage the healthcare ecosystem along with medical records. By using blockchain and smart contracts, they have to deploy permission-based systems using the solidity language. However, they did not analyze the supply chain management of cold chains.

Using smart contracts eliminates the need for a trusted third party or a middleman. A smart contract is a piece of code that executes when certain conditions are met. But the code of smart contracts is still subject to vulnerabilities that can be exploited to compromise the entire blockchain network. Gupta et al. [19] investigate various artificial intelligence tools and techniques to resolve the privacy problem in smart contracts. This article proposed a mechanism called Zither, which is used to handle the privacy issue of smart contracts. Bünz et al. [20] tested Zether as an Ethereum smart contract to calculate its gas cost. Gas cost is the cost necessary to perform a transaction on the network.

To address the problem of smart contracts in the supply chain system, Dolgui et al. [21] proposed an event-driven dynamic approach. In developing countries, emergency supply chain management which is also referred to as vaccine supply has been studied extensively [22]. To develop a traceability system for agriculture, the food supply chain proposed the combined technology of radio frequency identification and blockchain [23]. The authors in [24] suggested the use of blockchain technology to prevent food wastage by enabling the identification of food items. By exploring the blockchain properties of decentralization and traceability, Andoni et al. [25] proposed controlling the energy supply by using blockchain. To improve the traceability in the agriculture supply chain, Kamble et al. [26] adopt blockchain technology which opens the doors and encourages others to adopt blockchain for the relationship making in the supply chain system.

The services of blockchain are used in supply chain management; it provides decentralization and the immutability of data and records in the network. However, problems like the credibility of involved nodes, traceability of the product and accountability of the whole trading process still need to be addressed. The authors in [27] proposed an interplanetary file storage system (IPFS) that will return the hash of data stored on the blockchain. In addition, this system will provide smart contracts, ensuring the credibility of involving entities or nodes by showing their interaction in the system. Salah et al. [28] proposed block chain's immutable ledger which links to the decentralized file system (IPFS) which will provide transparency and traceability in the supply chain ecosystem.

During the process of the supply chain, drugs are transferred from the manufacturer to the supplier and then to end-users; during this process, counterfeit drugs can be merged at any level of the chain. Some pharmaceutical companies use holographic technologies to countermeasure fake drugs, but this kind of packaging is expensive, and it can also be cloned by counterfeit companies. Decentralized and high-security features of a blockchain could be the solution; however, the current blockchain cannot afford high throughput and the other problem with the public blockchain is the data that are available publicly to anyone, and therefore, if an organization wants to hide data from other organizations, then privacy might be an issue [29].

In the past, many permission-less networks were built on the blockchain which was unable to give privacy and authenticity to the user data. Because in permission-less networks, anybody can interact with the network by creating their address. But in the healthcare ecosystem, permissionless blockchain failed to manage the integrity and privacy of data related to drug management, patient information, and medical records. Additional access control policies were applied to achieve security, but these policies affect the efficiency of these healthcare systems. Many have deployed the permissionless blockchain but their transaction per second (TPS) is so limited.

To maintain data transparency, security, privacy, and reliable communication between communicated parties to make the

distribution and allocation of vaccines equally global-wise and to stop the counterfeited vaccine to enter the market, the author proposed a Blockchain-based Vaccine Distribution Scheme for Pandemics (FAIR) blockchain-based approach. Nair et al. [30] proposed an approach that allows fair distribution and allocation of vaccines as per demand generated from the global population. The author further proposed the algorithm and architecture represented between parties and computed network performance based on blockchain. They have calculated computation and communication costs of 1152 bits and 12.6 ms. Cui et al. [31] proposed an improved, blockchain-based, storage-efficient vaccine safety protection scheme. By using the cryptographic mechanism, cloud, and blockchain, they design a system to protect vaccine circulation. Further, the author evaluates the proposed conceptual model by using a consortium blockchain. Antal et al. [32] proposed a system that guarantees data integrity and immutability of beneficiary registration for vaccination and avoids identity theft. Further, a prototype was implemented using the Ethereum test network. The system shows promising results in terms of gas cost, throughput, and scalability. Kamenivskyy et al. [33] address the problem of miscommunication between different actors during the process of vaccine distribution by using blockchain. The author identifies distribution chain challenges via interviews and literature reviews which allowed him to devise a blockchain framework for vaccine distribution and evaluate its feasibility. The author proposed the framework using data flow diagrams which minimize the counterfeiting of vaccines and improve communication between stakeholders. The limitation of this work is that it was a conceptual broad-based system that does not mention the storing of patients' medical records; further, it was unable to deal with the physical and organizational challenges.

As stated above, these blockchain platforms are either permission-less or computationally expensive having fewer TPSs which makes them expensive to use. Most of the systems presented in the literature reviews are frameworks based on proof of concept and single-platform blockchains like a public or private blockchain; no framework is designed to work on both platforms. In the abovementioned systems, no author evaluates the performance of its framework in terms of TPS, propagation delay, the relation of several sealers, and block time and synchronization issues. All these factors are important to propose a blockchain-based supply chain system. We have considered all these factors and evaluated our framework by these performance metrics. Some of the related work represents the supply chain management of drugs using permission-less or private blockchain networks and some of them deploy it by using hyper ledger fabric which is computationally expensive because they use a proof of work consensus mechanism. To the best knowledge of the author, there has been no functional, vaccine supply chain model based on proof of authority (PoA) Ethereum-based blockchain model.

III. Proposed Scheme Framework

The overall process of vaccine supply chain management faces significant obstacles in terms of transparency, vaccine record fraud like expiration dates, counterfeit vaccines, and overall security problem in vaccine supply chain management.

TABLE I
DIFFERENT NOTATIONS USED IN THE PROPOSED FRAMEWORK

Symbol	Description
RA	Regulatory Authority
UA	Unique Address
PK	Public Key
U	User
VM	Vaccine manufacturer
DIS	Distributor
PM	Pharmacy
CM	Consumer
SC	Smart Contract
PR	Private Key

These obstacles have a deep impact on overall human health and life as the vaccine is a biomedical product and a fake vaccine can have a fatal impact on human health. The other problem like the transparency of data and record tempering lowers the efficiency of vaccine supply chain management. In vaccine supply chain management, challenges like counterfeit vaccines, transparency and record tempering need to be addressed. To resolve these issues, a transparent, immutable and secure vaccine supply chain (TISVSchain) framework based on the blockchain can be used. TISVSchain can be deployed on both private and public blockchains. To deploy this framework on a public blockchain, we have used the remix ide platform based on solidity language and to deploy it on a private blockchain Geth PoA visual studio code we have used. Table I shows the different notations used in the proposed framework.

The proposed working framework shown in Fig. 3 includes actors like RA, manufacturer, distributor, wholesaler, hospital/pharmacy, and the patient or end-user. If a manufacturer wants to produce a vaccine, it must get approval from RA; once approval is given for the specific vaccine, then the manufacturer is licensed to produce only that specific vaccine. If RA approves the manufacturer to produce the vaccine, then RA will assign a unique offline account address in the form of a 160-bit identifier to the manufacturer. This will be additional security only those manufacturers will be allowed to produce vaccines who have approval from the RA and have a unique account address (UA). To get access to the blockchain framework, the manufacturer will put his UA on the blockchain which has been provided by RA. After that, the vaccine manufacturer (VM) will decide which distributor can get the distribution of the vaccine.

