A Framework for Making Industry 4.0 Systems Secure Using Blockchains

by

Hafsa Aziz

A thesis submitted to the faculty of Information Security Department, Military College of Signals, National University of Sciences and Technology, Rawalpindi in partial fulfillment of the requirements for the degree of MS in Information Security

Sep 2021

CERTIFICATE

This is to certify that **Hafsa Aziz,** Student of **MSIS-15** Course Reg.No **00000170533,** has completed her MS Thesis title **"A Framework for Making Industry 4.0 Systems Secure Using Blockchains"** under my supervision. I have reviewed her final thesis copy and am satisfied with her work.

Thesis Co-Supervisor
(Dr. Fawad Khan)

Thesis Supervisor
Dated: 24th Sep 2021 (**Dr. Shahzaib Tahir Butt**)

Declaration

I hereby declare that no portion of work presented in this thesis has been submitted in support of another award or qualification either at this institution or elsewhere.

Dedication

"In the name of Allah, the most Beneficent, the most Merciful"

I dedicate this thesis to my Parents who have been a constant source of support and inspiration my whole life. I also dedicate this thesis to my Supervisors who guided me in this process, kept me on track, and all the effort they put in to help me, without them it would not have been possible. And a special thankyou to my teachers and fellows at MCS who aspired me to achieve more.

Acknowledgments

All praises to Allah for the strengths and His blessing in completing this thesis.

I would like to convey my gratitude to my supervisors, Dr. Shahzaib Tahir Butt and Dr. Fawad Khan, for their supervision and constant support. Their invaluable help of constructive comments and suggestions throughout the experimental and thesis works are major contributions to the success of this research.

Last, but not the least, I am highly thankful to my mother, father, and my dear friends. They have always stood by my dreams and aspirations and have been a great source of inspiration for me. I would like to thank them for all their care, love and support through my times of stress and excitement.

Abstract

Blockchain is an evolving technology which is used for storing all kinds of data like transactions. We have heard the name Blockchain only in terms of Cryptocurrency but it is not limited to that. It can also be used in industries other than Cryptocurrency and store various things like data or even multimedia such as pictures, music, and videos.

Blockchain, distributed ledger technology, Internet of things, and digital transformation are hot topics these days because they can transform the way all real world operations work. The use of IoT devices is growing. At one point IoTs were used for major industries but now it's a household name. According to Garter which is an analytics firm there will be 41 Billion IoT Devices by 2027 [1]. With the increase in the use of IoT devices, there will be a rapid increase in the amount of data they produce. Protecting and managing this Data efficiently and making sure that only the authorized users have access to it is important. The main focus of this study would be to identify the challenges associated with the adoption of industry 4.0 and present a novel framework based on Blockchain to solve the issues faced by this Industry. The outcome will be an implementation of Blockchain technology in 4th industrial revolution with special reference to Internet of things (IoT) with the help of Hyperledger. HyperLedger is an open-source project by Linux Foundation which was initially developed by IBM. It allows to develop and manage permissioned and private Blockchain systems by using top-notch algorithms and security features.

Table of Contents

List of Figures

List of Tables

Chapter 1

1. Introduction

1.1 Overview

Industry 4.0 is changing how organizations fabricate, improve and circulate their items. Makers are coordinating innovations, including the Internet of Things (IoT), distributed computing and investigation, and AI and AI into their creation offices and all through their tasks. These brilliant processing plants are furnished with cutting-edge sensors, installed programming, and advanced mechanics that gather and examine the information and consider better dynamics. Considerably higher worth is made when information from creation tasks is joined with practical information from ERP, production network, client assistance, and other endeavor frameworks to make unheard-of levels of permeability and understanding from previous data. This advanced advances lead to expanded computerization, proactive support, self-streamlining of interaction upgrades, and most importantly, another degree of efficiencies and responsiveness to clients not beforehand conceivable. Creating brilliant processing plants gives an unimaginable chance to the assembling business to enter the fourth modern upset. Examining enormous information gathered from sensors on the production floor guarantees continuous perceivability of assembling resources and can give apparatuses to perform prescient support to limit personal hardware time.

Blockchain, distributed ledger technology, the Internet of things, and digital transformation are hot topics these days because they can transform how all real-world operations work. Researchers have performed primary and secondary research on these topics, but not much literature is available on the interaction among Blockchain, industry 4.0, and IoT. The main focus of this study would be to identify the challenges associated with the adoption of industry 4.0 and present a novel framework based on Blockchain to solve the issues faced by this Industry. The outcome will be implementing Blockchain technology in the 4th industrial revolution, particularly the Internet of things (IoT).

1.2 Objective

IoT and Blockchain are two quickly advancing technologies that have the capability of influencing our lives consistently in coming years. In this proposition, we need to actualize a Blockchain solution for IoT data.

We will be HyperLedger Fabric as our Blockchain platform, which is a private permissioned Blockchain. Our goal is to show that HyperLedger can be utilized for dealing with IoT information.

Industry 4.0 introduces new technologies in IoT, and the lack of sufficient information/expertise in cybersecurity issues that comes with it results in many different challenges and risks. Industry 4.0 is the automation information and technologies we use daily. Some significant concerns include the lack of sufficient information/expertise in cybersecurity, resulting in many challenges and risks. If we talk about the IoT, the scarcity and interconnectivity of the devices, it is challenging to ensure all nodes involved, especially the user data. The confidentiality and integrity of data are always at risk.

Centralized Blockchain technology can act as a preferred foundation to overcome all these issues. A distributed ledger is well matched to produce device identification, authentication, and seamless, secure data transfer. Rather than rummaging a 3rd party for establishing trust, IoT sensors can exchange data through a Blockchain. The Blockchain is known as an advanced system in terms of security and privacy. It enables device autonomy (smart contract), individual identity, the integrity of information and supports peers to see communication by removing technical bottlenecks and inefficiencies.

The main objectives of the thesis are: -

- Revisiting the 4^{th} industrial revolution and analyzing the challenges across different domains.
- Studying Blockchain, discussing its advantages in the Internet of Things.
- Presenting and implementing a framework over an IoT dataset to mitigate the risks associated with industry 4.0.

1.3 Challenges

Industry 4.0 is a genuinely new and quickly advancing idea. Every association might have a unique way to deal with it, yet the fundamental thought is quite primary and can be sorted as:

- Collecting Data
- Analyze the information
- Generate results from dissected information
- Use the created results to alter the framework
- Finally, understand the advantages of a further developed framework
- Repeat the above advances

This appears to be simple in principle, yet the industry is testing its limitations. A portion of the difficulties are as per the following:

- Hardware Compatibility Issues: Most IoT information is caught utilizing different sensors, which are communicated to the cloud or workers using the IoT doors. If the association's current gadgets and machines are not recognized and seen, there could be similar issues with the sensors utilized to gather IoT information.
- Data Connectivity Issues include how the IoT gadgets converse with door or worker/cloud. Deciding on the proper arrangement of conventions and information design for sending information to the IoT stage is vital.

1.4 Benefits of Using Blockchain in Industry 4.0

The data structure in a Blockchain is append-only. So, the data cannot be altered or deleted. The transactions are recorded in chronological order. Therefore, all blocks are time stamped. It also uses Smart Contracts, Consensus Hash Keys, and work algorithms like "Proof-of-work" and "Proof-of-State" to mitigate third-party attacks.

Mushtaq & Haq (2019) [2] believe that due to rapid developments in Information technology and industrialization, methods have advanced at the beginning of the 4th Industrial Revolution, also known as integrated Industry or intelligent manufacturing. The concept of Industry 4.0 promises record progress in manufacturing technology with the advancement of production along with the value creation of digital transformation in products and services.

Industry 4.0 [3] will be supported by new technologies, including the Internet, cloud computing, machine learning, artificial intelligence, robotics, industrial integration, and service-oriented computing. Distributed ledger technology, famously known as Blockchain technologies, can't directly affect industry 4.0; however, it has implications. Some of the major problems during the supply chain of industry 4.0 include accountability, lack of tools of visibility, and comprehensive auditing.

Practically, some of the issues and challenges, such as product cloning, counterfeiting, trickier maintenance, and IP theft, are some of the critical problems relating to Industry 4.0. This paper is an effort to present the use of Blockchain technology in the 4th industrial era. In this research, I will highlight some essential industry 4.0 while using Blockchain technology and elaborate on Blockchain benefits for industry 4.0. This research also highlighted some areas of consideration where Blockchain technology can be beneficially used for Industry 4.0 progress.

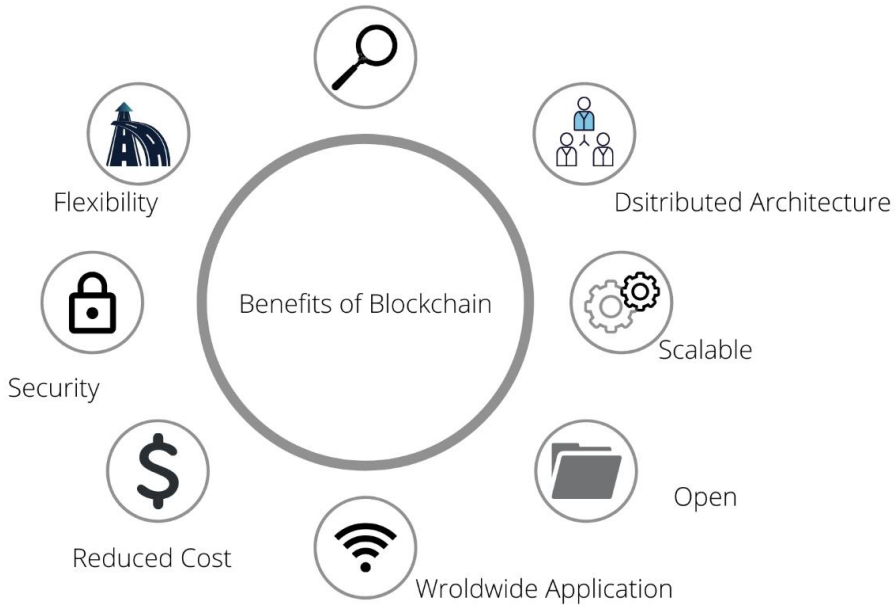

Figure 1 Blockchain Benefits

1.5 Approach

In this proposition, we are utilizing HyperLedger Fabric Blockchain for storing IoT information. As HyperLedger is a private authorization Blockchain, we can handle who will approach our IoT information. HyperLedger permits access just to approved entities as characterized in its Policy. HyperLedger additionally utilizes best-in-class encryption guidelines for its different exchanges. This makes the HyperLedger Fabric Blockchain Highly got from any malevolent movement. HyperLedger uses

endorsements for personality on the board. We can be a specific solitary approved element that can add information to our record along these lines. HyperLedger can permit read-compose admittance to different substances relying upon the certainty we have in that element. This allows us to control the security of our IoT information. We will use an IoT data set with the attributes of a home's date, time, and energy utilization captured by an IoT sensor. We will send this information to our HyperLedger Node. We will design a HyperLedger Network, which will comprise two organization nodes and two peer nodes.

Every association will have two peers each. Our organization will likewise contain one Orderer, which will be utilized for requesting our IoT exchanges. We will likewise do the presentation assessment of our organization using different boundaries like clump break, group size, and several messages into thought.

1.6 Outline

In Chapter 2, we will discuss the related work and discuss all the attributes of this thesis in detail. We will discuss Industry 4.0, Blockchain, and Hyperledger in depth. In Chapter 3, we shall discuss the methodology we will use Blockchains in industry 4.0 and our approach to do so. We will discuss Hyperledger Fabric and our proposed idea in detail. We will also discuss our system architecture and every aspect of the system in 3rd chapter. Chapter 4 will validate and analyze the results to evaluate the performance under different data conditions. In Chapter 5, we will discuss future work.

