A Blockchain-based Contactless Delivery System for COVID-19 and Other Pandemics

by

Pratiksha Mittal

A thesis submitted to the Graduate Faculty of
Auburn University
in partial fulfillment of the
requirements for the Degree of
Master of Science

Auburn, Alabama
August 7, 2021

Keywords: Blockchain, COVID-19, Delivery System, Pandemics.

Approved by

Ujjwal Guin, Chair, Assistant Professor of Electrical and Computer Engineering
Christopher Harris, Assistant Professor of Electrical and Computer Engineering
Mehdi Sadi, Assistant Professor of Electrical and Computer Engineering

Abstract

Our regular lives have been incredibly changed by the coronavirus (COVID-19) widespread. Inaccessible work and self-quarantine have constrained individuals all over the world to adjust. Numerous service providers, counting retail stores and restaurants, have had to alter their logistics plans. Whereas lessening and regulating human interaction aids in controlling and avoiding the infection, it includes a significant effect on numerous trade spaces, particularly those with physical stores. Contactless delivery has been proposed as a means of avoiding the spread of the coronavirus. Contactless delivery permits customers to get merchandise whereas holding crucial social distancing. It empowers individuals to have their regular necessities, such as essential supplies and drugs, delivered to their doorstep. Contactless delivery, on the other hand, diminishes direct contact between the delivery personnel and the customers. The items have vulnerable contacts with logistics personnel and other obscure third parties in expansion to peer-to-peer organizing. The supply chain routes stay an issue indeed, even though the items are conveyed without physical contact. As a result, there is an urgent requirement for creating a contactless delivery framework where the location traces of delivery personnel can track anonymously. In this paper, we show a novel blockchain-based framework for enabling order traceability over the supply chain. Our proposed system viably contributes to COVID-19 avoidance and control by recording and checking traces of delivery and the medical status of delivery personnel in a privacy-preserving way. As a test-bed, we created a Hyperledger Fabric-based blockchain model system. Various smart contract features are added and tested to show the effectiveness of the proposed scheme. Following its implementation and evaluation, we conduct thorough security and privacy analysis of this framework.

Acknowledgments

I would like to express my heartfelt gratitude to Prof. Ujjwal Guin, my graduate advisor, for his encouragement and guidance during my time at Auburn University. His encouragement and guidance paved the way for my successful research projects and thesis completion. I would like to express my gratitude to Prof. Anthony Skjellum of the University of Tennessee for his experience and insight into Blockchain. Also, a special thanks to Pinchen Cui, Ph.D., for his important contributions to this research. I want to extend my gratitude to the committee members of the thesis: Prof. Christopher Harris and Prof. Mehdi Sadi, for their time, support, and advice towards my research and thesis. Thank you to all of my labmates and colleagues for the valuable information I acquired during my course and study work. The lab exercises and brainstorming sessions taught me a lot about my field of study. Finally, I would like to thank my parents and friends for their unwavering support during my academic career.

Table of Contents

List of Figures

Chapter 1

Introduction

The COVID-19 is a highly infectious disease caused by novel coronavirus and the majority of people infected with the coronavirus will have mild to moderate respiratory symptoms and recover without needing any special care. However, people over the age of 65, as well as those with underlying medical conditions such as cardiovascular disease, diabetes, chronic respiratory disease, and cancer, are at a higher risk of developing a severe illness [2]. COVID-19 has been one of the most damaging pandemics in human history, resulting in disease burdens never seen before, high healthcare costs, and negative economic effects all over the world. More than 128.4 million people have been infected with the coronavirus as of March 31, 2021. There have been 2.81 million deaths worldwide as a result of these 128.4 million confirmed cases, resulting in approximately 2.2% mortality rate [3]. The coronavirus's virulence may be due to its remarkable surface stability [4], as it can live on stainless and plastic surfaces for more than seven days [5]. As a result, despite numerous attempts to contain the pandemic, the epidemic continues to spread. Despite the recent creation of vaccines for the virus, numerous studies suggest that in the coming months, people should continue to socially isolate themselves and take adequate precautions [6, 7].

COVID-19 has spread exponentially around the world since the first case was detected in late 2019 in Wuhan, China, causing the World Health Organization to declare it a pandemic on March 11, 2020 [2]. COVID-19 has a fatality rate of 2% to 5%, and the virus has caused many deaths worldwide due to its high infectiousness. To effectively avoid the spread of COVID-19, steps such as social distancing and a shelter-in-place order have been introduced. In response to the social distancing steps, the closure of all non-essential facilities and restaurants' restrictions to takeout service has sparked a boom in food delivery services.

A service like this has been hailed as a valuable, easy, and secure way to reduce the risk of infection from novel coronavirus infection sources. Nonetheless, this form of distribution can still pose a risk of disease transmission.

According to reports, more than 60% of contaminated cases in a public hospital in Hanoi, Vietnam's capital, have been related to food distribution by mildly ill or presymptomatic nonclinical workers at the hospital cafeteria. This has raised fears that food delivery may play a significant role in the disease's spread. Although an increasing number of people follow the shelter-in-place order, delivery personnel continue to fill customer orders. This has pushed them to the forefront of the COVID-19 pandemic. The possibility that delivery workers (1) come into direct contact with novel coronavirus–infected customers without ever exhibiting symptoms and (2) function as a presymptomatic sender, inadvertently transmitting the novel coronavirus to their safe customers, coworkers, or families, should be considered. According to facts, presymptomatic or asymptomatic transmission is one of the main routes through which the novel coronavirus spreads.

During a pandemic, delivery personnel is at a greater risk of transmitting the novel coronavirus and may becoming a "spreader." Here are several strategies for reducing such dangers:

- To prevent infection with COVID-19, many companies have started contactless delivery. For example, Instacart provides the "Leave at my door delivery" choice in developed countries such as the United States. In developing countries like Vietnam, GrabFood uses the contactless Grab transaction, in which delivery personnel leaves meals at a designated location while standing 2 meters away waiting for customers [8].

- Fresh face masks, gloves, and hand sanitizers must be strictly followed. To prevent infection with the novel coronavirus, delivery personnel should wear new face masks and gloves and use hand sanitizers regularly [8].

- In developing countries, digital payment or credit card payment is encouraged to limit contact with delivery personnel [8].

- Customers should throw away the packaging as soon as possible and wash their hands afterward [8].

1.1 Motivation

The transmission of the coronavirus is a major concern to public health and has a huge impact on people's lifestyles. New policies such as social distancing, remote working, and self-quarantining have been proposed and implemented worldwide to thwart the virus's spread. While reducing and regulating human interaction aids in the control and prevention of the virus, it has a significant impact on many business domains, especially those with physical stores. For example, a drop in consumer traffic directly affects retail stores and catering services, resulting in job changes and losses [9]. It is a tough balancing act to keep people safe while continuing to run regular business operations. Contactless delivery, as an alternative, will help to address this issue in part. Contactless delivery allows customers to receive goods while retaining fundamental social distancing. It enables people to have their everyday necessities, such as groceries and medications, delivered to their doorstep. On the other hand, the shipped products go through vulnerable encounters with delivery personnel and unknown third parties. As previously mentioned, the virus's stability can spread further due to its ability to live long periods on fomites like boxes or bags. Even in contactless delivery scenarios, we need to keep track of the delivery details. This helps researchers dig deeper into the virus's transmission path to see if any confirmed cases have been identified in the supply chain system.

Many countries have implemented mobile technology to combat the spread of the coronavirus, and they depend on such technologies to provide information to help them make better decisions about the lockdown exit strategy [10]. Different countries have taken the lead in requiring people to install surveillance apps such as Trace Together, Arogya setu, COVIDSafe etc. [11, 12, 13, 14, 15, 16, 17, 18, 19, 20] in order to facilitate touch tracing. Unfortunately, people may not have access to this knowledge to make risk-informed decisions when interacting with others. Despite the increased demand for home deliveries, delivery personnel is not regularly tested for coronavirus. As a result, when introducing a contactless delivery system, it is critical to building an infrastructure that allows for risk-informed decision-making. As a result, we suggest a blockchain-based framework for recording the medical status of delivery personnel and then tracing the infection pathway across the supply chain. Human-to-human interaction is reduced by using a contactless delivery system, and our proposed framework then helps all interested parties to obtain up-to-date information on supply chain risks.

Despite the fact that much has been done to combat the COVID-19 pandemic, there is no contactless delivery system that can provide contact tracing in the event of coronavirus exposure. Box delivery systems distribute shipments that could have traveled to many different places. Since these packages are guaranteed to be sanitized or washed, delivery personnel are often at risk of catching an infection from the package. Furthermore, they can come into contact with coronavirus while delivering in a highly contaminated area. If the delivery personnel is still in danger, the shipment is also in danger. As a result, the package receiver must keep track of the delivery personnel's position. Moreover, exercise caution when handling these items. As a result, the development of a contactless distribution system that allows delivery personnel's location traces to be tracked anonymously is critical.

1.2 Contributions

In this thesis, we show how a blockchain can be used to implement a system that can track and trace the location and medical status of the delivery personnel. As a result of COVID-19, several service providers, including retail stores and restaurants, have had to alter their logistics strategies. Hence, We introduce a novel blockchain-based platform for tracking individuals in contactless delivery systems, which will help prevent the coronavirus's spread. The primary contributions of this thesis are as follows:

- We introduce a new blockchain-based platform for tracking individuals in contactless delivery systems. All delivery personnel from organizations that are a part of this proposed system must update the ledger with the locations where they made deliveries. When a user submits a query, they can get a complete history from the immutable blockchain ledger while preserving the privacy of the person who uploaded the information. The consumer will then decide if a coronavirus infection was present and make a risk-based decision about proceeding with the delivery. The delivery person does not have to reveal his or her identity in order to protect privacy. Instead, each participant will be given a unique identifier. Our proposed blockchain architecture that is based on confirmation can enable traceability in contactless delivery systems.

- To incorporate the proposed blockchain architecture, the proposed infrastructure uses Hyperledger Fabric [21] and the non-resource intensive consensus algorithm Raft [22]. To generate CouchDB state databases, we use Hyperledger Fabric's docker containers. The use of docker containers is essential because it helps us isolate chaincodes [21]. Chaincode governs how smart contracts are packaged for deployment. We can guarantee the performance of concurrent transactions by isolating chaincodes. We provide the latency and throughput at different transaction rates and different batch sizes to evaluate the effectiveness of our proposed approach. Since it is an open-source, permissioned blockchain, Hyperledger Fabric was chosen as the blockchain system. Hyperledger Fabric uses a non-resource-intensive consensus algorithm to reduce transaction fees while still increasing performance. It aims to make pluggable component systems with high confidentiality, resilience, and scalability easier to implement. Users must first be given access to the network and applications before connecting to a Fabric blockchain because it is permission. Fabric networks can be divided into channels, allowing nodes to participate in several blockchains simultaneously.