When the production is complete and the vaccine is ready for delivery, it must be approved by the RA whether it meets the standard requirement or not. If the vaccine meets the standard, the RA will enter its standard rating from 1 to 5 in the blockchain, and then, it would get dispatched for distribution at every node the transaction information will be stored on the blockchain, and at each node, the agreement would be made by a smart contract. VMs will enter the information of authorized distributors and only those distributors will be able to distribute. A distributor would further dispatch the vaccine to the wholesaler, and the whole seller will dispatch it to pharmacies or hospitals. The blockchain will make sure the integrity and

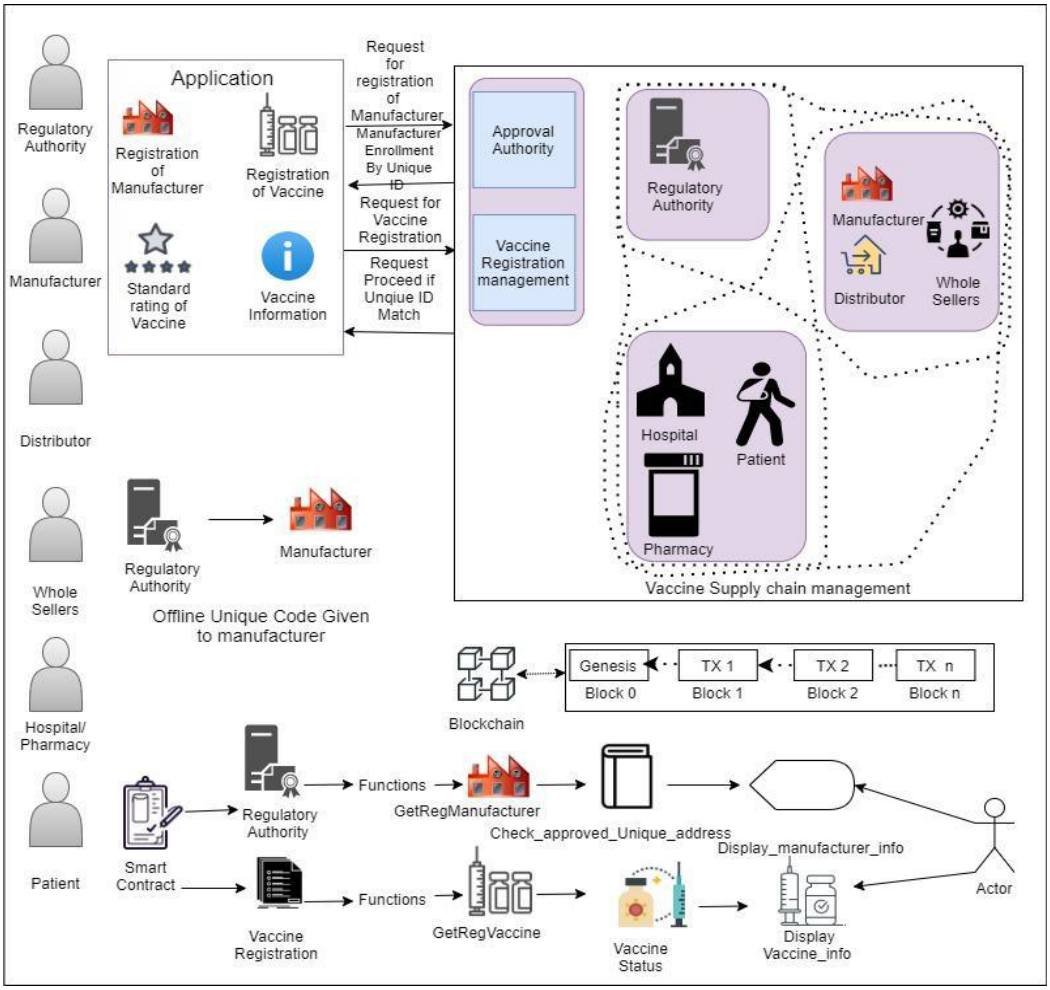

Fig. 3. Proposed working framework.

immutability of vaccine data at every node further; once it is received, the hospital can verify the data of the vaccine by scanning the barcode. Currently, we are using the name of a medicine that can be converted into a barcode. In the last step, the vaccine is received by the patient or consumer. They can also verify the integrity of the vaccine by scanning the barcode at every node the transaction is stored on the blockchain which ensures the immutability and integrity of data.

Fig. 3 shows the proposed framework in which actors like regulatory authorities, manufacturers, distributors, wholesalers, pharmacies/hospitals, and consumers take their part in vaccine supply chain management. The application of blockchain is based on smart contracts which are composed of the registration of the manufacturer and vaccine by giving an offline unique address to the manufacturer. If the unique address of the manufacturer matches, then that specific manufacturer can produce a specific vaccine. Distributors can deliver it to the wholesaler, from where it can be dispatched to hospitals/pharmacies, so consumers can buy and use it. On the left side, all the actors are mentioned in Fig. 3, and on the right side, the actor and their relevant activities are mentioned. The bottom of the diagram contains the flow of the entire process. In every step, all the information is stored on the blockchain which ensures the immutability, transparency, and security of vaccine supply chain management.

The proposed scheme framework is based on two main phases including the TISVSchain on the public blockchain and TISVSchain on the private blockchain.

These phases are the core of the entire model, and the complete concept is explained thoroughly in these phases.

A. Design and Development of TISVSchain on Public Blockchain

A public blockchain is a platform that allows anyone to access and sign in without any permission; it is more like an open-source platform. In a public blockchain, all the nodes of the network are given the authority to validate the blocks and verify the transactions. We have used remix ide based on solidity language to deploy the proposed framework on the public blockchain.

The TISVSchain consists of five major entities as described in the following.

1) *RA*: RA is an entity that is responsible for granting all kinds of approvals of vaccines including provider approval, service approvals, and rating services against the NQS National quality standard (NQS). In the USA, vaccine RA is the Center for Biologics Evaluation and Research (CBER) which is part of the Food and Drug Administration (FDA). In Pakistan, the Drug Regulatory Authority which is called (DRAP) is responsible for

the quality and approval of different vaccines. Also, in TISVSchain, maximum authority is given to the RA which is responsible to grant the manufacturing approval to manufacture the specific vaccine and giving a UA through which UA manufacturers can access the blockchain.

2) *VM*: VM is another important entity of the TISVSchain framework; once VM is approved and authorized by RA, then VM can manufacture vaccines and can give them to wholesalers and distributors only VM is authorized to decide which wholesaler and distributor are allowed to deal in that specific vaccine. For security purposes, VM can access the blockchain only through that UA which is given offline by RA to VM.
3) Blockchain: TISVSchain's most important entity is blockchain on which this framework is implemented as it is a peer-to-peer distributed platform that supports decentralized applications. On a distributed network like Ethereum, it should support smart contract execution and storage. We are using the remix ide tool based on solidity language to implement this framework as a public blockchain.
4) Consumer: The consumer is another important entity of TISVSchain as the vaccine is a biomedical product, and if the low quality or fake vaccine is used by the consumer, it can cause fatal results, so TISVSchain allows the consumer to verify the vaccine quality and its history by just scanning the barcode all the information like manufacturer name, approval authority information, manufacturing, and expiry date all can be available for the consumer.

The system model of TISVSchain is presented in Fig. 4. There are two kinds of messages over TISVSchain: transactions through smart contracts, and normal interaction between different entities like regulatory authorities, VMs, distributors, hospitals, and consumers. To understand the working of TISVSchain, we describe the several steps involved.

1) *Step 1 (Publish Smart Contract)*: The RA publishes its smart contract over a blockchain platform. The smart contract contains information regarding which kind of company is allowed to manufacture vaccines; further, it contains information about vaccine registration and approval procedures.
2) *Step 2 (Data-Store)*: Once the smart contracts are published by the RA, all the information is stored on the blockchain as it is a peer-to-peer network, so its copy is shared with all connected nodes.
3) *Step 3 (Request for Registration)*: The vaccine manufacturing company requests the RA to register the company so they can start producing the vaccine.
4) *Step 4 (Offline UA)*: When a company requests the RA for approval, the RA checks the standard of the company and gives the rating from 1 to 10; if company rates are equal to or greater than five points, the RA gives that company an offline 160-bit unique account number only by that provided UA company can access the smart contracts on the blockchain and put its information on the blockchain network.

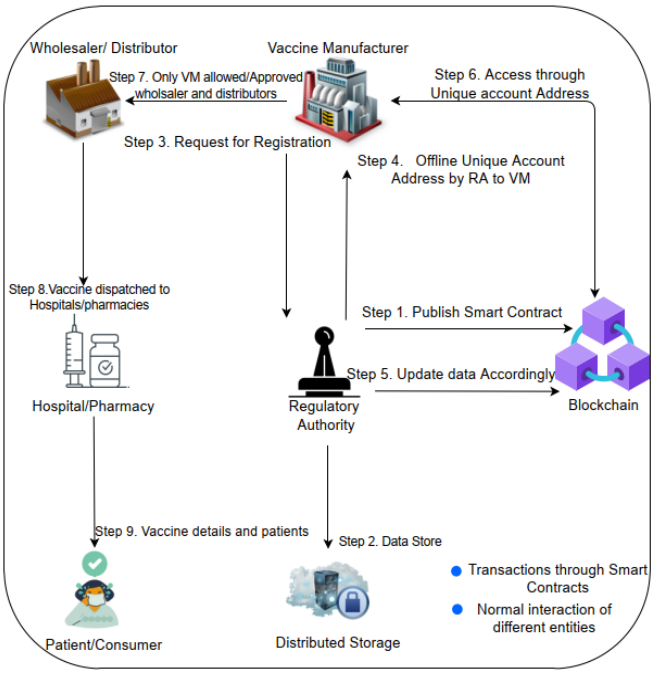

Fig. 4. TISVSchain system model.