Chapter 2

2. Related Work

2.1 Industrial Revolutions

In the past, people have always been dependent on technology in their very own way. Masses always used technology to ease their task and thrived to improve them over time, and this improvement resulted in the concept of the Industrial Revolution, which is now at the fourth stage [4]. We will discuss its phases below:

2.1.1 The First Industrial Revolution 1765

Almost at the start of the 19th-century, industries started to automate things mechanically, which resulted at the beginning of the new era that took over the agriculture industry, which was considered the strength of the societal economy. In this era, the masses witnessed significant economic changes due to the vast coal extraction from the steam engine, which boosted the infrastructure and economy.

2.1.2 The Second Industrial Revolution 1870

At the end of the 19th-century second era of the Industrial Revolution was witnessed in the form of different kinds of energy sources like Electricity, Gas, and Oil. These energy sources opened the gate for new inventions resulting in a rapid increase in steel demand and chemical synthesis. This also advances communication conduct and conveyance through technical improvement in the 20th century. This age is considered to be the most vital as it boosts the way we live today.

2.1.3 The Third Industrial Revolution 1969

This era in the middle of the 20th-Century witness the discovery of nuclear energy resources. This also bought the uprising of new technologies that include the invention of computers, telecommunication, and electronics that eventually open up opportunities for space, research, and biotechnology. This era achieves elevated automation through Programmable Logic Controllers and Robots.

2.1.3 The Fourth Industrial Revolution or Industry 4.0

Many people believe that industry 4.0 is the revolution that is happening right now and its magnitude is yet not known. It started at the brink of the third millennium with the rise of the Internet that challenges physics in virtual reality. This shapes the worldwide

economy, and different programs are introduced to help people perform their daily tasks effectively and efficiently.

The main prospect of Industry 4.0 is that billions of individuals are connected by mobile devices, with unprecedented process power, storage capacity, and access to knowledge, which are unlimited. And these potentials are going to be amplified by increasing technological advances in fields reminiscent of artificial intelligence, automation, self-directed vehicles, 3-D printing, Nano-tech, bio-tech, and quantum calculating.

2.2 Internet of Things

The IoT involves adding digital sensors and networking technologies to the devices and systems that we use daily within the analog world. [5] A number of the foremost well-known examples are Nest and Ecobee's good thermostats and Amazon's Alexa-powered devices together with the Echo smart speaker. Good thermostats have sensors in multiple rooms and hook up with your phone and the Internet to allow extended control over the temperature. They'll even be connected to algorithms to manage the temperature once you're not home or supported weather patterns and "detect" when you leave [6].

2.3 Challenges of Internet of Things and Industry 4.0

Industry 4.0 and IoT are about linking the devices and systems that were previously independent of each other; it isn't shocking that a significant shared concern is security. Because the trend of exploiting good devices increases, it'll be more durable to trace breaches and manage all of these devices [7]. Trade is moving quickly to deal with these security concerns, melding new technologies with standard IT security technologies like network security and encryption.

Another hurdle for each IoT and business 4.0 has been the shortage of standards. Having many suitable devices is excellent; however, if all of them record the knowledge in their format and need their protocol, integrating them into an automatic factory is price preventive and difficult. Manufacturing titans like Eclipse Foundation, Bosch functions on standard communiqué protocols and structural design like OPC UA, MQTT, and PPMP. These all aim to promote intelligent devices and those on the workshop floor in collaborating and supplying typical data formats. However, added data formats will mean a different issue in making one knowledge model [8].

There are extra challenges for Industry 4.0 and IoT because of the mere state of a number of the technologies. Like any nice transformation, there'll be transitions that hybridize older ways and technologies with the new, at the side of risks and rewards.

2.4 History of Blockchain

A cryptographically protected chain of blocks was initially defined by Stuart Haber and W Scott Stornetta in 1991. [9]. It was later altered in Cryptocurrency and Bitcoins when, in 2008, developers functioning under the pseudonym Satoshi Nakamoto released a white paper founding the model for a blockchain [10].

In 2014, Blockchain detached from Cryptocurrency, and its potential to be used in other businesses came to the surface. The blockchain system presented by Etherium, known as smart contracts, was introduced, representing financial instruments such as bonds.

2.4.1 Blockchain

Blockchain, as the name recommends, can be envisioned as a chain of blocks connected. These blocks can hold all kinds of data. However, what makes Blockchain extraordinary and exceptional is its unchanging and distributed nature [11].

It uses a peer-to-peer network. There are numerous peer nodes in a Blockchain network, each having a similar copy of the information known as a ledger. A ledger has a one-of-a-kind property of being permanent; it holds every piece of information, changes, and keeps a record of everything that's happening. This makes it hard to tamper with the blocks.

The first block in the Blockchain is named the genesis block. Each block comprises some information, its hash, and the hash of the preceding block. If a malicious or unconfirmed alteration is made in Block 2, its hash will be altered, and Block 3 will no longer be directed to the former block, making it easy to notice which block has been interfered with.

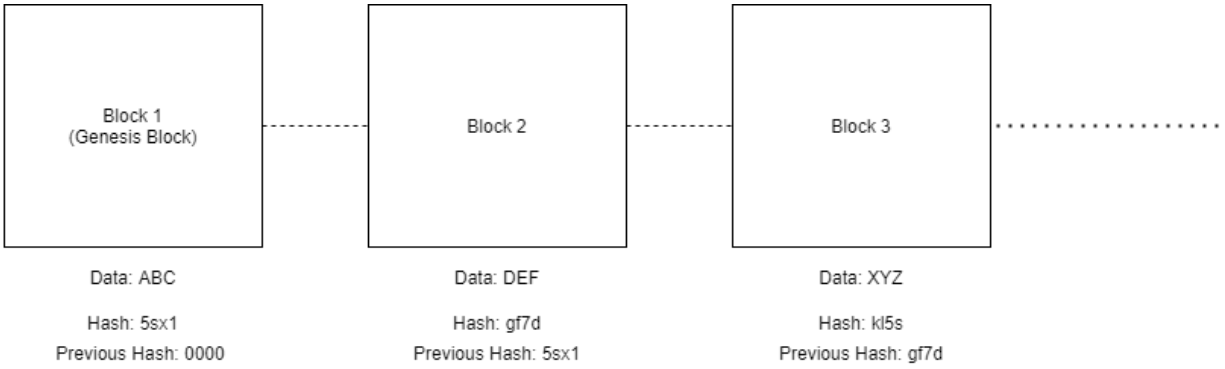

Figure 2 Blockchain Cycle

2.4.2 Blockchain Types

Public Blockchains:

In public Blockchain, the data is accessible to everyone on the network. As its permissionless, anyone can view, read, or write information on the Blockchain, and the information is available to all. No specific member has command over the information in a public blockchain. Public Blockchains are likewise decentralized and changeless. It implies that once a section is made on the Blockchain, it can't be changed or erased once the entries are approved. A public blockchain has a distributed ledger in which all nodes can participate in the validation of transactions. It has open reading and writing access, due to which any participating party can read, write, and view data on the Blockchain [12]. It is also immutable, so it cannot be modified or deleted once an entry is validated.

Private Blockchains:

A private blockchain [13] is sometimes called a consortium Blockchain. It is, as the name suggests, "private" and is governed by a single entity. The official employees require authorization to read, write, or verify the data. This type of Blockchain has multiple layers to oversee the data authorizations. For example, an admin wants to enhance the chain, but the employees at certain levels need altered access. Private Blockchains can be designed for industries such as finance [14], supply chain, IT, and government/military services. The transactions or the data in private chains are not publicly visible and can only be accessed by the authorized entities.

Public vs. Private Blockchains:

Public Blockchain	Private Blockchain
Public: All the participants on the network have access.	Permissioned: Only the authorized parties have access.
Anyone on the network can read, write, or verify the data.	Only the permissioned entities have the authority to read, write, or verify the data.
It is immutable; once the data entry is verified cannot be modified.	It is scalable; an organization can add or remove nodes on demand.
No participant has any control over the chain.	It is an invitation-only Blockchain with limited users having more admittance than the other.
It can be used in the public sector, such as Healthcare and Education, etc.	It can be used in the private sector, such as IT, finance, Government, etc.

Table 1 Public vs. Private Blockchains

2.4.3 Areas of Application

Healthcare

Blockchain can be implemented in creating Electronic Health records that can be accessed from anywhere. All data will be recorded in the general Ledger and can be used for public-private use, health insurance, and other related applications in healthcare. This kind of infrastructure can help the doctors gain the patient's entire medical history and prescribe suitable treatment after permission to access the data [15].

The Internet of Things (IoT) has widened the possibilities in medicine. The innovative medical devices can collect additional data and monitor the patient's health to give an extra insight into symptoms and enable remote care.

Challenges	Blockchain Solution
Private Doctor's Appointment (Missing Health History).	Patient data is stored on a distributed permission technology yet to be accessed

	at the time of need with no missing health attributes for ideal treatment.
Time-taking data processing mechanism for patient's health history.	The data will be updated in real-time on a network, and the data processing or extraction time will be reduced remarkably.
They are protecting data integrity and confidentiality.	Protecting the confidentiality of data requires ensuring that only authorized personnel has access to Data in the ledgers. The validity and consistency can be provided using mechanisms like **Consensus**.
Getting Daily health analysis from Smart Devices	The data collected from intelligent health applications on the phone or a smartwatch can be uploaded to the Blockchain ledger to give more insight to the doctors in case of emergencies.

Table 2 Healthcare Challenges and Blockchain Solution

Supply Chain System

The Blockchain is an advanced system that involves many entities to fulfill consumer demand from its raw form to the result. With the advanced Internet of Things technology, the supply chain managers and other involved entities have a clear picture of the whole infrastructure [16]. The IoT provides many possibilities like Real-time location-tracking, Condition monitoring, Forecast and Monitor the Product's movements and more. The complexity within the supply chain is created through transactions where there are many entities involved. It is essential to make sure that the product matches its informational integrity. The Blockchain infrastructure can offer transparency and traceability in the availability chain. It will provide verifiable, immutable transactions inside the supply chain. Over the past few years, firms love IBM, Walmart, urban center Insurance, Maersk, Nestle, Unilever, and Amazon, have

invested in pilot Blockchain-based mainly provide chain comes to develop and take a look at the technology.

Challenges	Blockchain Solution
Errors, Product delays, management	Distributed public general Ledger will help get a clear picture of the flow at every end.
Fraudulent Activities	The data will be updated in real-time on a network, and any change in data by and the unauthorized person will invalidate the whole chain, and it will be easy to detect the frauds.
Assuring trustworthy flow and Increase Consumer/Buyers trust	Protecting the confidentiality of data requires ensuring that only authorized personnel has access to Data in the ledgers; the validity and consistency can be confirmed using mechanisms like **Consensus**. The chain will only be validated if it has the approval of all the entities involved in the Supply Chain.
Transparency and Efficiency	As the distributed ledger data is shared and unchangeable without proper authorization, it requires less administrative work, overlooking and lowering charges for transactions.

Table 3 Supply Chain Challenges and Blockchain Solution

Legal

The traditional way of maintaining the records and paperwork in the legal industry has always been paper-based. The legal documents and contracts require the physical presence of the parties, a hard copy of documents, and a physical signature. This whole process requires a significant amount of time and detailed checks to maintain the

integrity and confidentiality of the legal documents throughout the entire process. This manual checking and maintenance of records are more prone to human error.