- Since it is based on blockchain technology, our proposed architecture not only guarantees reliable supply chain provenance but also protects the privacy of all parties concerned. Our system ensures delivery personnel's privacy by associating them with a unique identification number rather than a personal name since they are expected to provide confidential details to the service provider (i.e., a regular health check). The service provider is the only member of the blockchain who knows the mapping between delivery personnel and their ID number.

Chapter 2

Background and Related Work

A blockchain infrastructure's decentralized storage makes it ideal for a wide range of applications, such as various internet of things (IoT) applications [23], and supply chain traceability [24, 25, 26, 27, 28, 29, 30, 31]. Anyone can join and make transactions on a decentralized blockchain and participate in the consensus process. With no single point of failure, this decentralized model offers high robustness and durability for the blockchain database. It can either be listed as a public (permissionless) or private (permissioned) blockchain. The most well-known public blockchain applications, for example, are Bitcoin [1] and Ethereum [32]. On the other hand, a private blockchain is an invite-only network run by a central authority that requires members to go through a verification process before being accepted.

2.1 Blockchain Technology

Blockchain is a decentralized technology with specific features like impenetrable information infrastructure, transparency, and cryptographic encryption tools built-in [33]. It is a series of blocks that makes up a distributed ledger. The underlying cryptographic technology used to authenticate network participants makes blockchain's decentralized platform tamper-proof. Furthermore, Blockchain technology has several possible applications that can aid in handling the ongoing pandemic crisis. It can be used to streamline vaccine and drug clinical trials, raise public awareness, monitor donations, and fundraising events transparently, and serve as a credible data tracker [34, 35, 36]. Since once a block is authenticated and checked, it is chained to previous blocks with a specific hash; it takes many resources to change blocks added to the blockchain network. As a result, changing one block will alter this hash, alerting all participants, making it nearly impossible to update or remove data. Furthermore, all network users have access to the data stored on the blockchain, ensuring accountability among participants.

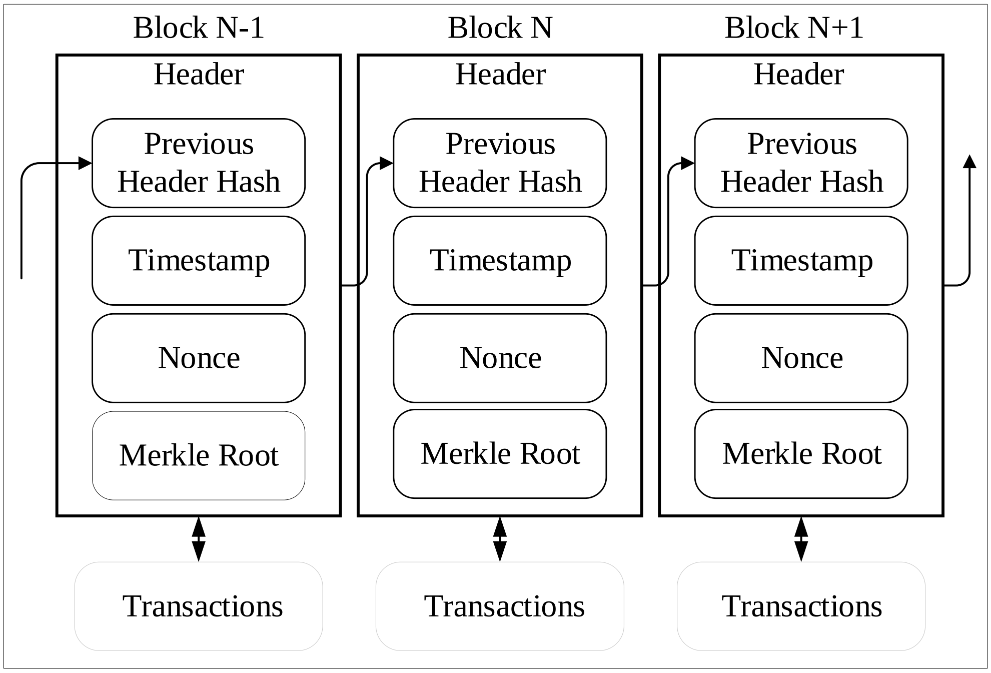


Figure 2.1: The blockchain infrastructure introduced in the Bitcoin paper [1].

Like a traditional public ledger, a blockchain is a series of blocks that contain a complete list of transaction records [37]. A blockchain is depicted in Figure 2.1 as an example [1]. A block has only one parent block if the block header contains a previous block hash. The first block in a blockchain is known as the genesis block that hasn't been parented by any other blocks. The structure of a block is depicted in Figure 2.2 [1]. Three types of block metadata make up the block header. First, there is a reference to a previous block hash, a 256-bit hash value that points to the previous block in the blockchain and connects this block to the previous block. The timestamp and nonce, a 4-byte field that starts at 0 and grows with each hash calculation, are the second collection of metadata. The Merkle tree root hash, the hash value of all the transactions in the block and is used to summarize all the transactions in the block effectively, is the third piece of metadata.

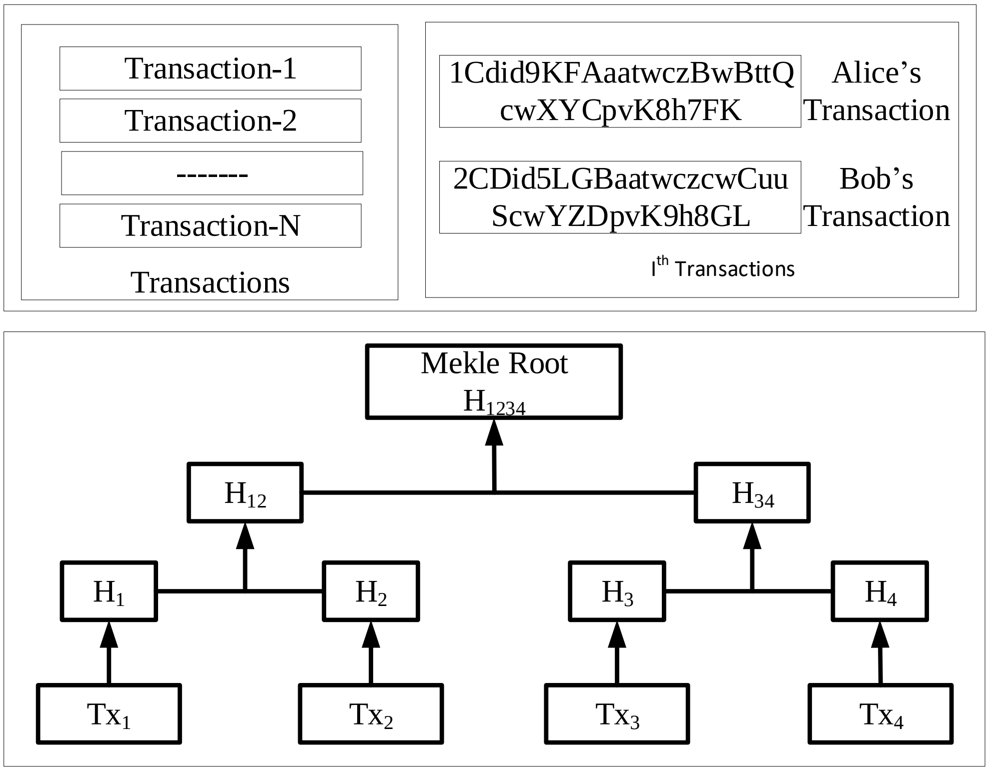


Figure 2.2: Structure of a block [1].

2.1.1 Taxonomy of blockchain systems

There are three types of blockchain systems currently in use: public blockchain, private blockchain, and consortium blockchain [38]. All records are available to the public in a public blockchain, and everyone can participate in the consensus process. On the other hand, a consortium blockchain will only allow a small number of pre-selected nodes to participate in the consensus process. When it comes to a private blockchain, only nodes from a single entity will be eligible to participate in the consensus process. Since it is entirely regulated by one entity, a private blockchain is considered a centralized network. Since only a small percentage of nodes are chosen to establish consensus, the consortium blockchain built by many organizations is partly decentralized [39].

All these three forms of blockchain infrastructure differs based on the following properties:

- Consensus process: The consensus mechanism of the decentralized blockchain may be joined by an entity from anywhere in the world. Both consortium and private blockchains are permissioned, unlike public blockchain. Every node in a public blockchain could participate in the consensus process. In a consortium blockchain, only a small number of nodes are responsible for validating the block. In the case of a private chain, it is entirely under the control of one entity, deciding on the final consensus process [37].

- Read permission: The primary distinction between public and private blockchains is that public blockchains are decentralized, and transactions are available to the public. In contrast, private and consortium blockchains allow the consortium or organization to determine if the stored information is public or limited [37].

- Immutability: It is almost impossible to tamper with transactions in a public blockchain since records are maintained on many participants. Transactions in a private blockchain or a consortium blockchain, on the other hand, can be tampered with [37].

- Anonymity : The key feature of public Blockchains is anonymity. In private and permissioned Blockchains identification is typically necessary for systems that are operated and controlled by known entities [37].

Satoshi Nakamoto was the first to propose the concept of blockchain in the seminal Bitcoin paper [1] in 2008 to address the double-spending problem in digital currency systems [40, 41]. The success of Bitcoin ignited an increase in interest in developing blockchain technology and applying it to various fields. The blockchain infrastructure is focused mainly on how consensus processes are applied. In today's blockchain networks, there are four basic consensus mechanisms, and they are Proof of Work (PoW) [42], Proof of Stake (PoS) [43], Practical Byzantine Fault Tolerance (PBFT) [44], and Delegated Proof of Stake (DPoS) [45]. Some blockchain systems also use a few other consensus mechanisms, such as Proof of Bandwidth (PoB) [46], Proof of Elapsed Time (PoET) [47], and Proof of Authority (PoA) [48].

Hyperledger Fabric [21] has recently gained interest in the implementation of various blockchain-based applications. Hyperledger is a permissioned blockchain that makes use of the Raft consensus algorithm [22]. Raft operates by having the cluster elect a leader. Raft is a consensus algorithm for maintaining a replicated ledger across every node. The raft has been described as crash fault tolerant (CFT). It achieves consensus by first appointing a prominent leader and then delegating complete control of the replicated log to that leader [22]. Since it is tokenless, anybody who is a participant of the blockchain infrastructure will participate in the consensus. Furthermore, it is non-resource intensive, decreases transaction fee costs, and improves performance. As a result, we use Hyperledger Fabric to incorporate our proposed contactless delivery system.