5) *Step 5 (Update Data Accordingly)*: The RA updates the data once a UA is assigned to the company, and then, they update the smart contract on the blockchain according to the requirement.
6) *Step 6 (Access Through the Unique Account)*: A company can only access the smart contract by a UA once it is assigned, then a company is considered a registered company by the RA, and it accesses the data on a blockchain.
7) *Step 7 (Authorized Distributors and Wholesalers)*: Registered VMs have the right to decide to give authorization to any distributor or wholesaler to deal in their manufactured vaccine and only those distributors and wholesalers would be allowed to work which are authorized by the vaccine manufacturing company.
8) *Step 8 (Hospitals and Pharmacies)*: Authorized distributors will deliver the vaccine to hospitals and pharmacies from where consumers can buy it.
9) *Step 9 (Vaccine Details and Patients)*: The last and the most important part of this system is the patients. Consumers/patients would be able to get the information about the vaccine in a transparent, immutable, and secure form just by scanning a barcode of the vaccine.

TISVSchain supports a transparent, immutable, and secure framework for the vaccine supply chain. Only a registered company that has been assigned a UA by the RA would be able to work in this framework and that UA is given by the RA offline to keep it more secure. Fig. 5 shows the working of TISVSchain on public blockchain based on remix ide. It shows how a company having a good standard rating and UA register can itself on the platform and further, how can it get approval for a vaccine, and how can a consumer get a piece of transparent and imputable information from the framework by just putting the name of the vaccine. All the information like company name, approval status, distributor name, manufacturing, and expiry date consumer can get by

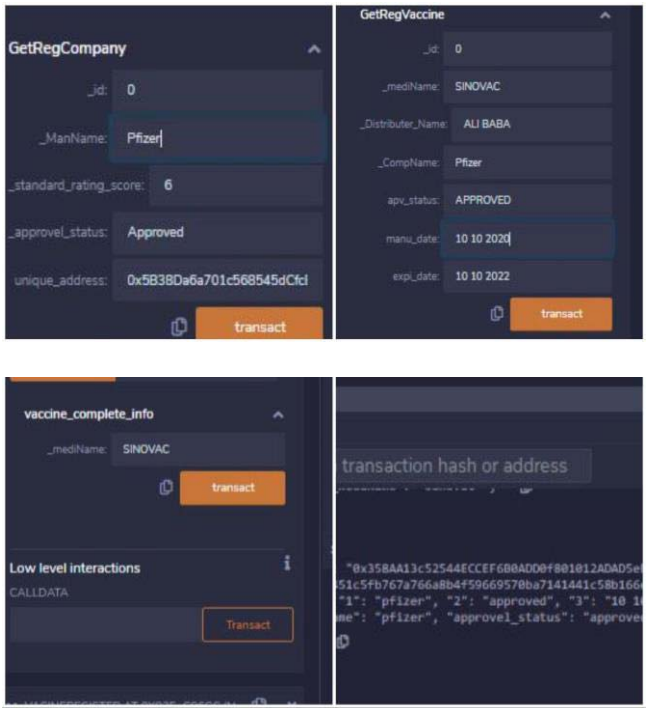

Fig. 5. Working on the proposed framework for a public blockchain.

Algorithm 1 GetRegCompany

Step 1	:	**if** (_standard_rating_score>5) Transaction Hash (0xd249bf3e60ebd312acf41f8de5602efb1215841278d2fcc6e428ab02558366ac)
Step 2	:	Assign a Unique account address (0x5.38Da6a701c568545dCfcB03FcB875f56beddC4)
Step 3	:	**else** String memory temp_standard_remark= "low standard rating improve quality"
Step 4	:	**End**

putting the name which can be converted into a barcode later for the consumer.

These are the algorithms on which the TISVSchain framework is working. Algorithm 1 is related to the registration of a company or manufacturer; in the first step, the algorithm will check the standard requirement if the standard rating is greater than 5, then in step 2, UA will be assigned to the manufacturer and if the standard rating is less than 5, then the algorithm will reject the registration of the company. Algorithm 2 is related to the verification of UA; in this algorithm, the log approved function passes two variable msg. sender a built-in function of solidity library and unique address; the algorithm takes these two inputs and checks if the unique address is true or false.

Algorithm 2 Verify the unique account address

(0x5.38Da6a701c568545dCfcB03FcB875f56beddC4)
(from)
(0xd9145CCE52D386f254917e481eB44e9943F39138)
(to Regulatory authority)

Step 1	:	emit LogApproved(Msg.sender, Unique_address) Transaction Hash 0x273.5cc12a1f54624405ff94c5bb73cb5fe6669197942cde5d1ab8ca2208323e
Step 2	:	**if** Approved_address [unique_address] = true
Step 3	:	**else** **return** false
Step 4	:	**End**

Algorithm 3 Get_Reg_Vaccine

0x5.38Da6a701c568545dCfcB03FcB875f56beddC4 (from)
0xd8b934580fcE35a11B58C6D73aDeE468a2833fa8
(to Vaccine registration smart contract)

Step 1	:	**if** (vaccine quality meet the requirements) (Transaction Hash) 0x1.40b76c6ecdb399dcfb28e80d1ca5866c671fde49a6d24047cedf989b236bf5
Step 2	:	**Then** check Msg.sender address == unique_account_address **return** true
Step 3	:	**else** **return** false
Step 4	:	**End**

Algorithm 3 is related to the registration of vaccines; once the company is registered, then the company or manufacturer must register themself for the specific vaccine they want to manufacture. In this algorithm, the UA of the manufacturer must match the one which was assigned during the company registration; only after the verification of that unique address, the algorithm will allow the registration of the vaccine. Algorithm 4 is related to vaccine detailed information. If the consumer, manufacturer, or RA wants to know the detail about any vaccine, this algorithm is designed to fulfill the requirement and it shows the vaccine detail like manufacturing and expiry date, approval status, vaccine name, and manufacturer information.

Algorithm 4 Vaccine detailed information

0x5.38Da6a701c568545dCfcB03FcB875f56beddC4
(from)
0xf8e81D47203A594245E36C48e151709F0C19fBe8
(to Consumer Smart contract)

Input	:	**Vaccine name**
Output	:	**Vaccine information** Transaction Hash (0xd7289f338801dbb0ebc5c6d1652965788eb646856289cbd8639c3a5bd18f2e77)
Step 1	:	**if** Msg.sender vaccine_name == vaccine name
Step 2	:	show (_mediName,company_name,approvel_status,manu_date, expi_date)
Step 3	:	**Else** **return** false
Step 4	:	**End**

Fig. 6 shows how VMs interact with smart contracts. In step 1, VM, which is acting as an actor, requests RA for the registration of the company; the smart contract of the RA shall check the company standards, and if it meets the criteria, then the request would be granted, and step 1 would be completed. In step 2, the RA would provide an offline UA and only by that assigned UA company would be considered as registered by the RA and would be able to access the blockchain for further process. In step 3, once the company is registered and wants to manufacture a vaccine, in this step by using a UA, the company will request RA by using smart contract 1 to register the vaccine. Smart contract 1 will verify the UA and then will proceed to smart contract 2 which will further verify the standard quality; if the vaccine standard quality is acceptable, smart contract 2 will register the vaccine.

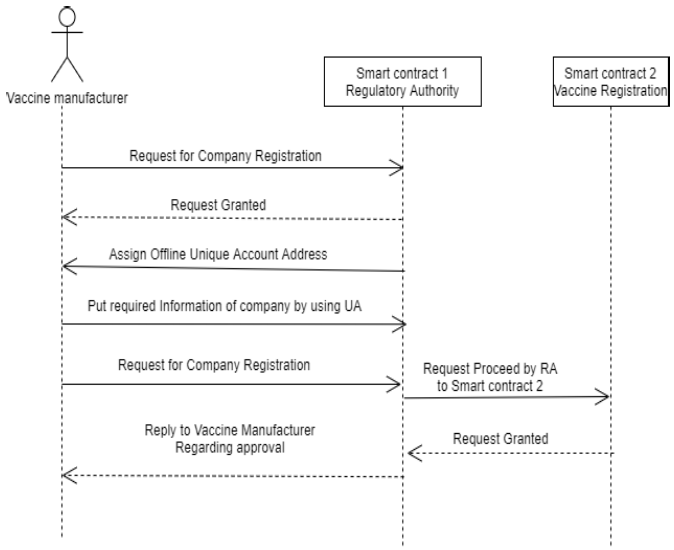

Fig. 6. Sequence diagram of VM interaction with smart contracts.