This Blockchain Smart contract is a centralized/decentralized and automated ledger that can be created to record all the contractual transactions like Chain of Custody, Intellectual property Laws, Marriage Contracts, Property Management, and Notarization. But with the ever-moving evolution of technology, Smart Contracts are used to maintain and process this kind of documents online. Still, there is always a question of the security of such legal contracts and procedures. The main risk of processing legal documents digitally is maintaining the authenticity and integrity with Blockchain technology the legal documentation process more secure and transparent, thereby leaving no human error [17].

Challenges	Blockchain Solution
Accessibility	Legal Authorities can use Blockchain to streamline their legal transactions and store all the legal documents using smart contracts and automated contract management systems.
Fraudulent Activities	The data will be updated in real-time on a network, and any change in data by an unauthorized person will invalidate the whole chain, and it will be easy to detect the frauds.
Transparency	Distributed ledger technology (DLT) records the transactions of assets digitally, making it accessible to all the parties at the time of need.
Efficiency	As the distributed ledger data is shared and unchangeable without proper authorization, it requires less administrative work, overlooking and lowering consumed time.

Table 4 Legal Challenges and Blockchain Solution

Relevance to National and Army Needs

The Internet of Things has broad military applications, linking ships, aircraft, tanks, drones, soldiers, and operational bases within a coherent network that enhances situational awareness, risk assessment, and response time. It is expected that the security development community will be searching for new military technologies focused on Blockchain technology with leading applicant areas such as cyber protection, encrypted messaging, robust communications, logistics support, and Internet of Things security networking. [18]

Challenges	Blockchain Solution
Access Management	In defense sites, it is crucial to know what a visitor does after he is granted access. That record can be maintained securely with Blockchain databases using Signature Chains, mitigating the possibility of tempered forms.
Fraudulent Activities	The data will be updated in real-time on a network, and any change in data by an unauthorized person will invalidate the whole chain, and it will be easy to detect the frauds.
Transparency	Distributed ledger technology (DLT) records the transactions of each Military asset digitally, making it accessible to all the parties at the time of need.
Efficiency	As the distributed ledger data is shared and unchangeable without proper authorization, it requires less administrative work, overlooking and lowering consumed time.

Table 5 Military Challenges and Blockchain Solution

2.5 Blockchain Implementation

Blockchain is a Distributed Ledger Technology (DLT) that makes any advanced resource's historical backdrop unalterable and straightforward using decentralization and cryptographic hashing. Blockchain is a particularly encouraging and progressive innovation since it lessens the risk of information loss, and tampering gets rid of fraud, and gives straightforwardness a saleable path [19]. Blockchain has the following key components [20]:

- Peer-to-peer network
- Distributed Ledger
- Cryptographic private keys
- Transactional records and networking details

Cryptography keys comprise of two keys [21] – Private and Public keys. These keys help in performing effective exchanges between two entities. Every individual has these two keys, which they use to create a protected membership identity. This makes sure that the individual is the central part of the Blockchain system. Blockchain is a peer-to-peer network the involving parties use digital signatures to reach a consensus and authorize the transactions by solving a mathematical verification. This is called proof of work.

2.5.1 Transaction Process

One of the Blockchain features is how it affirms and approves transactions. For instance, if two people wish to play out an exchange with a private and public key, the primary individual entity would join the exchange data to the public key of the next party. This Data is assembled into a block [22].

The block consists of a digital signature, a timestamp, and other significant, pertinent data. It should be noticed that the block does exclude the information of the people associated with the exchange. This block is then communicated across all the nodes on the network, and when the authorized individual uses his private key and matches it with the block, the transaction is successful.

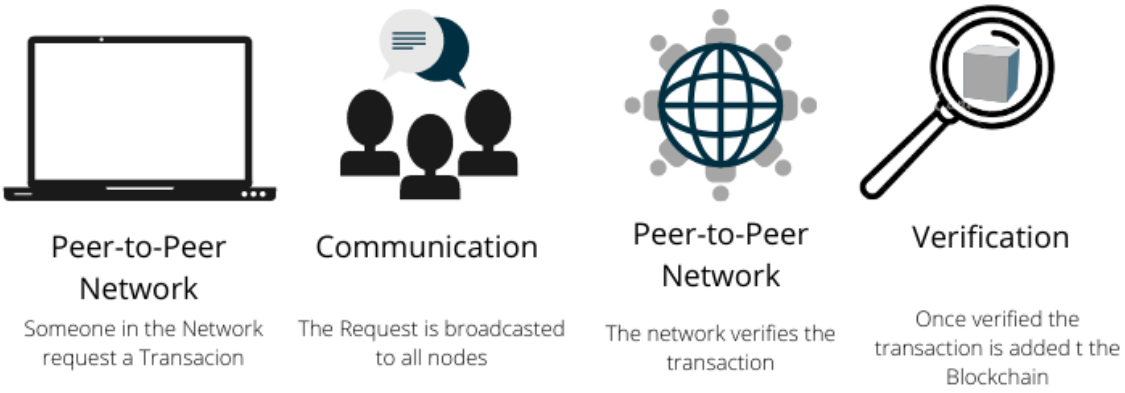

Figure 3 Transaction Process

2.5.2 Public Key Infrastructure (PKI)

PKI is utilized for giving secure correspondences in an organization [23]. It ensures every element in a network is substantial. The HyperLedger Fabric uses MSP, which utilizes PKI. The PKI has the following main components:

- Certificate Authority (CA): It issues digital certificates to authorized users to represent the possession of a public key.
- Registration Authority (RA): Approves the enrollment of a digital certificate with a public key. Each time when a verification check of any certification is requested, it goes to RA. The RA then accomplishes if to confirm the demand. RA can similarly give testimonies for obvious use cases trusting upon the authorizations permitted to it by CA.
- Certificate Database
- Digital Certificates
- Certificate Store where distributed certificates are kept

2.5.3 Public and Private Keys

The public key is dispersed through a digital certificate. The private key is kept secure. The connection between public and private keys is with the end goal that the party's public key can check a message marked by the authorized party's private key. The transmission keeps utilizing personal key guarantees the message is not altered and authenticated.

2.5.4 Digital Certificates

Digital Certificates could be viewed as closely resembling an individual's national ID [24]. It contains a bunch of properties that encourage us to recognize the proprietor of the Digital Certificate. It also incorporates the individual's public key alongside other pertinent data while the private key is left well enough alone and never included for the advanced authentication. This Data is encoded utilizing cryptography. Adjusting or altering the data in the Certificate will make it invalid. In HyperLedger use the X.509 standard for an advanced Digital Certificate. As long as Certificate Authority CA's character isn't undermined (i.e., its private key is left well enough alone), we can be confident that the Certificate has not been altered.

2.6 Blockchain and Hyperledger Fabric

Cachin [25] explains that Hyperledger is an open-source combination of cross-industry Blockchain technologies to create advancement. It is a worldwide alliance effort hosted by Linux Foundation that includes financial ledgers, banking, demand-supply, manufacturing, and different technologies. It nurtures and encourages the array of businesses in the Blockchain technologies that Include distributed ledger framework, intelligent contract engines, client libraries, graphical interfaces, utility libraries, and sample applications. This setup inspires the re-utilization of ordinary building blocks and allows the swift modernization of DLT parts [26]. The critical feature of Hyperledger are:

- Permissioned Network
- Confidential Transactions
- Pluggable Architecture
- Easy to Get Started

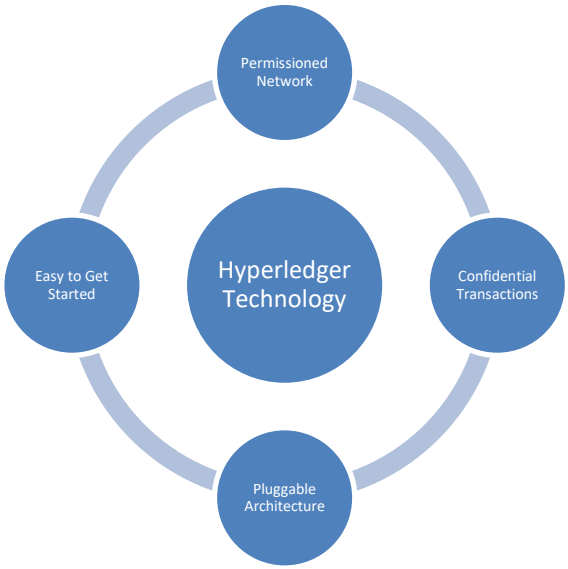

Figure 4 HyperLedger Fabric

Blockchain technologies that Include distributed ledger framework, smart contract engines, client libraries, graphical Hyperledger technology are about to revolutionize all industries. It can be a prominent playing in the market in the decades to come. This research will be showcasing this Blockchain Technology, which has the potential to change the way we think [27]. Some of the HyperLedger frameworks are:

- Iroha
- Sawtooth
- Indy
- Grid
- Burrow
- Fabric

It has the following tools:

- Cello
- Composer
- Explorer
- Quilt
- Ursa
- Caliper

2.6.1 HyperLedger Burrow

Burrow was released in December 2004; it is a permission Smart Contract system that provides a modular Blockchain with a permissioned smart contract interpreter built-in part to the specification of the Ethereum Virtual Machine (EVM). [28]

It has the following components:

Consensus Engine

It is responsible for maintaining the network and connection between nodes and order transactions to be utilized by the application engine.

Application Blockchain Interface (ABCI)

It delivers the interface description for the consensus and application engine to join.

Smart Contract Application Engine

This provides application builders with a strongly deterministic smart contract engine for operating complex industrial processes.

Gateway

Delivers programmatic interfaces for systems incorporations and consumer interfaces.

2.6.2 HyperLedger Grid

The grid can be used in a wide range of supply chain solutions. It is a structure that gives the best SDKs, industry principles, and libraries for the inventory network in a particular plan [29].

2.6.3 HyperLedger Indy

HyperLedger Indy is employed for managing identities using ledger technology. This enables organizations from totally different domains to use and verify one another identities. It provides numerous tools and identities for managing identities. It uses the sovran protocol. It allows users to manage their privacy. It uses the RBFT as its agreement protocol [30]. It's galvanized by plentum BFT that makes the system fault-tolerant and allows us to observe malicious nodes.

2.6.4 HyperLedger Sawtooth

Hyperledger Sawtooth detaches the central Ledger from the application environment. Thus, it simplifies the application use yet keeps the framework free from any danger [31].

With Sawtooth's secluded design, engineers can create applications in their preferred programming language and host, run and work it on framework fringe without impeding the center blockchain framework.

An application on Hyperledger Sawtooth can be founded on a center business rationale to run business activities, or it very well may be fabricated and run as a brilliant agreement computer-generated mechanism with a self-administering module to make, advise and implement the agreements between different individuals on the blockchain network.

Sawtooth's center framework permits these applications to exist together, permitting various uses to remain in a similar example of the blockchain network.

2.7 HyperLedger Fabric

Fabric is one of the open-source endeavors under the HyperLedger umbrella. It is used to provide customized Blockchain solutions [32]. It can be configured according to the specific need of an organization.

The functionalities of HyperLedger Fabric [33] are as follow:

- **Identity Management**
  Each activity in HyperLedger is to be endorsed by authorized certificates of authorities. These authorizations are provided by and Membership Service Provider (MSP).
- **Privacy and Confidentiality**
  The HyperLedger 'Channel' allows a direct line of communications between one authorized user to another instead of distributing it all over the chain.
- **Efficient Processing**
  HyperLedger is a customizable distributed ledger system, which means not all nodes copy the Ledger. Some have restricted access on a need-to-know basis, and some have all-access, increasing the whole system's efficiency.
- **Chaincode**
  Chaincode is the list of functionalities and rules a transaction needs to follow to be processed and approved.
- **Modular Design**
  The HyperLedger has a modular design that can be shaped as mandatory.