2.2 Blockchain for Traceability

The use of blockchain technology has been demonstrated for improving the healthcare segment in different regions [49]. Blockchain can be used in managing clinical trials as it can reduce the duration of the trial and ensure the patient records are transparent and traceable. It also helps in making data sharing more accessible and ensure that all regulations are followed. In medical supply chain management, blockchain can be used to track medical equipment and improve inventory planning [50]. Long supply chains provide unnecessary opacity, making forecasting and planning supplies difficult. Blockchain connects all entities in the supply chain and provides transparency and security; hence blockchain is well suited for the supply chain. It can be used to safeguard user privacy and does not share personal information widely and also enables users to exchange information on a case-by-case basis. A group of European privacy experts created a blockchain-based architecture for COVID-19 contact tracing via Bluetooth [49, 50]. Blockchain can also be used in the region of contact tracing [51, 52] and can help to keep track of the patient's movements [52]. Blockchain can also provide real-time information on contaminated areas and assists in the detection of virus-free areas [51, 52]. The coalition is a free app in the United States that allows users to keep track of their health. Other users are alerted to the possibility of interacting with an infected person. The solution tracks meetings using Bluetooth-enabled cryptography technology and generates anonymous random IDs to safeguard the user's identity, with all data saved locally on the user's phone [51].

Several researchers have indicated that blockchain technology be used to fix concerns related to the COVID-19 pandemic. These approaches can be categorized based on tracking technologies [53, 54] and using the tracked data to inform people about COVID-19 risks [54, 55, 49]. Furthermore, several blockchain frameworks have been suggested or introduced in supply chain management, such as Alipay's creation of a blockchain-based solution that enables humanitarian organizations to track and distribute relief supplies [50]. The transaction validation method can be accelerated because blockchain eliminates all third-party delegates and unavoidable delays in handling and processing. The VeChain network is one example of this accelerated process. Although partnering with production offices and facilities, the VeChain network ensures the credibility and reliability of new KN95 masks imported from China [56]. Every package shipped from China includes a VeChain NFT (non-fungible token) chip and a two-factor authentication QR code to verify the product's authenticity. To ensure that the masks are genuine, it tracks individual data such as product ownership and manufacturing position. The scan also reveals important details about the KN95 masks, such as manufacturing dates and locations, as well as logistical points in the supply chain.

The fact that blockchain can be programmed to adopt a decentralized architecture is one of the advantages of using it to store this data. Both organizations have the same permissions to access the blockchain information in a decentralized architecture. Many of the currently proposed systems, on the other hand, are based on a centralized infrastructure in which only approved users have access to data. Singapore's touch tracing solution, TraceTogether, is an example of this unified architecture. This application uses Bluetooth technology to keep track of possible coronavirus exposure amongst people [57, 58, 13]. The primary issue with these systems is that they violate user privacy. All Bluetooth-based communication tracing solutions are vulnerable to threats such as man-in-the-middle, sniffing, jamming, replay, and spoofing attacks due to Bluetooth's unreliable wireless interface.

A blockchain can be programmed to adopt a decentralized architecture is one of the advantages of using it to store data. Both organizations have the same permissions to access the blockchain information in a decentralized architecture. A blockchain-based approach with a decentralized architecture to solve this privacy problem is one example of previous work. A well-defined blockchain-enabled privacy-preserving trace enables an efficient communication tracing network by allowing information transfer without jeopardizing individual privacy. The BeepTrace framework [53] uses blockchain technology to provide encrypted and anonymous personal identification, allowing authorities and health care providers to notify individuals who may be at risk of infection as a result of contact with an infected person. To produce location data, the device uses two blockchains and a public key provided by the government or a public entity, as well as a diagnostician key to validate test results. The BeepTrace system uses blockchain technology to provide an encrypted and anonymous personal identity, allowing authorities and healthcare providers to reach out to people who may be at risk of infection due to contact with an infected person. The disadvantage of this method is that BeepTrace contact tracing solutions have high communication and server usage costs.

Chapter 3

Proposed Blockchain-based Contactless Delivery Framework

The current pandemic is causing major supply chain disruptions around the world. Industrial manufacturing has come to a halt, either due to a lockdown or because factories are not prepared or built to meet the modern social distancing model and to operate with minimal physical contact. Import and export bans have also affected the global supply chain. COVID-19's precise extent of instability in the global supply chain is difficult to determine at this time; however, it has resulted in severe supply and demand crises. There is either high demand or a high supply depending on the form of the product. An increase in demand for household essentials has resulted from panic purchasing. Likewise, medical equipment and pharmaceutical supply chains struggle to keep the entire chain intact and meet the high demand. In order to maintain "social distancing," we have become suspicious of physical touch. The need for shipping combined with the physical distance has resulted in a rise in demand for contactless parcel delivery, particularly for high-risk populations. Most post-delivery companies are now using contactless delivery more than ever before, and the process is now a proven workflow for them. According to Bloomberg, FedEx and UPS have scrapped the usual signature and authentication rules for most package deliveries in response to the Coronavirus pandemic. This is to protect consumers and delivery personnel. As the COVID-19 pandemic maintains its grip on many parts of the world, standard life patterns have become radically altered. A few months ago, most of us would not have given a trip to the grocery store or dining out with friends a second thought. Now, the simple act of going out to run a few errands has become an ordeal. That is why many people around the world have decided it is easier to shop online. Blockchain technology can help create a more resilient supply chain. All stakeholders can be anonymously linked with blockchain, creating a trustless climate. Immutable data logs support auditability, provenance, and accountability, while smart contracts with well-designed access constraints and automation provide a high degree of security and automation.

Before the pandemic, online shopping had been on the rise for years. The E-commerce market share increased to 16 percent in 2019, up from 14.4% in 2018 and 13.2% in 2017. With governments urging people to restrict their travel and follow social distancing guidelines, it is no wonder that e-commerce has exploded in popularity. In March and early April, online spending in the United States increased by 30% over the previous year, a substantial improvement over the 20% year-over-year rise seen in recent years. Consumers who want to avoid risking a trip to potentially crowded shopping centers have turned to online shopping, but many are searching for even more protection. As a result, contactless and touchless delivery solutions are becoming increasingly popular. Fast food and other delivery dining options have become the most common, However, it is now being introduced across various items, from prescription drugs to new cars. The pandemic of COVID-19 has ignited an increase in demand for easy-to-use online shopping options that allow people to avoid taking unnecessary risks. Contactless delivery is a modern delivery system that enables packages to be sent and received without being physically present. To ensure even greater protection, companies in the delivery supply chain should monitor not only packages but also possible locations in the supply chain where coronavirus exposure may have occurred. There is a need for a system that can log and transmit this information while protecting the users' privacy. For various service providers, delivery personnel, and consumers, we suggest using a blockchain-based architecture to provide a contactless delivery system for tracing delivery traces and the medical status of the delivery personnel.

The proposed blockchain framework's primary stakeholders are service providers, delivery personnel, and consumers. Each key member(node) must create and maintain their identity (i.e., address, account, or participant's identity) in the system. To ensure supply chain transparency, the service provider must monitor the blockchain ledger for any changes between the time an order is placed and the time it is delivered. If a difference exists, this will help [23]. A blockchain transaction has a target smart contract feature, a payload containing input values to the function call, and is always signed by the submitter. Smart contracts are used to execute the underlying functionalities, such as data storage and management. Smart contracts are code lines stored on a blockchain that is automatically executed when predetermined terms and conditions are met. The blockchain nodes execute these smart contracts by processing transactions submitted by the user. This can be achieved as an on-chain or off-chain operation.

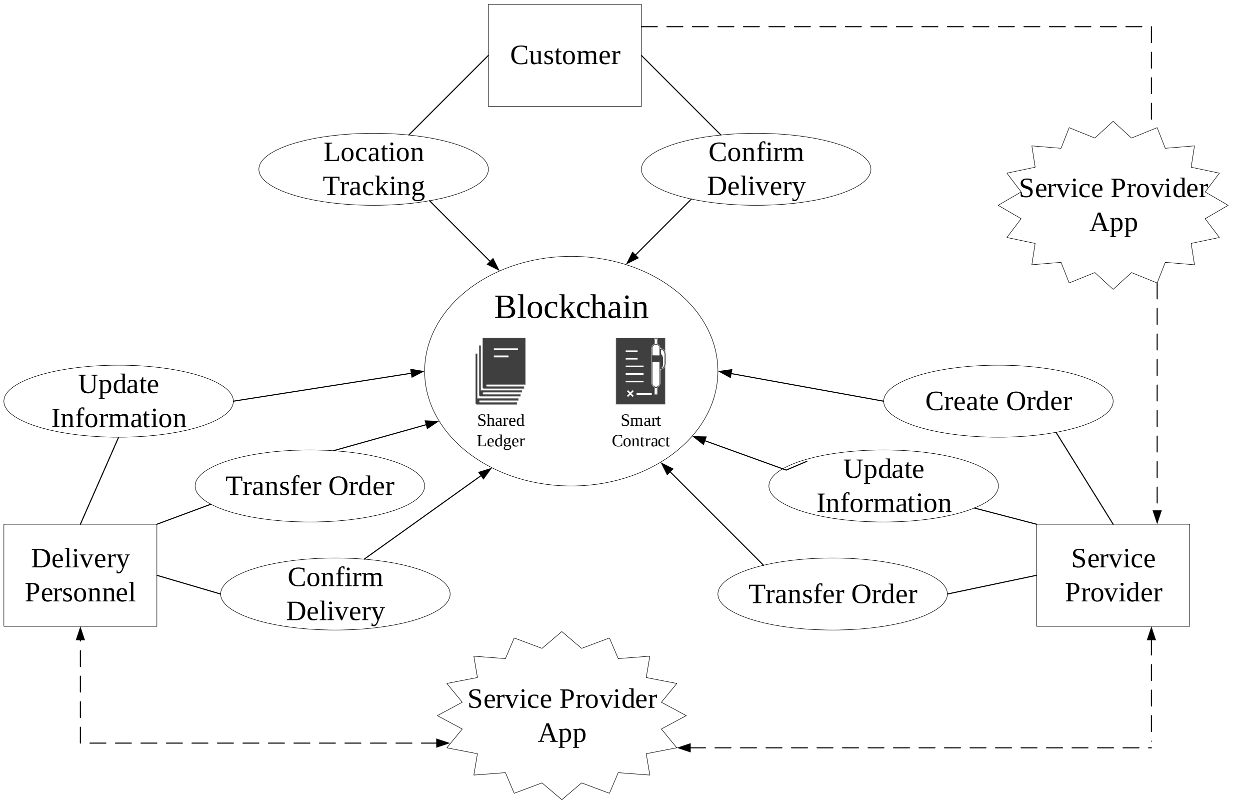


Figure 3.1: The proposed approach for our blockchain-based contactless delivery system.

3.1 Architecture of the proposed blockchain-based framework

In our proposed infrastructure, we use Hyperledger Fabric. The Hyperledger fabric's architecture is highly scalable and configurable, allowing for creativity, flexibility, and optimization across a wide variety of industries, including banking, finance, insurance, healthcare, human resources, supply chain, and even digital music delivery. This platform is also permissioned, which means that, unlike a public permissionless network, users are identifiable to one another rather than anonymous and therefore completely untrustworthy. Although participants do not completely trust one another, a network may be run under a governance model based on the trust that does exist, such as a legal agreement or a mechanism for resolving disputes. Hyperledger Fabric allows for plug-and-play modules such as consensus and membership services. Hyperledger Fabric enables various entities in a network to use their certificate authority and, as a result, incorporate a variety of cryptographic algorithms for signing, verifying, and attestation of identity. This is accomplished using an Membership Service Provider (MSP), which is a part of the Hyperledger Fabric that abstracts membership operations. All the cryptographic protocols and mechanisms involved in issuing certificates, validating certificates, and user authentication are performed by an MSP. An MSP defines its definition of identity and the rules that validate and authenticate those identities [59]. Hyperledger Fabric's adaptable and modular architecture makes it suitable for a wide range of industry applications. It employs a novel consensus approach that allows for scalability while preserving privacy.

