PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA
Ministry of Higher Education and Scientific Research
Mohamed Khider University – BISKRA
Faculty of Exact Sciences
Computer Science Department

Order n°: MASTER_Startup_2025

Thesis

Presented to obtain the diploma of academic Master in
Computer Science
Option: Information and Communication Networks and Technologies

PCP: A Blockchain Approach for Securing and Enhancing Transparency in Algeria's Pharmaceutical Supply Chain

By:
BOUDOUH Badis - DIDICHE ACHOUR Mohcene

Defended on 16-19/06/2025, in front of the jury composed of:

Name	Grade	Role
Lanani Sadok	MAA	Supervisor
Kahloul Laid	Professor	Co-Supervisor
Sahraoui Mohamed	Professor	President
Zerdoumi Oussama	MAA	Examiner

Academic year 2024-2025

Abstract

Algeria's pharmaceutical supply chain faces various challenges, including poor coordination among stakeholders, weak transparency, circulation of counterfeit drugs, and inefficient resource distribution. These issues compromise medication availability, threaten patient safety, and undermine public trust in the healthcare system. This thesis presents the Pharmaceutical Collaborative Platform (PCP), a blockchain-based solution built on Hyperledger Fabric, designed to modernize and secure Algeria's pharmaceutical supply chain. The platform enables transparent, tamper-resistant, and auditable transactions among manufacturers, suppliers, pharmacies, and regulatory authorities. Through the fundamental advantages of blockchain technology immutability, decentralization, and cryptographic security the Pharmaceutical Collaborative Platform (PCP) ensures end-to-end traceability of pharmaceutical products, prevents the circulation of counterfeit drugs, and supports regulatory compliance. The system architecture employs private channel, smart contracts, and a permissioned network to maintain data confidentiality. The platform's key capabilities include real-time inventory management, automated recall alerts, facilitating purchasing operations, and supporting inter-pharmacy exchanges. A prototype application was developed and its performance tested using Hyperledger Caliper across varying transaction loads, demonstrating scalability and reliability. PCP represents a strategic advancement toward an integrated, transparent, secure, and responsive pharmaceutical system in Algeria, providing a scalable model for blockchain-based supply chain management.

الملخص

تواجه سلسلة توريد الأدوية في الجزائر تحدياتٍ مختلفة، تشمل ضعف التنسيق بين الجهات المعنية، وضعف الشفافية، وتداول الأدوية المزيفة، وعدم كفاءة توزيع الموارد. تُعرّض هذه المشكلات توافر الأدوية للخطر، وتهدد سلامة المرضى، وتقوّض ثقة الجمهور في نظام الرعاية الصحية. تُقدّم هذه المذكرة منصة التعاون الدوائي (Pharmaceutical Collaborative PCP Platform) وهي حلّ قائم على تقنية بلوكتشين، مبني علىHyperledger Fabric ، لتحديث وتأمين سلسلة توريد الأدوية في الجزائر. تُتيح المنصة معاملاتٍ شفافة، ومقاومةً للتلاعب، وقابلةً للتدقيق بين المصنّعين والموردين والصيدليات والهيئات التنظيمية. بفضل المزايا الأساسية لتقنية بلوكتشين، من ثبات، ولامركزية، وأمان تشفيري، تضمن منصة التعاون الدوائي (PCP) إمكانية تتبّع المنتجات الدوائية من البداية إلى النهاية، وتمنع تداول الأدوية المزيفة، وتدعم الامتثال التنظيمي. يستخدم هيكل النظام قناتٍ خاصة، وعقودًا ذكية ، وشبكةً مُصرّحًا بها للحفاظ على سرية البيانات. تشمل القدرات الرئيسية للمنصة إدارة المخزون في الوقت الفعلي، وتنبيهات الاستدعاء الآلية، وتسهيل عمليات الشراء، ودعم التبادل بين الصيدليات. تم تطوير نموذج أولي للتطبيق واختبار أدائه باستخدام Hyperledger Caliper عبر أحمال معاملات متنوعة، وقد أظهر قابلية التوسع والموثوقية. يُمثل PCP تقدمًا استراتيجيًا نحو نظام صيدلاني متكامل شفاف وآمن وسريع الاستجابة في الجزائر، مُوفرًا نموذجًا قابلًا للتطوير لإدارة سلسلة التوريد قائمًا على تقنية البلوك تشين.

Acknowledgments

"And if you should count the favors of Allah, you could not enumerate them. Indeed, Allah is Forgiving and Merciful."
(Qur'an 16:18)

First and foremost, all praise and gratitude are due to **Allah**, the Most Gracious, the Most Merciful, for granting me the strength, patience, and wisdom to complete this work. Without His guidance and blessings, nothing would be possible.
I would like to express my deepest appreciation and love to my **family**, who have been my unwavering source of support and encouragement. Their endless love, sacrifices, and belief in me have been my greatest motivation throughout this journey.
A heartfelt thank you to my **professor**, whose invaluable guidance, patience, and insightful feedback have greatly contributed to my learning and the completion of this work. Your mentorship has been truly inspiring.

With sincere gratitude,
Boudouh Badis , DIDICHE ACHOUR Mohcene

Contents

List of Figures

List of Tables

General Introduction

The global pharmaceutical supply chain (PSC) is a critical infrastructure responsible for the manufacturing, distribution, and delivery of medications, directly impacting public health and patient safety. However, this complex network is frequently undermined by significant challenges, including the proliferation of counterfeit drugs, insufficient transparency, and persistent gaps in traceability. These issues pose severe risks to patients, lead to substantial economic losses, and erode public trust in healthcare systems. In Algeria, the pharmaceutical sector specifically faces obstacles related to inefficient coordination, difficulties in tracking product availability, and a lack of real-time market insights, which contribute to shortages and suboptimal resource distribution.

To address these pressing challenges, this thesis proposes the design, development, and evaluation of a blockchain-based platform, the Pharmaceutical Collaborative Platform (PCP), built on the enterprise-grade Hyperledger Fabric framework. The primary objective of this research is to create a decentralized, secure, and transparent system that ensures the end-to-end traceability of pharmaceutical products. By leveraging the inherent features of blockchain technology—such as immutability, cryptographic security, and shared, permissioned ledgers—the proposed solution aims to foster trust among key stakeholders: manufacturers, suppliers, pharmacies, and regulatory authorities. The system is designed to track the origin and movement of medications, ensure data integrity, facilitate real-time regulatory oversight, and improve the efficiency of critical processes like product recalls.

This work documents the complete lifecycle of the project, from conceptual design to practical implementation and performance analysis. The architecture involves a permissioned network where each organization operates its own nodes, interacting through smart contracts (chaincode) that govern the business logic of the supply chain. A client application with a RESTful API and web interface was developed to provide a user-friendly means of interacting with the blockchain network.

The thesis is structured as follows:

- **Chapter 1** provides a comprehensive overview of the pharmaceutical supply chain, its key stakeholders, processes, and the critical challenges it faces, establishing the imperative for a robust tracking mechanism.
- **Chapter 2** delves into the foundational concepts of blockchain technology and offers a detailed examination of the Hyperledger project, with a specific focus on the architecture and key features of Hyperledger Fabric.
- **Chapter 3** presents the detailed system design and architecture, outlining the network topology, channel configuration, smart contract logic, asset definitions, and transaction flows that form the blueprint for the solution.
- **Chapter 4** describes the practical implementation of the proposed system, including the environment setup, chaincode development, client application construction,

and concludes with a rigorous performance evaluation using Hyperledger Caliper to assess the system's throughput, latency, and stability under various loads.

Chapter 1

The Pharmaceutical Supply Chain: Processes, Stakeholders, and Critical Challenges

1.1 Introduction

The pharmaceutical supply chain (PSC) is a complex, globally interconnected network responsible for the discovery, development, manufacturing, and distribution of medicinal products from raw material suppliers to end-users [1], [2]. Its integrity and efficiency are paramount, directly impacting public health outcomes and patient safety [3]. However, the modern PSC faces numerous formidable challenges, including the pervasive threat of counterfeit drugs, persistent traceability issues, stringent and varied regulatory compliance demands, and significant transparency gaps [4], [5]. These challenges not only pose severe risks to patient health but also result in substantial economic losses for legitimate manufacturers and healthcare systems [6]. This chapter will provide a comprehensive overview of the pharmaceutical supply chain, delineating its key stakeholders and typical processes. It will then delve into the critical challenges that undermine its integrity, supported by statistics and case studies, emphasizing the urgent need for robust, reliable, and tamper-proof tracking mechanisms to safeguard public health.

1.2 The Pharmaceutical Supply Chain: Key Stakeholders and Processes

The pharmaceutical supply chain encompasses a series of intricate and interdependent processes involving multiple stakeholders, each playing a critical role in ensuring that safe and effective medicines reach the patient [2], [7].

1.2.1 Key Stakeholders

The primary stakeholders in the pharmaceutical supply chain include:

1. **Raw Material Suppliers**: These entities provide the Active Pharmaceutical Ingredients (APIs) and excipients necessary for drug formulation [2]. The quality and authenticity of these initial components are foundational to the safety of the final product.

2. **Manufacturers (Pharmaceutical Companies)**: These are responsible for the research, development, and production of finished pharmaceutical products (FPPs) [1]. They conduct rigorous quality control tests and adhere to Good Manufacturing Practices (GMP) [8].

3. **Wholesalers/Distributors**: These intermediaries purchase drugs in bulk from manufacturers and manage their storage and distribution to pharmacies, hospitals, and other healthcare providers [7]. They play a crucial role in inventory management and logistics, including maintaining cold chain integrity for temperature-sensitive products [9].

4. **Re-packagers and Secondary Packagers**: These entities may repackage drugs into different quantities or combine products, often requiring specific labeling and tracking [4].

5. **Pharmacies (Dispensers)**: Retail and hospital pharmacies are the primary points of contact for patients, responsible for dispensing medications and providing counseling [2].

6. **Hospitals and Healthcare Providers**: These institutions procure and administer medications directly to patients [7].

7. **Patients (Consumers)**: The end-users of pharmaceutical products, whose health and safety depend on the integrity of the entire supply chain [3].

8. **Regulatory Authorities**: Government bodies such as the U.S. Food and Drug Administration (FDA), the European Medicines Agency (EMA), and national regulatory agencies in other countries. They oversee the entire lifecycle of pharmaceutical products, setting standards, enforcing regulations, conducting inspections, and monitoring post-market surveillance [8], [10].

9. **Logistics Providers**: Specialized transportation and warehousing companies that handle the physical movement and storage of pharmaceuticals, often requiring specialized conditions (e.g., temperature control) [9].

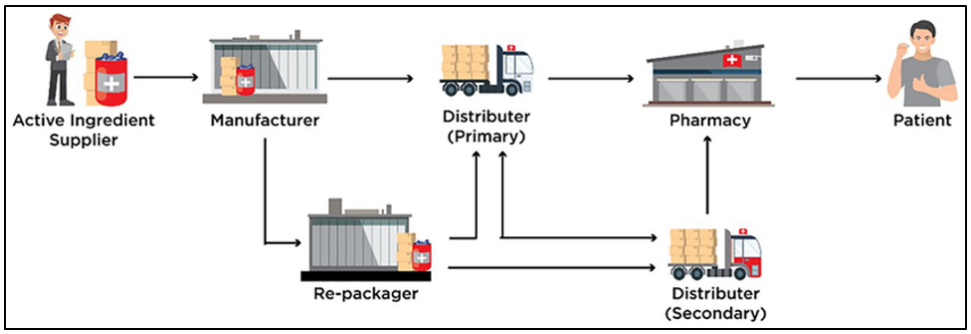

Figure 1.1: Drug supply chain stakeholders and their relationship [25].

1.2.2 Typical Processes

The journey of a pharmaceutical product is a multi-stage process:

1. **Research and Development (R&D)**: Pharmaceutical companies invest heavily in discovering and developing new drugs, including extensive clinical trials to prove safety and efficacy [1].
2. **Raw Material Sourcing**: Manufacturers procure APIs and excipients from qualified suppliers, often from various global locations [2].
3. **Manufacturing and Packaging**: APIs are formulated into FPPs (e.g., tablets, capsules, injectables) under strict GMP guidelines. Products are then packaged with appropriate labeling, including batch numbers, expiry dates, and often, unique identifiers [8].
4. **Quality Control**: Rigorous testing is conducted at multiple stages, from raw materials to finished products, to ensure compliance with quality standards [8].
5. **Primary Distribution**: Finished products are shipped from manufacturing sites to central distribution centers or primary wholesalers [7].
6. **Secondary Distribution**: Wholesalers distribute products to regional distribution centers, smaller distributors, hospitals, and pharmacies [7]. This stage can be complex and involve multiple handlers.
7. **Dispensing**: Pharmacists dispense medications to patients based on prescriptions or for over-the-counter sales [2].
8. **Post-Market Surveillance**: Regulatory authorities and manufacturers monitor the safety and efficacy of drugs once they are on the market, collecting data on adverse events and product quality issues [10].

This intricate flow, often spanning multiple countries and continents, presents numerous points of vulnerability that can be exploited if not managed with robust security and transparency measures [4], [9].

1.3 Major Challenges in the Pharmaceutical Supply Chain

Despite its critical importance, the PSC is fraught with challenges that can compromise product integrity and patient safety.

1.3.1 Counterfeit Drugs

The proliferation of counterfeit (also termed falsified or substandard) drugs is a significant global health crisis [3], [6]. Counterfeit medicines are deliberately and fraudulently mislabeled with respect to identity and/or source [11]. They may contain the wrong active ingredients, no active ingredients, insufficient quantities of active ingredients, or even toxic substances [12].

- **Statistics and Scope**:
  - The World Health Organization (WHO) estimates that 1 in 10 medical products circulating in low- and middle-income countries (LMICs) is substandard or falsified [12]. This figure can be even higher for specific product categories or regions.

- The OECD and the European Union Intellectual Property Office (EUIPO) reported that trade in counterfeit pharmaceutical products amounted to as much as USD 200 billion annually prior to the COVID-19 pandemic, and this figure is believed to have increased [6], [13]. In 2019, counterfeit pharmaceuticals represented 0.84% of total global pharma imports, a figure that is likely an underestimate due to the illicit nature of the trade [13].
- A significant portion of counterfeit drugs sold target life-threatening conditions, including medicines for cancer, malaria, HIV/AIDS, and cardiovascular diseases [12], [14]. The COVID-19 pandemic exacerbated this issue with a surge in falsified medical supplies, including vaccines, test kits, and personal protective equipment [15].

- **Impact**: Counterfeit drugs can lead to treatment failure, increased morbidity and mortality, adverse drug reactions, and the development of antimicrobial resistance [3], [12]. They also erode public trust in healthcare systems and legitimate pharmaceutical manufacturers [6].

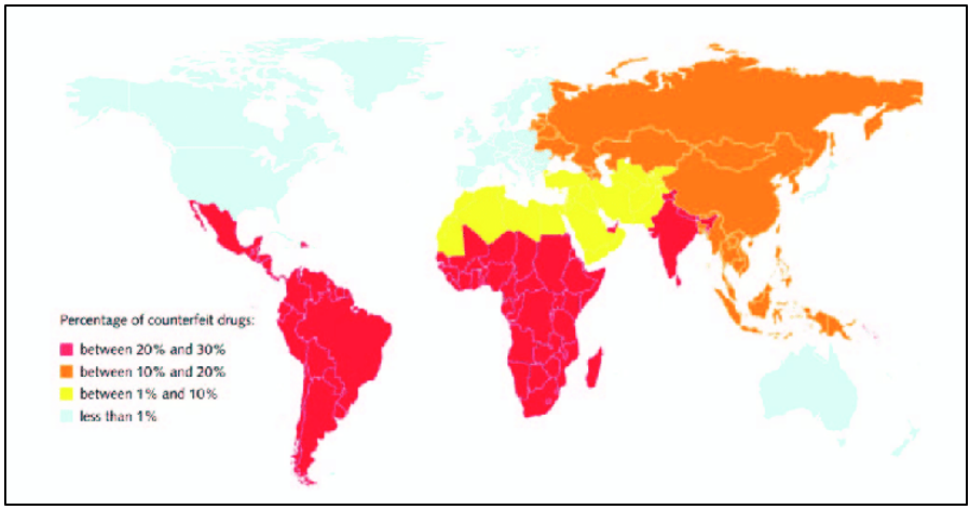

Figure 1.2: Global distribution of counterfeit drugs[26]

1.3.2 Traceability and Transparency Gaps

Lack of end-to-end traceability and transparency is a fundamental vulnerability in the PSC [4], [5]. The fragmented nature of the supply chain, with multiple handovers and often inadequate information systems, makes it difficult to track products from their origin to the point of dispensing [2], [16].

- **Consequences**:
  - **Facilitation of Counterfeiting**: Opaque supply chains provide opportunities for counterfeiters to introduce illicit products at various points without easy detection [4].
  - **Inefficient Recalls**: When a defective or harmful product needs to be recalled, lack of precise traceability can lead to slow and overly broad recalls, causing unnecessary disruption, increased costs, and continued patient risk [17]. For instance, the inability to quickly identify and isolate affected batches

can delay the removal of dangerous products from circulation [5]. A historical example often cited in supply chain literature is the 1982 Tylenol tampering case in the USA, which, while not a failure of routine traceability for recall, highlighted the devastating consequences of product integrity breaches and led to significant changes in packaging and regulatory requirements, underscoring the need for secure supply chains [18]. More recently, global recalls of valsartan-containing products due to nitrosamine impurities in 2018-2019 demonstrated the complexity of tracing affected batches back through intricate global API supply routes [19].

  - **Diversion and Theft**: Pharmaceuticals can be diverted from legitimate supply channels to illicit markets, or stolen and reintroduced, often without proper storage conditions, compromising their efficacy and safety [4], [16].
  - **Lack of Accountability**: Opacity makes it difficult to pinpoint responsibility when issues like contamination, spoilage, or counterfeiting occur [5].

1.3.3 Regulatory Compliance

The pharmaceutical industry is one of the most stringently regulated sectors [8]. Manufacturers and distributors must comply with a multitude of national and international regulations concerning drug quality, safety, manufacturing processes (GMP), distribution practices (Good Distribution Practices - GDP), and serialization (e.g., the U.S. Drug Supply Chain Security Act - DSCSA, EU Falsified Medicines Directive - FMD) [10], [20].

- **Challenges**:
  - **Complexity and Variation**: Regulations vary significantly across jurisdictions, creating a complex compliance landscape for companies operating internationally [10].
  - **Cost of Compliance**: Meeting these stringent requirements, including implementing track-and-trace systems, involves substantial investment in technology, processes, and personnel [4].
  - **Data Management**: Ensuring accurate and secure management of vast amounts of compliance-related data is a major operational challenge [5]. For instance, DSCSA requires product tracing information (transaction history, information, and statement) to be exchanged at each change of ownership in the supply chain [20].

1.3.4 Supply Chain Inefficiencies and Integrity Issues

Beyond counterfeiting and traceability, the PSC faces other integrity and efficiency challenges:

- **Cold Chain Management**: Many modern drugs, especially biologics and vaccines, require strict temperature control throughout the supply chain (cold chain) [9]. Lapses can render these products ineffective or even harmful. Lack of continuous monitoring and transparent data sharing makes it difficult to verify cold chain integrity [21].
- **Product Spoilage and Wastage**: Inefficient inventory management, poor storage conditions, or issues during transit can lead to product spoilage and significant financial losses [9].

- **Data Silos**: Stakeholders often operate with disparate information systems that do not readily communicate, leading to data silos and a lack of shared visibility across the supply chain [5], [16].

1.4 Impact on Public Health and Safety

The cumulative effect of these challenges on public health and safety is profound and multifaceted:

- **Direct Harm to Patients**: Consumption of counterfeit or substandard drugs can lead to ineffective treatment, poisoning, adverse reactions, and death [3], [12]. The WHO has reported numerous instances where falsified medicines have caused fatalities, such as contaminated cough syrup incidents in several countries [22], [23].
- **Erosion of Trust**: Incidents involving counterfeit drugs or supply chain failures erode public confidence in medicines, healthcare providers, and regulatory authorities [6]. This can lead to patients avoiding necessary treatments or seeking remedies from unregulated sources.
- **Spread of Disease and Antimicrobial Resistance**: Ineffective antimicrobial drugs (often counterfeit or substandard) contribute to the development and spread of drug-resistant infections, a major global health threat [12], [24].
- **Undermining Health Programs**: The infiltration of counterfeit essential medicines, such as those for malaria or HIV, can severely undermine public health programs and efforts to control endemic diseases, particularly in LMICs [14].