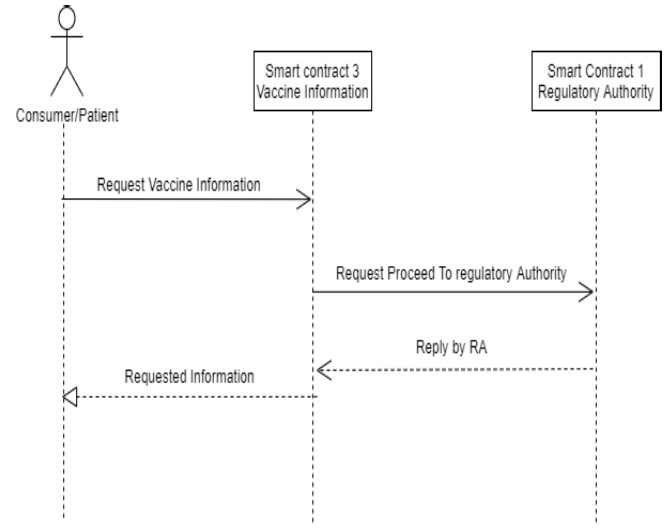

Fig. 7. Sequence diagram of consumer interaction with smart contracts.

Fig. 7 shows the consumer interaction with smart contracts. By scanning the barcode of the vaccine, consumer requests for vaccine information would be forwarded to smart contract 3 which is dedicated to vaccine information; further, smart contract 3 will fetch the information from smart contract 1 and will forward that information to users. This can be done by using smart contract 1 but that would cost a consumer more money. The smart contract 3 is very lightweight and has very less gas cost which costs very less money to the user and provides a transparent, immutable, and secure form of information about the vaccine.

B. Development of TISVSchain on Private Blockchain

A private blockchain consists of a closed network owned by an organization or entity and is limited to only authentic users. When the owner of a private blockchain allows, then, a new user can be added to the network. Access like the creation of new blocks and adding transactions are allowed to only those nodes given control by the owner of the blockchain. The level of security increases due to inaccessibility and authorization increases. We are going to deploy TISVSchain on a private

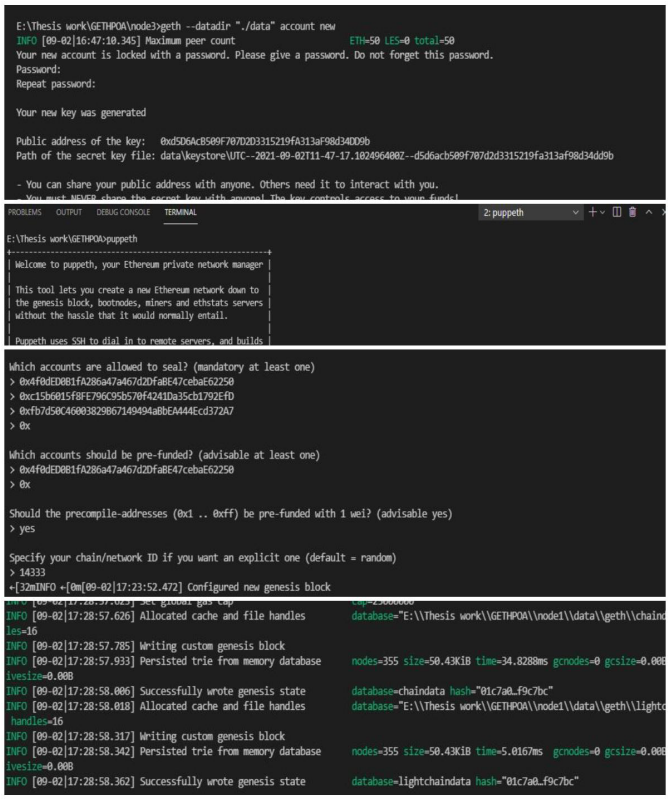

Fig. 8. Creation and configuration of nodes and genesis block.

blockchain by using a PoA consensus mechanism on the Geth visual studio code platform.

PoA is considered good for private blockchain networks in PoA; the miners are called validators and instead of wealth like in proof stake, the validator needs to stake their own identity. The person needs to confirm their identity first to be able to validate a transition. The validation performed is stored on the blockchain, and it is linked to the real identity of the validator. This means that to become an authorized validator of PoA-based blockchain network, the validator needs to confirm its real identity. When a transaction has been validated, the identity of the validator is authenticated on-chain by approved protocols. A small group of validators authenticates the identity of the validator to improve the security and efficiency of consensus. PoA does not require high computational power as proof of work (POW) required or a huge amount of wealth to stake as proof of stake. PoA is considered the best consensus method for private and consortium blockchain networks. We are going to implement TISVSchain on a private blockchain by using Geth on visual studio code.

Geth visual studio code provides a virtual platform to create nodes and to connect them virtually as a private blockchain. It has two options for consensus mechanisms, POW and PoA. We are going to choose PoA as a consensus mechanism because we are implementing our framework on a private blockchain. Odd numbers of blocks are preferable in this platform, so we are taking three nodes and then five nodes network to test the performance of TISVSchain on the private blockchain network.

Fig. 8 shows how the private network is deployed on Geth visual studio code. The first step is to Geth folder and then make nodes; an odd number of nodes is preferable. Nodes

can be made simple command mkdir node; after making the nodes, we have to make an Ethereum account for which the simple of geth – datadir ". /data" account new is used.

After making an Ethereum account on each node, we have to set a password that will give us the public Ethereum address of that particular node which can be used later on for making the connection between different nodes. After that, we have to make a genesis file that contains all the information about the network; for the genesis file, the puppet tool can use. A puppet is a build-in tool available with Geth used for the generation and configuration of genesis files. During the creation of the genesis file, the tool will ask about the configuration like the name of the genesis file, block time, and consensus algorithm. Once the genesis file is configured, we need to export that file to run the network by connecting all the nodes to the same genesis file. To start the network with the same genesis file, geth – datadir. /data init/blockpoa.json command can be used.

A boot node is another kind of node which would be part of the network but will not mine any block. The boot node is used to connect all other nodes of the network. First, we need to create a node folder, and then, we will generate the boot key by using the command boot node -genkey boot. key. After the creation of the boot key, we will start the nodes by using that boot key with the help of the command boot node -node key boot. key. The procedure will provide us with an encoder that will help us to make a peer-to-peer network; we will pass that node from other nodes for connectivity purposes. To start all the nodes, we have to enter the Ethereum password which is difficult to enter every time that is why we will hard code that password into each node to start the network command like boot node -node key "./boot. key" -verbosity 7 - and "127.0.0.1:30301" will be used from boot node, which tells the network nodes about the boot.key address and port for starting the network. Once the network is started, further commands have to give to the node according to their required field; the nodes which have mining access got the command geth – networking 14333 – datadir "./data" – boot nodes (node address) – port 30303 – ipcdisable – sync mode full – HTTP – allow-insecure-unlock – HTTP. core domain "∗" – HTTP. port 8545 – unlock (Public address) – password password.txt – mine console this command provides network ID which 14 333 boot node address, port number, other commands for HTTP access, public address or Ethereum, password and in the end most important thing which make this node a miner node is mine console command.

Other nodes which have simple access but do not mine any block use the command geth – networking 1 s4333 – datadir "./data" – boot nodes (node address) – port 3030 – ipcdisable – sync mode full – HTTP –allow-insecure-unlock – HTTP. core domain "∗" – HTTP. port 8546 – unlock (Public address) – password password.txt console; the only difference between the command for other nodes is that they just use console command instead of – mine console; for every new node, the port and the RPC port number should be different, and RPC is used for remote procedure call functionality.