In our architecture, we use Hyperledger Fabric along with the non-resource intensive consensus algorithm Raft. The Raft consensus algorithm is a distributed crash fault tolerance algorithm that ensures the system can decide and process client requests in the event of a failure [22].The Raft protocol employs a "leader and follower" model, in which a channel's ordering nodes dynamically elect a leader, who then replicates messages to the follower nodes. The three states of raft nodes are always follower, candidate, or leader. First, every node acts as a follower. If the leader has been elected, the follower can accept the log entries sent by a leader. However, in case there is no leader, elected followers can cast votes for a leader. Nodes self-promote to the candidate state if no log entries or heartbeats are obtained for a fixed period. Nodes in the candidate state ask for votes from other nodes. If a candidate receives a majority of votes, it is elevated to the position of leader. The client sends a command to the leader node in a request. Then the dominant node logs the request and sends it to all follower nodes. The request will be appended to the follower node's log, and a confirmation message will be sent. The command log will be sent to the managed state machine once the leading node has received most of the confirmation messages from the following nodes. The follower node will send the log to the state machine it manages once the leading node has done so. The result is sent to the client by the dominant node. Raft can be described as a replicated log management consensus algorithm, which ensures that followers' logs are identical to the leader's logs, allowing the entire distributed system to function as a single entity even in the event of a failure.

The main members of our blockchain-based system securely record order information, delivery traces, and medical status in the blockchain while monitoring each delivery personnel's delivery traces and medical status in a private manner. As shown in Figure 3.1, our proposed framework allows customers may submit an order to a service provider, who will then update the blockchain with all relevant details about the order. The delivery personnel then updates the blockchain with details about the package's status and delivery locations after the service provider's information has been published. There are two functions that are not shown in Figure 3.1: delete order and edit order. These two features are only accessible to the service provider and can only be used if the customer requests them. The customer can access the blockchain at any point during the process to 1) check the position of the delivery personnel and 2) view any details about possible coronavirus exposure. In this section, we will focus on the details and implementation of the proposed framework. We implement the proposed framework using the following steps:

3.1.1 Create Order

The calling entity will use this function to build and upload a new order to the blockchain. The service provider is the only one who can call this function. The service provider should simply concatenate the current date with the customer's last name and pass through this function to create the order ID. Furthermore, the service provider is responsible for uploading the health status of the delivery personnel assigned to the order. The *createOrder()* function checks to see whether the caller of this function is a valid entity, based on a predefined set of access policies(Figure 3.2) after the order number is generated and the health status of the delivery personnel is obtained. The order ID, entity uploading the order, item information and availability, delivery personnel details, and customer details will all be successfully uploaded to the blockchain if this passes. Several major restaurant chains, for example, have begun offering delivery services. To ensure safe delivery during a pandemic, our proposed blockchain-based system will be a priceless asset for these restaurants and restaurant chains. Restaurant workers will accept food delivery requests from customers and upload the order, and destination information to the blockchain using the *createOrder()* functions.

3.1.2 Update Information

The *update()* function is used to update the details on the blockchain for delivery personnel. The ID number of the delivery personnel and their current location are passed as arguments to this feature. The service provider can use the *update()* feature to update the delivery personnel's ID number and pick up location in a blockchain transaction. To protect the privacy of the delivery personnel, a unique identification number will be used to link them to the order. The employee ID number of the delivery personnel, for example, may be used. Only the delivery personnel and their manager will be able to link the number to the correct person. The delivery personnel uses *update()* to include all locations they stop at on the delivery route when delivering. If delivery personnel is sick, the service provider may track down all of the stops along the route and isolate anyone who might have been exposed. The customer can keep track of this information by querying the blockchain to see if the order has been exposed to any contamination. This function generates a new block containing the modified information and connects it to the order block since the ledger is immutable. The restaurant will then choose an employee to deliver the food after the order has been verified. The health status of the delivery person will need to be submitted to the blockchain using the *update()* feature, as most dining establishments already require their employees to undergo daily health screenings. The location of each stop will be uploaded into the blockchain using the *update()* function if the delivery personnel has several stops on their route for multiple deliveries.

3.1.3 Transfer Order

A function in our system is used to transfer ownership of an order from one entity to the next. To transfer order, the current owner effectively hands it off to the next person in the delivery chain. The service provider is the initial owner, and the order is then transferred to the delivery personnel. The order will be passed to the customer when the delivery personnel is able to deliver it. The order ID and information about the new owner are passed as arguments to the *transferOrder()* feature. This function can only be used by the service provider and delivery personnel, according to our access policy. This function, when called, instructs our smart contract to switch the current owner to the new owner. The *transferOrder()* function adds protection to the supply chain by allowing backtracking to find out where a package went missing or was stolen. In addition, the transfer order function ensures non-repudiation by allowing users to monitor the item's official ownership at each stage of the delivery chain. For instance, after assigning delivery personnel to deliver the food, a restaurant uses the *transfer()* function to transfer ownership of the order to delivery personnel. When the order is delivered to the customer, delivery personnel uses the *transfer()* function the ownership of the order is transferred to the customer.

3.1.4 Confirm Delivery

Receiving confirmation that the order has been completed is the final stage in our framework. Since our system is based on a contactless delivery system, it is the customer's duty to verify that the delivery has been completed. The customer can use the *setDelConfirmation()* function to accomplish this. As arguments, this function accepts the order ID, transfer confirmation , and delivery location. The arguments will be compared to their intended order ID, transfer confirmation, and delivery location values when this transaction occurs. If the information is right, the delivery will be deemed effective, and the transfer's status will be updated on the blockchain. Otherwise, the blockchain data can be used to trace a problem back to its source. Furthermore, the customer cannot demand the order's creation to the service provider by confirming delivery. Since we are establishing a contactless system, the delivery person will place the food on the customer's doorstep, inform them of their delivery, and then proceed with further deliveries as usual. Even the delivery personnel does the delivery confirmation using the *setDelConfirmation()* function. Only when both delivery personnel and customer confirms the delivery then only the order delivery will be completed. The customer must use the *setDelConfirmation()* function to confirm that they received the food.

3.1.5 Location Tracking and Health Monitoring

The customer and service provider may use the *getTrace()* and *getMedStatus()* functions to monitor the delivery personnel's position and health status. Both of these functions are functionally identical and take the same argument: order ID. When the function is named, it will immediately query the blockchain for the function being used and return either the location information or the medical status of the delivery personnel. In the case of an infection, contact tracing may be used to map a possible infection route in the delivery system by tracking the location and medical condition of the delivery personnel. Contact tracing would allow the service provider to identify all delivery personnel that was involved with the same route and remove them from the delivery options. This also allows the customer to be aware if their package could be contaminated and then take necessary precautions to protect themselves. In addition to consumer protection, the delivery personnel's privacy is protected because they are only identified by an identification number. The customer may use the *getMedStatus()* and *getTrace()* functions to query the blockchain for details about the delivery person's health status and location at any time after placing the order. This is advantageous because if a cust6omer became sick after delivery, they could search the blockchain to see if the delivery personnel is sick. This will also allow the restaurant to keep an eye on the blockchain and contact customers who may have been served by infected delivery personnel, and track down any other delivery personnel who may contact the sick one.

3.1.6 Delete Order

If a customer places an incorrect order or no longer requires it, they may ask the service provider to delete it. If the service provider agrees, the customer's order will be removed by calling the *delOrder()* function. Only the order ID is passed as an argument to this function. Only if no delivery personnel has been assigned to the order can it be removed. There is no way to delete an order that has already been transferred to delivery personnel. We ensure that no intermediary entities can remove the order and then steal the package by restricting access to this function to only the service provider.

3.1.7 Edit Order

If the customer wants to change some of the order's information, they may ask the service provider to do so. If the service provider accepts the request, they may use the *editOrder()* function to start a transaction. This function can only be called by the service provider. The order ID and the customer's details are passed as arguments to this function. There is no way to change an order that has already been transferred to delivery personnel.

By limiting access to this request to only the service provider, any adversaries are prevented from maliciously altering information about the order, possibly resulting in a lost or stolen delivery.