1.5 The Imperative for Reliable, Tamper-Proof Tracking Mechanisms

The vulnerabilities and challenges inherent in the current pharmaceutical supply chain underscore an urgent and critical need for innovative solutions that can provide reliable, immutable, and transparent tracking of medicines [4], [5], [16]. Such mechanisms are essential to:

1. **Combat Counterfeiting**: By enabling robust verification of product authenticity at multiple points in the supply chain, from manufacturer to dispenser [17].
2. **Enhance Traceability**: Allowing real-time tracking of individual drug packages, facilitating efficient recalls, and identifying points of diversion or contamination [5].
3. **Improve Regulatory Compliance**: Simplifying the process of reporting and verifying compliance data for regulatory authorities [4].
4. **Increase Transparency**: Providing shared, trusted visibility into the supply chain for all authorized stakeholders, fostering accountability and collaboration [16].
5. **Strengthen Data Integrity**: Ensuring that records of transactions and product movements are secure, tamper-proof, and auditable [5].

Emerging technologies, particularly blockchain, offer promising capabilities to address these needs by creating decentralized, immutable ledgers for tracking pharmaceutical products and managing supply chain data [17]. The subsequent chapters of this dissertation will explore how such technologies, specifically Hyperledger Fabric, can be leveraged to build a more secure, transparent, and trustworthy pharmaceutical supply chain.

1.6 Conclusion

This chapter provided a foundational exploration of the pharmaceutical supply chain (PSC), delineating its core actors, operational stages, and the persistent vulnerabilities that compromise both its efficiency and integrity. Among the most pressing challenges identified were the proliferation of counterfeit drugs, the lack of end-to-end traceability, fragmented regulatory compliance, and operational inefficiencies. These challenges, while global in scope, are particularly acute in developing economies such as Algeria, where infrastructural limitations and coordination gaps further exacerbate the risks to public health. In light of these findings, it is evident that traditional supply chain management practices and technologies are insufficient to safeguard the pharmaceutical ecosystem. There is a clear and urgent need for a transformative approach that ensures secure, transparent, and verifiable tracking of pharmaceutical products across their lifecycle. This necessity sets the stage for the subsequent exploration of blockchain technology, introduced in the next chapter, as a promising solution for enabling traceability, integrity, and trust within the PSC.

Chapter 2

Blockchain

2.1 Blockchain Technology

2.1.1 Introduction

Blockchain is a distributed ledger technology that enables secure, transparent, and tamper-resistant recording of transactions across a decentralized network. Initially conceptualized as the foundation for cryptocurrencies, blockchain has evolved into a versatile infrastructure with applications spanning finance, supply chain, healthcare, and identity management. Its core features immutability, decentralization, consensus mechanisms, and cryptographic security make it well-suited for environments requiring data integrity and trust without reliance on centralized intermediaries [40], [31]. Through the use of blocks that are cryptographically linked and validated via consensus protocols, blockchain ensures that each transaction is traceable and verifiable by all network participants, thereby enhancing transparency and auditability in distributed systems [59], [57].

2.1.2 Definition

Blockchain, a technology devised in 2008 by the enigmatic figure known as Satoshi Nakamoto [57], whose true identity remains undisclosed (widely speculated to be an individual or group residing in Japan), was originally conceived to function as the decentralized, digital, public ledger for the cryptocurrency Bitcoin, aiming to address the issue of double-spending in digital currency transactions. In simple terms, blockchain operates as a distributed database wherein transactions are recorded in blocks, forming a continuous chain. While its primary application was in digital currency, blockchain has since demonstrated potential across various domains, including smart contracts, smart property, insurance, music, healthcare, manufacturing, supply chain, arts, government, and the Internet of Things (IoT). This versatile technology has the capacity to reshape our societal and professional landscapes [37].

Illustrated in Figure 1, a blockchain essentially consists of interconnected blocks, each containing data pertinent to the transaction, such as the transferred amount, sender and recipient identities, date, and time. Additionally, every block is assigned an index, a timestamp indicating its creation time, a nonce value crucial for hash calculation, and the hash of the preceding block, establishing a sequential chain-like structure. The genesis block, the initial block in the chain, lacks a previous block's hash, denoted as NULL. The index serves as a unique identifier for each block, starting from 0 for the genesis block and incrementing with each subsequent block. Timestamps denote the creation time of blocks, while nonces, 32-bit integers, influence the resulting hash calculation of each block

[37].

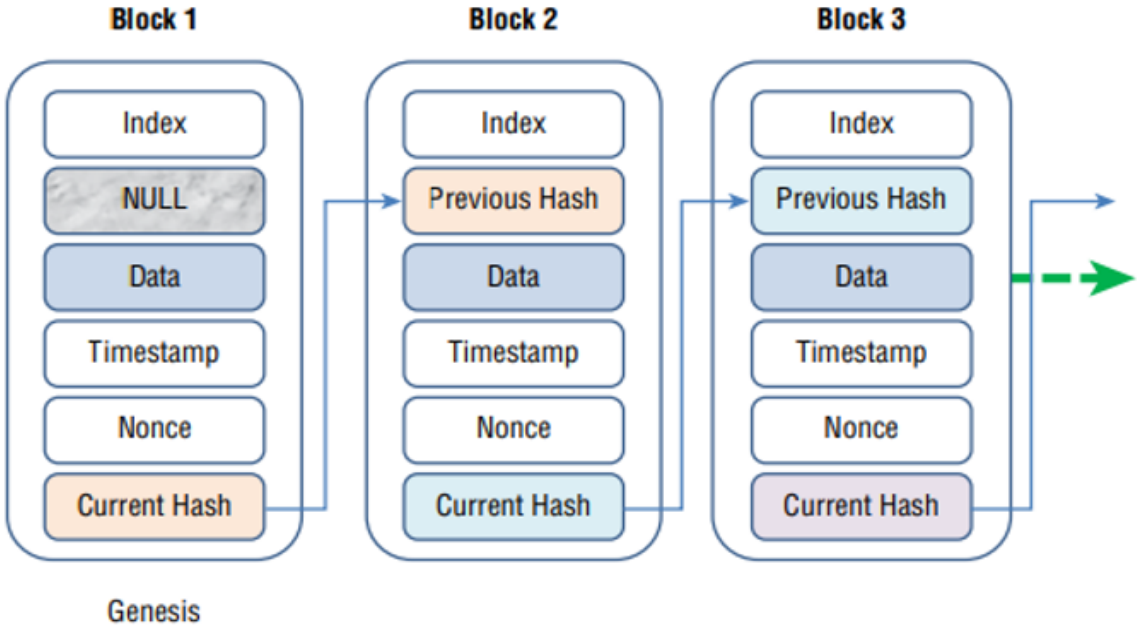

Figure 2.1: The schematic diagram of a blockchain [37].

Utilizing its index, the previous block's hash, its data, timestamp, and nonce value, each block undergoes a process of hashing through a cryptographic hash function, such as SHA-256, as depicted in Figure 2. A hash function is a mathematical algorithm capable of converting data of variable sizes into fixed-size output. Unlike encryption, a hash function is irreversible; thus, given the hash of a current block, it is impossible to deduce the original information contained within the block that underwent hashing [37].

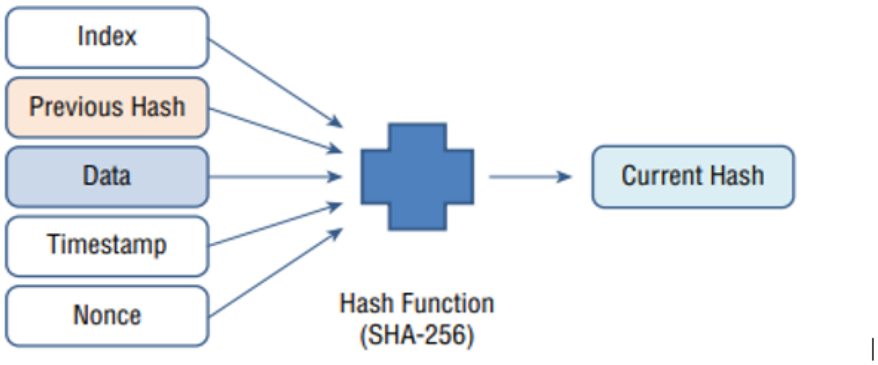

Figure 2.2: Block Hash generation process in Blockchain using SHA-256[37].

2.1.3 Characteristics of Blockchain

Decentralization

Decentralization in blockchain refers to the distribution of control and decision-making from a central point to a distributed network [28]. Unlike traditional centralized systems where a single entity holds authority and maintains the ledger, blockchain networks typically distribute the ledger across numerous participating nodes (computers) [27]. This

architecture enhances resilience, as the system can continue to operate even if some nodes fail or are compromised [29]. In a decentralized system, no single participant has unilateral power to alter records or dictate the rules of the network, fostering a trustless environment where participants can interact directly without relying on a central intermediary [30]. This contrasts significantly with centralized databases vulnerable to single points of failure and control [28].

Immutability

Immutability is a cornerstone of blockchain technology, signifying that once data is recorded on the blockchain, it cannot be altered or deleted [27], [31]. Each block in the chain contains a set of transactions, and once a block is validated and added to the chain, it is cryptographically linked to the previous block [28]. This sequential linking makes any attempt to tamper with historical data computationally infeasible, as it would require recalculating all subsequent blocks, an effort that would be readily detectable by the network participants [29]. This permanence of records ensures data integrity and auditability, which is crucial for applications requiring a verifiable and tamper-proof history of transactions [31].

Immutability and Cryptographic Hashing

The immutability of a blockchain is largely achieved through the extensive use of cryptographic hashing [27]. A hash function is a mathematical algorithm that takes an input (or 'message') of any length and produces a fixed-length string of characters, known as a hash or digest [32]. Even a minor change in the input data will result in a drastically different hash output [28]. In a blockchain, each block contains the hash of the previous block in its header, creating a chain-like structure [27]. If an attacker attempts to alter data in a past block, the hash of that block would change. Consequently, the hash stored in the subsequent block would no longer match, and this discrepancy would cascade throughout the entire chain, immediately signaling a compromise to all network participants [29], [32]. This cryptographic linkage ensures that the integrity of the entire chain is maintained.

Transparency vs. Privacy

Blockchain technology presents a spectrum regarding transparency and privacy, largely dependent on the specific type of blockchain architecture [28]. Public blockchains, such as Bitcoin or Ethereum, offer high transparency, where all transaction data (though typically pseudonymized) is publicly viewable by anyone [27]. This complete visibility can be beneficial for accountability but may not be suitable for all applications, especially those handling sensitive information [30]. In contrast, permissioned or private blockchains, like Hyperledger Fabric, are designed for enterprise use and offer greater control over privacy [31], [33]. In these systems, participation is restricted, and data visibility can be limited to authorized parties through mechanisms like channels, allowing organizations to transact and share information selectively while still benefiting from the distributed and immutable nature of the ledger [33]. Thus, while transparency is a key feature, blockchain systems can be engineered to meet varying privacy requirements [28].

Consensus Mechanisms

Consensus mechanisms are protocols that enable distributed nodes in a blockchain network to agree on the validity of transactions and the state of the ledger, without relying on

a central authority [27], [34]. Since multiple participants maintain copies of the ledger, a method is required to ensure that all copies are consistent and that new blocks are added to the chain in an agreed-upon manner [28]. Various consensus algorithms exist, each with different trade-offs in terms of security, scalability, and energy consumption [29]. Common examples include Proof-of-Work (PoW), used by Bitcoin, which requires nodes to solve complex computational puzzles, and Proof-of-Stake (PoS), where block validators are chosen based on the number of coins they hold or "stake" [34]. In permissioned blockchains, consensus mechanisms like Raft or Practical Byzantine Fault Tolerance (PBFT) are often employed, as they are designed for environments where participants are known and have a degree of trust, offering faster transaction finality [33], [34]. The choice of consensus mechanism is critical to the security and performance of a blockchain network [28].

Auditability

One of the fundamental characteristics of blockchain technology is auditability, which enables transparent and tamper-evident tracking of all historical transactions recorded on the ledger. Due to its decentralized, append-only data structure and use of cryptographic hashing, blockchain ensures that every transaction is time-stamped and immutable, facilitating real-time and retrospective verification without reliance on a central authority [40], [57]. This property is particularly vital in domains such as healthcare, finance, and supply chain management, where regulatory compliance and data integrity are critical. For instance, Hussien et al. highlight that blockchain's auditability significantly enhances the management and traceability of electronic health records by allowing authorized entities to verify every interaction with data [58]. Similarly, studies discuss how auditability contributes to blockchain's reliability by providing a transparent history of data modifications, making it highly suitable for sensitive applications [59]. Although early foundational works such as Nakamoto's Bitcoin whitepaper [57] and the Ethereum Yellow Paper [41] do not use the term explicitly, they describe core mechanisms—such as public ledger transparency and verifiable state transitions—that underpin the auditability feature in modern blockchain implementations [31].

Smart Contracts

Smart contracts are self-executing contracts with the terms of the agreement directly written into lines of code [27], [35]. They reside on the blockchain and automatically execute predefined actions when specific conditions, encoded within the contract, are met [28]. Essentially, smart contracts automate the enforcement, management, performance, and payment of agreements [31]. Once deployed on the blockchain, smart contracts are immutable and their execution is deterministic, meaning they will produce the same output given the same input for all participants [35]. This eliminates the need for intermediaries to verify and execute contract terms, thereby reducing transaction costs and increasing efficiency [29]. In the context of Hyperledger Fabric network for the pharmaceutical industry, smart contracts (referred to as chaincode) are pivotal for automating processes like tracking medication batches, managing compliance approvals, and overseeing distribution, ensuring that predefined rules and agreements are automatically enforced across the supply chain [31], [33], [38].

2.1.4 Evolution of Blockchains

The evolution of blockchain technology is often categorized into generational shifts, each characterized by the introduction of new functionalities and a broader scope of applica-

tions [28], [39].

Blockchain 1.0: Cryptocurrencies

The genesis of blockchain technology is inextricably linked with the advent of Bitcoin in 2008 [57], marking the era of Blockchain 1.0 [27], [39]. The primary innovation of this phase was the creation of a peer-to-peer electronic cash system [57] that enabled decentralized and secure transactions without the need for traditional financial intermediaries [29]. The core focus was on cryptocurrencies – digital or virtual tokens secured by cryptography – with applications centered on value transfer, digital payments, and remittance [28], [40]. The underlying blockchain served as a distributed public ledger for these currency transactions, emphasizing immutability, transparency (of transactions, not identities), and censorship resistance through mechanisms like Proof-of-Work consensus [27].

Blockchain 2.0: Smart Contracts

The second generation, often termed Blockchain 2.0, emerged with the introduction of Ethereum around 2013-2015 [39], [41]. This phase significantly expanded the utility of blockchain beyond mere cryptocurrencies by introducing the concept of smart contracts [35], [31]. As previously discussed, smart contracts are self-executing programs stored on the blockchain that automatically enforce the terms of an agreement [27]. This innovation transformed blockchains into general-purpose programmable platforms, enabling the development of decentralized applications (DApps) and decentralized autonomous organizations (DAOs) across various sectors, including finance (DeFi), asset management, and identity verification [28], [41]. Blockchain 2.0 thus represented a shift from a distributed ledger for financial transactions to a global decentralized computing platform [39].

Blockchain 3.0: Decentralized Applications (DApps) and Scalability

Blockchain 3.0 represents the ongoing and future evolution, focusing on addressing the limitations of earlier generations, particularly scalability, interoperability, and governance, to support widespread adoption of DApps across numerous industries beyond finance [39], [40]. This phase aims to enhance the efficiency, transaction throughput, and user experience of blockchain solutions [28]. Research and development in this era concentrate on novel consensus algorithms (e.g., Proof-of-Stake variants), layer-2 scaling solutions (e.g., state channels, sidechains), cross-chain communication protocols for interoperability between different blockchains, and more sophisticated governance models [39], [42]. The goal of Blockchain 3.0 is to make blockchain technology more practical and accessible for a broader range of real-world applications, including supply chain management, healthcare, voting systems, and intellectual property rights management [40], [42], aligning closely with the objectives of enterprise solutions like Hyperledger Fabric.

2.1.5 Types of Blockchains

Blockchains can be broadly classified based on their permission model, which dictates who can participate in the network and access the data [28], [33]. The primary types include public, private, and consortium blockchains.

Public Blockchains

Public blockchains are permissionless, meaning anyone can join the network, participate in the consensus process (e.g., mining or staking), and view the ledger's transaction history [27], [28]. Bitcoin and Ethereum are prominent examples of public blockchains [29], [41]. They are characterized by high decentralization and censorship resistance. While transactions are transparent and auditable, user identities are typically pseudonymous, linked to cryptographic addresses rather than real-world identities [27]. The security of public blockchains often relies on cryptoeconomic incentives to encourage honest participation [29]. However, they can suffer from scalability issues due to the large number of participants and the computational demands of consensus mechanisms like Proof-of-Work [39].

Private Blockchains

Private blockchains, also known as permissioned blockchains, are controlled by a single organization [28], [33]. This central organization determines who can join the network, participate in consensus, and access data. Transactions are not publicly visible and are typically restricted to network participants who have been granted specific permissions [31]. Private blockchains offer higher transaction speeds and greater scalability compared to public blockchains because the number of validating nodes is limited and often known [33]. They also provide a higher degree of privacy and control, making them suitable for enterprise applications where data confidentiality and regulatory compliance are critical [40]. While they benefit from blockchain's immutability and traceability, the level of decentralization is lower than in public blockchains, as a single entity ultimately governs the network [28].

Consortium Blockchains (Federated Blockchains)

Consortium blockchains, or federated blockchains, are a hybrid model governed by a group of organizations rather than a single entity (as in private) or no single entity (as in public) [28], [33]. In this model, consensus is achieved by a pre-selected set of nodes representing the participating organizations [40]. This type of blockchain is well-suited for collaborations where multiple entities need to share information and transact securely, but where a fully public solution is not appropriate, and no single entity should have complete control [33]. Consortium blockchains offer a balance between the transparency and decentralization of public blockchains and the privacy and control of private blockchains [28]. They can achieve better scalability and privacy than public chains while maintaining a degree of decentralization among the consortium members [39]. Hyperledger Fabric, designed for enterprise solutions involving multiple collaborating organizations (such as in a pharmaceutical supply chain with manufacturers, suppliers, pharmacies, and regulators), is a prime example of a platform that facilitates the creation of consortium blockchains [33].

Each type of blockchain offers distinct advantages and trade-offs regarding decentralization, security, privacy, scalability, and governance, making the selection dependent on the specific requirements and trust model of the intended application [28], [40].

2.2 Hashing and Encryption

The security, immutability, and integrity of a blockchain network are not inherent properties but are established through the systematic application of robust cryptographic primitives [66]. The two most fundamental of these are hashing and encryption. While often

conflated, they serve distinct purposes. Hashing is primarily employed to ensure data integrity and create the immutable, chained structure of the ledger [67]. Encryption, conversely, is utilized to maintain data confidentiality and control access within the network, a critical feature in permissioned blockchains like Hyperledger Fabric [68]. Understanding the precise technical application of these mechanisms is critical to appreciating the security architecture of a blockchain system.

2.2.1 Block Hashing: Ensuring Data Integrity and Immutability

In a blockchain network, hashing is the process of transforming the data within a block into a fixed-size, unique string of characters known as a hash [69]. This process is executed using a cryptographic hash function, with the Secure Hash Algorithm 256 (SHA-256) being the predominant standard in many blockchain implementations, including Bitcoin [70] and as a common option in Hyperledger Fabric [71]. The generation of a block hash is a deterministic process. Specifically, the key components of the block's header are concatenated and then processed by the hash function [67]. The block header typically contains:

- The Hash of the Previous Block: This is the most critical element for creating the "chain." By including the hash of the preceding block in the current block's header, a direct and unbreakable cryptographic link is formed [70]. Any alteration to a previous block would change its hash, which would then be reflected in the subsequent block's "previous hash" field, causing a cascading invalidation of the entire chain from that point forward.