2.8 Comparison Between Hyperledger and Other Blockchains

Hyperledger vs. Ethereum

Ethereum is a public, disseminated, and decentralized Blockchain type intended to execute Smart Contracts. Since it is a decentralized stage, each participant(node) in the organization approaches a similar copy of the Blockchain network. At whatever point another block is added to the Ethereum Blockchain, it will be added to the all-inclusive duplicate that exists with all individual hubs in the organization [34].

On the other hand, Hyperledger is an open-source Blockchain venture created and facilitated by the Linux Foundation. In any case, it is worldwide cooperation among driving organizations across an account, banking, IoT, innovation, and assembling enterprises. It is a permissioned Blockchain structure intended for creating adjustable Blockchain applications to oblige precise business needs. Since Hyperledger was made remembering the necessities of associations, it has a secluded design and capacities as a fitting and-play system that permits ventures to modify Blockchain applications as per their special requirements. Hyperledger involves a large group of instruments and activities that convey high adaptability, privacy, and versatility.

Hyperledger vs. Quorum

Quorum is a centered blockchain stage based around Ethereum. It gives a layer on top of Ethereum, which empowers it to perform private exchanges and makes it more robust by utilizing various agreement calculations. It is created by J.P.Morgan [35], which intends to execute a Global Network Payments activity to assist manages an account utilizing dispersed organizations.

Hyperledger has an enormous technology stack, including membership services, blockchain services, and chain code services. At the same time, Quorum is an Ethereum platform with modified services.

Hyperledger supports at least 500 transactions per second, while Quorum supports 100 transactions per second.

Hyperledger vs. R3 Corda

R3 Corda was one of the leading players to get the Distributed Ledger Technology's latent capacity. While the remainder of the world was centered around Bitcoin, R3 zeroed in on the private part of Blockchain

Hyperledger is necessary for a multi-venture exertion, facilitated by The Linux Foundation and initially sourced by IBM, while Corda is the principal result of the R3 consortium [36]. One intends to interconnect various diverse business areas, while different accepts selection among finance organizations as a worldwide autonomous organization.

Chapter 3

3. Methodology

3.1 Blockchain and IoT Projects

The Blockchain is known as an advanced system in terms of security and privacy. Due to these unique features, its adoption in Fintech and countless other areas has become the norm of the day. Its usage in the Internet of things (IoT) is gaining market trust. Besides its application in evolutionary innovation like IoT devices, it is challenged by computational cost, high bandwidth overhead, and delays. Research studies have found ways to improve the efficiency of Blockchain and to overcome these issues. For IoT, Blockchain can act as a preferred foundation. However, Dorri and Kanhere (2017) [37] are of the view that eliminating the proof of work (POW) and the concept of coins can make Blockchain better. Several other improvements ideas are under the testing phase.

3.1.1 IoT Challenges

IoT is a rapidly evolving industry; from organizational use to personal, it has found its way into every common task of our lives. With all the benefits, the use of web-based devices has its challenges [38]. Some of the significant challenges right now are:

Outdated Hardware: People buy these web-enabled devices and at the time they are secure, but as the world of IT is continuously evolving, malicious users always are looking for a way to find a backdoor.

Rouge IoT Devices: Even though it isn't generally conceivable to ensure 100% security, the thing with IoT gadgets is that most of the clients don't know if their device is hacked. When there is a considerable size of IoT gadgets, it gets hard to screen every one of them in any event for the specialist co-ops. It is because an IoT gadget needs applications, administrations, and conventions for correspondence. Since the quantity of devices is expanding altogether, the number of things to be overseen increases significantly. Henceforth, numerous gadgets continue working without the clients realizing that they have been hacked.

Data Safety: The safety camera installed in anyone's home or office are there to protect them from intruders. But these devices do have a lot of information about the

individual's daily activities. If they fall into the wrong hands can be dangerous. The data stored on a cloud server can be tampered with no trace, leading to industrial espionage. The Industry needs a base security protocol that prevents the data from falling into the wrong hands.

3.1.2 Blockchain Solution for IoT Challenges

Security: Data security and reliability is one the main issues where IoT is concerned. Malicious users have figured out how to access IoT gadgets like accessing vehicles distantly, home security, or phones. This may not sound a lot, yet consider that IoT gadgets are utilized in the clinical business. If third-party access embedded IoT gadgets, the threat could be dangerous. These issues can be resolved using Blockchain that employs the best encryption standard to ensure IoT data security.

Integrity: It is integral for some systems to maintain the integrity of the data and ensure that it has not been altered. A Blockchain system ensures that integrity is maintained as the transactions cannot be changed without proper access and Consensus.

Availability: The blockchain system ensures that the system is available at all times. The services are always available when needed by an authorized user due to the distributed ledger system. The Blockchain permits users to support networks with frequent users and retain the blocks in a decentralized model with several chain duplicates on the system.

Confidentiality: Blockchain ensures that only authorized users have access to the system and information. To provide this, it uses mechanisms like the use of hash functions to secure the identities of authorized users.

3.1.3 Previous Research

The Blockchain is known as an advanced system in terms of security and privacy. Technology is growing day by day, and new things are introduced almost every day.

But with growing technology, the factor of increasing security and efficiency is also increasing. Centralized Blockchain technology can act as a preferred foundation to overcome all these issues.

Lately, the execution of specific IoT devices and methods in many industrial sections has drawn much study interest. The creators of (reference) introduced a use case for the Agri-Food [39], which proposed the transparency of the inventory through IoT. The

point was to explore the utilization of RFID and NFC-based gadgets to achieve direct on-the-field straightforwardness and constant data creation, considering perseverance through a cloud-based information base that isn't decentralized. This is undoubtedly the traditional worldview the majority of the current IoT-based arrangements have embraced by a long shot. However, the utilization of IoT and Blockchain advancements is still an examination field under-investigated yet worth investigating.

3.2 Proposed Idea

In this proposition, we are utilizing HyperLedger Fabric Blockchain for putting away IoT information. As HyperLedger is a private Blockchain, we can control who will access IoT information. HyperLedger permits access just to approved users as characterized in its Policy. HyperLedger likewise utilizes state of the craftsmanship encryption principles for transactions. This makes the HyperLedger Fabric Blockchain highly sure from malicious users.

HyperLedger uses X.509 authentications for managing the identities of authorized users. This makes sure that only those parties have access to the data. HyperLedger can permit reading or writing to diverse elements relying upon the confidence we have in that user. This helps us to control the security of our IoT information.

We will design a HyperLedger Network, which will comprise two organizations and four peers. Every organization will have two peers each. Our organization will likewise contain one Orderer, which will be utilized for requesting our IoT exchanges.

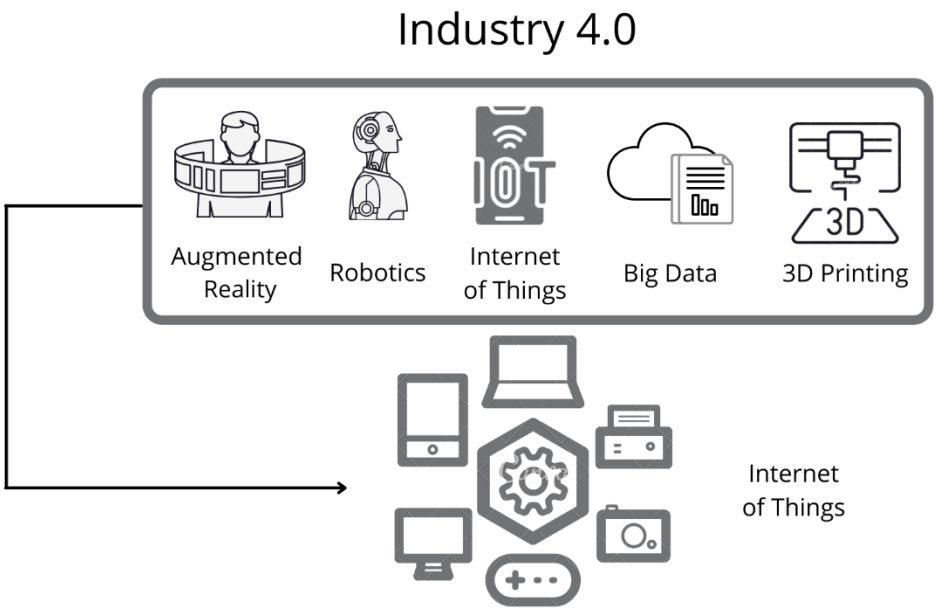

Figure 5 Industry 4.0

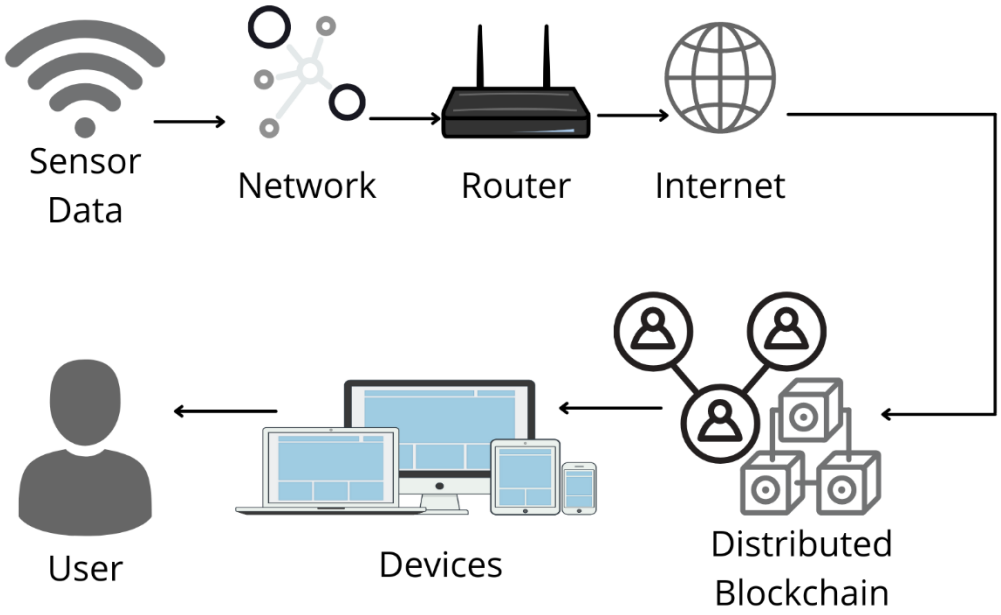

Figure 6 Process of IoT using Blockchains

3.2.1 Hyperledger Blockchain Configuration

The HyperLedeger Fabric is the core of the Blockchain network. We need to design different substances, peers, associations, strategies, channels, and much more. A large portion of the HyperLedger configuration goes into the yml or yaml records.

HyperLedger consists of the following binaries for creating several types of configurations:

Configtxgen: It is used for creating the first block of the Ledger. The first block is also the genesis block which is essential for bootstrapping the Orderer node and the channel configurations.

Cryptogen: It is used for creating cryptographic material for various individuals of the organization.

3.2.2 Network Architecture

We use docker containers for designing different elements in the Blockchain Network [40]. For our Blockchain network, we have compartments for the entitles given below:

- Peers
- Orderer
- CouchDB
- Fabric Certificate Authority
- cli-to access all the peers

These containers are fragments of a sole Docker instance; even the chain code is executed in a distinct container.

3.2.3 Docker Containers

Docker is a service tool that provides OS-level virtualization to deliver applications in bundles called containers. These containers are secluded from each other and pack their product, libraries, and set up records; they can speak with one another through all-around characterized channels [41]. Some of the benefits of using Docker are: [42]

Performance: As Docker containers do not consist of an OS, they have a much smaller footprint like virtual machines. They start quickly and are faster and more flexible,

Portable: Docker containers can be used to move one application to another system, provided that it will perform the same way as it did on the other system when last tested.