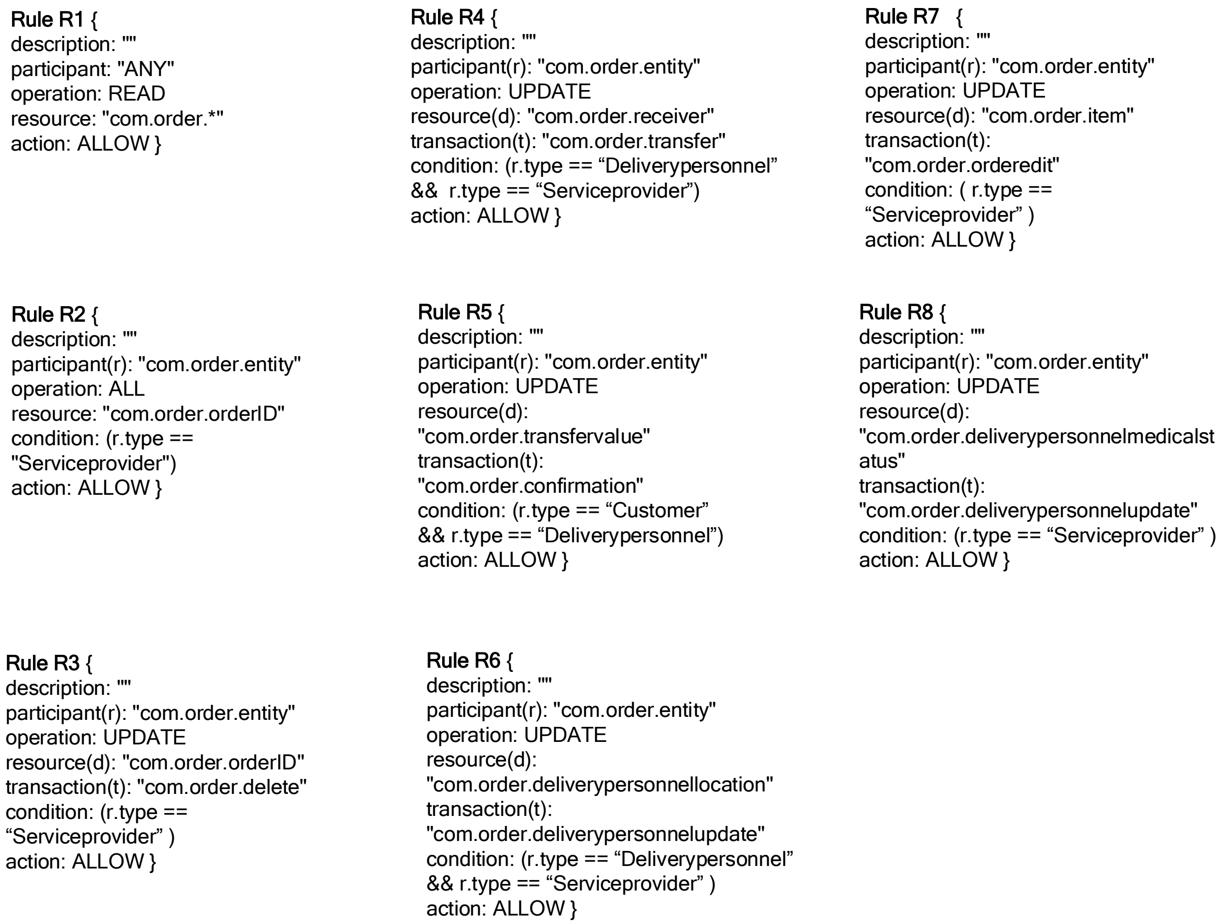
3.2 Usage in the Service Industry

Many restaurants were forced to innovate to raise sales after dining rooms were forced to close across the country in March. According to research by the financial services firm Rewards Network, a substantial portion (42%) added delivery. According to Rewards Network, 31% said they intended to continue investing in the program, indicating that they believe demand for delivery will remain stable. Grubhub's average order size during the second quarter was $39, up 20% year over year, according to a letter to shareholders sent in august 2020. For example, in June 2020, the average DoorDash order was about $36 compared to $33 in January 2020. To reduce the chance of person-to-person transmission for both customer and the delivery personnel, customers request contactless delivery, in which couriers drop off the food at customers door or a specified location without any personal interaction. Due to concerns about the coronavirus, a growing number of food and grocery delivery services in the United States are giving option to the customers to have their orders left at their doorstep. As people skip public transportation and focus on home delivery instead of visiting restaurants and supermarkets, delivery personnel who offer rides and deliver grocery or restaurant orders are on the front lines of the coronavirus epidemic. McDonald's, Starbucks, KFC, and Pizza Hut have all introduced contactless delivery systems in an effort to reduce coronavirus transmission from person to person [60, 61].

Food distribution is arguably one of the most desired facilities during a pandemic. To monitor the status of orders, several large restaurant chains have introduced some kind of delivery service. Unfortunately, none of them provide any detail about the delivery personnel's COVID-19 exposure. Our proposed architecture, on the other hand, would provide a scalable system that can serve both large restaurant chains and smaller restaurants. As a result, our proposed blockchain-based framework would be an invaluable tool in ensuring safe delivery during a pandemic for these restaurants. Our framework would allow the service providers to set up a delivery system that is safe and secure. Also, they could monitor without the help of any third party. Using the *createOrder()* and *update()* functions listed in Section 3.1, restaurant personnel will be able to accept food delivery requests from customers and after assigning the delivery personnel upload the order and delivery location information to the blockchain. Customers will be able to monitor the status of their orders as well as their location using these functions. The restaurant will then pick an employee to deliver the food after the order has been established. The health status of the delivery person will simply need to be submitted to the blockchain using the *update()* feature, as most dining establishments already require their employees to undergo daily health screenings. The location of each stop will be uploaded into the blockchain using the text update() function if the delivery person has multiple stops for multiple deliveries on their path. If they become sick afterwards, the restaurant will notify those on the delivery route, as well as the employees, that they were possibly exposed. Since we are creating a contactless system, the delivery person will simply place the food on the customer's doorstep, inform them of their delivery, and then proceed with other deliveries as normal. When the customer receives the food, they must use the *setDelConfirmation()* function to confirm that they received it. The customer may use the *getMedStatus()* and *getTrace()* functions to ask the blockchain for details about the delivery person's health status and location at any time after placing the order. This is advantageous since, if a customer became ill after delivery, they could search the blockchain to see if the delivery personnel is sick as well. This will also allow the restaurant to keep an eye on the blockchain and reach out to customers that were possibly served by an infected delivery person, as well as track down any other delivery personnel who may have come into contact with the sick one.

3.3 Access Control

By associating a Policy with a resource, the fabric uses access control lists (ACLs) to manage resource access. Policies are essential to the operation of fabric because they enable the identity (or collection of identities) associated with a request to be compared to the policy associated with the resource required to complete the request. Endorsement policies are used to decide whether a transaction has been endorsed correctly. The policies specified in the channel configuration are referenced as both alteration and access control policies, and they are defined in the channel configuration itself. We use an access control policy to regulate and protect the operations in the blockchain system. They are controlling which individuals are required to perform which operations are possible with access control. Figure 3.2 depicts the main access control policies of our prototype framework. The policies are enforced to give access to the operations; otherwise, the entity will be denied access. The policy $R1$ allows all users to read all of the blockchain's resources. Only the service provider has access to $R2$, which allows him to create, change, and delete orders. This is to keep the blockchain system's operations secure. Only the service provider can delete an order with $R3$, while both the service provider and the delivery personnel can transfer ownership of an order with $R4$. Both service providers and delivery personnel handle transfer operations; hence, both service providers and delivery personnel can access the transfer operation. Both the customer and delivery personnel can confirm the item's delivery with $R5$. The order delivery will be considered only when both customer and delivery personnel provide confirmation. Only the delivery personnel and the service provider can change the location of the delivery personnel with $R6$. Only the service provider has access to $R7$ and $R8$, which allow only the service provider to update the order information and the health status of the delivery personnel, respectively. This is to track and trace the location and medical status of the delivery personnel. Despite the fact that $R6$ and $R8$ refer to the same feature, $R8$ is used to prevent delivery personnel from updating their own medical status. This rule is in place to ensure that the medical condition being updated is accurate and to avoid illegitimate information.



```
Rule R1 {
description: ""
participant: "ANY"
operation: READ
resource: "com.order.*"
action: ALLOW }
```

```
Rule R2 {
description: ""
participant(r): "com.order.entity"
operation: ALL
resource: "com.order.orderID"
condition: (r.type ==
"Serviceprovider")
action: ALLOW }
```

```
Rule R3 {
description: ""
participant(r): "com.order.entity"
operation: UPDATE
resource(d): "com.order.orderID"
transaction(t): "com.order.delete"
condition: (r.type ==
“Serviceprovider” )
action: ALLOW }
```

```
Rule R4 {
description: ""
participant(r): "com.order.entity"
operation: UPDATE
resource(d): "com.order.receiver"
transaction(t): "com.order.transfer"
condition: (r.type == “Deliverypersonnel”
&&  r.type == “Serviceprovider”)
action: ALLOW }
```

```
Rule R5 {
description: ""
participant(r): "com.order.entity"
operation: UPDATE
resource(d):
"com.order.transfervalue"
transaction(t):
"com.order.confirmation"
condition: (r.type == “Customer”
&& r.type == “Deliverypersonnel”)
action: ALLOW }
```

```
Rule R6 {
description: ""
participant(r): "com.order.entity"
operation: UPDATE
resource(d):
"com.order.deliverypersonnellocation"
transaction(t):
"com.order.deliverypersonnelupdate"
condition: (r.type == “Deliverypersonnel”
&& r.type == “Serviceprovider” )
action: ALLOW }
```

```
Rule R7   {
description: ""
participant(r): "com.order.entity"
operation: UPDATE
resource(d): "com.order.item"
transaction(t):
"com.order.orderedit"
condition: ( r.type ==
“Serviceprovider” )
action: ALLOW }
```

```
Rule R8 {
description: ""
participant(r): "com.order.entity"
operation: UPDATE
resource(d):
"com.order.deliverypersonnelmedicalst
atus"
transaction(t):
"com.order.deliverypersonnelupdate"
condition: (r.type == “Serviceprovider” )
action: ALLOW }
```

Figure 3.2: Access Control Policies.

Chapter 4

Results and Discussions

Our proposed architecture will include a contactless, safe delivery system. It is cost-effective for small businesses while still being flexible for larger companies. We provide quantitative evidence for the success and implementation of our framework in this section. We will also discuss how we keep our system protected and secure for everyone involved.

4.1 Performance Evaluation

The method of evaluating the performance of a system under test is known as performance evaluation. This evaluation can include system-wide metrics like response time or latency and activity-specific metrics like the time it takes to write a block to persistent storage. Any performance evaluation aims to comprehend and record the system's or subsystem's performance [62]. Benchmarking is a method of comparing one system to another or to previous measurements of the same system. As a blockchain benchmark tool, Hyperledger Caliper [63] is used.