- The Merkle Root: Rather than hashing every transaction individually within the block's header, a summary of all transactions is created using a Merkle Tree [72]. In this structure, transactions are paired and hashed, and the resulting hashes are recursively paired and hashed until a single hash remains, the Merkle Root. This root provides a highly efficient way to verify the integrity of the transaction set [73]. If even a single transaction is altered, the Merkle Root will change, thus altering the block's overall hash.

- Timestamp: A timestamp records the approximate time of the block's creation [70].

- Nonce: In Proof-of-Work (PoW) blockchains like Bitcoin, a "nonce" (number used once) is an arbitrary number that miners repeatedly change in order to find a block hash that satisfies a specific difficulty target [70]. While Hyperledger Fabric uses a different consensus mechanism (e.g., Raft or PBFT) and does not require mining, a similar concept or block number serves to ensure each block's hash is unique [68].

The combination of these header fields is then passed as input to the SHA-256 algorithm, which produces a 256-bit (32-byte) hash value [74]. For example: Block Hash = SHA-256(Previous Block Hash + Merkle Root + Timestamp + Nonce) This resulting hash serves as the unique identifier for that block and is included in the header of the next block, perpetuating the chain.

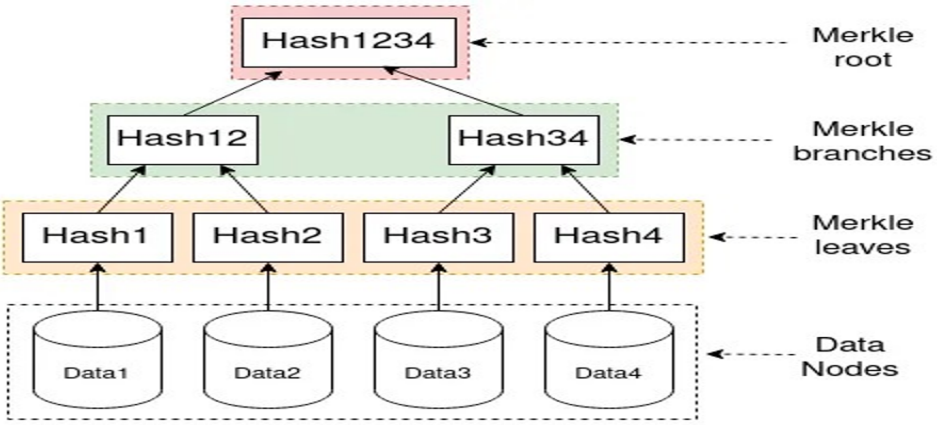

Figure 2.3: The structure of a Merkle Tree [81].

2.2.2 The Rationale for Utilizing SHA-256

The selection of SHA-256 is deliberate and based on its key cryptographic properties, which are essential for the security of a distributed ledger [74]:

- Deterministic: The same input will always produce the exact same output. This is crucial for verification, as nodes across the network can independently compute and agree upon a block's hash [69].
- Pre-image Resistance: It is computationally infeasible to determine the input data (the block header) from its output (the hash). This prevents an attacker from reverse-engineering a valid block header to forge a block [75].
- Second Pre-image Resistance (Collision Resistance): It is computationally infeasible to find a different input that produces the same hash as a given input [75]. This property ensures that an attacker cannot create a fraudulent block with different transactions that results in the same hash as a legitimate block, thereby preventing forgery.
- Avalanche Effect: A minor change to the input data, even a single bit, results in a drastically different output hash. This guarantees that any tampering with block data becomes immediately evident [69].

It is crucial to note that hashing is not encryption; it is a one-way function designed for integrity verification, not for confidentiality [67]. The data within the block remains readable on the ledger unless it is separately encrypted.

2.2.3 Encryption: Securing Data and Controlling Access

While hashing secures the chain's integrity, encryption is employed to protect the confidentiality of data, both in transit and at rest on the ledger. In an enterprise context such as the pharmaceutical supply chain, confidentiality is paramount. Not all participants should have access to all data; for instance, contractual details between a Manufacturer and a Supplier should not be visible to a Pharmacy [76]. Hyperledger Fabric implements a multi-layered approach to encryption and access control, primarily leveraging Public Key Infrastructure (PKI) [68]. The core encryption algorithm used for digital signatures and identity verification is the Elliptic Curve Digital Signature Algorithm (ECDSA) [77]. Here is how encryption and related cryptographic techniques are applied:

- Transaction Endorsement and Digital Signatures: Before a transaction is submitted to the network, it must be endorsed by the required organizations as defined by the chaincode's endorsement policy [78]. The client application signs the transaction proposal using the user's private key. The endorsing peers then verify this signature using the user's corresponding public key (contained in their digital certificate) before executing the chaincode [68]. Upon successful execution, the peer signs the transaction response with its own private key. This use of ECDSA ensures authenticity, non-repudiation, and integrity at the transaction level [77].

- Confidentiality of Data on the Ledger: For sensitive information, data can be encrypted before it is written to the chaincode's state. This can be achieved through symmetric encryption (e.g., AES-256) or by using more advanced cryptographic techniques available in Fabric, such as private data collections, which allow defined subsets of organizations on a channel to endorse, commit, or query private data without having to create a separate channel [79].

- Securing Network Communication: All peer-to-peer and client-to-peer communication within a Hyperledger Fabric network is secured using Transport Layer Security (TLS) [68]. This establishes an encrypted channel for data in transit, preventing eavesdropping and man-in-the-middle attacks. Each node and client in the network has a TLS certificate and key pair, and mutual TLS (mTLS) is used to ensure that both parties in any communication are authenticated before an encrypted session is established [80].

In summary, the blockchain's security model relies on the synergistic application of SHA-256 for creating an immutable and tamper-evident ledger structure, and public-key cryptography (primarily ECDSA) for authenticating participants and signing transactions. These are complemented by TLS for securing network communications, providing a comprehensive security framework for enterprise applications [68], [76].

2.3 The Hyperledger Project

2.3.1 Overview of Hyperledger

Hyperledger is an open-source collaborative effort hosted by the Linux Foundation, aimed at advancing cross-industry blockchain technologies [45]. Unlike public blockchains such as Bitcoin or Ethereum, which are permissionless and often associated with cryptocurrency, Hyperledger focuses on developing frameworks and tools for building enterprise-grade distributed ledger solutions tailored to business needs. These frameworks support a wide range of industries, including finance, healthcare, supply chain, and logistics.

Hyperledger was initiated in 2015 when several companies with a shared interest in blockchain technology recognized the potential benefits of collaboration over independent efforts. By pooling their resources, these organizations aimed to develop open-source blockchain frameworks that could serve as a foundation for industry-wide adoption. Under the stewardship of the Linux Foundation, Hyperledger has rapidly expanded, now encompassing over 230 member organizations, 10 active projects comprising 3.6 million lines of code, and a global community of nearly 28,000 participants. The initiative promotes the vision of modular, open-source blockchain platforms designed for ease of use and broad applicability, positioning Hyperledger as a key driver in the evolution of enterprise blockchain technology [45].

2.3.2 Core Objectives and Design Philosophy

The primary mission of Hyperledger is to create enterprise-grade, distributed ledger frameworks and standards that foster innovation and interoperability across various sectors [45]. It emphasizes permissioned blockchains , where participants must be authenticated and authorized to join the network. This approach ensures identity verification, data privacy, and regulatory compliance key requirements for businesses operating in sensitive environments.

Hyperledger's architecture is designed to be modular and pluggable , allowing developers to swap out components such as consensus mechanisms, smart contract engines, and identity management systems. This flexibility enables enterprises to tailor blockchain solutions to their specific operational and regulatory demands without compromising performance or security [45].

2.3.3 Key Hyperledger Frameworks

While Hyperledger encompasses multiple frameworks, the most prominent include:

- Hyperledger Fabric: A modular, permissioned framework designed for flexible deployment in enterprise contexts. It supports private channels, pluggable consensus, and smart contracts written in general-purpose languages like Go and Node.js [45].
- Hyperledger Sawtooth: Developed by Intel, it supports both permissioned and permissionless networks with a focus on modularity and scalability. Sawtooth introduces a unique consensus algorithm called Proof of Elapsed Time (PoET) optimized for resource-efficient validation [45].
- Hyperledger Indy: is a distributed ledger specifically designed to support decentralized identity systems. It offers a suite of tools, libraries, and reusable components that facilitate the creation and management of self-sovereign digital identities anchored on blockchains or other distributed ledger technologies [45].
- Hyperledger Iroha: is a blockchain platform developed with a focus on simplicity and ease of integration into infrastructure projects requiring distributed ledger solutions. It became the third distributed ledger platform under the Hyperledger umbrella—alongside Fabric and Sawtooth—in October 2016. Initially developed by Soramitsu in Japan, Iroha was proposed to Hyperledger through a collaboration between Soramitsu, Hitachi, NTT Data, and Colu [45].

Each framework serves different enterprise needs, but this thesis will focus primarily on Hyperledger Fabric due to its suitability for pharmaceutical supply chain traceability.

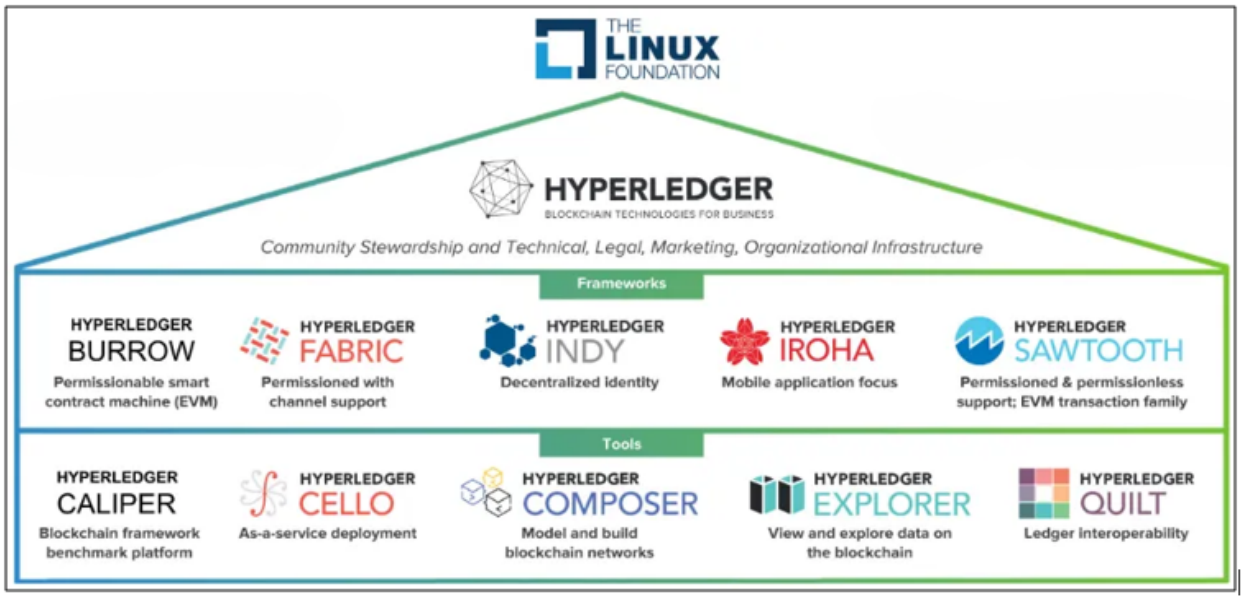

Figure 2.4: High-level overview of Hyperledger frameworks and tool and their application domains [45]

2.3.4 Why Hyperledger for Enterprise?

Enterprise environments often require strict access controls, high performance, and regulatory compliance factors not adequately addressed by public blockchains. Public blockchains operate on a permissionless model, where anyone can join and participate, leading to concerns around identity, scalability, and data confidentiality. In contrast, Hyperledger frameworks offer permissioned membership , robust privacy features, and customizable consensus mechanisms, making them ideal for applications in regulated industries such as finance, healthcare, and supply chain management [46].

Key reasons for selecting Hyperledger in enterprise settings include:

- Identity Management : Enterprises need to know who is participating in the network. Hyperledger provides strong identity verification through certificate authorities (CAs) and membership service providers (MSPs), ensuring only trusted parties can transact [46].
- Data Privacy : With features like private channels , Hyperledger allows selective data sharing between specific stakeholders. For example, in a pharmaceutical supply chain, suppliers and manufacturers may share confidential pricing agreements via a dedicated channel without exposing this information to other network participants [46].
- Performance and Scalability : Unlike public blockchains that suffer from throughput limitations due to consensus bottlenecks, Hyperledger frameworks like Fabric implement efficient consensus algorithms (e.g., Raft) that allow faster transaction processing and better scalability for large-scale deployments [46].
- Regulatory Compliance : Many industries, especially those in healthcare and finance, must adhere to stringent regulations regarding data handling and audit trails. Hyperledger's permissioned nature and immutable ledger provide a solid foundation for meeting these compliance requirements [60].

These attributes make Hyperledger particularly well-suited for complex, multi-party business ecosystems where trust, transparency, and efficiency are critical. As noted in industry reports, Hyperledger has been widely adopted in real-world applications ranging from trade finance to pharmaceutical traceability, demonstrating its maturity and effectiveness in enterprise environments [45],[46].

In summary, the Hyperledger project represents a strategic evolution in blockchain technology, shifting focus from decentralized financial systems to enterprise-grade applications that prioritize identity, privacy, and performance. Its modular design and permissioned architecture make it an ideal platform for implementing secure and scalable blockchain solutions tailored to the needs of modern businesses, particularly in supply chain and regulatory contexts.

2.4 Related Work and Differentiation

This section reviews prior research and real-world initiatives that have applied blockchain technology to pharmaceutical supply chains, emphasizing their methodologies, scopes, and limitations. It then contrasts these approaches with the design principles and objectives of the proposed Pharmaceutical Collaborative Platform (PCP), which is tailored to the Algerian context.

2.4.1 International Blockchain-Based Supply Chain Initiatives

Numerous blockchain implementations have emerged over the past decade aiming to secure pharmaceutical supply chains against counterfeiting, inefficiencies, and regulatory non-compliance. Among the most notable examples:

- MediLedger Project: Developed by Chronicled in partnership with pharmaceutical companies such as Pfizer and Genentech, the MediLedger Project utilizes a permissioned Ethereum-based blockchain to ensure compliance with the U.S. Drug Supply Chain Security Act (DSCSA). Its core functions include product verification, serialized drug tracking, and the management of authorized trading partner (ATP) relationships [82].
- IBM and FDA Collaboration: IBM partnered with the U.S. Food and Drug Administration (FDA) to pilot a blockchain network aimed at enhancing drug traceability and sharing of clinical data. The study primarily examined the feasibility of using blockchain to handle high-throughput data related to patient safety and drug provenance [83].
- PharmaLedger (EU Horizon 2020): This consortium of 29 partners, funded by the European Union, explored blockchain applications in e-leaflets, supply chain traceability, and clinical trials. While the project adopted a consortium-based blockchain model, it emphasized regulatory harmonization within EU member states [84].

These initiatives validate the applicability of blockchain in regulated pharmaceutical environments and highlight the importance of data integrity, compliance, and interoperability.

2.4.2 Limitations of Existing Systems

Despite their successes, current blockchain-based pharmaceutical systems exhibit several limitations that restrict their scalability and adaptability, particularly in emerging economies:

- Infrastructure Dependence: Many systems rely on advanced digital infrastructure, such as real-time serialization hardware, cloud services, or distributed identity management tools. These dependencies can be barriers in regions where digital maturity is limited or where connectivity is intermittent [85].
- Narrow Functional Scope: Some solutions, including MediLedger, primarily focus on compliance verification and serialization. While this aligns with regulatory mandates in developed countries, it overlooks operational challenges such as real-time inventory control, pharmacy-to-pharmacy exchange, and logistics chain visibility [86].
- Low Customizability: Several platforms are developed as software-as-a-service (SaaS) solutions, limiting their customizability and local ownership. Stakeholders must often rely on the vendor for updates or integration, potentially introducing data sovereignty and control concerns [87].

These limitations suggest a need for blockchain systems that are locally deployable, functionally comprehensive, and adaptable to both technological and regulatory constraints of diverse regions.

2.4.3 Research-Oriented Blockchain Models for Drug Supply

Beyond industrial applications, a growing number of academic studies have proposed blockchain-based frameworks for pharmaceutical traceability:

- Kumar et al. (2021) proposed a blockchain-integrated model for anti-counterfeit drug tracking that uses QR codes and Ethereum smart contracts. However, the model was conceptual and lacked a tested implementation in real-world networks [88].
  - Esposito et al. (2020) explored blockchain for cold-chain logistics in vaccine delivery. Their proposed architecture focused on integrating IoT devices with smart contracts to enforce temperature compliance. However, it did not address organizational governance or privacy-preserving data sharing among stakeholders [89].
  - Hussien et al. (2019) focused on medical record traceability and introduced an auditability mechanism using a hybrid blockchain model. Although relevant for data transparency, their work did not extend to supply chain logistics or pharmaceutical inventory management [90].

  These studies highlight innovative directions but remain largely theoretical or limited in scope when compared to full supply chain digitization projects.

2.4.4 Distinctive Contributions of the Pharmaceutical Collaborative Platform (PCP)

The Pharmaceutical Collaborative Platform (PCP) addresses many of the abovementioned gaps through a multi-layered architectural and operational design. Its distinguishing features include:

- Local Deployment on Hyperledger Fabric: Unlike cloud-based platforms, PCP uses a self-hosted Hyperledger Fabric network, giving local stakeholders complete control over infrastructure, governance, and data. This is particularly advantageous in countries like Algeria, where data sovereignty and regulatory oversight are critical [48].
- Comprehensive Supply Chain Scope: PCP is designed to cover the entire pharmaceutical supply lifecycle—from manufacturing, warehousing, and distribution to dispensing and regulatory auditing. It supports smart contract automation for batch registration, recall issuance, inter-pharmacy stock exchange, and product verification, moving beyond the basic serialization offered in earlier projects.
- Data Privacy through Channels: By leveraging Fabric's private channel architecture, the platform allows organizations to exchange data confidentially while maintaining a shared view of validated transactions. This ensures selective transparency for regulators while preserving competitive confidentiality among commercial stakeholders.
- Support for Resource-Constrained Settings: The platform is built to function in low-to-moderate infrastructure environments. Its modularity allows gradual scaling, while its use of permissioned identities ensures secure access without the computational burden of public blockchain consensus algorithms.
- Regulatory Integration: A key stakeholder in the PCP architecture is the pharmaceutical regulatory body (PcpOrg), which interacts with the ledger in real time to audit transactions, validate compliance, and trigger recall operations. This institutional role is often absent or underdeveloped in comparable systems.

In conclusion, while several blockchain initiatives have made strides in improving pharmaceutical supply chains, they are often tailored to high-infrastructure environments with strong regulatory coherence. PCP offers a contextually grounded alternative that extends blockchain functionality to address local governance, data sovereignty, and operational challenges in the Algerian pharmaceutical sector. Its unique blend of Hyperledger Fabric capabilities, privacy-aware design, and end-to-end process coverage positions it as a novel and impactful solution in the field.

2.5 Hyperledger Fabric

Hyperledger Fabric has emerged as a prominent enterprise-grade, permissioned distributed ledger technology (DLT) platform, offering a modular architecture and robust features suitable for a wide array of industrial applications, including complex supply chains [33], [47]. Its design philosophy diverges significantly from public, permissionless blockchains, prioritizing identity management, granular access control, and transactional confidentiality [48].