Segregation: A Docker container containing one of your applications also incorporates the necessary adaptations of any supporting programming that your application requires.

3.2.4 Block Structure in HyperLedger

The HyperLedger consists of the following major components [43]:

World State

World state stores the current states of different conditions of the Ledger. The current state of these conditions can be effortlessly read from the World state, which tries not to cross the whole exchange log and consequently saves time. The state of the Ledger is represented as key-value sets which are refreshed, created, and deleted regularly.

Blockchain State

It is a log of a multitude of transactional records that lead us to the world state. These transactions are coordinated into blocks connected to shape the Blockchain, allowing us to record all the experiences that prompted the current world state.

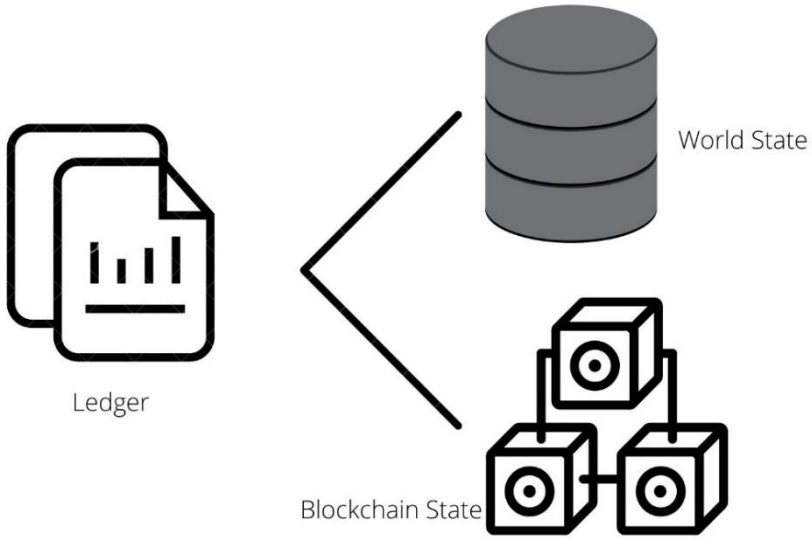

Figure 7 HyperLedger Block Structure

Hyperledger Block has three main parts, which are:

Block header: The header contains the Block number, hash of the previous block, and hash of the current block.

Block Metadata: Metadata contains the time block was composed, public key, signature, and square author's endorsement. From that point, the block committer additionally adds a flag that tells whether an exchange is legitimate/invalid. This Data about the legitimate/weak interaction isn't utilized in the hash as the hash gets made while making the block, and this flag is added when keeping in touch with the record.

Data: This part contains a rundown of requested exchanges. These exchanges are added to obstruct information at the point when the block is made. These exchanges have a primary and justifiable structure

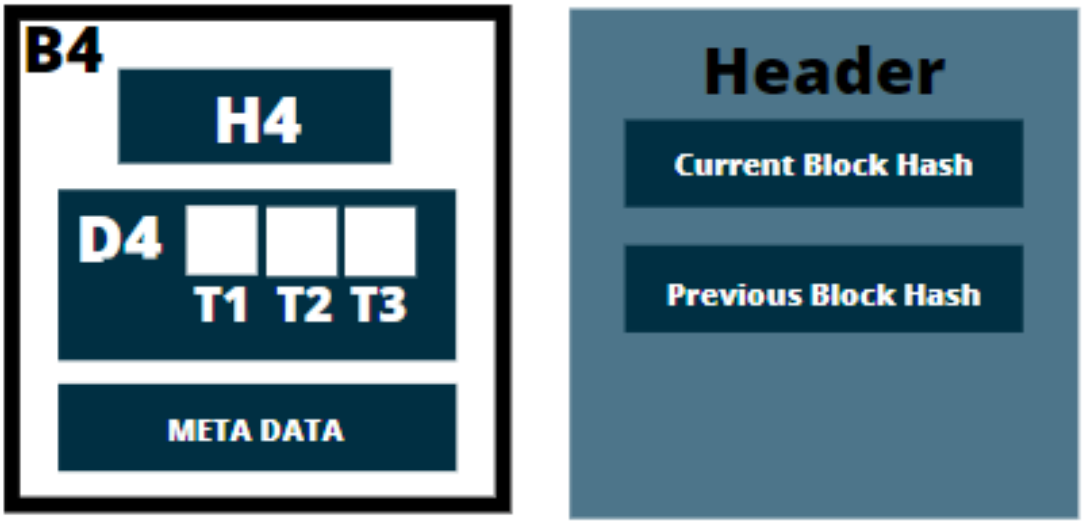

Figure 8 Block Structure in HyperLedger

3.2.5 HyperLedger Transactions

The Transactions contain any change happening in the world state. It consists of the following components:

Header:

The header contains significant metadata about the exchange, for instance, the name and form of the proper chain code.

Proposal:

The proposition incorporates the information boundaries gave to the chain code by an

application making the proposed update of the record. This proposition delivers many input factors once the chaincode runs, which, along with the current world state, decides the new world state.

Endorsements:

It is a rundown of transactions that are marked and are adequate to meet the policies. Just one transaction is remembered for the exchange even though there might be various supports. This is because every underwriting successfully encodes the specific exchange reaction from its association which implies that including any exchange reaction that doesn't coordinate adequate support would be a misuse of the asset as it will get dismissed and stamped invalid what's more, it would not refresh the world condition of the record.

Signatures:

This contains a cryptographic mark that is made by the utilization of the customer. It is used to watch that the subtleties of the exchange were not adjusted as it requires the application's private key to produce it.

Response:

This segment catches the world state's when esteems as a Read-Write (RW-set) set. It is a chain code yield, and if the exchange is approved effectively, refreshing the world state will be applied to the record.

3.2.6 HyperLedger Database

HyperLedger upholds two sorts of state databases which comprise CouchDB and levelDB [44]. CouchDB is a discretionary outer state information base alternative. LevelDB is the default database of key-value states installed in the peer cycle. Together CouchDB and level DB can accumulate any twofold data; however, CouchDB likewise bolsters JSON. This permits running rich questions against the displayed JSON information. The two of them again uphold getting and setting dependent on keys and running inquiries dependent on keys. Querying keys by range is conceivable, and composite keys can be demonstrated against different boundaries to permit identical searches. Utilizing CouchDB and displaying resources as JSON allows us to run complex, rich questions against the information esteems. These sorts of inquiries permit us to see and investigate the information the Ledger. The reaction of these inquiries

doesn't go to the Orderer as exchanges. However, they are straightforwardly shipped off the customer application. The queries are not rational for update interactions; as a result, returned isn't steady, but if the application can deal with the security amid the submit time and Chaincode implementation time or the potential fluctuations in the resulting exchanges dealt with. CouchDB runs adjacent to the contact as a diverse information base degree, so there are numerous contemplations regarding arrangement, the executives, and responsibilities.

3.3 System Architecture

Our system is composed of 2 parts:

- IoT Systems
- Private Blockchains

3.3.1 System Setup

Our Hyperledger Blockchain configuration [25] comprises two organizations, org1 and org2, each with two peers. CA1 and CA2 are the Certificate Authorities for each organization. Peer 0 and Peer 1 are the names of our peers. The domains org1 and org2 are used to distinguish between distinct organizations' peers [45].

The transactional flow will be like this:

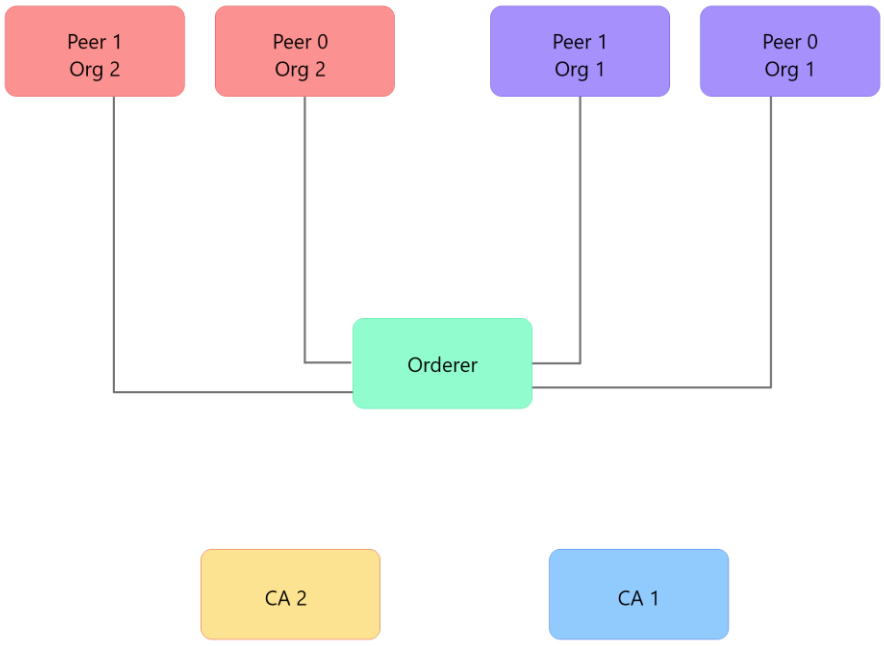

Figure 9 Transactional Flow in Hyperledger

3.3.2 Operational Flow

Our Blockchain system supports two main operation types.

- Insert information into the Ledger
- Scan data from the Ledger

the subsequent two operations don't seem to be supported as elementary to the Blockchain principal.

- Change any entry within the Ledger
- Deleting any value from the Ledger.