Fig. 9 shows the inside data of the genesis block which contains information like chained, block time, a hash of the block, and the type of consensus mechanism used for the network; in other words, the genesis file contains all the information

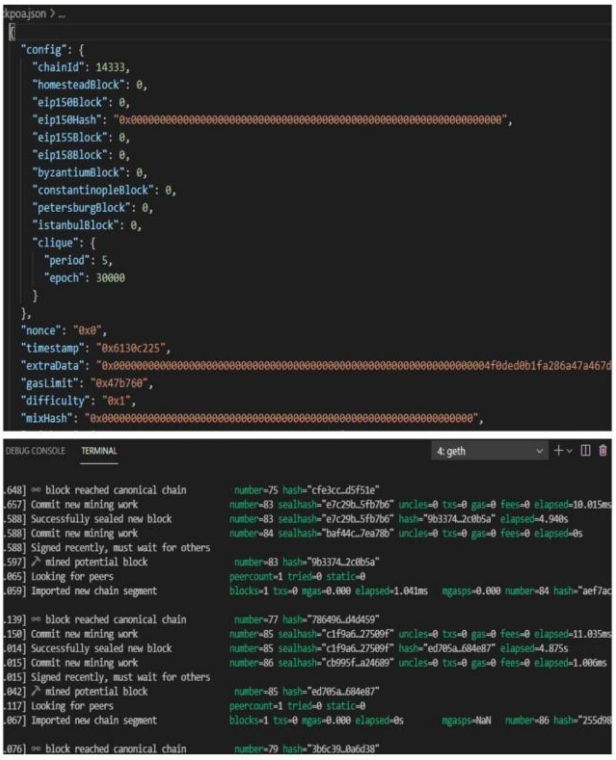

Fig. 9. JavaScript Object Notation (JSON) genesis block and other mining nodes.

related to the network. Fig. 7 also shows the mining process of the block. It can be seen that a block mine time is 4.94 s, and the actual configured time is 5 s; the delay can come from multiple factors, but overall, our network is running and it is mining the blocks.

The overall performance of the network is very efficient; we must deploy TISVSchain on private and public blockchains; both have their benefits but the private blockchain gives more security and control to the TISVSchain framework. The public blockchain is a platform that allows anyone to be a part of the network open to everyone. This is the nature of public blockchain; however, we have added the security by offline UA which makes the network able to allow only those users who have UAs but still it is a public network. On the other hand, in the private network which has a secure nature, only the authentic nodes are allowed to access the network and a new user can only be added when the owner of the private blockchain allows it. As mentioned earlier, only those nodes will be able to mine who have been given the rights during the configuration of the genesis block which gives more security and control to the TISVSchain framework. However, we have deployed the framework on both platforms, and we will discuss their efficiency and deployment cost in Section IV.

IV. Results and Discussion

This section explains the results and analysis and explains theoretical analysis and simulation results. The remix-integrated development environment is an open-source desktop and web application. It has plugins with GUI and has a faster development cycle. A remix is used for the entire journey of smart contract development as well as used for teaching and learning Ethereum. A remix is a platform for development

tools that are used as a plugin architecture, and it also allows you to write solidity contracts straight from the browser. Remix has modules for testing, deploying, and debugging smart contracts. IDE tools are available at the GitHub repository, and remix-IDE is available at remix.ethereum.org. Remix allows you to write solidly language-based smart contracts straight from the browser. It has three different environments and a JavaScript VM which means all the transactions will be executed in the sandbox blockchain in the browser. Nothing will be persisted when reloading the page because JavaScript has its blockchain.

The second environment is injected provider; in this environment, remix will connect to injected web3 provider like Metamask. The third environment is the web3 provider. In this environment, the remix will be connected to a provider like parity, Geth, or any Ethereum client. To implement smart contract virtually remix, provide 15 UAs with 100 either each to test the smart contracts. To do any transaction on the blockchain, it costs some gas remix providers a 3 000 000 gas limit to test the smart contracts. Remix has a file explorer option, solidity compiler, and deploy run transaction features. To deploy the smart contract in Ethereum, the contract is assigned a unique address which is 160 bit, and then, its code is uploaded to the blockchain. Once the smart contract is successfully created and consists of a predefined executable code, contract address, and a contract balance, and then, different parties can interact by sending the contract-invoking transaction to a specific known contract address. Solidity has a similar syntax to JavaScript, and it is a high-level programming language that supports inheritance, polymorphism, and libraries. Contracts are structured similar to classes in object-oriented programming language when using solidity for contract development. Solidity has some features like global variables, modifiers, and events. It defines special variables like block and msg. They always exist in the namespace and are used to access information about a blockchain. These variables are used for the retrieval of the origin address, the data sent alongside the invocation transaction, and the amount of the ether.

A. Simulation and Verification of Results

The performance of the TISVSchain framework in this section is analyzed and compared to different existing blockchain-based schemes use for the drug supply chain. The existing system mostly used hyper ledger fabric like those used by Jamil et al. [15], and we are using the Ethereum platform based on the PoA consensus mechanism; further, the proposed framework is deployed on both private and public blockchain networks. In the case of a public blockchain, we must deploy TISVSchain on remix ide by using solidity language as it is a virtual test network; users do not have to pay for executing their transaction. We have used Dell Inspiron 5559 which is Intel[1] Core i5-6200 with four logical processors and 8 GB of RAM running on Windows 8.1 Professional 64-bit edition. However, to check the efficiency of smart contracts, TGC which is transaction gas cost is a good metric. If the TGC value is lowered, it is for the execution of a particular smart contract or function that less computational power is required. We have measured the TGC value for different transactions over TISVSchain. This includes the deployment of three smart contracts which are the RA, vaccine registration, and consumer smart contract, and execution of functions like get_reg_vaccine, check_approved_uniqaddr, get_reg_vaccine, and vaccine_complete_info. To keep the gas cost as low as possible, we have optimized our program code. We have used mapping instead of an array to keep the GAS cost low.

[1]Trademarked.

TABLE II
TGC OF ETHEREUM SMART CONTRACTS AND FUNCTIONS

Smart Contracts	Transaction Gas Cost	Ether Cost	Price in US Dollars	Price in Pounds
Vaccine Registration	453152	0.0380648	$149.70	92.48
Regulatory Authority	303125	0.0254625	$100.14	46.90
Consumer	103531	0.0084895	$33.07	23.85
Functions				
Get_Reg_Company	100235	0.0082193	$32.022	23.08
Check_approved_UniqAddr	8132	0.0006668	$2.59	1.87
Get_Reg_Vaccine	50120	0.0026075	$16.01	11.54
Vaccine_complete_info	8053	0.0007481	$2.91	2.10

TABLE III
EFFECT OF NUMBER OF SEALERS AND BLOCK TIME ON LOST BLOCKS

Block-Time	Lost Blocks when Number of Sealers are				
	1st Sealer	2nd Sealers	3rd Sealers	4th Sealers	5th Sealers
5s	38	40	87	102	132
10s	15	16	42	79	91
15s	18	17	35	71	88
The 20s	8	13	28	67	76
25s	11	14	25	61	68

Table II shows different smart contracts and functions with their required gas cost required for the completion of transactions.

We can see that 859 808 is the total GAS cost to deploy all three smart contracts on Ethereum public network. The total gas cost mentioned above is required only for the deployment of the smart contracts and only once. We have converted the GAS cost into either and then into U.S. dollars which is not very much expensive as smart contracts deployment needs one-time payment. Functions required very affordable gas costs. Most of the time, vaccine_complete_info function will be used by the consumer which uses very little GAS and cost approximately U.S. $2.91 which shows how efficient TISVSchain is computational. Other smart contracts like get_reg_vaccine cost almost U.S. $32 to the company that wants to manufacture some vaccine and needs approval from the RA; if a company wants to check the offline UA that it is registered or not, we have a separate function check_approved_uniqaddr which will just cost 8132 GAS which is equal to U.S. $1.87.

TABLE IV
COMPARISON OF LOST BLOCKS

Block-time	Lost-Blocks	
	TISVSchain	PET-chain
5s	38	45
10s	15	17
15s	18	23
20s	08	3

This shows how efficient performance-wise and cost-wise TISVSchain is effective.

We have used different block times and a different number of sealers to analyze their effect on the lost blocks, as shown in Table III. We have seen that lost blocks and block time are inversely proportional from top to bottom in Table III; when block time increases, the number of lost blocks decreases. Because greater block time gives more time to the sealer to get the data, validate it, and sign the transaction. Further, we have observed that with the increased sealer number, the lost blocks also increase because when a signed block broadcasts, then a new block is proposed by the backup sealer which causes the lost blocks. For the block to be part of the blockchain network, it required more than 50% of sealer verification but because of synchronization issues caused by lost blocks, delay the process. It can be seen in Table III that as the number of sellers increases, the number of lost blocks also increases from left to right but if we look from top to bottom in Table III, lost block decreases with the increase of block time as more block time gives time to the node to process the block which decreases the number of lost blocks.