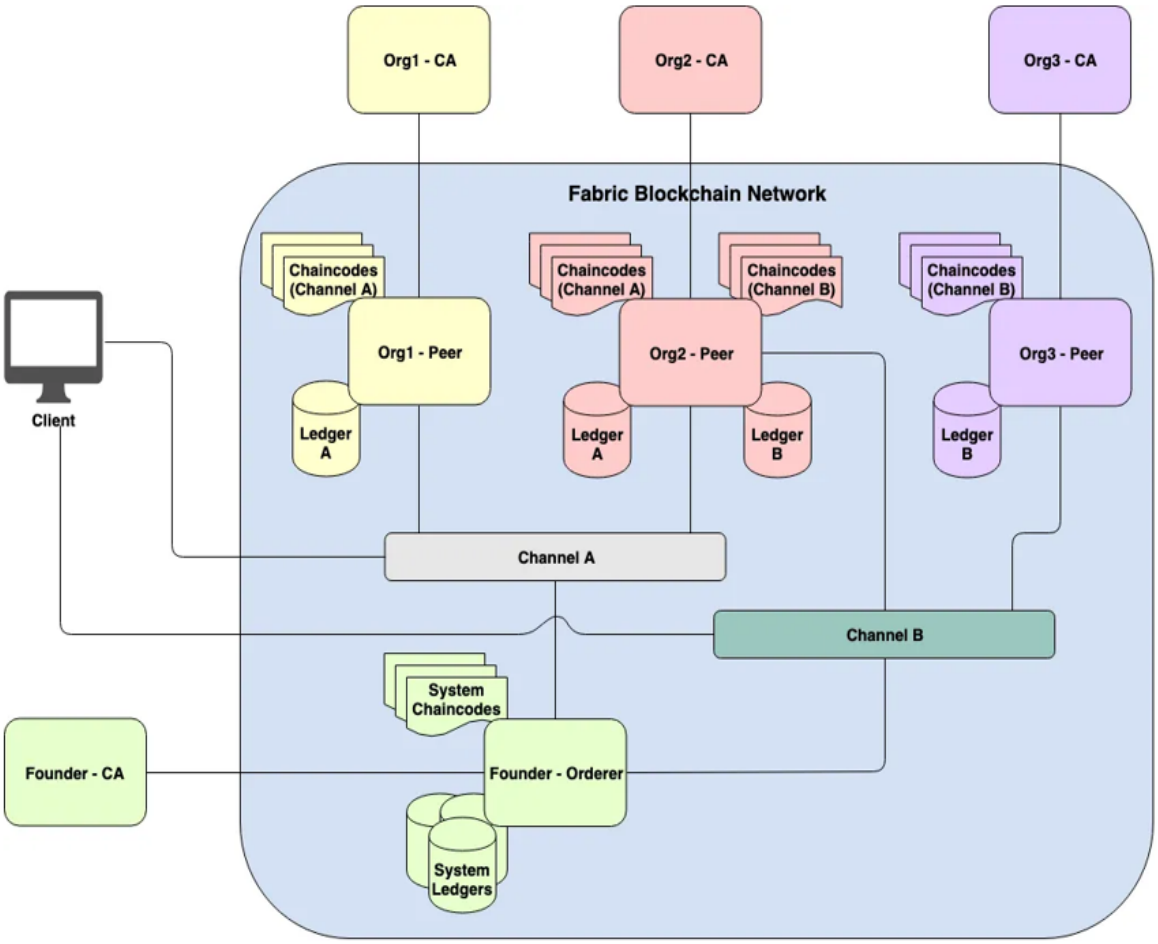

Figure 2.5: Hyperledger fabric network [36].

2.5.1 What is Hyperledger Fabric?

Hyperledger Fabric is an open-source, permissioned blockchain framework and one of the Hyperledger projects hosted by The Linux Foundation [33]. Unlike public blockchains where any participant can join, view transactions, and contribute to the consensus process, Hyperledger Fabric is designed for enterprise consortia where participants are known, and their identities are authenticated [48], [49].It provides a foundation for developing solutions with a modular architecture, allowing for pluggable components such as consensus mechanisms, membership services, and ledger storage options [33]. Fabric's primary goal is to enable businesses to build robust, scalable, and secure blockchain applications tailored to specific industry use cases, where trust and accountability among a defined set of participants are paramount [47]. It is not a cryptocurrency; rather, it is a platform for executing distributed business logic (chaincode) and maintaining a shared, immutable ledger of transactions among permissioned members [33].

2.5.2 Hyperledger Fabric Architecture

The architecture of Hyperledger Fabric is designed to be modular, scalable, and support confidential transactions through various innovative concepts [33], [48]. Its key components interact to process transactions and maintain the distributed ledger.

Core Components:

1. **Peers (Peer Nodes)**: Peers are fundamental network entities that host ledgers and chaincode (smart contracts) [33]. A peer can play different roles:
   - **Endorsing Peers**: These peers receive transaction proposals from client applications, simulate the transaction by executing the relevant chaincode, and generate a read/write set. If the execution is successful, the endorsing peer cryptographically signs the transaction proposal response (endorsement) and returns it to the client [48].
   - **Committing Peers**: Every peer in a channel is a committing peer. They receive ordered blocks of transactions from the ordering service, validate these transactions against endorsement policies and ensure ledger consistency, and then commit the valid transactions to their copy of the ledger [33].

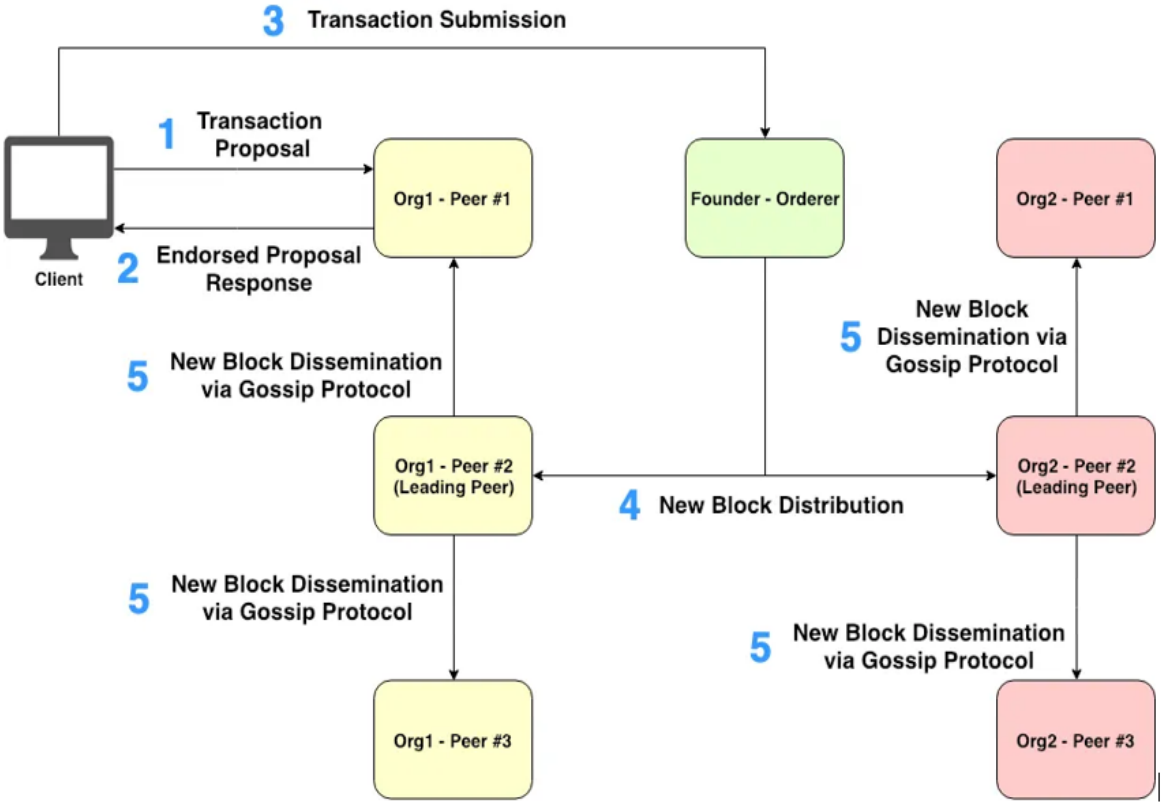

Figure 2.6: Fabric block dissemination scheme using Peers [53].

As shown in the Figure above, step-by-step workflow of Fabric block dissemination scheme using *Leading Peers*:

1. ***Client*** sends a transaction proposal to the chosen ***Endorsing Peer(s)***.
2. Each ***Endorsing Peer*** generates a transaction response and sends the endorsed response back to ***Client***.
3. ***Client*** submits the transaction attached with the endorsed response(s) to ***Orderer***.

4. ***Orderer*** creates a block of ordered transactions and in turn distributes the created block to each of ***Leading Peers*** associated with organizations.
5. Each ***Leading Peer*** disseminates the received block to ***other Peers*** belonging to the same organization through the *gossip data dissemination protocol* [53].

2. **Orderers (Ordering Service Nodes)**: The ordering service is responsible for establishing the total order of transactions within the network [33]. It receives endorsed transactions from client applications, sequences them into blocks, and then broadcasts these blocks to all committing peers in the relevant channels [48]. Fabric supports different ordering service implementations, such as Raft, which provides crash fault tolerance (CFT) [50]. The ordering service does not execute transactions or maintain the ledger state; its primary role is to ensure consistent transaction order [33].
3. **Certificate Authorities (CAs)**: Fabric uses a Membership Service Provider (MSP) to manage identities and access control [33]. CAs are responsible for issuing and validating digital certificates (typically X.509 certificates) that bind cryptographic identities to network participants (peers, orderers, client applications, administrators) [48]. This ensures that all actions on the network are attributable to a verified identity, forming the basis of its permissioned nature [49].

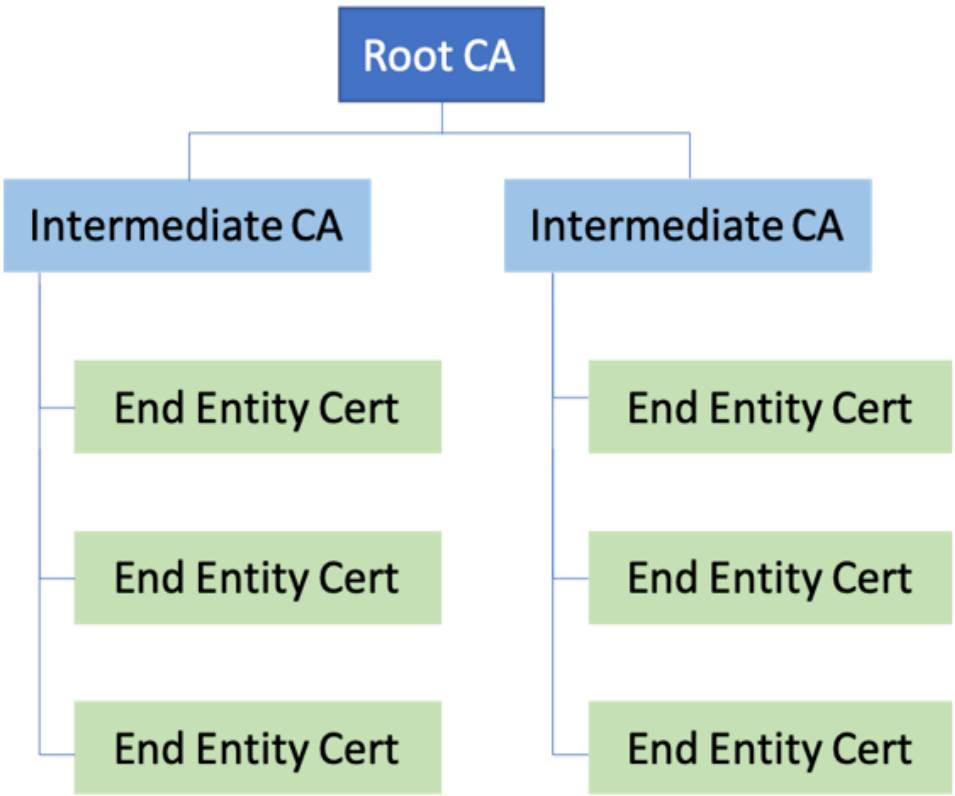

Figure 2.7: Relationship between Root CA, Intermediate CA and End Entities [56]

4. **Channels**: Channels are private ”subnets” of communication between two or more specific network members, allowing them to conduct confidential transactions that are isolated from other participants on the broader network [33].

Each channel has its own ledger, and chaincode invoked on a channel is only accessible to peers that are members of that channel [48]. This mechanism enables data partitioning and confidentiality, which is critical for consortia where participants may be competitors or have specific data privacy requirements [33].

5. **Chaincode (Smart Contracts)**: In Hyperledger Fabric, smart contracts are referred to as **chaincode** [33]. Chaincode is application logic written in general-purpose programming languages (e.g., Go, Node.js, Java) that governs how assets are managed and transactions are processed on the ledger [48]. It is installed on peers and instantiated on a channel. When invoked, chaincode executes against the ledger state and can propose updates to it [33].
6. **Ledger**: Each peer participating in a channel maintains a copy of that channel's ledger [33]. The Fabric ledger consists of two distinct but related parts:
   - **World State**: This is a database (e.g., LevelDB or CouchDB) that maintains the current value of the set of ledger states. It provides efficient access to the latest values of assets and is updated when transactions are committed [48].
   - **Blockchain (Transaction Log)**: This is the immutable, append-only log that records all transactions in cryptographically linked blocks. It provides the verifiable history of all state changes [33].

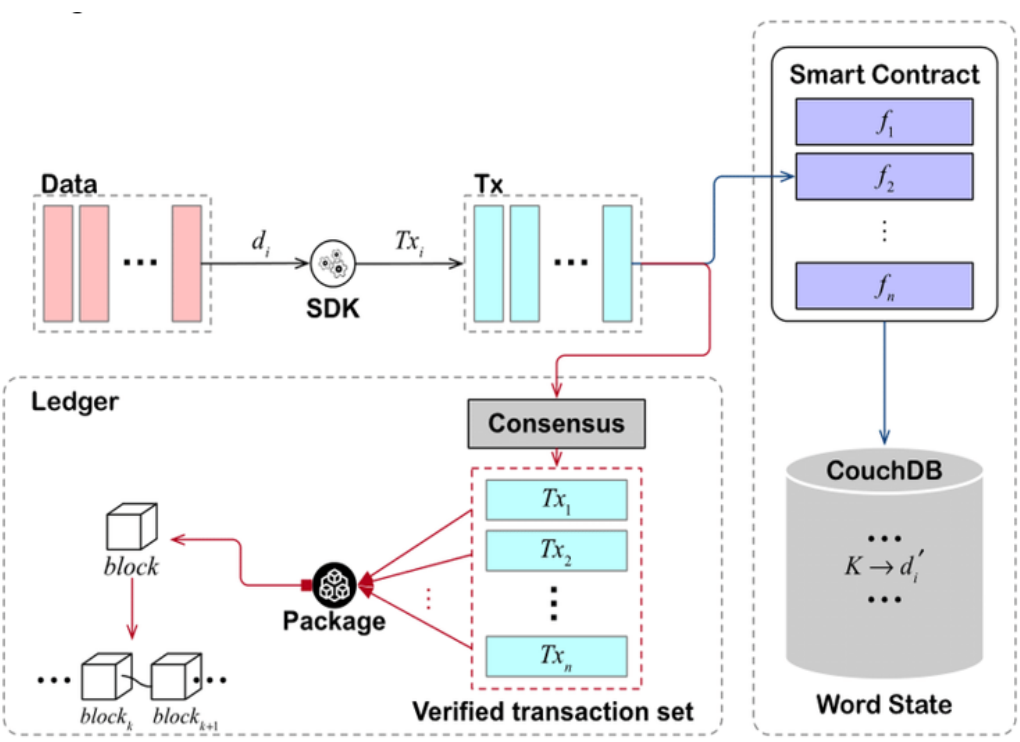

Figure 2.8: Structure of the ledger in Hyperledger Fabric [54].

Transaction Flow:

The transaction flow in Hyperledger Fabric, often referred to as "execute-order-validate," is distinct from many other blockchain platforms [33], [48]:

1. **Proposal (Execute)**: A client application sends a transaction proposal to a set of endorsing peers defined by the chaincode's endorsement policy.
2. **Endorsement (Execute)**: Endorsing peers simulate the transaction by executing the chaincode, generate a read/write set (RWSet), and sign the proposal response. No ledger updates occur at this stage.
3. **Submission (Order)**: The client collects endorsed proposal responses. If the endorsements satisfy the policy, the client submits the transaction (proposal responses and endorsements) to the ordering service.
4. **Ordering (Order)**: The ordering service sequences transactions into blocks and disseminates these blocks to all peers on the channel.
5. **Validation & Commit (Validate)**: Committing peers receive the blocks. Each transaction within a block is validated against the endorsement policy and for read-set consistency (to ensure no intervening state changes have occurred for the read data since endorsement). Valid transactions update the world state, and the block is appended to the peer's local blockchain [33]. Invalid transactions are marked but still recorded on the ledger for auditability [48].

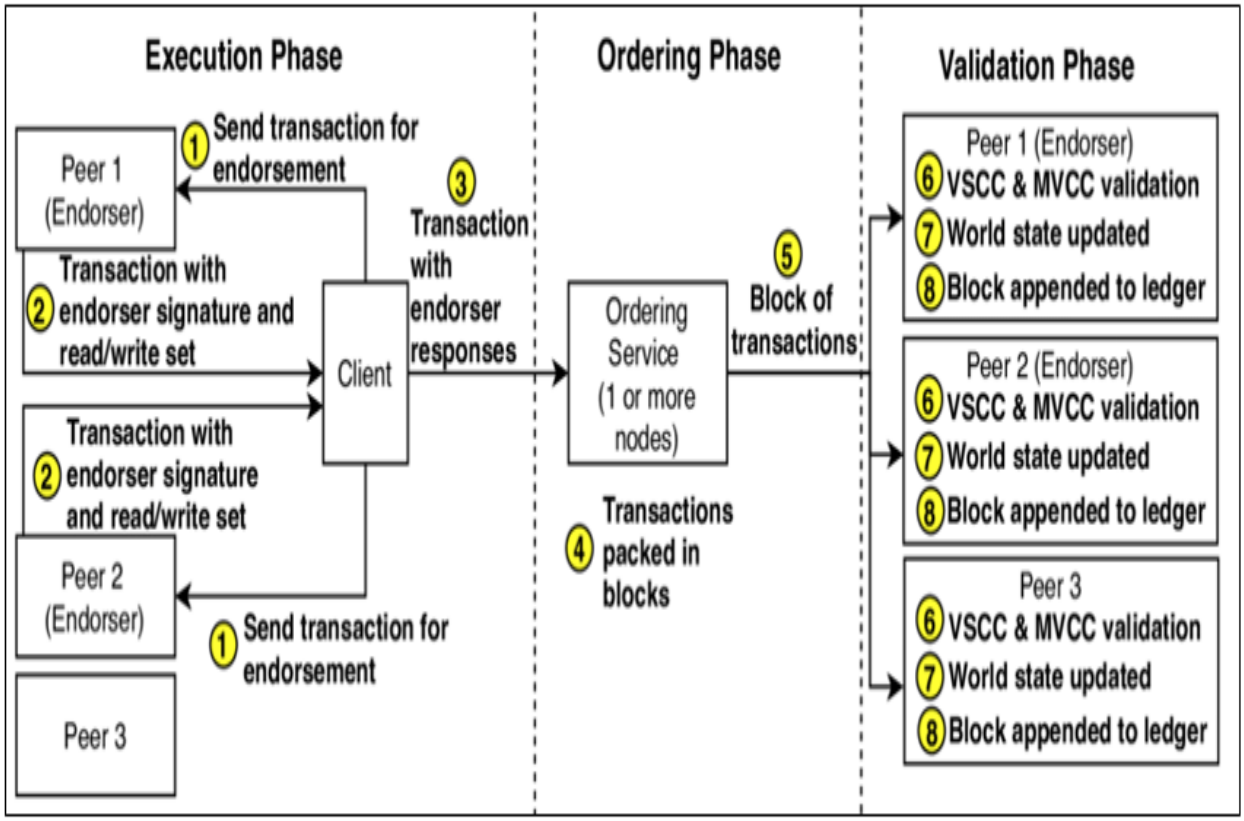

Figure 2.9: Transaction Flow in Hyperledger Fabric [55]

2.5.3 Key Features of Hyperledger Fabric

Hyperledger Fabric's architecture provides several distinguishing features that make it suitable for enterprise applications [33], [47], [48]:

1. **Permissioned Network**: Participants must be authenticated and authorized to join and transact on the network. This is achieved through the MSP and CAs, ensuring a known and accountable environment [49].