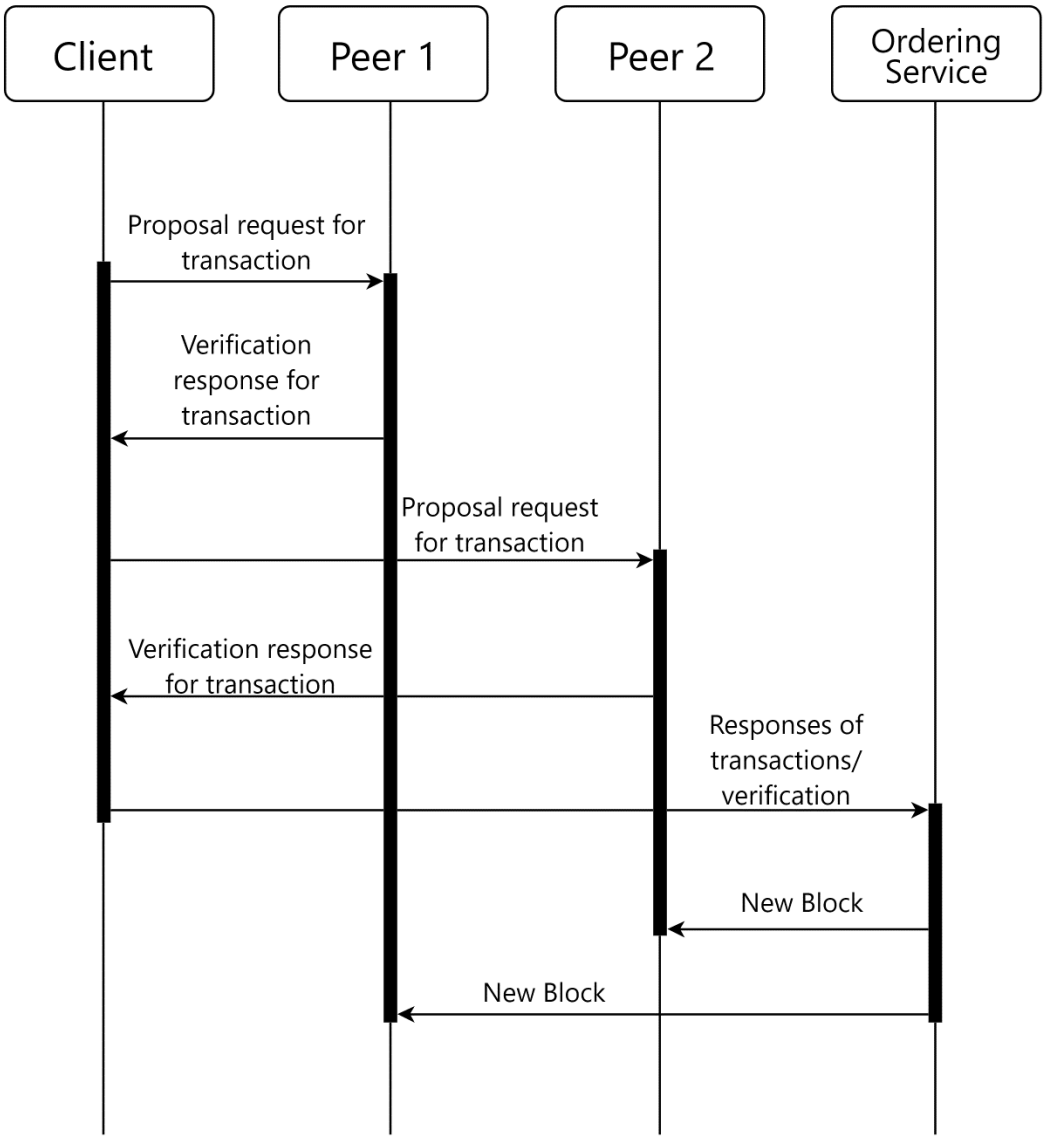

Figure 10 Operational Flow of Hyperledger

For insertion, we tend to use the timestamp of the payload as the key. For reading, we use the most recent timestamp to retrieve the last inserted value in the Ledger.

3.3.3 Importing Data into the Ledger

We will import an IoT data set to the Ledger. The dataset will contain sensor data with a timestamp to keep track of information change. The client running on fabric SDK will receive this Data, and at the node, a JavaScript application will receive this data set and create a transactional flow [46]. The existing peers will then approve the transaction in each organization. Once all the peers agree on the data, it will then be added to the Ledger.

3.3.4 Chaincode

HyperLedger was the primary platform to support go, node.js and java as sensible contract languages. Chaincode is just a smart contract written in any of the supported languages that implement the prescribed interface. The HyperLedger chain code runs in a separate Docker container, free the peer who is endorsing it. Chaincode acts as a middleware that uses the transactions submitted by the applying to manage the state of the Ledger. We tend to use go-language for writing the chain code.

Mostly, the chain code encapsulated the business logic united by the assorted business members within the network so synonymously that it may be known as a" smart contract." [47] The ledger state created by one chain code isn't directly accessible to a different chaincode inside a similar network. However, a chaincode can invoke another chaincode in the same network to create its state accessible if it's permission to try and do so. chaincode lifecycle operations are as follows:

Packaging: The chaincode has the defined package and different properties like name and version. It conjointly includes a nonobligatory installation policy that may be syntactically delineated within the same endorsement policy as described in the Endorsement Policy and a collection of chaincode-owned entity signatures. The signatures are accustomed to establishing chain code ownership, modifying the package contents, and sight packet manipulation or tampering. If there is over one chaincode owner, then the chaincode should be signed by multiple owners with multiple identities. During this case, we will create a signed CDS package that is passed serially to different

owners for signatures. after you deploy a chaincode with solely the identity signature of the node provision the install transaction.

Install: The transaction deployment does the next things. First, it programs the clever settlement or chaincode right into a preferred layout referred to as ChaincodeDeploymentSpec. Second, it additionally proceeds with the setup of the packaged chaincode at the peer node. The chaincode is to be established on every endorsing peer node of the channel. It must now no longer be found at the peer nodes that aren't endorsing peer nodes as it could affect the confidentiality of the chaincode logic.

Instantiating: For initializing associated making a chaincode on the channel, the instantiate dealing is employed. This kind of transaction invokes the Lifecycle System Chaincode that connects the chaincode to a channel. A similar chaincode operated severally, and on an individual basis on every channel it's instantiated, which suggests that the state is unbrokenly isolated to the channel no matter what percentage channels the same chaincode could also be installed. The creator of an instantiate transaction should befit the chaincode internal representation policy enclosed in the Signed chaincode and must also be an author on the channel organized as half of the channel creation process. This can be necessary for channel security to forestall unauthorized entities from deploying chaincodes or creating members on associate unbound channels to execute chaincodes.

Update: HyperLedger permits upgrading the chaincode as well. It is often elevated by changing its version number, which is there within the chaincode. Alternative components like owners and representation policy may be updated whereas upgrading; however, these are optional. However, the name of the chaincode ought to keep identical while upgrading; else, it might be thought-about a unique chaincode. Before upgrading, the new good contract or chaincode should be put in on all the endorsing peers. Upgrade group action instantly binds the updated chaincode to the channel. The preceding channels could have a similar chaincode set up, but the previous form can still run the prior chaincode version autonomously. In alternative words, the upgrade group action solely affects the channel wherever the upgrade transaction is submitted.

HyperLedger aims to add the add and stop feature as transactions that might enable, disable and re-enable a chaincode while not uninstalling it.

3.3.5 Blockchain Network Setup

To produce the network that includes cryptographic material for our exclusive entities, we utilized the cryptogen furnished with the assistance of using HyperLedger. It takes directions from a **crypto-config.yaml** document that incorporates our network shape and lets us generate keys and Certificates for numerous entities defined withinside the enter file.

HyperLedger configurations are set and up to date within the shape of transactions. HyperLedger offers a binary **configtxgen** or configuration transaction generator for producing those configurations

The **configtx** is used for creating the following:

- Channel configuration transactions
- Genesis Block
- Anchor peer replace transactions

configtx carries all of the configurations and rules for Orderer, peers, organizations. It additionally has rules which outline the rights of every organization.

The **configtx** also contains the policies and the name of the various entities utilized in the network. The guidelines are categorized as:

- Readers
- Writers
- Admins

3.3.6 Integration with Hyperledger Explorer

Hyperledger Explorer aims to form an easy web application for Hyperledger to view/query blocks, transactions and associated data, network data (name, status, list of nodes), chain codes/transaction families (view/invoke/deploy/query), and the other relevant information keep within the Ledger. [48]

The Fabric SDK will then be integrated with Hyperledger Explorer to view the blockchain structure. It will show the real-time processing of the transactions, blocks, and more. [49]

Chapter 4

4. Usecase, Results and Analysis

4.1 Smart Electronic Meter Use case

A smart meter is a high level energy meter that records the energy utilization of a consumer and gives added data to the utility by utilizing a two-way communication. Consumers are better educated in the utilization of their energy, so they can settle on better choices when they are utilizing the electricity. Providers then again will not require to physically peruse the records of utilized energy as they would get this data automatically.

The Smart meter will be connected to an internet device which will transmit the energy utilization in real-time to the service provider. The service provider will then receive the data and authenticate the source the data is transmitted from. If the source is authenticated the service provider will send the data through the Hyperledger Fabric and commit the entry to the ledger. The consumer can use the phone or desktop interfaces can be used to view the current utilization and manage their bills accordingly.

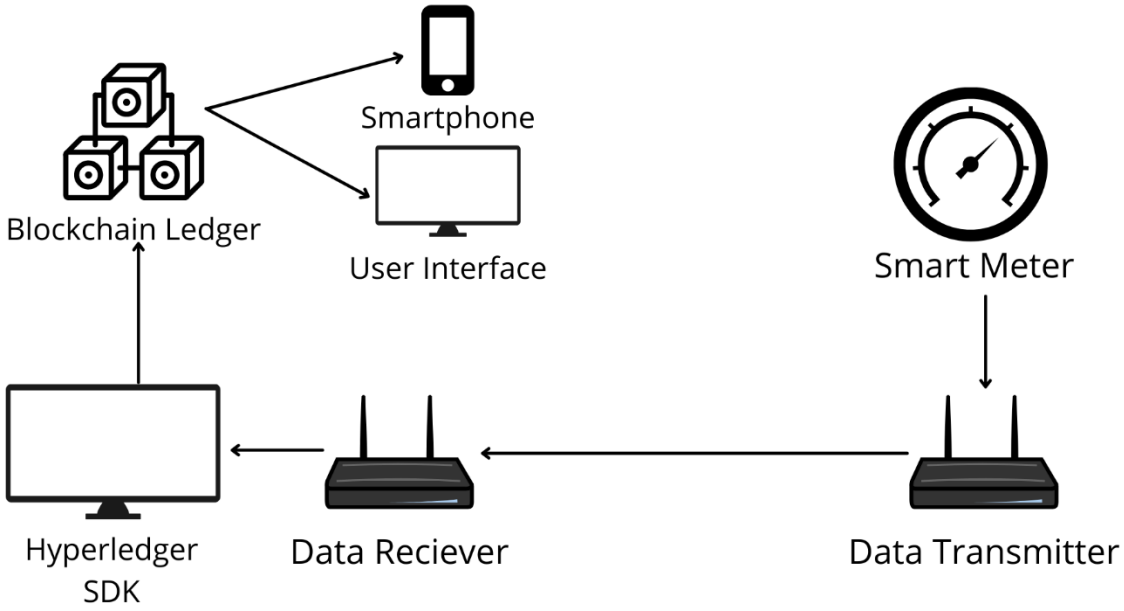

Figure 11 Smart Electronic Meter Use case

4.2 System Requirements

The pre-requisites for deploying the framework are:

- Ubuntu OS
- HyperLedger Fabric SDK 1.4
- HyperLedger Explorer
- cURL — latest version
- Docker — version 17.06.2-ce or greater
- Docker Compose — version 1.14.0 or greater
- Golang — version 1.11.x
- Nodejs — version 8.x (other versions are not in support yet)
- NPM — version 5.x
- Python 2.7

4.3 Processed Data Set

We are using a Family power consumption data set collected over six months. The Data contains the following attributes:

- Date in format dd/mm/yyyy
- Time in format hh:mm: ss
- Voltage average voltage per minute

We will store this Data in our HyperLedger fabric framework. We will add the entries in our HyperLedger Blockchain in bulk and individually to test the performance of our network. We will conduct the performance analysis on two functions:

- Adding new blocks to the network will depict the time utilized in adding new blocks of different sizes to the chain. The blocks will contain new data from the sensor.
- Adding new transactions to the network. The transaction can be to view, add, edit or delete a specific block in the chain. We will analyze the time utilized to perform that particular task.

4.4 Transaction Throughput

To check the time per transaction, which is the time distinction between once entry gets submitted, and the time it gets committed across the network, confirming the transaction. In contrast to protocols like Bitcoin or other public Blockchains, wherever the integrity of the transaction is decided to employ a probabilistic approach, Fabric's consensus method results in a settled finality approach. It takes 30-50 seconds to start the material network with all the containers set up.

4.5 Adding new Transactions

The following attributes were taken into consideration while analyzing:

- Timeout: The time it takes for the orderer node to create the next batch of data to be processed.
- Number of Entries: the number of data entries a batch contains.
- Size: The number of bytes per batch or entry.

4.5.1 Batch 1

We took our dataset and divided it into a few batches to analyze the performance for adding new transactions. For the first one, we took a set of 8 entries, all with varying numbers of records. We uploaded the data in our framework and calculated the time it took to process it. The graph below shows the "Processing Time" for each "Number of Entries."