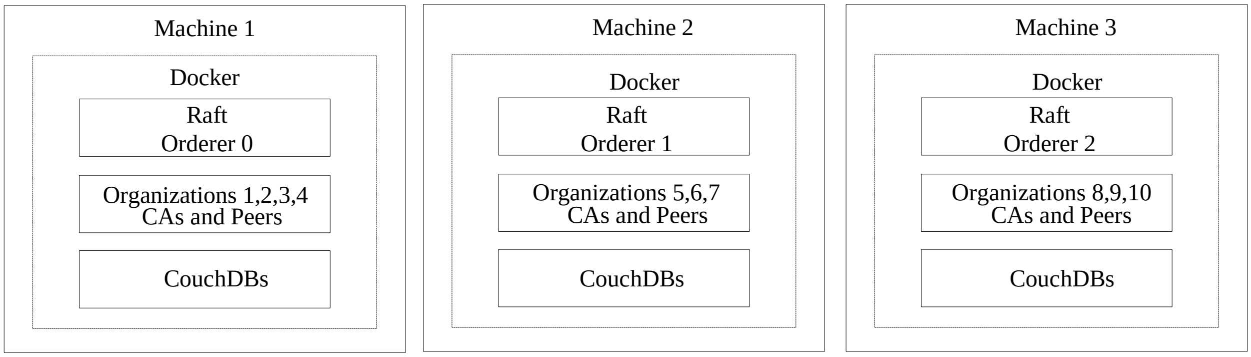
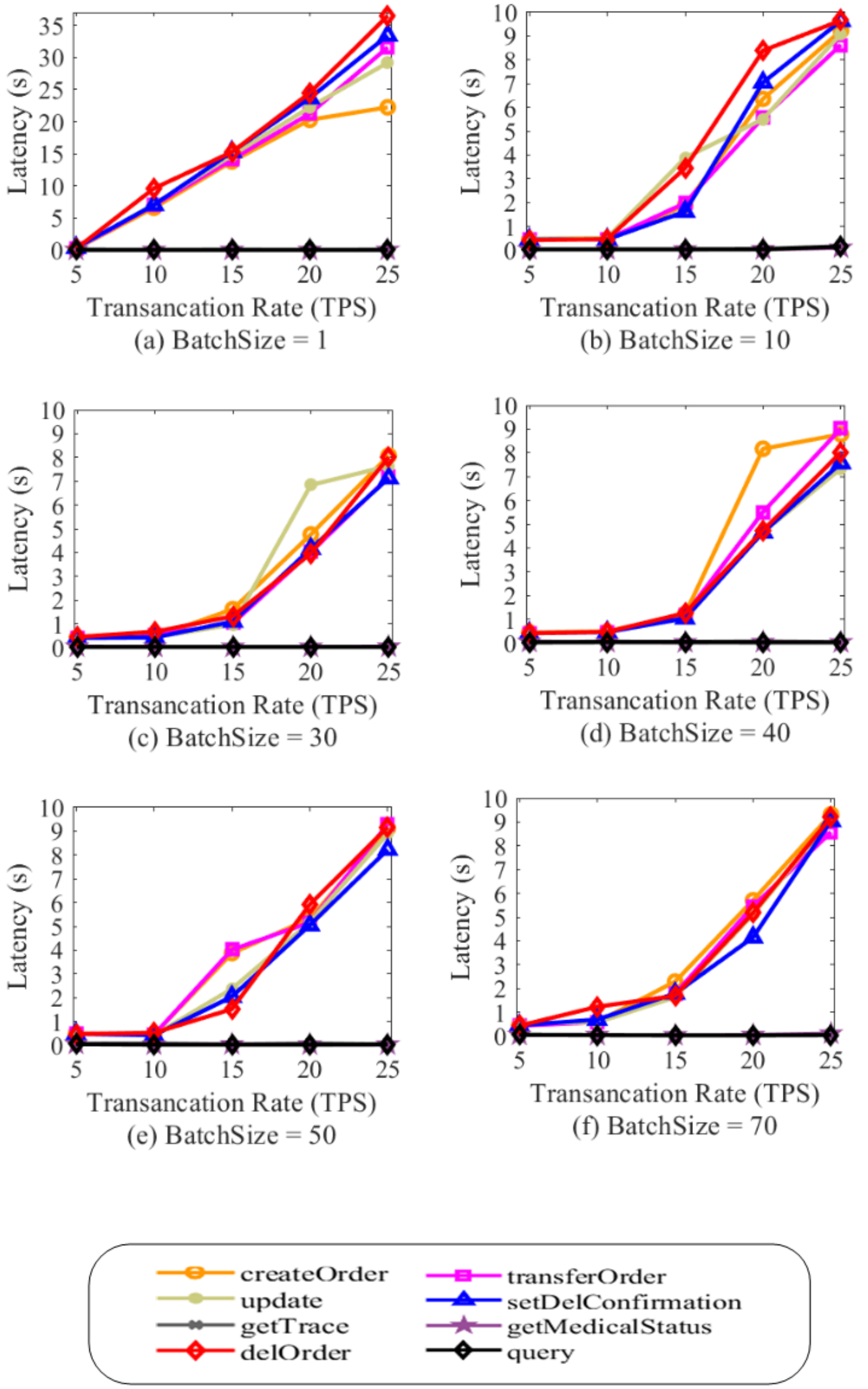


Figure 4.1: Implementation of proposed Blockchain-based framework

We assessed throughput and latency to assess our proposed blockchain-based system. For our testing environment, we used three desktop computers, each with an eight-core processor and 16GB RAM. Using Hyperledger Fabric 1.4.1 docker containers and CouchDB state databases, we created ten organizations in a single channel [64]. We deployed three simulated customers using Raft on our three machines. We simulated five service providers on machine one to create the orders. Figure 4.1 depicts the implementation of the proposed blockchain based framework.

By stressing our system with varying transaction rates and batch sizes, we were able to evaluate its latency and throughput. To see how these variables impact our framework's end-to-end latency and throughput, we used batch sizes of 1, 10, 30, 40, 50, and 70 transactions and transaction rates of 5, 10, 15, 20, and 25 transactions per second. Figure 4.2 depicts the latency of various functions during various transactions of varying batch sizes. We can see that as the number of transactions per second grows, the latency grows as well. In addition, our findings show that increasing batch size reduces latency. For a batch size of 1, the relationship between latency and transaction rate is basically linear. In the range of 15 to 20 transactions per second, the latency significantly increases for batch sizes greater than one. The number of blocks in which the transactions were packaged and committed can explain the increase in latency. When the batch size is increased from 1 to 10 transactions, the difference between the number of blocks committed is small, compared to the difference between the number of blocks when the batch size is increased from 30 to 40 transactions.

Figure 4.3 indicates throughput with different transaction rates of 1, 10, 30, 40, 50, and 70 transactions per second and different batch sizes of 5, 10, 15, 20, 25 transactions per second. The throughput grew linearly as the transaction rate increased. As batch size grows, there are more transactions per block, resulting in a reduction in the total number of blocks. This is what helps the throughput to grow in tandem with the transaction rate. As a device reaches its maximum capacity, throughput stays fairly constant as the number of concurrent transactions grows. The throughput increased linearly as the number of transactions per second increased until it reached saturation. This means that all peer blocks were full, and the container's CPU and disk I/O were being used up.



(a) BatchSize = 1

(b) BatchSize = 10

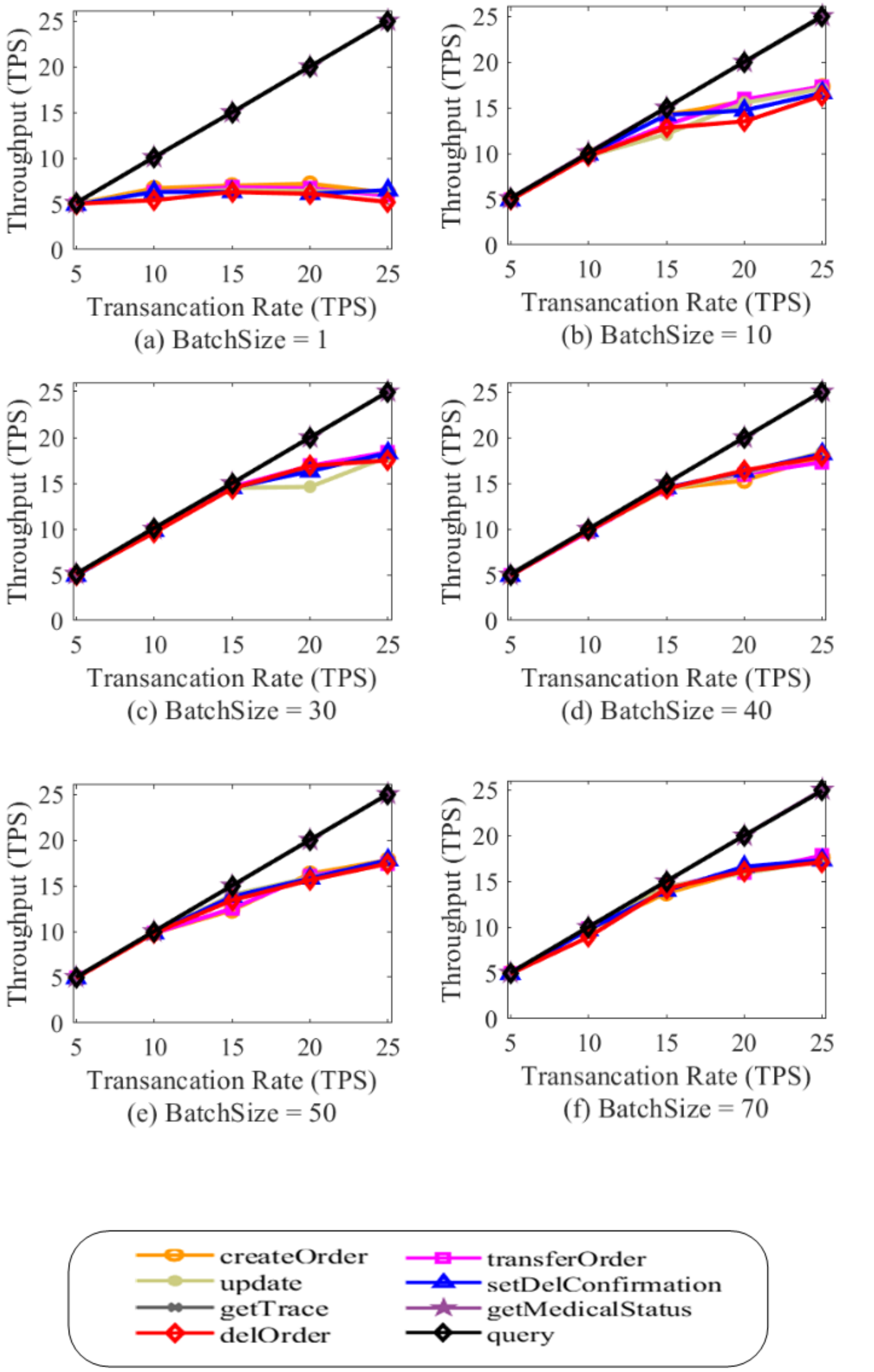
(c) BatchSize = 30

(d) BatchSize = 40

(e) BatchSize = 50

(f) BatchSize = 70

Figure 4.2: Latency versus transaction rate with different batch sizes.



(a) BatchSize = 1

(b) BatchSize = 10

(c) BatchSize = 30

(d) BatchSize = 40

(e) BatchSize = 50

(f) BatchSize = 70

Figure 4.3: Throughput versus transaction rate with different batch sizes.

We need to consider what each function does in order to clarify the difference in function linearities on our graphs. The *createOrder()*, *update()*, *transferOrder()*, and *setDelconfirmation()* functions read and write on blockchain, while the *query()*, *getTrace()*, and *getMedicalStatus()* functions are read-only. We see similar throughput and latency behaviors for functions that perform both read and write operations. The functions that use read-only operations, on the other hand, have lower latency than the read and write functions. The read and write latency increases linearly for the read and write functions in the trial with a batch size of 1. The latency of all other block sizes is less than 9 seconds. As previously stated, as the transaction arrival rate increased, the throughput increased linearly until it flattened out around the saturation stage. The peers then became saturated, absorbing all of the container's available CPU and disk I/O. When our transaction rate hits about 25 transactions per second, we note a bottleneck in throughput. According to our findings, 30 transactions have the best combination of low average latency and high average throughput. Network delay, consensus delay among multiple orderers, chaincode execution time, endorsement delay, and block validation delay are all factors that affect performance.

Our framework implementation aims to show how a blockchain-based system can track the coronavirus exposure of a delivery personnel, which helps limit the spread of COVID-19. Despite the current performance climate, our proposed architecture may still function properly. Pongnumkul et al. [65] compared the efficiency of Ethereum and Hyperledger Fabric as private blockchain networks with differing numbers of transactions and found that Hyperledger Fabric has a higher throughput and lower latency than Ethereum. Hence, we found Hyperledger Fabric more preferable for our implementation. Thakkar et al. [66] showed that the throughput increased linearly as predicted with an increase in transaction arrival rate until it flattened out at around the saturation point of 140 tps. The latency increased dramatically when the arrival rate approached or exceeded the saturation stage. Similarly, latency increases linearly as the number of transactions per second increases in our system. In addition, throughput increased linearly until it flattened about 25 tps. Our framework is set up to run on a single channel. The total machine throughput should be proportional to the channel numbers at all times. The throughput improved as the number of channels increased and the latency decreased [66]. Hence, our result observation shows that our framework is feasible for a variety of applications. We can further optimize the performance of our framework to scale up. Furthermore, growing computing capacity, modifying endorsement policies, and using a different state database could help to improve system efficiency [66].