2. **Modularity and Pluggability**: Fabric's design allows for key components like consensus, identity management (MSP), and ledger storage (world state database) to be pluggable. This enables enterprises to customize the platform to their specific requirements [33].
3. **Data Confidentiality (Channels)**: Channels allow for the creation of private communication pathways among specific participants, ensuring that transactions and data are only visible to authorized parties within that channel [33]. This is crucial for scenarios where sensitive information needs to be shared selectively.
4. **Scalability and Performance**: The execute-order-validate model, along with the separation of transaction execution from ordering, contributes to improved scalability and performance compared to systems that require all nodes to execute all transactions [48]. Endorsement policies can be tailored to distribute the workload.
5. **Support for General-Purpose Programming Languages for Chaincode**: Developers can write chaincode in familiar languages like Go, Node.js, and Java, which lowers the barrier to entry and facilitates the development of complex business logic [33].
6. **No Native Cryptocurrency**: Fabric does not require a built-in cryptocurrency to operate or incentivize miners, unlike public blockchains. This can simplify regulatory considerations for enterprises and focuses the platform on business process automation [47].
7. **Rich Query Capabilities**: When using CouchDB as the world state database, Fabric supports rich JSON-based queries against the ledger data, enabling more complex data retrieval and analysis than simple key-value lookups [33].
8. **Endorsement Policies**: Fabric allows for the definition of granular endorsement policies at the chaincode level, specifying which peers (or how many from different organizations) must endorse a transaction before it is considered valid [48]. This provides flexibility in defining the level of trust and validation required for different types of transactions.

2.5.4 Leveraging Hyperledger Fabric for Enhanced Pharmaceutical Supply Chain Management

Given its architecture and core features, **Hyperledger Fabric** provides a robust foundation for addressing the persistent challenges in pharmaceutical supply chains. These challenges include counterfeit drug prevention, regulatory compliance, traceability, and efficiency. Fabric's modular and permissioned blockchain framework aligns closely with the strategic objectives of supply chain management, offering notable benefits such as transparency, trust, auditability, and automation [43], [44], [51], [52].

Enhanced Traceability and Provenance:

Fabric's immutable ledger enables detailed, tamper-proof recording of every stage in the lifecycle of a pharmaceutical product—from raw material sourcing at the factory, through supplier distribution, to pharmacy dispensing [51], [52]. Each transaction is

cryptographically signed and timestamped, allowing for a verifiable, auditable trail of custody and origin. This real-time traceability is essential for ensuring product integrity and combating counterfeit drugs [44], [51].

Transparency and Trust Among Stakeholders:

By enabling authorized entities—Factory, Supplier, Pharmacy, and Pharmaceutical Government—to share and access synchronized data via a common permissioned ledger, Fabric promotes operational transparency [33], [51]. This shared visibility builds trust among participants and reduces disputes. Furthermore, channel-based data segregation ensures confidentiality, allowing sensitive business information to be selectively disclosed while still meeting regulatory requirements [33], [48].

Strengthened Regulatory Oversight and Compliance:

The involvement of a regulatory authority as a network participant in Fabric enables near real-time compliance monitoring. Regulators can verify licensing, temperature controls, and distribution legitimacy, while chaincode enforces rules automatically [31], [52]. This integration ensures that blockchain not only documents compliance but actively facilitates it.

Efficient and Targeted Product Recalls:

In the event of safety concerns or defective products, the blockchain's provenance data allows rapid identification of affected batches and their current status across the supply chain [51], [52]. Instead of broad, costly recalls, Fabric supports swift, targeted interventions. Chaincode can automate notifications to downstream actors, reducing manual coordination and public health risks.

***Data Integrity, Security, and Auditability*:**

Blockchain's immutability ensures that once batch data, shipment records, or quality checks are entered, they cannot be altered without detection [31], [48]. Fabric's use of cryptographic identities, endorsement policies, and fine-grained access control protects data against unauthorized changes. Additionally, the permanent and verifiable nature of records enhances auditability, enabling internal and external auditors to trace all activity systematically [58], [51].

***Smart Contract Automation*:**

Fabric supports complex logic execution via chaincode, enabling process automation such as shipment validation, real-time alerting for anomalies (e.g., temperature breaches), automated payment release upon delivery confirmation, or mandatory regulatory reporting [31], [51]. This significantly reduces manual intervention, improving both accuracy and efficiency.

***Alignment with Supply Chain Best Practices*:**

The design principles of Fabric address the broader benefits recognized in supply chain literature: enhanced **traceability**, **transparency**, **trust**, **efficiency**, and **fraud reduction** [43], [44]. These qualities are not only desirable but often mandated in pharmaceutical logistics to ensure safety, compliance, and ethical stewardship of medicine distribution.

2.6 Conclusion

This chapter introduced the conceptual underpinnings and architectural features of blockchain technology, with an emphasis on its relevance to enterprise-grade systems such as supply chains. Through an analysis of its core properties, immutability, decentralization, cryptographic security, consensus mechanisms, and auditability, blockchain was shown to offer significant advantages over traditional centralized systems in contexts where data integrity, provenance, and stakeholder trust are paramount. The discussion then shifted to Hyperledger Fabric, a permissioned blockchain framework that aligns closely with the needs of complex, multi-organizational ecosystems like pharmaceutical supply chains. Key components such as peer nodes, ordering services, smart contracts (chaincode), and private channels were detailed, emphasizing how Fabric supports modularity, confidentiality, identity management, and transaction scalability. In sum, Hyperledger Fabric's design not only meets the general requirements for secure and auditable data sharing but also supports fine-grained control over access and functionality, making it a strong candidate for building blockchain-based pharmaceutical platforms. The next chapter builds upon this technical foundation to outline the architectural blueprint of the proposed Pharmaceutical Collaborative Platform (PCP), applying these concepts to a real-world case.

Chapter 3

Network Design and Architecture

3.1 Introduction

The pharmaceutical supply chain plays a critical role in safeguarding public health. However, it is often plagued by major challenges such as lack of transparency, inefficiencies, and insufficient trust among stakeholders. These shortcomings can result in severe consequences, including the distribution of counterfeit drugs, delayed or ineffective product recalls, and an inability for regulatory bodies to perform real-time monitoring and oversight.

To address these pressing issues, this project proposes the development of a blockchain-based system built on *Hyperledger Fabric*. The primary objective is to establish a decentralized, tamper-resistant platform that ensures end-to-end traceability, data integrity, and accountable interactions among the key entities in the supply chain.

This chapter provides a detailed design blueprint of the proposed system architecture. It outlines the conceptual framework, the structural composition of the Hyperledger Fabric network, the design and functionality of the smart contracts (chaincode), and the mapping of critical pharmaceutical processes into blockchain-based transactions. The ultimate aim is to deliver a scalable, secure, and transparent architecture that facilitates product provenance tracking, enhances recall responsiveness, and enables real-time regulatory access.

The chapter proceeds with:

- A high-level overview of the system.
- A detailed explanation of the network topology and channel configuration.
- Smart contract structure and transaction logic using UML models.
- Mapping of real-world business processes to transaction flows via sequence diagrams.
- A comprehensive look at the security and privacy mechanisms.
- A list of the tools and technologies used for development and deployment.

This design will serve as the technical foundation for the implementation phase described in Chapter 4.

3.2 Proposed Architecture

The proposed system leverages the core strengths of **Hyperledger Fabric** specifically its permissioned nature, support for private channels, and robust smart contract capabilities to establish a secure and collaborative environment among key actors in the pharmaceutical supply chain(see Figure 3.2).

Participating Organizations

The network consists of four main organizations:

- **FactoryOrg (Manufacturer)**: Responsible for producing medications and registering production batches on the blockchain.
- **SupplierOrg (Distributor)**: Receives medications from manufacturers, stores them, and delivers them to pharmacies.
- **PharmacyOrg (Pharmacy)**: Receives medication from suppliers and records dispensation events to patients.
- **PcpOrg (Regulatory Authority)**: Acts as the governing body responsible for auditing transactions, monitoring compliance, and issuing product recalls.

Interaction Overview

All organizations are connected through a shared **Hyperledger Fabric blockchain network**, which serves as a single, immutable source of truth. Every critical supply chain event—production, shipment, delivery, or dispensation—is captured as a blockchain transaction.

From → To	**Transaction Description**
FactoryOrg → SupplierOrg	Shipment of medication batches
SupplierOrg → PharmacyOrg	Delivery of medications
PharmacyOrg → Patient (conceptual)	Dispensation of medication
All Organizations → Blockchain	Transaction recording
PcpOrg Blockchain	Regulatory audits, recall issuance

Table 3.1: Key interactions between organizations

Note: The patient is not a direct network participant but represents the endpoint of the pharmaceutical distribution chain.

Architectural Goals:

This architecture ensures full traceability of medications from origin to patient, promotes data integrity through an immutable ledger, and enforces access control based on cryptographic organizational identity. It further empowers **PcpOrg** to conduct real-time regulatory monitoring and initiate recall actions.

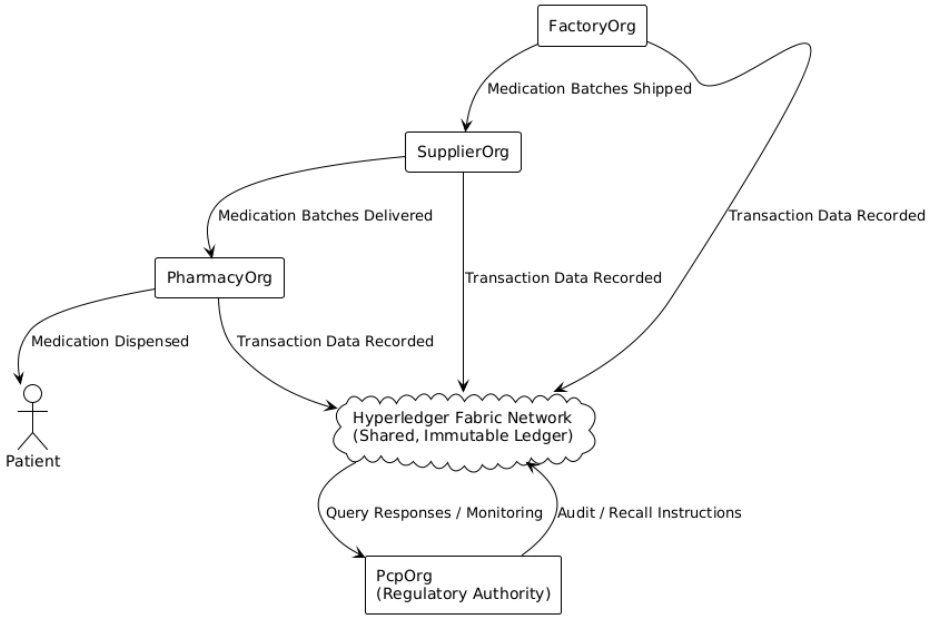

Figure 3.1: Conceptual overview of the pharmaceutical supply chain using Hyperledger Fabric

3.3 Hyperledger Fabric Network Architecture

3.3.1 Network Topology and Participants

The backbone of the proposed pharmaceutical supply chain system is a permissioned **Hyperledger Fabric** network composed of five key organizations: `FactoryOrg`, `SupplierOrg`, `PharmacyOrg`, `PcpOrg` (regulatory authority), and `OrdererOrg` (responsible for transaction ordering and block creation).

Each organization contributes its own resources to the network, including peer nodes, certificate authorities (CAs), and membership service providers (MSPs) for identity and access control. The following summarizes the role of each participant:

FactoryOrg

- **Role:** Manufactures pharmaceutical products and registers new medication batches on the ledger.
- **Components:** `ca.factory.example.com`, `peer0.factory.example.com`
- **Functions:** Batch creation, shipment initiation, raw material traceability.

SupplierOrg

- **Role:** Handles storage and distribution of medications to pharmacies.
- **Components:** `ca.supplier.example.com`, `peer0.supplier.example.com`
- **Functions:** Shipment reception, forwarding, and inventory management.

PharmacyOrg

- **Role:** Receives medications and records dispensation to patients.
- **Components:** `ca.pharmacy.example.com`, `peer0.pharmacy.example.com`
- **Functions:** Dispensation recording, querying recalled products.

PcpOrg (Regulatory Authority)

- **Role:** Oversees compliance, audits transactions, and initiates regulatory actions such as recalls.
- **Components:** `ca.pcp.example.com`, `peer0.pcp.example.com`
- **Functions:** Audit queries, compliance validation, recall issuance.

OrdererOrg

- **Role:** Manages the ordering service, ensuring proper sequencing of transactions and distribution of blocks to peers.
- **Components:** `ca.orderer.example.com`.
- **Consensus Protocol:** Raft (for crash fault tolerance and decentralized control).

All peer nodes from the four primary organizations (`FactoryOrg`, `SupplierOrg`, `PharmacyOrg`, and `PcpOrg`) are joined to a shared channel named `pharma-supply-channel`. This channel facilitates the exchange of all relevant transactions related to the lifecycle of pharmaceutical products.

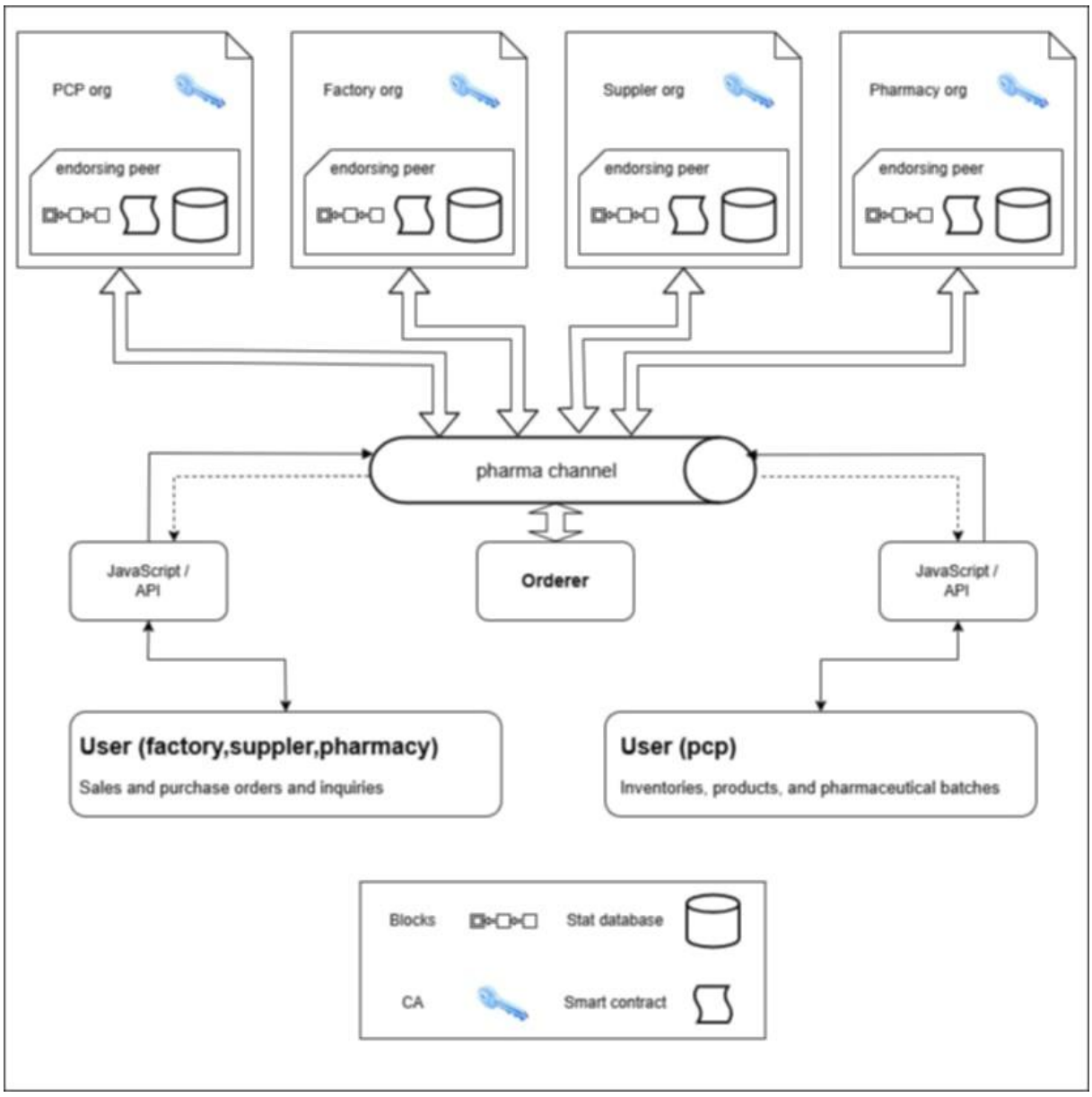

Figure 3.2: Detailed topology of the Hyperledger Fabric network, showing the organizations, their CAs, peers, ordering node, and their participation in the shared `pharma channel`.

3.3.2 Channel Design

To ensure data isolation, confidentiality, and secure collaboration between participants, **Hyperledger Fabric** introduces the concept of *channels*. A channel is a private communication subnet that allows a specific group of organizations to share data and execute smart contract logic independently from other members of the network.

In the proposed pharmaceutical supply chain system, a single primary channel named `pharma channel` is created to handle all critical transactions related to product lifecycle management.

Channel Name: `pharma channel`

Participating Organizations:

- `FactoryOrg`
- `SupplierOrg`
- `PharmacyOrg`
- `PcpOrg`
- `OrdererOrg`

Purpose: This channel facilitates the flow of all essential supply chain transactions, including:

- Medication batch creation and registration
- Inter-organizational shipment and receipt confirmation
- Dispensation records by pharmacies
- Regulatory audits and recall actions issued by `PcpOrg`

Access Control: While all participating organizations are members of the same channel, access to specific smart contract functions and data is restricted through:

- Identity-based permissions
- Role-based checks embedded in the chaincode logic

3.3.3 Ledger Structure

In **Hyperledger Fabric**, the ledger is a foundational element that ensures transparency, consistency, and auditability of all network activities. Every peer node that joins a channel maintains its own complete copy of the ledger for that channel.

The ledger is composed of two main components:

1. World State The world state is a key-value data store that contains the latest value of each asset. In this system, **CouchDB** is used as the state database for all peers, providing advanced query capabilities through JSON-based selectors. This enables flexible and efficient access to current asset data, particularly for reporting and audit queries initiated by `PcpOrg`.

2. Blockchain (Transaction Log) The blockchain is an immutable, append-only sequence of transaction blocks. It records the full history of all changes to the world state. Each block is cryptographically linked to the previous one, ensuring tamper-evidence and providing a verifiable audit trail for all on-chain activities.

3.3.4 Smart Contract Design (Chaincode)

This section describes the modular structure of the smart contracts and the assets they manage throughout the pharmaceutical supply chain.

1. Chaincode Structure

The chaincode is implemented using JavaScript and is split into two distinct contracts to ensure clear separation of concerns:

PcpCommunication Responsible for participant registration, product and batch management, and offer publishing.

- Registers and authenticates entities.
- Adds pharmaceutical products and batches.
- Handles batch and product recall.
- Publishes commercial offers referencing batches.

CommercialTransactionsContract Manages inventory and exchange operations between organizations.

- Initializes and updates inventory per entity.
- Manages product batch transfers through exchange requests.
- Validates batch activity via chaincode calls.

Design Considerations

- Chaincode intercommunication via `invokeChaincode`.
- CouchDB is used for storing JSON-based assets with defined `docType`.

2. Asset Definitions

- **Entity:** Represents participants with credentials and metadata.
- **Product:** Contains product-specific data including manufacturer info and dosage.
- **Batch:** Defined inside each product, includes quantity and expiration data.
- **Offer:** Represents a set of products made available for exchange.
- **Inventory:** Maintains batch availability for each organization.
- **ExchangeRequest:** Manages transfer requests and their statuses.