Another important thing is propagation delay which is the time difference from when a node announces the discovery of a new block to the time when other nodes receive that information if the delay increases will cause synchronization issues in the network. Table III also gives information about propagation delay: a greater number of the lost block will increase more delay in the network which will lead to synchronization issues. This means that by increasing the number of sealers, the propagation delay also increases. It is analyzed that increasing numbers of sealers will result in a greater number of lost blocks, and as the number of lost blocks increases, propagation delay will also increase which will cause synchronization issues between the nodes. When the block time increased from top to bottom in Table III, the number of lost blocks decreased. Another important factor that we are going to discuss is TPS.

Our proposed framework, the technology, and the platform we used and deploy are novel in the field of vaccine supply chain management, but the same technology is used in the Privacy Enhancing Technology (PET) chain, which is designed for user general data protection [34]. In Table IV, we have compared the lost blocks of TISVSchain with PET chain on different block times and find out satisfying results. When the lost block increases, it affects and increases propagation which causes synchronization issues in the network so if the number of lost blocks decreases, the overall efficiency of the framework is increased.

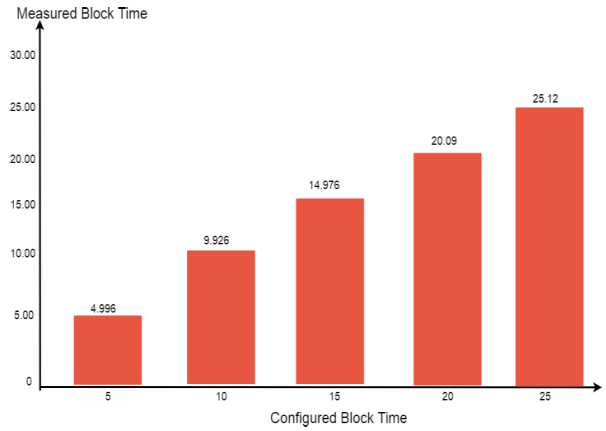

Fig. 10. Configured block time versus measured block time.

The 10–15 TPSs are supported by Ethereum public network [35]. However, it is observed in the case of a private network that can achieve a much higher TPS value. We have run our blockchain network for different blocks of time and by using different gas limits to measure the TPS we have used an equation. In the genesis file, the block time and gas limit are configured. However, due to synchronization issues and network delays, configured block time is different from the actual block time.

Fig. 10 illustrates how configured block time is different from measured block time. This difference can be caused by different reasons like network delays and synchronization issues. Therefore, we have measured the average block time by running the blockchain for a couple of hours on different block times. It can be seen in Fig. 10 that block time is 5, then the average is 4.996, and when we have a block time of 25 and the average time is 25.12, it shows that for lesser block time, the performance is better and if we must choose an ideal block time, it can be 15 for the current framework as the number of the lost block will be lesser for this choice and which will result in lesser propagation delay.

The technology, the method we used and deploy is novel in the field of vaccine supply chain management, but it is already used in a framework designed for user general data protection [34]. In Fig. 11, we have compared the measured block time of the PET chain with our framework-measured block time and find out satisfying results. Even for the block time of ten TISVS chains, the measured block time is better than the PET chain.

To compute the TPS for three different gas limits (20 000 000, 40 000 000, and 80 000 000), we have used measured block time; the more the gas limit, the more transactions it can accommodate. Hence, we have chosen these three different gas limits to see the results. From Fig. 10, it is already clear that the measured block time is different from configured block time because of some synchronization issues and network delay. Hence, we have calculated the TPS by measured block time by following the equation as used in [34]:

$$\text{TPS} = \text{Gas Limit}/\text{TGC}^{*}\text{Block time}.$$

The equation used for computing TPS required a gas limit and we have given it three different gas limits, it required

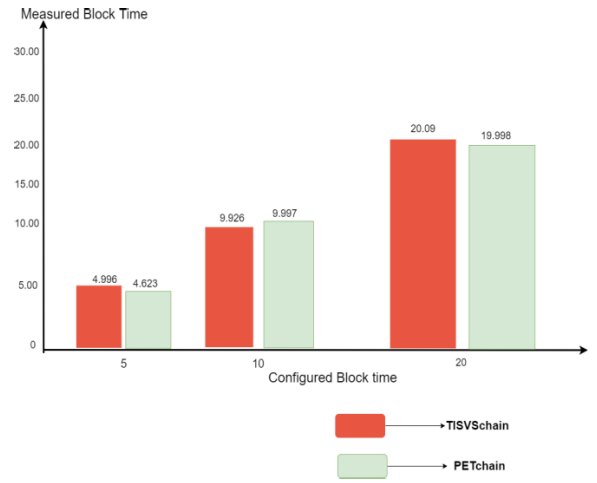

Fig. 11. TISVSchain and PET-chain measured block time comparison.

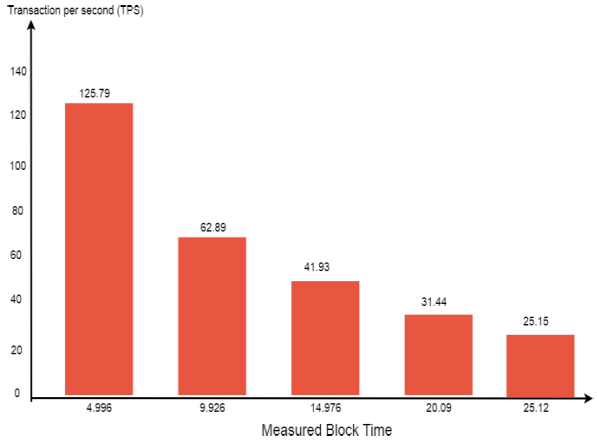

Fig. 12. TPS calculation by using 20 000 000 gas limits.

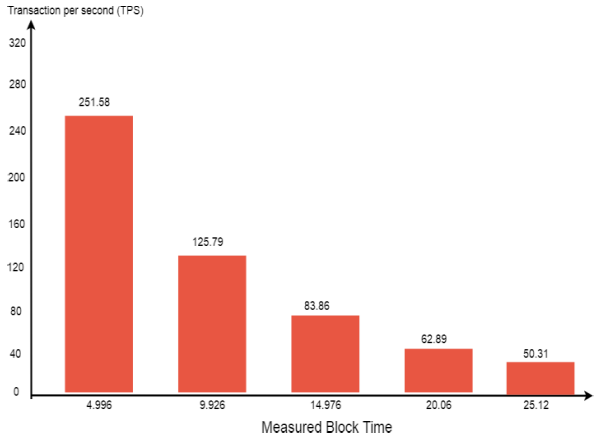

Fig. 13. TPS calculation by using 40 000 000 gas limits.

TGC which we have got from Table II; we have taken the average of gas cost; further, it required the block time, but the configured block time is changed from measured so for getting the accurate results we have used the measured block time.

Fig. 12 shows the calculated TPS against the measured block time by using the gas limit of 2 000 000. We have put the value of the gas limit, an average of TGC, and measured block time in the equation to get the result of TPS. It is observed that with the increase of block time, the TPS value decreased so for getting a high TPS value block time should be below. But the problem with low block time results in a more lost block.

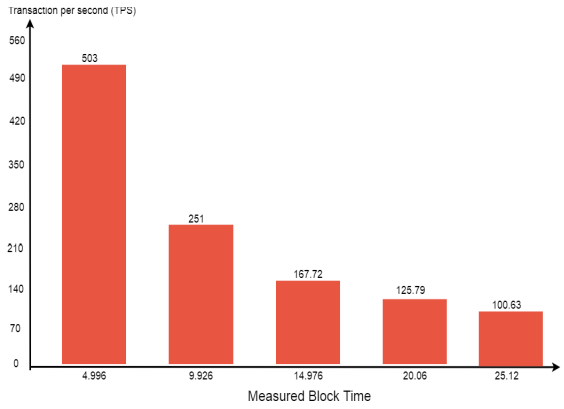

Fig. 14. TPS calculation by using 80 000 000 gas limits.

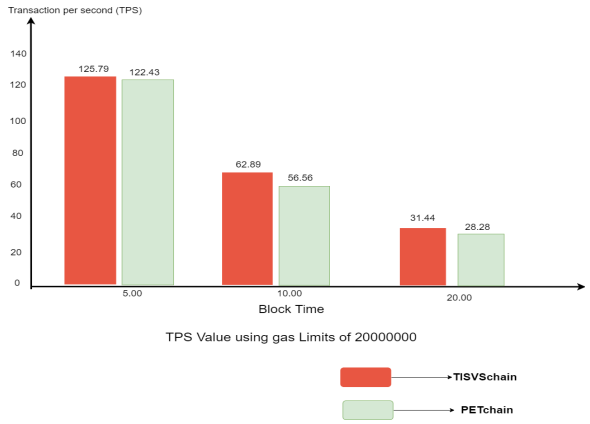

Fig. 15. TPS comparison of TISVSchain and PET chain using 20 000 000 gas limits.