4.2 User Privacy

To protect consumer privacy, it's critical to keep the health-related data of delivery personnel safe. Our system requires service providers and delivery personnel to keep track of delivery locations as well as the medical status of the delivery personnel. Since it is based on blockchain technology, our proposed architecture guarantees reliable supply chain provenance and protects the privacy of all parties concerned. Our system ensures delivery personnel's privacy by associating them with a unique identification number rather than a personal name since they are expected to provide confidential details to the service provider (i.e., a regular health check). Our system does not require the service provider or delivery personnel to upload the name of the delivery person in order to protect the medical privacy of the delivery personnel. Instead, each participant will be given a unique identifier. The delivery personnel will be assigned a unique identification number randomly for that day. The next day a different unique identification number will be assigned to the delivery personnel. Only the service provider will know the mapping between the unique identification number and the delivery personnel. Only their identification number is stored in the blockchain to protect the privacy of delivery personnel. When a customer inquires about the delivery person's location or medical status, they can only see the person's ID number and the details they are querying. The mapping between ID and person will be known only by the service provider and the person who delivers the service.

4.3 Security and Reliability of the Framework

One of our proposed blockchain-based framework's objectives is to track delivery personnel's traces in the supply chain. This is essential in order to set up a contact tracing system if the delivery personnel are infected. It is important to assess the framework's security in order to ensure that the data stored in our blockchain is safe and cannot be tampered with. We must ensure that the entities involved are unable to maliciously interfere with any of the blockchain data, in addition to blockchain protection. Only registered users have access to the blockchain because it is a permissioned blockchain. We also use an access control policy to grant and limit write access to the various parts of our framework's database. All entities can read the data, but only a few can write it. Even with permissioned entry, one might argue that our system has two distinct concerns: illegitimate medical test results and illegitimate location information.

4.3.1 Illegitimate Medical Test Result

It is really important to have correct health related data of delivery personnel. As customer and service provider needs to take risk-informed decisions depending on delivery personnel's medical status. Suppose delivery personnel turns out to be COVID positive. In that case, one can trace the medical status of the delivery personnel from the blockchain and take the risk-informed decision and inform the customers accordingly. When an employee provides an inaccurate COVID-19 test report to the service provider accidentally or intentionally, it may result in an invalid medical result updated to the blockchain. The test must be official and checked by an authentic institution, such as a hospital or a COVID-19 test center, to answer this issue. The service provider will not upload the test result to the blockchain until the results have been confirmed. Furthermore, by introducing a separate blockchain function specifically, for this reason, medical test results could be validated by approved officials. We may introduce additional functions to remove or change the data if an incorrect medical test is submitted to the blockchain. We would set up a new access policy provision to limit access to these functions to only trusted individuals. Delivery personnel will go through daily health check screening and provide the medical test result to the service provider. The only service provider will be allowed to update the delivery personnel's test result to the blockchain. Our access policy will prevent editing its medical status. This will prevent the updation of delivery personnel's incorrect COVID-19 test results to the blockchain.

4.3.2 Illegitimate Location Information

In the blockchain, an illegitimate update of delivery personnel location information happens when a permissioned user updates the incorrect location information, either accidentally or on purpose. If delivery personnel by mistake or intentionally updates wrong delivery location information, then it creates a discrepancy. The customer will claim that the order is not delivered. In that case, we need to trace back the delivery personnel's location. We implement location checking into our blockchain-based architecture to account for this possibility. We need a transaction to update the current location of the transfer when an order is (*i*) transferred from owner to owner or (*ii*) transferred to the customer. If a service provider is transferring an order to a delivery person, the service provider updates the blockchain with their current location. To avoid an invalid location update, this should match the current expected location of the order. When the package is delivered, the delivery personnel must also update their current location, which will be compared to the expected location. The customer can eventually update their current location after receiving the order, which will be compared to the (*i*) original order delivery address and (*ii*) location that the delivery personnel uploaded for the order transfer. If there are any inconsistencies in place, checking the blockchain records is an easy way to figure out where the problem started. A red flag will be raised in case of a discrepancy that the delivery personnel is not at the delivery location. In that case, the service provider can query the blockchain and see if the delivery personnel's location is not the same as that of the expected delivery location. Then service provider can question the delivery personnel about what went wrong. This feature avoids the updation of wrong delivery personnel location update to the blockchain. This will help in building a proper safe, and secure contactless delivery system.

4.4 System Usage during Post COVID-19 Pandemic

Demand for delivery services has increased as a result of the pandemic. Online delivery has become a part of the daily life of customers. Even after the COVID-19 pandemic gets over, the requirement for contactless delivery will persist. Customers' safety is a primary priority and will continue to be a source of concern. The vaccination information of delivery personnel can also be updated to the blockchain to make the system more secure in a contactless way. If the vaccination information is added, our architecture will help in having a more safe and secure contactless delivery system. Our framework can be used to assist local businesses in developing and operating a safe and reliable contactless delivery system, even though the world is not in the grip of a pandemic. Our framework can be used to enable local businesses to build and manage a safe and secure contactless delivery system even though the world is not in the grip of a pandemic. Because of the ease, customers would most likely become accustomed to using delivery services. More companies would be able to survive and remain in operation for longer periods of time if they are allowed to continue serving consumers regardless of whether or not there is a crisis. Our architecture can be used in the future since it provides a safe and secure solution for contactless distribution.

4.5 Future Research Direction and Conclusion

With blockchain, we can securely and immutably exchange any transaction/information in real-time between related parties present as nodes in the chain. Blockchain technology has several applications that could help with the current pandemic crisis. While it may not prevent the emergence of new viruses, it can be used to establish the first line of rapid defense by connecting a network of connected devices whose primary purpose is to stay alert about disease outbreaks. As a result, the use of blockchain-enabled systems will aid in the prevention of pandemics by allowing for early disease identification, rapid drug trials, and effective management of outbreaks and treatment [67]. Companies in the delivery supply chain should track shipments and potential locations in the supply chain where coronavirus exposure might have occurred to ensure even greater safety. A system that can log and transmit this information while protecting the users' privacy is needed. Existing blockchain-based approaches can be classified based on how they use monitoring technology and how they use the collected data to warn people about COVID-19 threats. Existing strategies, on the other hand, have some flaws. Some methods are expensive in terms of connectivity and server use, and some Bluetooth-based solutions are vulnerable to adversarial attacks. We propose using a blockchain-based architecture to provide a contactless delivery system for tracing delivery traces and the medical status of delivery personnel for different service providers, delivery personnel, and customers.

The emphasis of future research will be on adding vaccination information to the blockchain for the delivery personnel. To minimize the spread of Covid-19, most countries are now providing COVID-19 vaccines to their citizens as soon as possible. Vaccination helps to prevent the transmission of coronavirus. Keeping distribution personnel's vaccine records up to date would help to prevent the spread of COVID-19. Additional work can be done to add the delivery proof to the blockchain. This will help when the customer raises a missing order request if delivery personnel updates the delivery proof, like taking pictures after keeping the packet at the customer's door. In that case, the service provider can trace the delivery proof and prove that the order was correctly delivered at their door. On the other hand, if there is no delivery proof, the service provider can question the delivery personnel about the discrepancy.

In conclusion, we have presented a blockchain-based framework to provide a secure and safe contactless delivery system for COVID-19 and other pandemics.For each order created and delivered in the framework, one could track delivery personnel's medical test status, a trace of travel of delivery personnel to different locations. All the service providers, delivery personnel, and end users or customers could benefit from the framework since it helps the customer to have a contactless delivery system. Finally, we have proposed a blockchain-based platform for delivering products in COVID-19 and other pandemics in a stable and safe contactless manner. One could monitor delivery personnel's medical test status and trace travel of delivery personnel to various locations for each order produced and delivered in the system. The platform will benefit both service providers, distribution personnel, and end-users or consumers because it allows customers to provide a contactless delivery system. To test the efficacy of our proposed solution, the results depicted latency and throughput at various transaction rates and batch sizes. To ensure that this architecture is safe and accurate, we conducted a thorough attack analysis. Our proposed architecture, which is based on blockchain technology, ensures secure supply chain provenance and safeguards the privacy of all parties involved. To ensure that order is kept sanitized and treated safely, further research is needed. The vaccination information of delivery personnel can also be updated to the blockchain to make the system more secure in a contactless way. Even if the world is not in the grip of a pandemic, our framework can be used to help local businesses develop and operate a safe and secure contactless delivery system. Customers will most likely become accustomed to using delivery services as a result of the convenience. Since it offers a safe and reliable solution for contactless delivery, our architecture can be used in the future.

Bibliography

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," http://bitcoin.org/bitcoin.pdf, 2008.

[2] WHO, "Coronavirus," https://www.who.int/health-topics/coronavirus/#tab=tab_1, 2021.

[3] J. H. University, "Covid-19 dashboard by the center for systems science and engineering (csse) at johns hopkins university (jhu)," https://coronavirus.jhu.edu/map.html, 05/14/2021.

[4] R. Wathore, A. Gupta, H. Bherwani, and N. Labhasetwar, "Understanding air and water borne transmission and survival of coronavirus: Insights and way forward for sars-cov-2," *Science of the total environment*, vol. 749, p. 141486, 2020.

[5] N. Van Doremalen, T. Bushmaker, D. H. Morris, M. G. Holbrook, A. Gamble, B. N. Williamson, A. Tamin, J. L. Harcourt, N. J. Thornburg, S. I. Gerber *et al.*, "Aerosol and surface stability of sars-cov-2 as compared with sars-cov-1," *New England Journal of Medicine*, vol. 382, no. 16, pp. 1564–1567, 2020.

[6] G. Briscese, N. Lacetera, M. Macis, and M. Tonin, "Compliance with covid-19 social-distancing measures in italy: the role of expectations and duration," National Bureau of Economic Research, Tech. Rep., 2020.

[7] D. Delen, E. Eryarsoy, and B. Davazdahemami, "No place like home: Cross-national data analysis of the efficacy of social distancing during the covid-19 pandemic," *JMIR public health and surveillance*, vol. 6, no. 2, p. e19862, 2020.

[8] T. H. Nguyen and D. C. Vu, "Food delivery service during social distancing: Proactively preventing or potentially spreading coronavirus disease–2019?" *Disaster Medicine and Public Health Preparedness*, vol. 14, no. 3, pp. e9–e10, 2020.

[9] V. Venkatesh, "Impacts of covid-19: A research agenda to support people in their fight," *International Journal of Information Management*, p. 102197, 2020.

[10] E. Gibney, "Whose coronavirus strategy worked best? scientists hunt most effective policies," *Nature*, vol. 581, no. 7806, pp. 15–17, 2020.