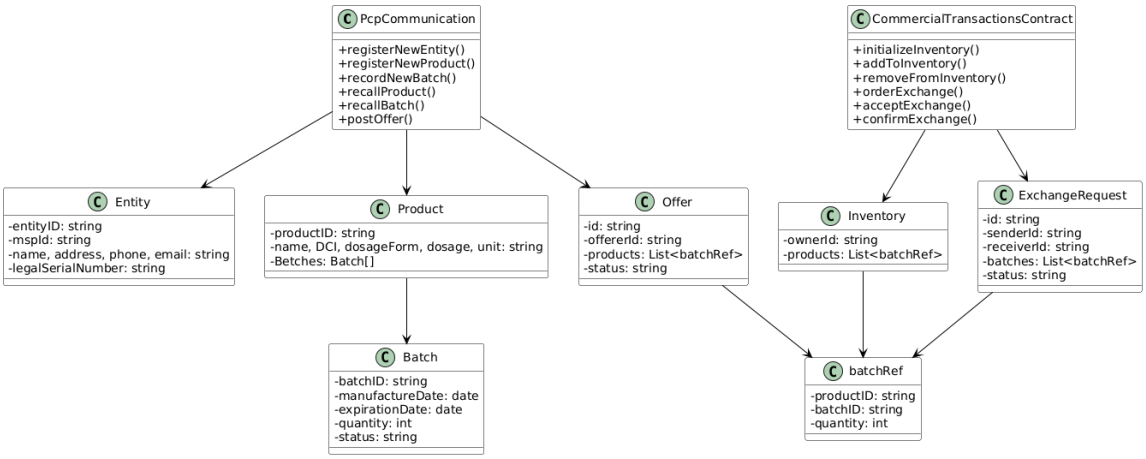

Figure 3.3: UML diagram showing smart contracts and their related asset classes.

3.3.5 Smart Contract Logic

The chaincode defines the core transactional behaviors that govern the pharmaceutical supply chain. Two smart contracts encapsulate the business logic governing entity registration, inventory handling, and exchange workflows.

PcpCommunication

- **registerNewEntity:** Allows each MSP to register authenticated entities with required metadata and password hashing.
- **registerNewProduct & recordNewBatch:** Factories may register pharmaceutical products and record their associated production batches.
- **recallProduct & recallBatch:** Enables the manufacturer to mark a product or batch as recalled with an explanatory reason.
- **postOffer:** Allows factories and suppliers to publish offers referencing inventory items. Availability is validated by querying the inventory.

CommercialTransactionsContract

- **initializeInventory:** Initializes an empty inventory for a given entity.
- **addToInventory / removeFromInventory:** Used to manage incoming and outgoing batch transfers.
- **orderExchange:** Creates a structured exchange request, referencing product and batch IDs.
- **acceptExchange:** Receiver validates and deducts quantities from their inventory.
- **confirmExchange:** Sender confirms receipt and adds the batch to their own inventory.
- **Cross-contract verification:** Ensures batch status is checked in real time via `isBatchActive()` in `PcpCommunication`.

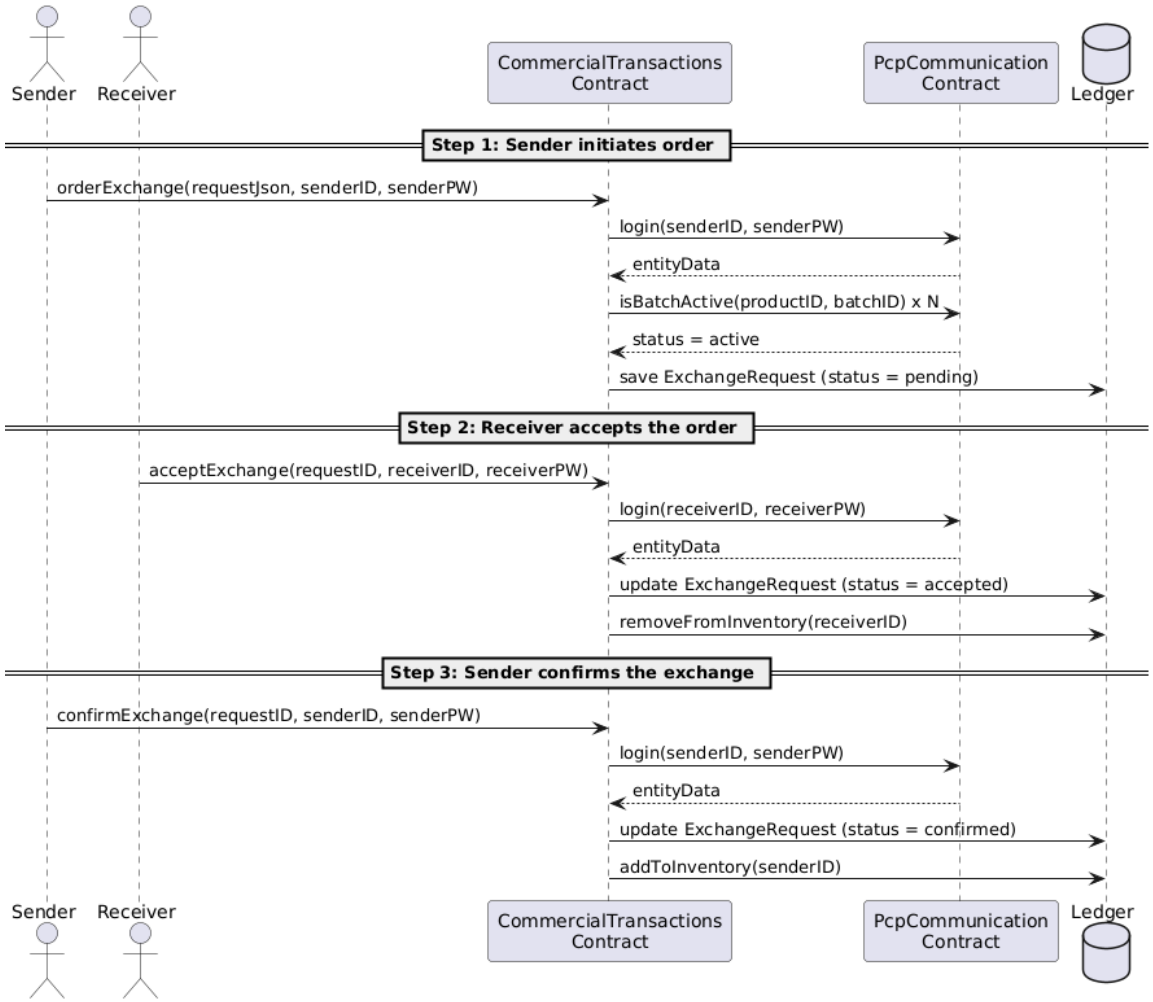

Figure 3.4: Sequence diagram illustrating the exchange workflow between sender and receiver via smart contract logic.

3.3.6 Authentication Policies

Hyperledger Fabric enforces authentication and trust through the use of endorsement policies. These policies determine which peers must approve a transaction before it is considered valid and committed to the ledger.

PcpCommunication This contract requires co-endorsement by `PCP` and one other organization. The policy is formally defined as:

```
OR(
  AND('PCP.peer', 'Supplier.peer'),
  AND('PCP.peer', 'Pharmacy.peer'),
  AND('PCP.peer', 'Factory.peer')
)
```

This ensures that regulatory oversight (via PCP) is enforced on every critical action performed by any participant.

CommercialTransactionsContract This contract supports broader interaction patterns and is deployed with the following policy:

```
OR(
  AND('Pharmacy.peer', 'Supplier.peer'),
  AND('Pharmacy.peer', 'Factory.peer'),
  AND('Factory.peer', 'Supplier.peer'),
  AND('Factory.peer', 'PCP.peer')
)
```

This configuration enables flexible multi-party workflows while still enforcing accountability through dual endorsement.

3.4 Transaction Flow

This section describes how physical business processes are digitized and enforced using blockchain-based smart contracts. Each real-world interaction is mapped into a secure transaction.

3.4.1 Manufacturing and Dispatching a Batch

Scenario: A factory produces and dispatches a new medication batch.

Steps:

- `registerNewProduct()` – Registers a new product.
- `recordNewBatch()` – Adds a batch to the product.
- `initializeInventoryBatches()` – Synchronizes batches with inventory.
- `postOffer()` – Publishes available batches.

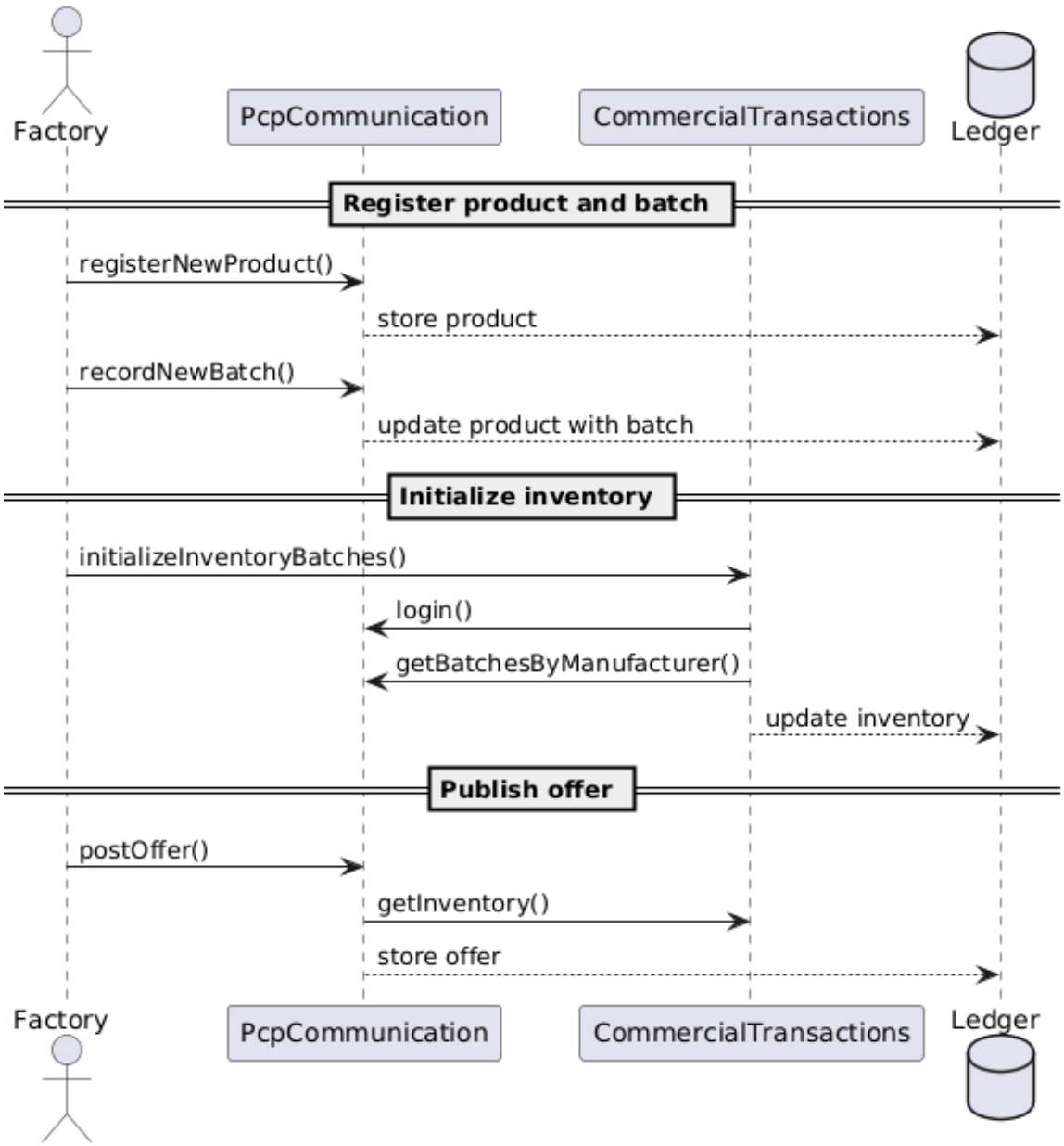

Figure 3.5: Sequence diagram – Batch production and offer publishing.

3.4.2 Product Recall

Scenario: A factory recalls a faulty product or batch.

Steps:

- `recallProduct()` or `recallBatch()` – Updates status to ”recalled”.
- Ledger is updated with new status visible to all organizations.

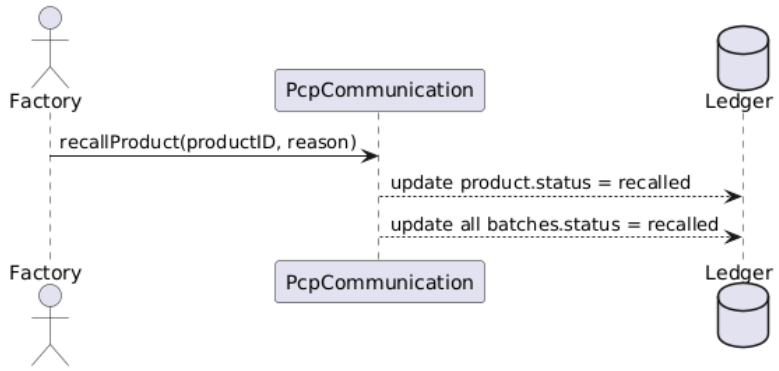

Figure 3.6: Sequence diagram – Product or batch recall.

3.5 Security and Privacy

The system ensures robust security and privacy mechanisms through multiple layers, relying on Hyperledger Fabric's permissioned model and additional cryptographic protections.

Identity Verification

- Transactions are signed using digital certificates issued by the Certificate Authorities (CAs) of each participating organization.
- The smart contracts use Fabric's `clientIdentity` module to extract and verify the submitter's identity and associated MSP.

Channel and Data-Level Privacy

- The network utilizes a dedicated channel, `pharma-supply-channel`, which isolates data among authorized participants.
- Chaincode logic restricts access to functions based on roles and organizational policies.

Tamper-Evident Records

- All data is immutably recorded on the blockchain ledger.
- Transaction logs are traceable, making all recalls, product creations, and inventory changes verifiable.

Patient Data Privacy (Future Scope)

- While the current implementation does not manage patient data, it is designed to support:
  * Hashing identifiers.
  * Application-layer field encryption.
  * Integration with Fabric's Private Data Collections.

Tools and Technologies Used

The system was built using a combination of modern tools and technologies that support decentralized application development, containerized deployment, and model-driven architecture.

- **Hyperledger Fabric 2.4.5:** A modular and extensible permissioned blockchain platform that supports private channels, chaincode execution, and MSP-based identity management.
- **JavaScript (Chaincode):** All smart contracts were implemented using the Fabric Contract API in JavaScript, offering compatibility with JSON-based data and ease of rapid development.
- **CouchDB:** Used as the state database. Supports JSON-based document storage and advanced querying via selectors, enabling efficient asset filtering.
- **Docker:** Employed for deploying and managing blockchain components as containers. Ensures consistency and portability across environments.
- **Git:** Source control system used to manage project versions and team collaboration.
- **Fabric SDK:** Provides programmatic access for submitting transactions and interacting with the ledger from external applications.
- **UML Tools:** PlantUML and other modeling tools were used to design and visualize architectural and behavioral aspects of the system.

3.6 Conclusion

This chapter presented the complete architectural design of the blockchain-based pharmaceutical supply chain system. It included the network topology, smart contract structures, asset definitions, transaction workflows, and security considerations.

The chosen tools and technologies including Hyperledger Fabric, JavaScript, CouchDB, and Docker were selected for their robustness, flexibility, and compatibility with enterprise-grade systems.

This design provides a solid foundation for the actual system implementation, which will be covered in detail in the next chapter.

Chapter 4

Implementation and Evaluation of the Proposed Network

4.1 Introduction

This chapter focused on the implementation and the evaluation of the proposed system that was theoretically designed in Chapter Three. The system is based on the use of *Hyperledger Fabric* blockchain technology, aiming to enhance transparency, strengthen traceability, and ensure reliability within the pharmaceutical supply chain. This is achieved by building a distributed network that includes key stakeholders in the chain such as the manufacturer, supplier, pharmacy, and the governmental regulatory authority.

The objective of this chapter is to document the practical and operational aspects of the project, starting from setting up the development environment and installing the necessary software, to configuring the network, generating digital certificates, initializing channels, and developing the smart contracts (*chaincode*). It also covers the client application developed to enable users to interact with the network in a flexible and user-friendly manner, whether for executing transactions or querying data. Additionally, the chapter presents the technical challenges encountered during the implementation process and the solutions adopted to overcome them.

All stages will be presented gradually and systematically, starting with the specification of hardware and software requirements, followed by an explanation of the tools used for installing and setting up *Hyperledger Fabric*, generating cryptographic materials and channel genesis blocks, and configuring network files. Subsequently, the development of smart contracts in Go will be detailed, including the design of the core data structures, implementation of key system functions, and definition of identity and access control policies.

Finally, the client application component will be presented, developed using an appropriate SDK toolkit, explaining how to connect to the network, send transactions, and retrieve data. The chapter concludes with a review of the main challenges faced during implementation and the proposed solutions to address them.

This chapter paves the way for the next one, which will focus on testing the system and evaluating its effectiveness in achieving the intended objectives in a realistic simulation environment.

4.2 Setting Up the Hyperledger Fabric Environment

This section provides a detailed step-by-step guide to setting up the Hyperledger Fabric environment on **Windows 10**, using **WSL 2 (Windows Subsystem for Linux)**, **Docker**, and other necessary tools.

Docker Docker is a container-based software platform that enables developers to build, package, and run applications in isolated environments called containers. Each container includes the application code and its dependencies, allowing consistent and reliable execution across diverse environments. Unlike virtual machines, containers share the host operating system's kernel, providing lightweight virtualization with minimal resource overhead. Docker simplifies the development and deployment lifecycle by enabling rapid testing, portability, and scalability of applications[65].

4.3 Client Application

4.3.1 Purpose and Role of the Application

The client application was developed as an integral component of the system to enable real-time interaction between the registered organizations and the blockchain network. Rather than relying on CLI tools or manual smart contract invocations, the RESTful API and accompanying frontend provide a more intuitive and accessible interface for performing essential operations such as product registration, batch tracking, offer management, and trade transactions.

It bridges the gap between the users and the smart contracts deployed on Hyperledger Fabric, enabling secure and role-specific access.

4.3.2 General Architecture (Node.js + fabric-network)

The backend of the application is built using **Node.js** and **Express.js**, and leverages the official `fabric-network` library to interact with the blockchain. Each organization has:

- A dedicated wallet storing its identity credentials.
- A corresponding `connection.json` file used to establish a secure connection to the network.

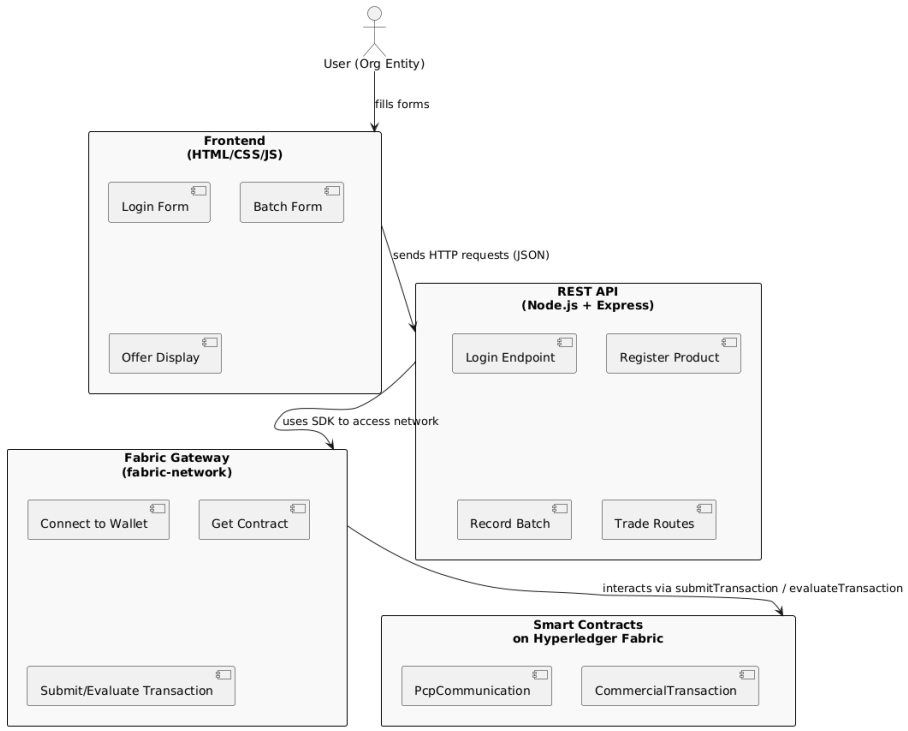

Figure 4.1: High-level architecture: Frontend ↔ REST API ↔ Hyperledger Gateway ↔ Smart Contracts

The REST API acts as middleware, exposing endpoints that trigger smart contract functions and delivering the results back to the user through HTTP responses.