When we change the gas limit from 20 000 000 to 40 000 000, the TPS value also increases and almost doubles by doubling the gas limit value. The same as observed in Figs. 11 and 13 also shows us that by increasing the block time, the TPS value starts decreasing; further, it is clarifying the relationship of the gas limit with TPS. By increasing the gas limit, the TPS value also increased. Now all we need to select an appropriate block time which can cause low delay and high TPS.

Fig. 14 shows us the result obtained when we increased the gas limit up to 80 000 000, the TPS value also increased. On a time block of 5, it gives us 503 TPS which is quite high, and this is because more transactions can be accommodated into a block by having a high gas limit. But if we increase the block time, the TPS value will start decreasing which means that for a high TPS value, low block time and a high gas limit are recommended.

However, selecting an appropriate block time is difficult; when we select a low block time, it causes a greater number of lost blocks which results in propagation delays and starts causing synchronization issues. Hence, we need to select an appropriate block time that gives us a high TPS value and low delay in the network.

In Fig. 15, we have compared our measured value of TPS with the PET chain using 20 000 000 gas cost [34]. Our framework results are satisfactory and effective; it gives better TPS value, which proves the efficiency of TISVSchain.

The number of sealers hurts block time; when we increase the number of sealers, the measured block time also increases.

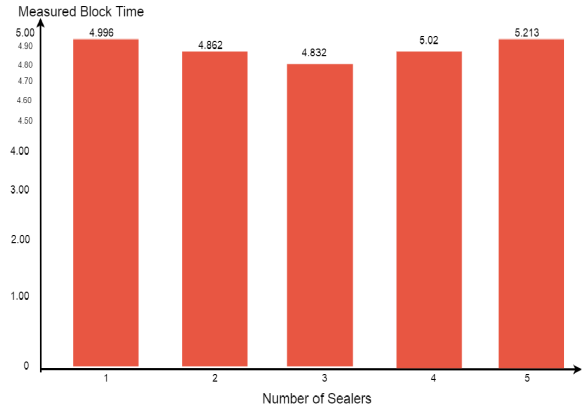

Fig. 16. Block time versus number of sealers.

We have run the blockchain for a different number of sealers for different block times and got the result that by increasing the number of sealers, the block time will also increase, as shown in Fig. 16.

This happens because to be part of a blockchain more than half of the sealers need to verify the block. Hence, the greater numbers of sealers will require more time for verification which will increase the measured block time and the number of lost blocks which can lead to synchronization issues. Therefore, more than half of the nodes are not recommended as a sealer. In a five-node network, there should be 2 or a maximum of three sealers for better results.

V. Conclusion

In this article, we have presented a flexible, blockchain-based data management framework for vaccine supply chain management to resolve the problem of fake or counterfeit drugs and to make the process of the vaccine supply chain transparent, decentralized, audible, traceable, and immutability. We designed a novel framework that can be deployed both on a private and public blockchain. Our smart contracts based on Ethereum were designed to minimize gas costs as much as possible for regulatory authorities, VMs, vaccine suppliers, and consumers to trace vaccine operation records and to make the process transparent. Additionally, to enhance the security offline, a UA is assigned by the RA to authenticate manufacturers; only by that UA, they can access the network. Our smart contract was able to detect vaccine manufacturing and expiry date.

We have described the design, implementation, and evaluation of the proposed framework for Ethereum. We have implemented our framework on public blockchain by using remix ide based on solidity language and five nodes private blockchain network for performance evaluation and found out that high TPS achieved by having a high gas limit and low block time. However, it was also observed that low block time results in a high number of lost blocks which leads to propagation delay and synchronization issues. In our evaluation, block time of 15 was good for the result which gives us high TPS and low lost blocks.

We have observed that the number of sealers should be less or equal to half of the total nodes to reduce synchronization issues. Overall, our results indicate that using blockchain increases the immutability, transparency, and security of vaccine supply chain management.

In the future, the framework can be deployed in many node networks, and then, its feasibility and performance can be checked by deploying the system in a real environment as we have deployed the framework in a virtual environment with a limited node network, but the real performance can be evaluated to test this framework in a real environment which includes a greater number of nodes. The user's feedback system can be added to enhance the visibility and efficiency of the framework so that in the future, customer reputation systems can be added.

Vaccines are effective when they are kept under a certain temperature. The efficiency of the vaccine will compromise below or above that temperature so by using some sensors, a cold chain process of vaccine should be added in the future to make this framework efficient. Our main objective was to design an efficient blockchain-based framework that can run both on public and private blockchain platforms and to compute its performance metrics in terms of gas cost, TPS value, propagation delay, and synchronization issue and check the effect of block time on the number sealer. We have achieved our goal but, in the future, work can be done in the customer reputation system and vaccine cold chain process.

References

[1] J. Dhandapani and R. Uthayakumar, "An EOQ model for a high cost and most wanted vaccine considering the expiration period," *J. Anal.*, vol. 27, no. 1, pp. 55–73, Mar. 2019.

[2] M. A. Qureshi, K. N. Qureshi, G. Jeon, and F. Piccialli, "Deep learning-based ambient assisted living for self-management of cardiovascular conditions," *Neural Comput. Appl.*, vol. 34, no. 13, pp. 10449–10467, Jul. 2022.

[3] U. H. Kartoglu, K. L. Moore, and J. S. Lloyd, "Logistical challenges for potential SARS-CoV-2 vaccine and a call to research institutions, developers and manufacturers," *Vaccine*, vol. 38, no. 34, p. 5393, 2020.

[4] K. N. Qureshi, A. Ahmad, F. Piccialli, G. Casolla, and G. Jeon, "Nature-inspired algorithm-based secure data dissemination framework for smart city networks," *Neural Comput. Appl.*, vol. 33, pp. 10637–10656, Apr. 2020.

[5] M. Uddin, "Blockchain medledger: Hyperledger fabric enabled drug traceability system for counterfeit drugs in pharmaceutical industry," *Int. J. Pharmaceutics*, vol. 597, Mar. 2021, Art. no. 120235.

[6] D. Akunyili, "Fake and counterfeit drugs in the health sector: The role of medical doctors," *Ann. Ibadan Postgraduate Med.*, vol. 2, no. 2, pp. 19–23, Feb. 2007.

[7] M. Westerkamp, F. Victor, and A. Küpper, "Tracing manufacturing processes using blockchain-based token compositions," *Digit. Commun. Netw.*, vol. 6, no. 2, pp. 167–176, May 2020.

[8] S. K. Dwivedi, R. Amin, and S. Vollala, "Blockchain based secured information sharing protocol in supply chain management system with key distribution mechanism," *J. Inf. Secur. Appl.*, vol. 54, Oct. 2020, Art. no. 102554.

[9] G. Arzu Akyuz and T. Erman Erkan, "Supply chain performance measurement: A literature review," *Int. J. Prod. Res.*, vol. 48, no. 17, pp. 5137–5155, Sep. 2010.

[10] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, "Blockchain technology and its relationships to sustainable supply chain management," *Int. J. Prod. Res.*, vol. 57, no. 7, pp. 2117–2135, Apr. 2019.

[11] S. A. Abeyratne and R. P. Monfared, "Blockchain ready manufacturing supply chain using distributed ledger," *Int. J. Res. Eng. Technol.*, vol. 5, no. 9, pp. 1–10, 2016.

[12] K. Korpela, J. Hallikas, and T. Dahlberg, "Digital supply chain transformation toward blockchain integration," in *Proc. 50th Hawaii Int. Conf. Syst. Sci.*, 2017, pp. 1–10.

[13] Y. Tribis, A. El Bouchti, and H. Bouayad, "Supply chain management based on blockchain: A systematic mapping study," in *Proc. MATEC Web Conf.*, vol. 200, 2018, p. 00020.

[14] A. Kumar, R. Krishnamurthi, A. Nayyar, K. Sharma, V. Grover, and E. Hossain, "A novel smart healthcare design, simulation, and implementation using healthcare 4.0 processes," *IEEE Access*, vol. 8, pp. 118433–118471, 2020.