[11] B. Goh, "China rolls out fresh data collection campaign to combat coronavirus," 2020.

[12] N. I. Centre, "Aarogya setu mobile app," https://www.mygov.in/aarogya-setu-app/, 05/14/2021.

[13] H. Stevens and M. B. Haines, “Tracetogether: pandemic response, democracy, and technology,” *East Asian Science, Technology and Society: An International Journal*, vol. 14, no. 3, pp. 523–532, 2020.

[14] G. of Singapore, “Tracetogether app,” https://www.tracetogether.gov.sg/, 03/11/2021.

[15] R. Gupta, M. Bedi, P. Goyal, S. Wadhera, and V. Verma, “Analysis of covid-19 tracking tool in india: Case study of aarogya setu mobile application,” *Digital Government: Research and Practice*, vol. 1, no. 4, pp. 1–8, 2020.

[16] S. Meixner, “Phone scans, gps tracking and wristbands: How other countries do covid-19 contact tracing,” https://www.abc.net.au/news/2020-04-28/coronaviruscovid19-contact-tracing-apps-around-the-world/12189438, 04/27/2020.

[17] A. Lodders and J. M. Paterson, “Scrutinising covidsafe: Frameworks for evaluating digital contact tracing technologies,” *Alternative Law Journal*, vol. 45, no. 3, pp. 153–161, 2020.

[18] A. government Department of Health, “Australian government: Department of health, covidsafe app,” https://www.health.gov.au/resources/apps-and-tools/covidsafe-app, 12/15/2020.

[19] CDC, “Cdc, older adults at greater risk if diagnosed with covid-19,” https://www.cdc.gov/coronavirus/2019-ncov/need-extra-precautions/older-adults.html, 04/16/2021.

[20] N. Bai, “Why experts are urging social distancing to combat coronavirus outbreak,” https://www.ucsf.edu/news/2020/03/416906/why-experts-are-urging-social-distancing-combat-coronavirus-outbreak, 2020.

[21] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich *et al.*, “Hyperledger fabric: a distributed operating system for permissioned blockchains,” in *Proceedings of the Thirteenth EuroSys Conference*, 2018, pp. 1–15.

[22] hyperledger fabric, “The ordering service,” https://hyperledger-fabric.readthedocs.io/en/release-2.2/orderer/ordering_service.html, 2020.

[23] P. Cui, U. Guin, A. Skjellum, and D. Umphress, “Blockchain in iot: Current trends, challenges, and future roadmap,” *Journal of Hardware and Systems Security*, vol. 3, no. 4, pp. 338–364, 2019.

[24] P. Cui, J. Dixon, U. Guin, and D. Dimase, “A blockchain-based framework for supply chain provenance,” *IEEE Access*, vol. 7, pp. 157 113–157 125, 2019.

[25] P. Cui and U. Guin, “Countering botnet of things using blockchain-based authenticity framework,” in *2019 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*. IEEE, 2019, pp. 598–603.

[26] U. Guin, P. Cui, and A. Skjellum, "Ensuring proof-of-authenticity of iot edge devices using blockchain technology," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. IEEE, 2018, pp. 1042–1049.

[27] X. Xu, F. Rahman, B. Shakya, A. Vassilev, D. Forte, and M. Tehranipoor, "Electronics supply chain integrity enabled by blockchain," *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, vol. 24, no. 3, pp. 1–25, 2019.

[28] 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*, vol. 1, no. 3, pp. 1–12, 2018.

[29] K. Biswas, V. Muthukkumarasamy, and W. L. Tan, "Blockchain based wine supply chain traceability system," 2017.

[30] S. Chen, R. Shi, Z. Ren, J. Yan, Y. Shi, and J. Zhang, "A blockchain-based supply chain quality management framework," in *2017 IEEE 14th International Conference on e-Business Engineering (ICEBE)*. IEEE, 2017, pp. 172–176.

[31] T. Bocek, B. B. Rodrigues, T. Strasser, and B. Stiller, "Blockchains everywhere-a use-case of blockchains in the pharma supply-chain," in *2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*. IEEE, 2017, pp. 772–777.

[32] Ethereum, "Ethereum developer resources," https://ethereum.org/developers/, 2020.

[33] A. Kalla, T. Hewa, R. A. Mishra, M. Ylianttila, and M. Liyanage, "The role of blockchain to fight against covid-19," *IEEE Engineering Management Review*, vol. 48, no. 3, pp. 85–96, 2020.

[34] A. Khurshid, "Applying blockchain technology to address the crisis of trust during the covid-19 pandemic," *JMIR medical informatics*, vol. 8, no. 9, p. e20477, 2020.

[35] D. Mishra, A. Haleem, and M. Javaid, "Analysing the behaviour of doubling rates in 8 major countries affected by covid-19 virus," *Journal of Oral Biology and Craniofacial Research*, vol. 10, no. 4, pp. 478–483, 2020.

[36] D. Resiere, D. Resiere, and H. Kallel, "Implementation of medical and scientific cooperation in the caribbean using blockchain technology in coronavirus (covid-19) pandemics," *Journal of Medical Systems*, vol. 44, pp. 1–2, 2020.

[37] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[38] E. Foundation, "On public and private blockchains," https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/, 2015.

[39] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An overview of blockchain technology: Architecture, consensus, and future trends,” in *IEEE International Congress on Big Data (BigData congress)*, 2017, pp. 557–564.

[40] DoubleSpending, “On public and private blockchains,” https://en.bitcoin.it/wiki/Double-spending, 03/31/2021.

[41] G. O. Karame, E. Androulaki, and S. Capkun, “Double-spending fast payments in bitcoin,” in *Proceedings of the 2012 ACM conference on Computer and communications security*, 2012, pp. 906–917.

[42] U. Mukhopadhyay, A. Skjellum, O. Hambolu, J. Oakley, L. Yu, and R. Brooks, “A brief survey of cryptocurrency systems,” in *2016 14th annual conference on privacy, security and trust (PST)*. IEEE, 2016, pp. 745–752.

[43] W. Li, S. Andreina, J.-M. Bohli, and G. Karame, “Securing proof-of-stake blockchain protocols,” in *Data Privacy Management, Cryptocurrencies and Blockchain Technology*. Springer, 2017, pp. 297–315.

[44] M. Castro, B. Liskov *et al.*, “Practical byzantine fault tolerance,” in *OSDI*, vol. 99, no. 1999, 1999, pp. 173–186.

[45] D. Larimer, “Delegated proof-of-stake consensus,” 2018.

[46] M. Ghosh, M. Richardson, B. Ford, and R. Jansen, “A torpath to torcoin: Proof-of-bandwidth altcoins for compensating relays,” NAVAL RESEARCH LAB WASHINGTON DC, Tech. Rep., 2014.

[47] D. Yaga, P. Mell, N. Roby, and K. Scarfone, “Blockchain technology overview,” *arXiv preprint arXiv:1906.11078*, 2019.

[48] Openethereum, “openethereum/parity-ethereum,” https://github.com/openethereum/parity-ethereum, 2021.

[49] D. Marbouh, T. Abbasi, F. Maasmi, I. Omar, M. Debe, K. Salah, R. Jayaraman, and S. Ellahham, “Blockchain for covid-19: Review, opportunites and a trusted tracking system,” 2020.

[50] I. U. Blog, “How blockchain can help in the covid-19 crisis and recovery,” https://blog-idcuk.com/blockchain-help-in-the-covid-19-and-recovery/, 2020.

[51] Coalition, “Coalition,” https://www.coalitionnetwork.org/, 2020.

[52] cryptopolitan, “Phbc announces blockchain monitor to track virus-free zones,” https://www.cryptopolitan.com/phbc-blockchain-monitor-for-virus-free-zones/, 2021.

[53] H. Xu, L. Zhang, O. Onireti, Y. Fang, W. B. Buchanan, and M. A. Imran, “Beeptrace: Blockchain-enabled privacy-preserving contact tracing for covid-19 pandemic and beyond,” *arXiv preprint arXiv:2005.10103*, 2020.

[54] J. Song, T. Gu, X. Feng, Y. Ge, and P. Mohapatra, "Blockchain meets covid-19: A framework for contact information sharing and risk notification system," *arXiv preprint arXiv:2007.10529*, 2020.

[55] H. Choudhury, B. Goswami, and S. K. Gurung, "Covidchain: An anonymity preserving blockchain based framework for protection against covid-19," *arXiv preprint arXiv:2005.10607*, 2020.

[56] B. Magazine, "Blockchain and crypto firm vechain utilized to confirm authenticity of coronavirus kn95 masks," https://www.blockchainmagazine.net/blockchain-and-crypto-firm-vechain-utilized-to-confirm-authenticity-of-coronavirus-kn95-masks/, 2020.

[57] N. Ahmed, R. A. Michelin, W. Xue, S. Ruj, R. Malaney, S. S. Kanhere, A. Seneviratne, W. Hu, H. Janicke, and S. K. Jha, "A survey of covid-19 contact tracing apps," *IEEE Access*, vol. 8, pp. 134 577–134 601, 2020.

[58] J. Bay, J. Kek, A. Tan, C. S. Hau, L. Yongquan, J. Tan, and T. A. Quy, "Bluetrace: A privacy-preserving protocol for community-driven contact tracing across borders," *Government Technology Agency-Singapore, Tech. Rep*, 2020.

[59] hyperledger, "Security model," https://hyperledger-fabric.readthedocs.io/en/release-2.2/security_model.html, 2020.

[60] J. Guzman, "Coronavirus spurs noncontact food delivery in us," https://thehill.com/changing-america/well-being/prevention-cures/486889-coronavirus-prompts-non-contact-food-delivery-in, 2020.

[61] S. A. O'Brien, "Now you can get your food delivered without any human contact," https://www.cnn.com/2020/03/05/tech/instacart-leave-at-my-door/index.html, 2020.

[62] hyperledger fabric, "Hyperledger blockchain performance metrics white paper," https://www.hyperledger.org/learn/publications/blockchain-performance-metrics, 2018.

[63] hyperledger, "Couchdb as the state database," https://hyperledger-fabric.readthedocs.io/en/release-2.2/couchdb_tutorial.html, 2020.

[64] D. Merkel, "Docker: lightweight linux containers for consistent development and deployment," *Linux journal*, vol. 2014, no. 239, p. 2, 2014.

[65] S. Pongnumkul, C. Siripanpornchana, and S. Thajchayapong, "Performance analysis of private blockchain platforms in varying workloads," in *26th International Conference on Computer Communication and Networks (ICCCN)*. IEEE, 2017, pp. 1–6.

[66] P. Thakkar, S. Nathan, and B. Viswanathan, "Performance benchmarking and optimizing hyperledger fabric blockchain platform," in *26th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)*. IEEE, 2018, pp. 264–276.

[67] T. K. Sharma, “How blockchain can solve major challenges of covid-19 faced by healthcare sectors?” https://www.blockchain-council.org/blockchain/how-blockchain-can-solve-major-challenges-of-covid-19-faced-by-healthcare-sectors/, 2020.