4.3.3 Identity Management and Authentication (Login / Signup)

Authentication is handled at the application level. Upon registration (`signup`), each organization provides:

- `entityID`
- `entityPW`
- Additional metadata (address, email, phone number, etc.)

Before performing any action on the blockchain, the user must authenticate via a `login` endpoint. Each request thereafter includes both `entityID` and `entityPW` in the payload.

Note: This approach is acceptable for development and testing, but lacks encryption and session management. Enhancements are discussed in section 4.3.6.

4.3.4 Interaction with Smart Contracts

The application dynamically connects to the desired smart contract (`PcpCommunication` or `CommercialTransaction`) based on the action requested. This is achieved via:

Listing 4.1: Smart contract interaction snippet

```
async function getContract(org, chaincodeName) {
  const ccpPath = path.resolve(__dirname, 'connection-profiles', `${
    ↪ org}.json`);
  const ccp = JSON.parse(fs.readFileSync(ccpPath, 'utf8'));

  const walletPath = path.join(__dirname, 'wallet');
  const wallet = await Wallets.newFileSystemWallet(walletPath);

  const identityLabel = `${org.charAt(0).toUpperCase() + org.slice(1)}
    ↪ _User1`;

  const gateway = new Gateway();
  await gateway.connect(ccp, {
    wallet,
    identity: identityLabel,
    discovery: { enabled: true, asLocalhost: true },
  });

  const network = await gateway.getNetwork('mychannel');
  const contract = network.getContract(chaincodeName);

  return { contract, gateway };
}
```

Each endpoint determines the chaincode and organization involved and performs either a `submitTransaction` (write) or `evaluateTransaction` (read-only).

4.3.5 Main Functions in the REST API

Below is a summary of key API endpoints grouped by category:

Authentication & Entity Management

- `POST /api/:org/signup`
- `POST /api/:org/login`

Product and Batch Management

- `POST /api/:org/registerProduct`
- `POST /api/:org/record-batch`
- `POST /api/:org/recallProduct`
- `POST /api/:org/recallBatch`

Offer Handling

- `POST /api/:org/postOffer`
- `POST /api/:org/listActiveOffers`

Trade Operations

- `POST /api/:org/orderExchange`
- `POST /api/:org/acceptExchange`
- `POST /api/:org/confirmExchange`
- `POST /api/:org/getMyOrderSend`
- `POST /api/:org/getMyOrderReceive`

Inventory Management

- `POST /api/:org/initializeInventory`
- `POST /api/:org/getInventory`
- `POST /api/:org/getAllProducts`
- `POST /api/:org/getAllBatches`

Listing 4.2: Product registration API call

```
await contract.submitTransaction(
  'registerNewProduct',
  entityID, entityPW,
  productID, name, DCI, dosageForm, dosage, unit
);
```

4.3.6 Critical Notes and Suggestions for Improvement

While the application performs its role effectively as a testing and demonstration tool, the following limitations were identified:

Current Limitations

- Plain text passwords are used without encryption.
- No session or token-based authentication.
- Repeated inclusion of credentials in each request.
- No HTTPS or transport-level encryption.
- No role-based access control or fine-grained permissions.

Recommended Enhancements

- Implement password hashing (e.g., bcrypt).
- Introduce JWT-based session tokens.
- Use Fabric CA for dynamic identity enrollment.
- Separate frontend and backend layers for better scalability.
- Secure all communications using HTTPS.
- Add audit logging for critical operations.

4.3.7 User Interface (HTML/CSS/JS)

In parallel with the REST API, a simple yet functional web interface was developed using **HTML**, **CSS**, and vanilla **JavaScript**. This UI allows users to test and visualize all blockchain interactions without using CLI tools or Postman.

Available Functions

- Login and signup for organizations.
- Product and batch registration.
- Product and batch withdrawal.
- Posting and browsing offers.
- Managing order exchanges (send, accept, confirm).
- Inventory visualization.

Communication Method

The frontend uses the JavaScript `fetch()` API to send and receive JSON-formatted requests/responses.

Listing 4.3: Login request example

```
fetch("/api/factory/login", {
  method: "POST",
  headers: { "Content-Type": "application/json" },
  body: JSON.stringify({ entityID, entityPW })
})
.then(response => response.json())
.then(data => {
  console.log("Login successful:", data);
})
.catch(error => console.error("Login error:", error));
```

Screenshots and Descriptions

To better illustrate the functionality of the client application, the following screenshots present the key pages and operations available to users through the web interface:

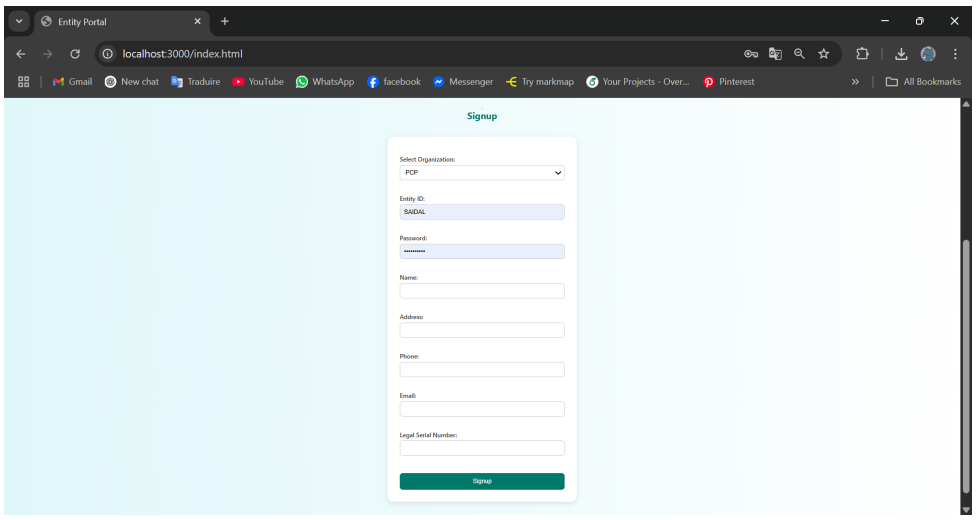

Figure 4.2: Signup pagen.

This page allows new organizations (e.g., factory, supplier, pharmacy) to register on the platform by entering a unique `entityID`, `entityPW`, and additional metadata. It is the first step to gain access to the system.

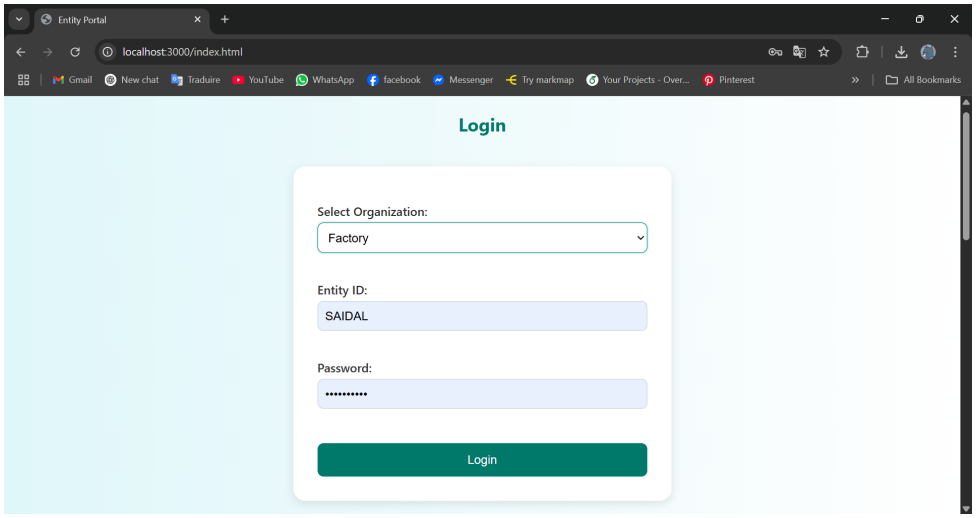

Figure 4.3: login pagen.

Registered users authenticate using their `entityID` and `entityPW`. Successful login establishes identity and allows subsequent secure interactions with the network.

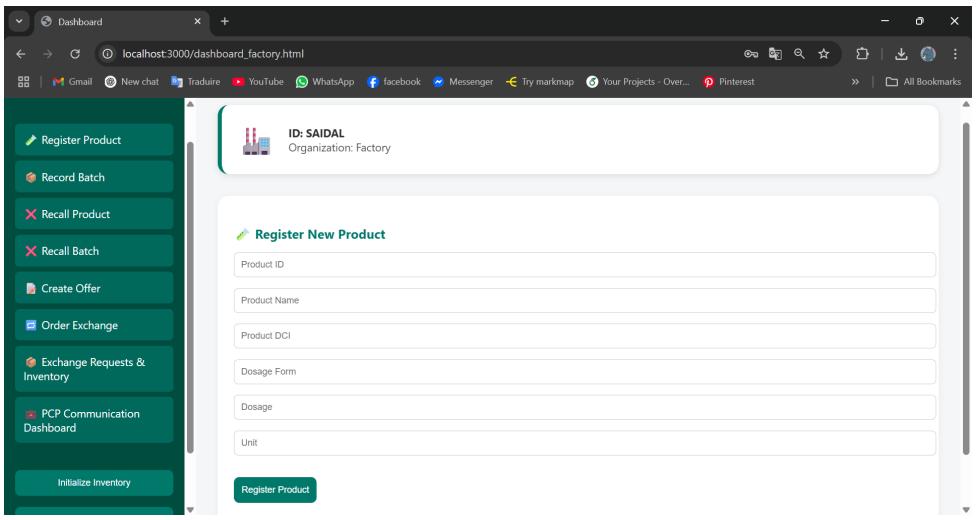

Figure 4.4: Product registration form.

This interface is used by manufacturers to register new pharmaceutical products on the blockchain, including metadata like product ID, name, dosage form, dosage, and unit.

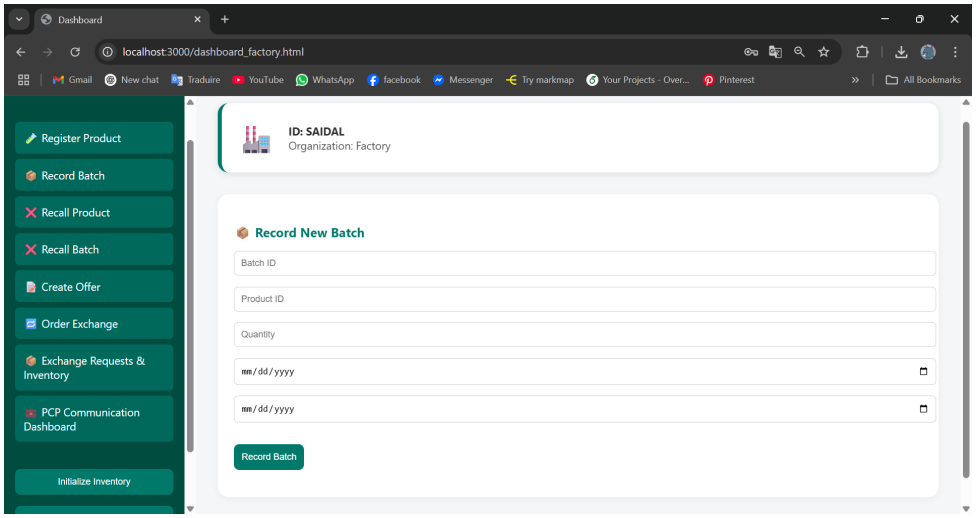

Figure 4.5: Batch registration form.

Factories can record new batches linked to previously registered products. Each batch includes production data, expiration dates, and quantity.

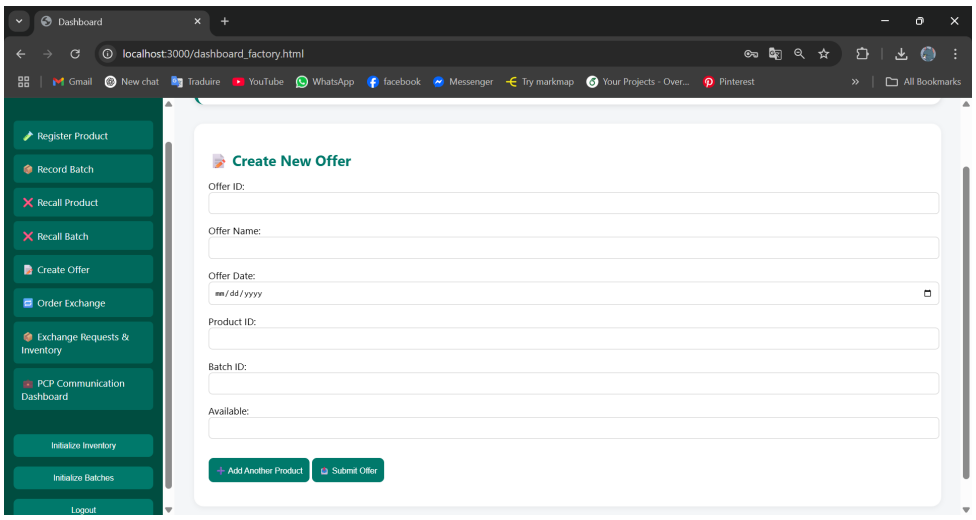

Figure 4.6: Offer publication interface.

Suppliers can publish offers of available products/batches. Offers include pricing, available quantities, and validity periods.

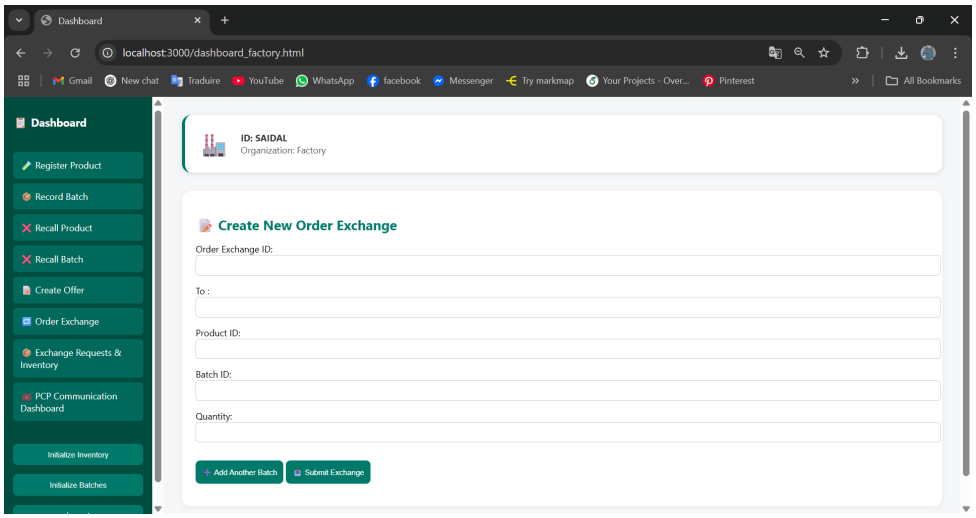

Figure 4.7: Exchange orders view.

This view enables users to initiate, accept, and confirm order exchanges, facilitating structured transactions between organizations.

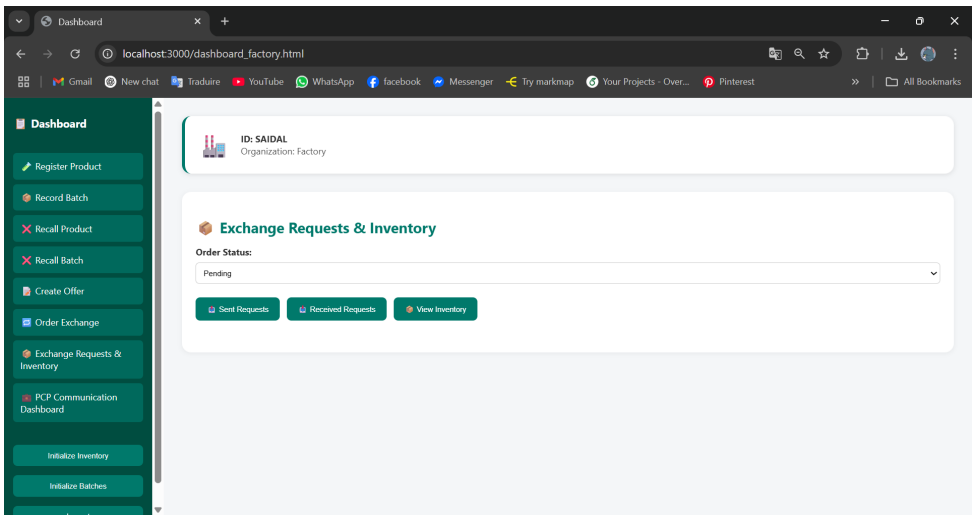

Figure 4.8: Inventory View.
A summarized interface where organizations can view their current product stock, quantities, and batch details.

4.3.8 Summary

The client application acts as a critical bridge between users and the blockchain network. By abstracting smart contract calls through REST endpoints and providing a usable interface, it makes the system accessible to non-technical users. While currently optimized for testing and demonstration, it establishes a solid foundation for building secure, scalable, and production-ready interfaces.

4.4 Performance Evaluation

The performance evaluation phase aims to assess the efficiency, responsiveness, and scalability of the proposed blockchain-based pharmaceutical supply chain solution developed using Hyperledger Fabric. To achieve this, we employed Hyperledger Caliper to conduct controlled benchmarking experiments targeting both read and write operations under varying loads and stability conditions.

4.4.1 Performance Measurement Criteria – Definitions

Throughput Throughput refers to the number of successful transactions completed per second (TPS). It serves as a primary indicator of how much load the system can handle and is crucial for evaluating scalability and system capacity [61].

Latency Latency is the time delay between submitting a transaction and receiving confirmation, measured in seconds. It reflects the responsiveness of the system under different workloads and directly impacts user experience [62].

Max/Min Latency Maximum and minimum latency refer to the highest and lowest recorded delays for processing a transaction during tests. These metrics help

assess system consistency, performance peaks, and worst-case response scenarios [63].

Stability Stability describes the system's ability to maintain consistent throughput and latency during sustained or repeated workloads. It reflects the robustness and reliability of the network, particularly under pressure [64].

4.4.2 Benchmarking Tools and Setup

Hyperledger Caliper Hyperledger Caliper is a benchmarking framework designed specifically for blockchain networks. It allows developers to evaluate throughput, latency, and resource utilization of blockchain-based systems. In our study, Caliper was integrated with the deployed Fabric network to simulate transaction load and measure system performance metrics accurately.

CouchDB as State Database CouchDB was used as the state database for the Fabric network. This NoSQL document-oriented database is well-suited for chaincode queries, offering native support for rich queries using JSON and Mango queries. It enables flexible access to world state and can influence performance behavior significantly compared to default LevelDB.

Hardware and System Specifications All performance tests were executed locally on the following hardware and software environment:

Component	**Specification**
Device Name	DESKTOP-M7PKFD2
Processor	Intel Core i5-8265U @ 1.60GHz to 1.80GHz
RAM	8.00 GB (7.85 GB usable)
System Type	64-bit OS, x64-based Processor
Operating System	Windows (via WSL Ubuntu)
State Database	CouchDB

Table 4.1: Test Machine Specifications

4.4.3 Benchmark Scenarios

To evaluate the performance of both read and write operations, we designed two distinct benchmarking scenarios, each consisting of:

- **Progressive Load Testing:** Incrementing send rate from 100 to 1000 TPS.
- **Stability Testing:** 5 identical rounds at a fixed send rate of 500 TPS.

Write Scenario

- Operation: `registerEntity` from the `PcpCommunication` contract.
- Module: `registerEntity.js`
- Purpose: Simulates ledger write operations (entity registration).