[15] 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, p. 505, Apr. 2019.
[16] P. Sylim, F. Liu, A. Marcelo, and P. Fontelo, "Blockchain technology for detecting falsified and substandard drugs in distribution: Pharmaceutical supply chain intervention," *JMIR Res. Protocols*, vol. 7, no. 9, Sep. 2018, Art. no. e10163.
[17] A. Erokhin, K. Koshechkin, and I. Ryabkov, "The distributed ledger technology as a measure to minimize risks of poor-quality pharmaceuticals circulation," *PeerJ Comput. Sci.*, vol. 6, p. e292, Sep. 2020.
[18] J.-H. Won and H. Lee, "The current status of drug repositioning and vaccine developments for the COVID-19 pandemic," *Int. J. Mol. Sci.*, vol. 21, no. 24, p. 9775, Dec. 2020.
[19] R. Gupta, S. Tanwar, F. Al-Turjman, P. Italiya, A. Nauman, and S. W. Kim, "Smart contract privacy protection using AI in cyber-physical systems: Tools, techniques and challenges," *IEEE Access*, vol. 8, pp. 24746–24772, 2020.
[20] B. Bünz, S. Agrawal, M. Zamani, and D. Boneh, "Zether: Towards privacy in a smart contract world," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Kota Kinabalu, Malaysia: Springer, 2020, pp. 423–443.
[21] A. Dolgui, "Blockchain-oriented dynamic modelling of smart contract design and execution in the supply chain," *Int. J. Prod. Res.*, vol. 58, no. 7, pp. 2184–2199, 2019.
[22] Y. K. Dwivedi, M. A. Shareef, B. Mukerji, N. P. Rana, and K. K. Kapoor, "Involvement in emergency supply chain for disaster management: A cognitive dissonance perspective," *Int. J. Prod. Res.*, vol. 56, no. 21, pp. 6758–6773, Nov. 2018.
[23] F. Tian, "An agri-food supply chain traceability system for China based on RFID & blockchain technology," in *Proc. 13th Int. Conf. Service Syst. Service Manag. (ICSSSM)*, Jun. 2016, pp. 1–6.
[24] S. Ahmed and N. J. N. Ten Broek, "Blockchain could boost food security," *Nature*, vol. 550, no. 7674, p. 43, 2017.
[25] M. Andoni, V. Robu, and D. Flynn, "Blockchain: S crypto-control your own energy supply," *Nature*, vol. 548, no. 158, 2017. [Online]. Available: https://www.nature.com/articles/548158b
[26] S. S. Kamble, A. Gunasekaran, and R. Sharma, "Modeling the blockchain enabled traceability in agriculture supply chain," *Int. J. Inf. Manage.*, vol. 52, Jun. 2020, Art. no. 101967.
[27] A. Shahid, A. Almogren, N. Javaid, F. A. Al-Zahrani, M. Zuair, and M. Alam, "Blockchain-based agri-food supply chain: A complete solution," *IEEE Access*, vol. 8, pp. 69230–69243, 2020.
[28] K. Salah, N. Nizamuddin, R. Jayaraman, and M. Omar, "Blockchain-based soybean traceability in agricultural supply chain," *IEEE Access*, vol. 7, pp. 73295–73305, 2019.
[29] R. Singh, A. D. Dwivedi, and G. Srivastava, "Internet of Things based blockchain for temperature monitoring and counterfeit pharmaceutical prevention," *Sensors*, vol. 20, no. 14, p. 3951, Jul. 2020.
[30] A. R. Nair, R. Gupta, and S. Tanwar, "FAIR: A blockchain-based vaccine distribution scheme for pandemics," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2021, pp. 1–6.
[31] L. Cui, Z. Xiao, F. Chen, H. Dai, and J. Li, "Protecting vaccine safety: An improved, blockchain-based, storage-efficient scheme," *IEEE Trans. Cybern.*, early access, Apr. 13, 2022, doi: 10.1109/TCYB.2022.3163743.
[32] C. Antal, T. Cioara, M. Antal, and I. Anghel, "Blockchain platform for COVID-19 vaccine supply management," *IEEE Open J. Comput. Soc.*, vol. 2, pp. 164–178, 2021.
[33] Y. Kamenivskyy, A. Palisetti, L. Hamze, and S. Saberi, "A blockchain-based solution for COVID-19 vaccine distribution," *IEEE Eng. Manag. Rev.*, vol. 50, no. 1, pp. 43–53, Mar. 2022.
[34] I. T. Javed, F. Alharbi, T. Margaria, N. Crespi, and K. N. Qureshi, "PETchain: A blockchain-based privacy enhancing technology," *IEEE Access*, vol. 9, pp. 41129–41143, 2021.
[35] T. Fatokun, A. Nag, and S. Sharma, "Towards a blockchain assisted patient owned system for electronic health records," *Electronics*, vol. 10, no. 5, p. 580, Mar. 2021.

Muhammad Rehman received the B.S. degree in computer engineering from UET Taxila, Taxila, Pakistan, in 2018, and the M.S. degree in information security from Bahria University, Islamabad, Pakistan, in 2021.

He is currently working as an IT and Cyber Security Auditor with EY Ford Rhodes, Karachi, Pakistan. His research interest is in the area of blockchain technology and security auditing.

Ibrahim Tariq Javed received the Ph.D. degree in computer science from Institut Mines-Telecom, Telecom SudParis, Evry, France, in 2018.

He worked as an Associate Professor with Bahria University, Islamabad, Pakistan. He also obtained a post-doctoral fellowship co-sponsored by the European Commission under the Marie Skłodowska-Curie Program and Science Foundation Ireland through Lero—the Irish Software Research Centre. He is currently working as a Research Fellow with Blockhain@UBC. He has been able to publish his research in top-tier journals and conferences. His research interests include blockchain technology, Web3.0, decentralized applications, privacy, identity, and trust management.

Kashif Naseer Qureshi received the Ph.D. degree from the University of Technology Malaysia (UTM), Johor Bahru, Malaysia, in 2016.

He is currently an Associate Professor with the University of Limerick, Limerick, Ireland. He is a Cisco and Microsoft Certified Network Professional. He has many years of research experience in several areas, such as vehicular ad hoc network (VANET), wireless sensor network (WSN), wireless body area network (WBAN), security, privacy-preserving data aggregation, computer forensics, and cloud security. He has authored around 158 articles in international journals and conference proceedings and served in several conferences, IPCs, and journal editorial boards. He has also various projects related to routing and cyber security domains. His research interests include the Internet of connected Vehicles (IoV), electronic vehicles charging management planning and recommendation (EV), and the Internet of Things (IoT) use cases implementation in WSNs.

Dr. Qureshi is a reviewer for various reputable academic journals.

Tiziana Margaria (Member, IEEE) has broad experience in the use of formal methods for high-assurance systems, in particular concerning functional verification, reliability, and compliance of complex heterogeneous systems. In Lero, she heads research projects on scientific workflows, in particular for data analytics, on model-driven service-oriented software design for evolving systems, and on holistic hardware/software (HW/SW) cybersecurity. Current applicatio domains are embedded systems, healthcare, and smart advanced manufacturing. The aforementioned are her research topics and application domains most relevant to Advanced Learning in Evolving Critical Systems (ALECS).

Ms. Margaria is currently the Vice-President of the European Association of Software Science and Technology (EASST), the President of the ERCIM Working Group on Formal Methods for Industrial Critical Systems (FMICS), a Steering Committee Member of the European Joint Conferences on Theory and Practice of Software (ETAPS), a Managing Editor of the Springer Journal on Software Tools for Technology Transfer (STTT), and the Co-Founder of the TACAS and ISoLA series of conferences. She is a fellow of the Irish Computer Society and the Society for Design and Process Science (SDPS).

Gwanggil Jeon (Senior Member, IEEE) received the B.S., M.S., and Ph.D. *(summa cum laude)* degrees from the Department of Electronics and Computer Engineering, Hanyang University, Seoul, South Korea, in 2003, 2005, and 2008, respectively.

He was a Post-Doctoral Fellow with the University of Ottawa, Ottawa, ON, Canada, an Assistant Professor with Niigata University, Niigata, Japan, and a Prestigious Visiting Professor with the Università Degli Studi di Milano Statale, Milan, Italy. He is currently a Full Professor with Incheon National University, Incheon, South Korea.

Dr. Jeon was a recipient of the IEEE Chester Sall Award in 2007, the ETRI Journal Paper Award in 2008, and Industry-Academic Merit Award by Ministry of SMEs and Startups of Korea Minister in 2020.