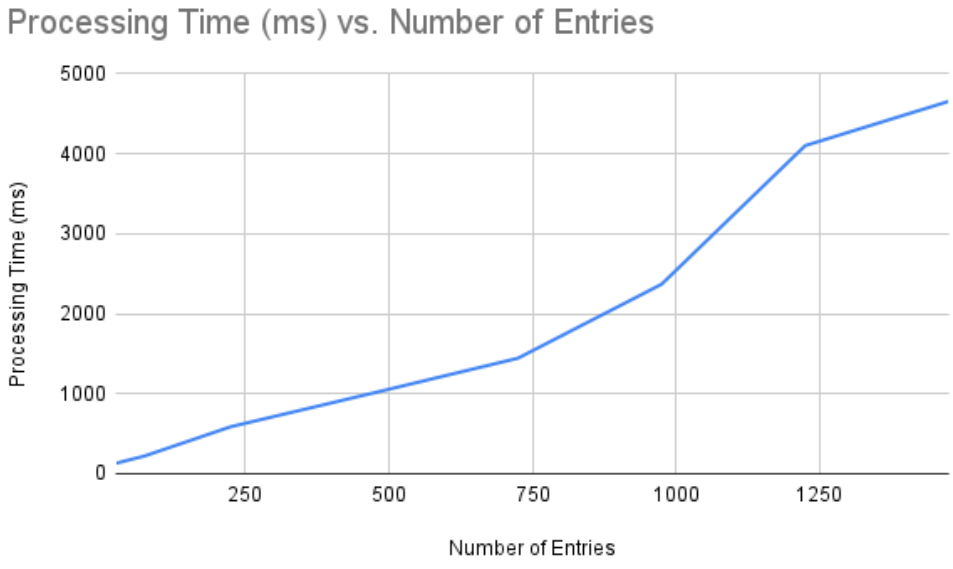

Figure 12 Line Graph Processing Time per Transaction for Batch 1

4.5.2 Batch 2

For Batch 2, we took a batch of 6 entries, all with varying numbers of records. We uploaded the data in our framework and calculated the time it took to process it. The graph below shows the "Processing Time" for each "Number of Entries."

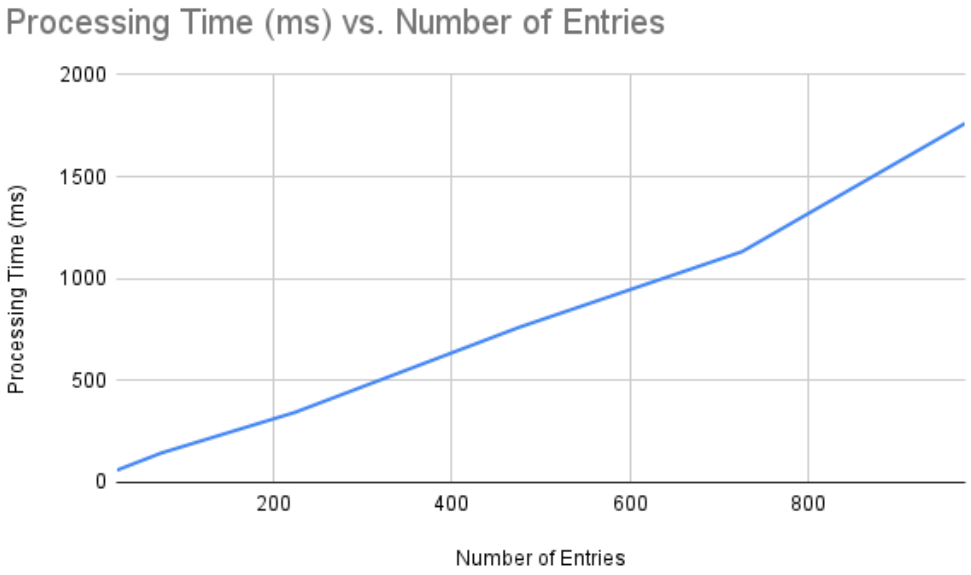

Figure 13 Line Graph of Processing Time per Transaction for Batch 2

4.5.3 Comparison between the Batches

We compared the processing time for each batch and concluded that the processing time increases as the volume of the data increases.

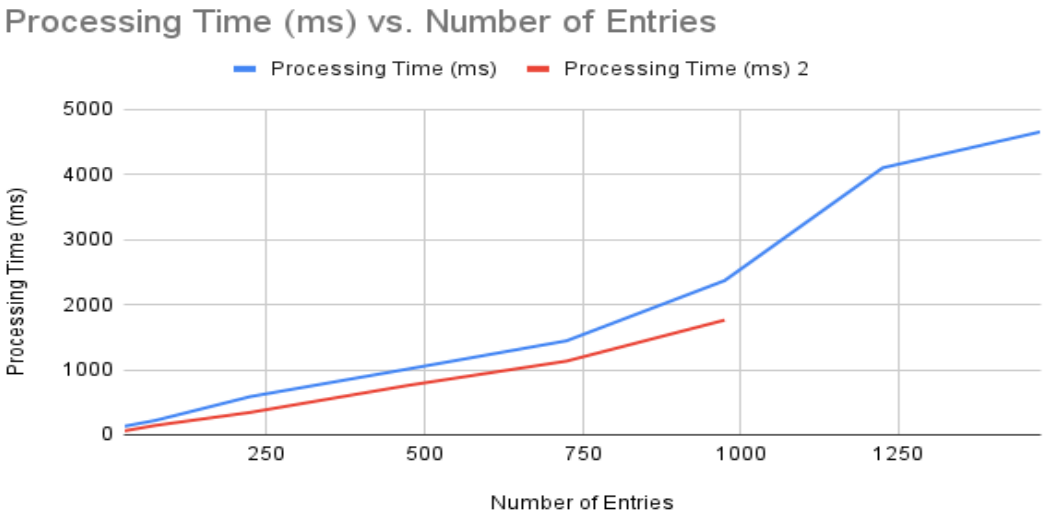

Figure 14 Line Graph Comparison between the Transaction Batches

4.6 Adding new Blocks

4.6.1 Batch 1

We took our dataset and divided it into a few batches to analyze the performance for adding new Blocks. For the first one, we took a set of 5 entries, all with varying numbers of records. We uploaded the data in our framework and calculated the time it took to process it. The graph below shows the "Processing Time" for each "Number of Entries."

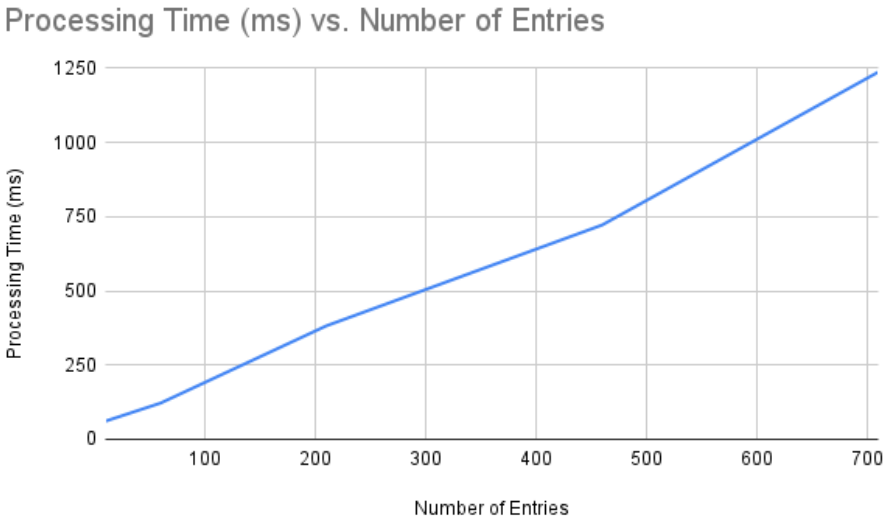

Figure 15 Line Graph Processing Time per Block Addition for Batch 1

4.6.2 Batch 2

For Batch 2, we took a batch of 6 entries, all with varying numbers of records. We uploaded the data in our framework and calculated the time it took to process it. The graph below shows the "Processing Time" for each "Number of Entries."

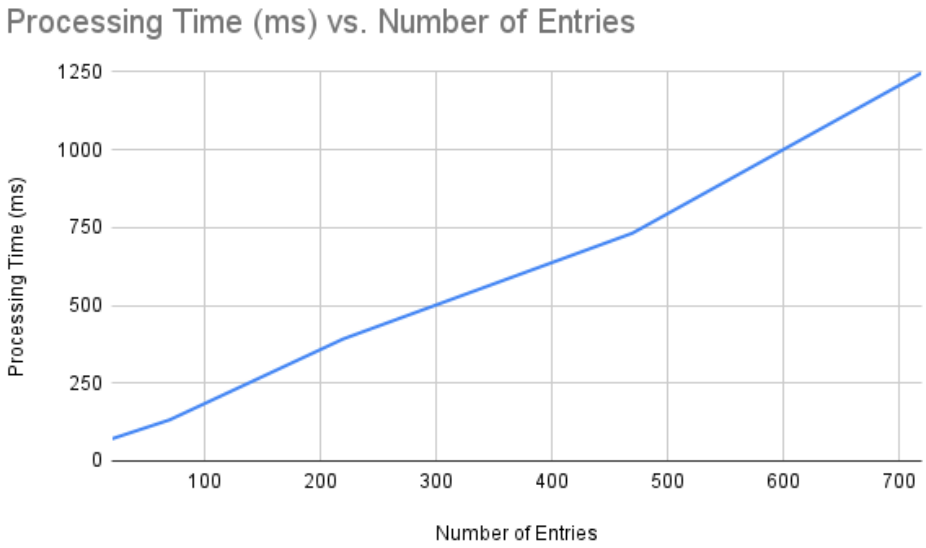

Figure 16 Line Graph Processing Time per Block Addition for Batch 2

4.6.3 Comparison between the Batches

We compared the processing time for each batch and concluded that the processing time stays the same for a similar number of entries even if they have an increased amount of data.

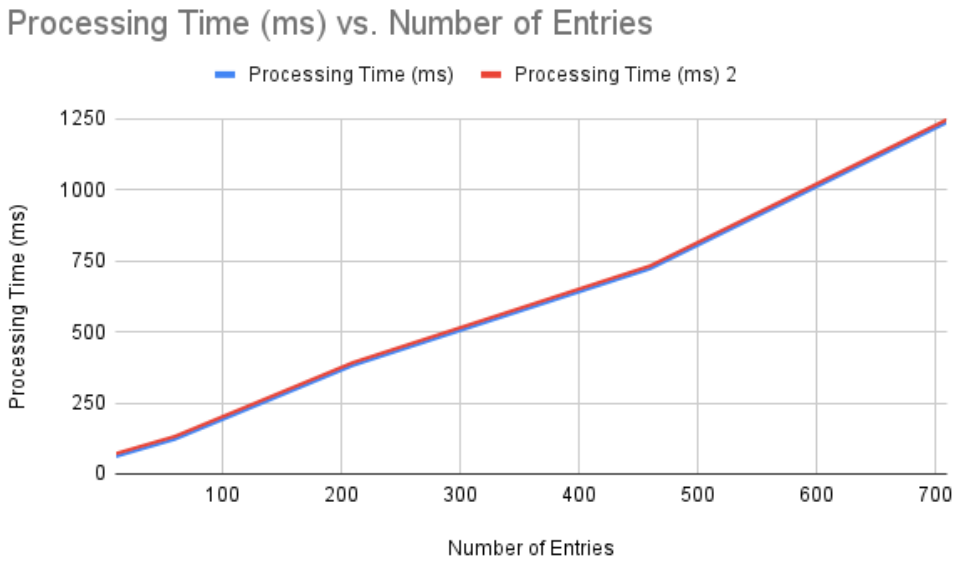

Figure 17 Line Graph Comparison between the Block Addition Batches

4.7 Result Summary

As we will see from the graphs that the time for writing will increase because the number of records or the transactions increases. We tend to conjointly see that the performance varies as we check our network with varied parameters. We will also see the version for parameter set 2 is healthier than parameter set 1. For parameter set 1, we employ a batch timeout of 3 seconds and a message count of 10. This suggests that a block would be superimposed to the Ledger if either the amount of messages has reached ten or 3 seconds is passed, whichever is earlier. For parameter set 2, we tend to use a batch timeout of 4 seconds and a message count of 20. Thus increasing the batch timeout and max message count doesn't essentially improve the performance. As for adding the Blocks manually with an explicit range of entries, we will see each batch take a virtually equal quantity of time. For Blocks, we use a batch timeout of 8 seconds. We will conclude that timeout and size play a vital role in the performance of the network. Increasing one parameter does not essentially mean development in the whole

performance. A balance is to be maintained between these values reckoning on a load of transactions expected.

Chapter 5

5. Future Work

5.1 Conclusion

The implementation of private Blockchain using Hyperledger Fabric works with the success that permits us to store IoT data that's trustworthy and verified. Our network works well for many transactions; however, having only two orderers limits its performance regarding the number of transactions it will handle. Our configuration orderers are ready to take 800-1400 transactions counting on numerous parameters like the batch timeout, size, etc. We tend to conclude that the HyperLedger platform can manage IoT data and the in-built endorsements, coding, and linguistic communication to ensure the security, validity, and integrity of the data. All the transactions in HyperLedger are TLS encrypted, ensuring that knowledge cannot be compromised throughout the internal network communications.

5.2 Future Implementation

In the future, the Hyperledger Fabric can be experimented with an in-depth network consisting of numerous IoT devices, as well as however not restricted to different models of Raspberry Pi, Odroid XU4, Asus Tinker Board, and Nvidia Jetson nano [50]. The system needs to appraise different configurations and integration models to live the performance matrices regarding hardware capabilities, process and memory constraints, power consumption, other agreement protocols on the network, scalability, and network latency. It'll outline a model to choose wherever to deploy a complete server or edge server or use our already deployed IoT devices for various tasks, including consensus networks on an equivalent device.

5.2.1 Future Implementation with Kafka

Kafka is principally a deficiency of open-minded, dispersed, evenly adaptable, submit a log. A submit log is fundamentally an added information structure. There are no change or cancellation prompts, no read or write locks, and the most pessimistic scenario intricacy O (1). With their relating Zookeeper group, there might be numerous Kafka hubs in the Blockchain organization. We intend to stretch out our design to help Kafka in which we have more than one Orderer.

5.2.2 Future Implementation with Raft

Our IoT Blockchain network execution was finished with a solo design that utilizes one Orderer. Be that as it may, we intend to stretch out our plan to a Raft-based requesting administration as well. Pontoon support opened up in HyperLedger since rendition 1.3. Utilizing Raft will make our organization more versatile and issue open-minded. It will likewise give a massive increase as far as execution and burden adjusting. Additionally, overseeing pontoon hubs is similarly simpler than Kafka and doesn't need the overhead of arranging and Managing the Zookeeper outfit alongside Kafka hub.

5.2.3 Future Implementation in Different Industries

The medical care industry copes with profoundly delicate data which should be overseen safely. Electronic Health Records (EHRs) hold different sorts of precise and delicate info, including names, addresses, government-managed retirement numbers, protection numbers, and clinical history. Such close-to-home information is significant to the patients, medical care specialist organizations, insurance supports, and examination foundations. In any case, the public arrival of this exceptionally delicate individual information presents genuine protection and security risks to patients and medical care specialists. Henceforth, we predict the pre-requisite of innovations to address personal information security challenges in medical services applications. Blockchain is a promising arrangement that gives straightforwardness, security, and protection utilizing agreement-driven decentralized information the executives on top of shared appropriated processing frameworks. This way, to tackle the referenced issues in medical care applications, in this paper, we explore the utilization of private blockchain advancements to assess their possibility for medical care applications. We make testing situations utilizing HyperLedger Fabric to investigate various rules and use-cases for medical services applications. Furthermore, we consider the agent experiment situations to survey the blockchain-empowered security standards for information classification, protection, and access control. The trial assessment uncovers the advantages of private blockchain advances regarding security, guideline consistency, similarity, adaptability, and versatility.

If we talk about the Legal industry, private Blockchain innovation can give a protected, suitable, permanent, and timestamped method for data sharing, which may conceivably reform the administration of reports and sharing of personal data between clients. Facebook and other online media delegates have unhindered admittance to whatever is

posted by clients. Blockchain innovation's decentralized and scrambled nature guarantees security without depending on a representative, like Facebook or Dropbox, who has extreme control and admittance to its clients' information. The key base is an application that works with encoded document sharing utilizing blockchain innovation, and Storj is another application that works with decentralized, scrambled start to finish record stockpiling. Blockchain Apparatus' experimental run program is additionally used to notarise and timestamp archives. These activities, which run on blockchain innovation, may hold the possibility of reforming secret reports dividing among parties in the suit, customers and legal advisors, courts and agents, and giving a safe and permanent record for the subbed administration of authoritative archives.

References

[1] Prediction/Usage of IoT Stats, "https://www.vxchnge.com/blog/iot-statistics," [Online].

[2] A., & Haq, Mushtaq, "Implications of Blockchain in industry 4. o. In 2019 International Conference on Engineering and Emerging Technologies," 2019.

[3] N. Mohamed and J. Al-Jaroodi, "Applying Blockchain in Industry 4.0 Applications".

[4] J. Robert E. Lucas, "The Industrial Revolution: Past and Future," 2004.

[5] K. Ashton, "That 'Internet of Things' thing".

[6] G. A. Kaivan Karimi, "What the internet of things (iot) needs to become," 2013.

[7] Ateeq Khan and Klaus Turowski, "A Survey of Current Challenges in Manufacturing Industry and Preparation for Industry 4.0".

[8] R. H.Weber, "Internet of Things – New security and privacy challenges".

[9] Stuart Haber, W. Scott Stornetta, Dave Bayer, "Improving the Efficiency and Reliability of Digital Time-Stamping".

[10] Harish Sukhwani, Jos´e M Mart´ınez, Xiaolin Chang, Kishor S Trivedi, and Andy Rindos, "Performance modeling of pbft consensus process for permissioned blockchain network," 2017.

[11] ShiEmin Gün Sirer, Dawn Song, Roger Wattenhofer, "On Scaling Decentralized Blockchains," *Kyle Croman, Christian Decker, Ittay EyalAdem.*

[12] Dijiang Huang, "Building private blockchains over public blockchains (pop): an attribute-based access control approach, ACM," 2019.

[13] M. Vukoli´c, "Rethinking permissioned blockchains," 2017.

[14] B. i. Finance, "https://www.financedigest.com/iot-for-the-financial-sector.html," [Online].

[15] Z. Alhadhrami, S. Alghfeli and M. Alghfeli, "Introducing blockchains for healthcare".

[16] Maciel M. Queiroz, "Blockchain and supply chain management integration: a systematic review of the literature".

[17] Leiter, "Legal Engineering on the Blockchain: ‘Smart Contracts’ as Legal Conduct," 2018.

[18] B. i. Defence, "https://www.eda.europa.eu/webzine/issue14/cover-story/blockchain-technology-in-defence," [Online].

[19] BOJANA KOTESKA, "Blockchain Implementation Quality Challenges: A Literature".

[20] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos and G. Das, "Everything You Wanted to Know About the Blockchain: Its Promise, Components, Processes, and Problems".

[21] What are public and private key pairs and how do they work, "https://securityboulevard.com/2019/05/what-are-public-and-private-key-pairs-and-how-do-they-work/," [Online].

[22] How does a transaction get into the blockchain?, "https://www.euromoney.com/learning/blockchain-explained/how-transactions-get-into-the-blockchain," [Online].

[23] What is PKI and How Does it Work?, "https://www.keyfactor.com/resources/what-is-pki/," [Online].

[24] P. Wohlmacher, "Digital certificates: a survey of revocation methods".

[25] C. Cachin, "Architecture of the Hyperledger Blockchain Fabric".

[26] A. F. Pavlos Charalampidis, "When Distributed Ledger Technology meets Internet of Things -- Benefits and Challenges".

[27] Top Hyperledger Frameworks & Hyperledger Tools For Blockchain Technology, "https://www.upgrad.com/blog/hyperledger-frameworks-hyperledger-tools-blockchain-technology/," [Online].

[28] S. S. Chinmay Saraf, "Blockchain platforms: A compendium, IEEE," 2018.

[29] H. Grid, "https://www.hyperledger.org/use/grid," [Online].

[30] Pierre-Louis Aublin, Sonia Ben Mokhtar, and Vivien Qu´ema Pierre-Louis Aublin, 2013.

[31] D. l. software, "https://www.hyperledger.org/use/sawtooth," [Online].

[32] Kazuhiro Yamashita, Yoshihide Nomura, Ence Zhou, Bingfeng Pi, and Sun Jun, "Potential risks of hyperledger fabric smart contracts, IEEE," 2019.

[33] Hyperledger function, "https://hyperledger-fabric.readthedocs.io/en/release-1.4," [Online].

[34] P. S. Martin Valenta, Comparison of Ethereum, Hyperledger Fabric and Corda, 2017.

[35] Corda, Hyperledger, Quorum – What's the difference "https://www.tradefinanceglobal.com/posts/corda-hyperledger-quorum-whats-the-difference/," [Online].

[36] Richard Gendal Brown, James Carlyle, Ian Grigg, and Mike Hearn, 2016.

[37] J. R. Dorri, "Towards an optimized Blockchain for IoT. In 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI)," 2017.

[38] A. Bassi, "IoT Challenges".

[39] I. o. T. industry, "https://builtin.com/blockchain/blockchain-iot-examples," [Online].

[40] H. Network, "https://hyperledger-fabric.readthedocs.io/en/release-1.2/network/network.html," [Online].

[41] Kitti Klinbua, "Translating tosca into docker-compose yaml file, IEEE," 2017.

[42] Docker: Top 7 Benefits of Containerization, "https://hentsu.com/docker-containers-top-7-benefits/," [Online].

[43] Examining the Behaviour of Hyperledger Fabric when World State is tampered, "https://kctheservant.medium.com/exploring-the-behaviour-of-hyperledger-fabric-when-world-state-is-tampered-764676fe90f2," [Online].

[44] S. Database, "https://hyperledger-fabric.readthedocs.io/en/release-2.2/couchdb_as_state_database.html," [Online].

[45] Hyperledger, "https://hyperledger-fabric.readthedocs.io/en/release-2.2/whatis.html," [Online].

[46] Node.js, "https://hyperledger.github.io/fabric-sdk-node/," [Online].

[47] Konstantinos Christidis, "Blockchains and Smart Contracts for the Internet of Things," 2016.

[48] hyperledger.org, "https://wiki.hyperledger.org/display/explorer/Hyperledger+Explorer," [Online].

[49] H. Explorer, "Hyperledger Explorer Documentation," [Online].

[50] Adnan Iftekhar, Xiaohui Cui, Qi Tao, and Chengliang Zheng, "Hyperledger Fabric Access Control System for Internet of Things Layer in Blockchain-Based Applications".

[51] Hyperledger Fabric: the flexible Blockchain framework that’s changing the business world:, "https://www.ibm.com/Blockchain/hyperledger," [Online].

[52] C. Cachin, "Architecture of the hyperledger Blockchain fabric. In Workshop on distributed cryptocurrencies and consensus ledgers (Vol. 310, No. 4)," 2016. [Online].

[53] That is Hyperledger? Hyperledger Business Blockchain Technologies:, "https://medium.com/@kotsbtechcdac/what-is-hyperledger-hyperledger-business-Blockchain-technologies-df97580e2923," [Online].