Read Scenario

- Operation: `login` from the `PcpCommunication` contract.
- Module: `login.js`
- Purpose: Simulates query operations without ledger modification.

4.4.4 Results and Analysis

Write Operations Analysis

Target TPS	Throughput (TPS)	Avg Latency (s)	Max Latency (s)	Min Latency (s)
100	99.8	0.16	0.71	0.06
200	130.3	3.19	4.80	0.22
300	111.1	4.86	7.33	0.18
400	131.8	4.62	6.35	0.67
500	106.3	5.98	9.02	2.43
600	88.1	8.83	10.67	3.17
700	101.7	7.64	9.44	3.37
800	88.9	8.59	11.11	2.95
900	118.5	4.65	7.54	2.48
1000	154.1	4.55	6.29	2.14

Table 4.2: Write Operation Performance under Progressive Load

Progressive Load Results

Round	Throughput (TPS)	Avg Latency (s)	Max Latency (s)	Min Latency (s)
1	150.9	4.22	5.51	0.35
2	154.5	4.15	5.46	0.34
3	160.0	3.86	5.32	0.71
4	118.8	6.08	7.13	0.35
5	164.6	3.75	5.11	0.55

Table 4.3: Write Operation Stability Results at 500 TPS

Stability Testing Results at 500 TPS

Read Operations Analysis

Progressive Load Results .

Target TPS	Throughput (TPS)	Avg Latency (s)	Max Latency (s)	Min Latency (s)
100	95.7	0.21	2.11	0.01
200	199.7	0.02	0.07	0.01
300	208.4	0.36	2.10	0.01
400	400.5	0.04	0.19	0.01
500	467.5	0.45	0.69	0.07
600	487.1	0.94	1.48	0.12
700	523.8	1.08	1.52	0.05
800	551.3	1.10	1.57	0.19
900	563.1	1.15	1.61	0.04
1000	568.9	1.22	1.69	0.09

Table 4.4: Read Operation Performance under Progressive Load

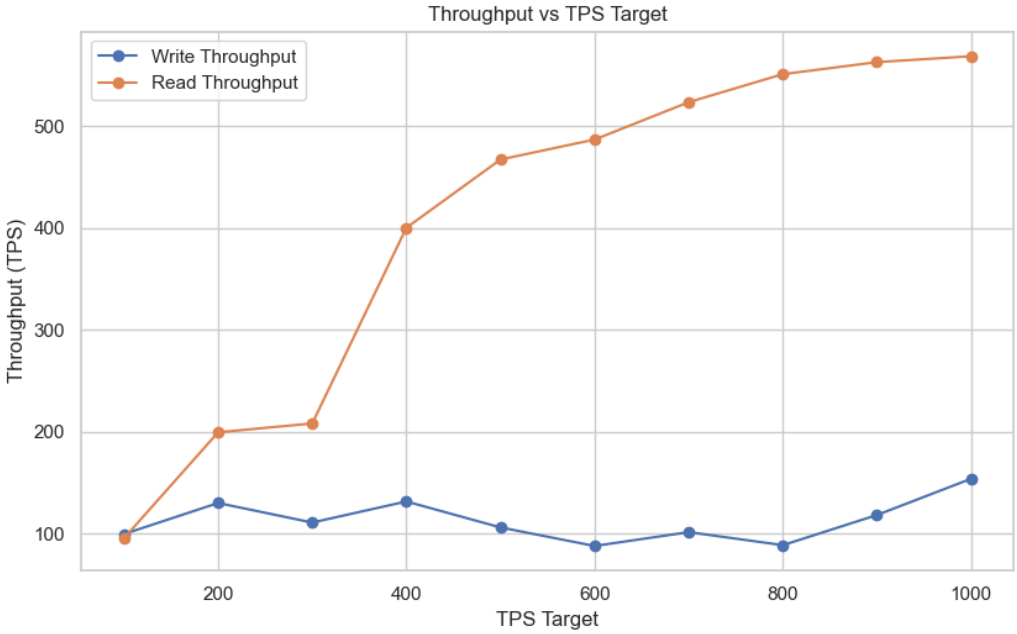

Figure 4.9: Throughput vs TPS Target for Read and Write Operations

Observation: The system demonstrated excellent scalability for read operations, maintaining near-target throughput. Write operations performed commendably up to moderate TPS, highlighting the platform's capability to manage diverse loads efficiently and reliably.

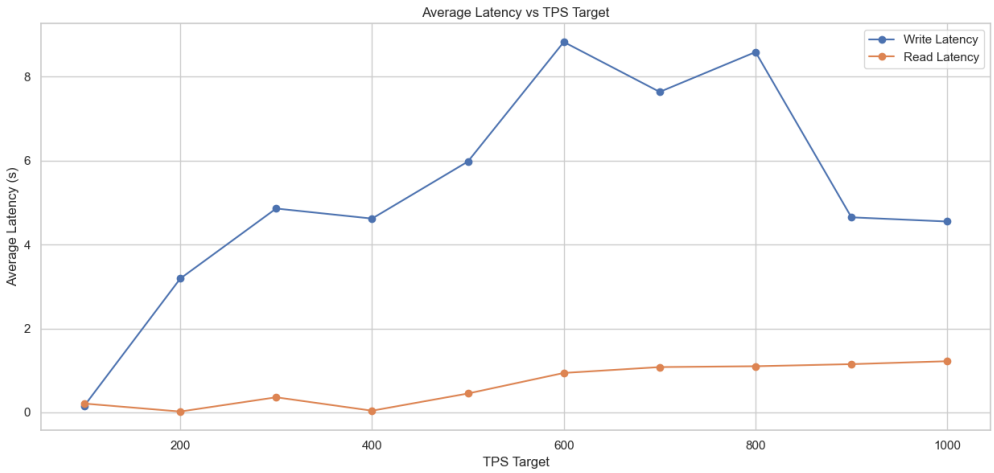

Figure 4.10: Average Latency vs TPS Target for Read and Write Operations

Observation: Write operations experience significant latency increase with pressure, while read latency remains consistently low, demonstrating efficient query performance.

Stability Testing Results at 500 TPS .

Round	Throughput (TPS)	Avg Latency (s)	Max Latency (s)	Min Latency (s)
1	499.4	0.03	0.07	0.01
2	499.6	0.03	0.07	0.01
3	499.5	0.03	0.10	0.01
4	499.3	0.02	0.08	0.01
5	499.8	0.02	0.13	0.01

Table 4.5: Read Operation Stability Results at 500 TPS

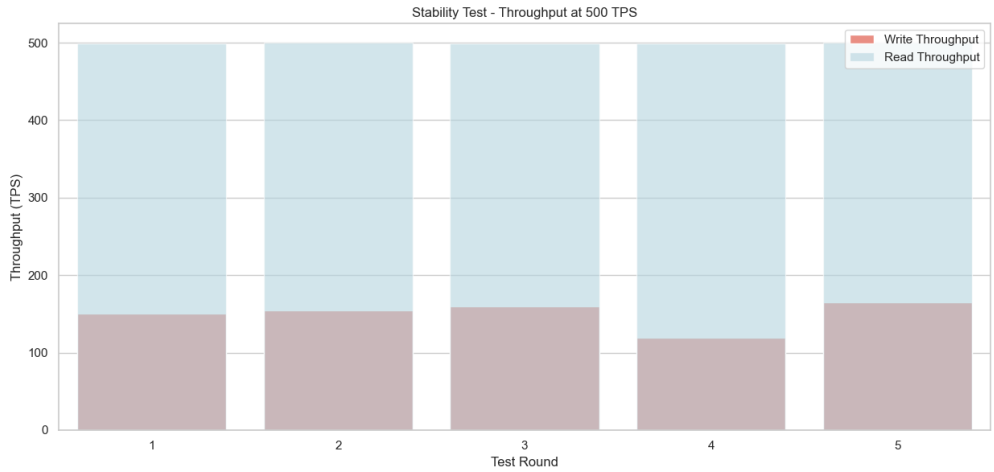

Figure 4.11: Stability Test: Throughput over 5 Rounds at 500 TPS

Observation: Throughput results were highly consistent across all rounds, especially for read operations. This reflects the robustness and stability of the system under

continuous pressure, making it well-suited for real-world, high-frequency environments.

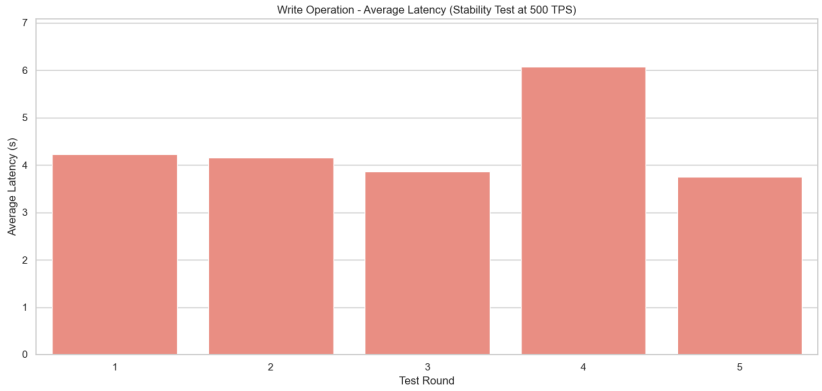

Figure 4.12: Write Operation Latency (Stability Test at 500 TPS)

Observation: Despite the natural complexity of write operations, latency remained within a stable and acceptable range. This underlines the system's strong performance in handling sustained write workloads with consistency and reliability.

Figure 4.13: Read Operation Latency (Stability Test at 500 TPS)

Observation: Read latency remained remarkably low and stable across all tests. This showcases the system's efficiency in processing queries under load and confirms its readiness for real-time, data-intensive applications.

4.4.5 Discussion of Results

The performance evaluation of the proposed blockchain-based pharmaceutical supply chain solution demonstrates promising and encouraging results. Both read and write operations were carefully analyzed under incremental and constant transaction loads, revealing that the system is well-suited for practical deployment in real-world scenarios.

– **Strong Read Performance and High Scalability:** The system delivered excellent results for read operations. Throughput scaled linearly with increasing load, and latency remained low. Stability tests confirmed consistency, indicating readiness for read-heavy environments.

- **Good Write Operations Performance:** Despite higher complexity, write transactions were successful across all loads. While latency increased under pressure, throughput remained within practical limits.
- **Resilience and Stability Under Pressure:** Stability tests at 500 TPS showed that both read and write operations maintained consistent functionality, confirming system robustness.
- **Architecture Considerations and Impact of CouchDB:** The use of CouchDB significantly enhanced read responsiveness due to rich-query support. However, its internal complexity including document revision tracking and indexing — led to slightly reduced write throughput and increased latency under high load. This is a known tradeoff when choosing expressive query capabilities over raw write speed.

In conclusion, the system offers a reliable and scalable foundation for decentralized pharmaceutical supply chain applications. With minor architectural and resource optimizations, it can be further enhanced to support larger-scale deployments.

4.5 Conclusion

This chapter detailed the implementation of the proposed pharmaceutical supply chain system using Hyperledger Fabric. The development environment was configured on Windows using WSL2 and Docker, followed by the customization of Fabric components to suit the network's needs.

Two smart contracts were developed to separate concerns and improve modularity: **PcpCommunication** handled identity and metadata management, while **CommercialTransaction** managed inventory, orders, and exchanges. These contracts were implemented in Go, using JSON data structures designed for optimal compatibility with CouchDB as the state database.

To enable user interaction, a lightweight backend application was created using Node.js and Express.js. This application exposed RESTful APIs that connected users to the blockchain network. A web-based frontend interface, built with HTML, CSS, and JavaScript, allowed users to perform key operations such as product and batch registration, offer posting, order exchanges, and inventory visualization. These features enabled interaction without relying on command-line tools, improving accessibility for non-technical users.

Annotated screenshots were provided to demonstrate the system's primary workflows and user experience. Although the prototype had initial limitations in terms of authentication and session management, it fulfilled its core purpose of offering a secure and transparent platform for pharmaceutical transactions.

The implementation successfully achieved a modular smart contract structure, an automated deployment setup for a multi-organization Fabric topology, and an integrated user interface through RESTful services. These outcomes establish a solid technical foundation for the next chapter, which focuses on evaluating the system's performance under simulated operational conditions.

General Conclusion

This master's thesis successfully addressed the critical challenges of transparency, traceability, and trust within the pharmaceutical supply chain by designing, implementing, and evaluating a decentralized application using Hyperledger Fabric. The primary objective was to develop a secure and auditable platform for all key stakeholders—the Factory, Supplier, Pharmacy, and a governmental Regulator—to collaborate effectively and ensure the integrity of medications from production to dispensation.

Throughout this project, a comprehensive solution was realized. A permissioned Hyperledger Fabric network was architected with four distinct organizations, each with its own peers and Certificate Authority, ensuring authenticated and role-based participation. Two modular smart contracts, `PcpCommunication` and `CommercialTransactions`, were developed in JavaScript to govern the core business logic, including participant registration, product and batch creation, inventory management, inter-organizational exchanges, and product recalls. To facilitate user interaction, a full-stack client application was built, featuring a Node.js REST API that connects to the Fabric network and a web-based frontend that provides an intuitive interface for all supply chain operations.

The performance evaluation, conducted with Hyperledger Caliper, demonstrated the system's viability for real-world application. The results highlighted excellent read performance and scalability, with throughput scaling linearly and latency remaining consistently low, which is crucial for query-intensive regulatory and inventory-checking tasks. While write operations showed higher latency under heavy load—a known trade-off for the transactional complexity and rich-query capabilities afforded by CouchDB—the system remained stable and functional, confirming its robustness.

The main contribution of this work is the creation of a functional and technically sound blueprint for a blockchain-based pharmaceutical supply chain management system tailored to address challenges observed in contexts like Algeria. It provides a practical demonstration of how Hyperledger Fabric can be leveraged to enhance data integrity, enable real-time regulatory oversight, and drastically improve the efficiency of processes like product recalls.

Despite the successful implementation of the prototype, several limitations were identified that pave the way for future work. The client application's security can be significantly enhanced by replacing plain-text credential handling with industry-standard practices such as password hashing (e.g., bcrypt) and implementing session management using JWT-based tokens. For greater privacy, especially if patient data were to be incorporated, Hyperledger Fabric's Private Data Collections could be utilized to keep sensitive information confidential on a need-to-know basis. Further research could also focus on integrating IoT sensors for automated cold chain monitoring, expanding the network to include additional stakeholders, and conducting

larger-scale performance tests to prepare for a production-grade deployment.

In conclusion, this thesis validates the significant potential of permissioned blockchain technology to revolutionize the pharmaceutical industry. By establishing a single, immutable source of truth, the proposed system offers a robust solution to combat counterfeiting, streamline compliance, and ultimately build a more resilient and trustworthy supply chain that better protects public health.

References

[1] Katana MRP, "Pharma Supply Chain: Basics, Challenges, and Examples," *Katana MRP Blog*. [Online]. Available: katanamrp.com/blog/pharma-supply-chain-logistics/.

[2] Medpak, "Pharmaceutical Supply Chain Management: Key Steps & Challenges," *Medpak*. [Online]. Available: medpak.com/pharmaceutical-supply-chain-management/.

[3] A. O. Oyeniran *et al.*, "Optimizing Pharmaceutical Supply Chains for Public Health Resilience," *International Journal of Engineering Research and Development (IJERD)*, vol. 20, no. 11, 2023. [Online]. Available: ijerd.com/paper/vol20-issue11/2011429446.pdf.

[4] Scilife, "Compliance tips for supply chain management in pharma industry," *Scilife Blog*. [Online]. Available: scilife.io/blog/supply-chain-compliance-pharma.

[5] FreightAmigo, "Combating counterfeit pharmaceuticals with blockchain," *FreightAmigo Blog*. [Online]. Available: freightamigo.com/blog/combating-counterfeit-pharmaceuticals-with-blockchain/.

[6] TrueMed, "The Economic Impact of Counterfeit Healthcare Products," *TrueMed Blog*. [Online]. Available: truemedinc.com/blog/the-economic-impact-of-counterfeit-healthcare-products/.

[7] Jubilant HollisterStier, "Pharmaceutical Supply Chain Management Best Practices," *Jubilant HollisterStier Blog*. [Online]. Available: `https://www.jublhs.com/articles/pharmaceutical-supply-chain-management-best-practices/`.

[8] European Medicines Agency, "Good manufacturing practice," *European Medicines Agency*. [Online]. Available: https://www.ema.europa.eu/en/human-regulatory-overview/research-development/compliance-research-development/good-manufacturing-practice.

[9] Ubisense, "The Cold Chain Crisis: How Pharma Companies Can Prevent Spoilage and Loss," *Ubisense News & Insights*. [Online]. Available: `https://ubisense.com/cold-chain-crisis-pharma/`.

[10] QbD Group, "Post-Market Surveillance," *QbD Group Services*. [Online]. Available: `https://www.qbdgroup.com/en/services/regulatory-affairs/post-market-surveil`

[11] International Federation of Pharmaceutical Manufacturers & Associations (IFPMA), "Falsified medicines," *IFPMA Topics*. [Online]. Available: `https://www.ifpma.org/areas-of-work/improving-health-security/falsified-medicines/`.

[12] S. Ozawa *et al.*, "Prevalence and Estimated Economic Burden of Substandard and Falsified Medicines in Low- and Middle-Income Countries: A Systematic Review and Meta-analysis," *JAMA Netw. Open*, vol. 2, no. 1, p. e187662, Jan. 2019. [Online]. Available: `https://pmc.ncbi.nlm.nih.gov/articles/PMC6324280/`.

[13] OECD/EUIPO *et al.*, *Trends in trade in counterfeit and pirated goods*. 2019. [Online]. Available: https://doi.org/10.1787/g2g9f533-en

[14] A. Sharma, R. Singh, and G. N. Singh, "Counterfeit medicine: a major public health concern and effective remedies for combatting the crisis," *Authorea Preprints*, Mar. 2024. [Online]. Available: `https://www.researchgate.net/publication/389664146_Counterfeit_medicine_a_major_public_health_concern_and_effective_remedies_for_combatting_the_crisis`

[15] Interpol, "Fake medicines," *Interpol Crimes: Illicit Goods*. [Online]. Available: https://www.interpol.int/Crimes/Illicit-goods/Shop-safely/Fake-medicines.

[16] FasterCapital, "Immutable Transparent Nature," *FasterCapital*. [Online]. Available: fastercapital.com/keyword/immutable-transparent-nature.html.

[17] M. A. Aloui, N. Zouai, S. Bourekkache, and O. Kazar, "A Blockchain-Based Approach to Securing the Pharmaceutical Supply Chain," *FABAD Journal of Pharmaceutical Sciences*, 2025. [Online]. Available: dergi.fabad.org.tr/wp-content/uploads/2025/03/50-1-009-1531838.pdf.

[18] J. M. Deutsch, "How the Tylenol murders of 1982 changed the way we consume medication," *PBS NewsHour*, Sep. 29, 2014. [Online]. Available: https://www.pbs.org/newshour/health/tylenol-murders-1982.

[19] H. K. Lee *et al.*, "Effects of the July 2018 worldwide valsartan recall and shortage on global trends in antihypertensive medication use: a time-series analysis in 83 countries," *BMJ Open*, vol. 13, no. 1, Jan. 2023, Art. no. e068233. [Online]. Available: https://bmjopen.bmj.com/content/13/1/e068233.

[20] AmerisourceBergen, "Understanding Drug Supply Chain Security Act (DSCSA)," Sep. 2023. [Online]. Available: https://www.amerisourcebergen.com/-/media/assets/amerisourcebergen/dscsa/dscsa-overview-september-2023.pdf.

[21] Clarke Global Logistics, "Common Challenges in Pharmaceutical Cold Chain Logistics," *Clarke Global Logistics Blog*, Mar. 2025. [Online]. Available: https://www.clarkeglobal.com.au/pharmaceutical-cold-chain-logistics-challanges/.

[22] World Health Organization, "Medical Product Alert N°6/2022: Substandard (contaminated) paediatric medicines," WHO News & Events, Oct. 5, 2022. [Online]. Available: https://www.who.int/news/item/05-10-2022-medical-product-alert-n-6-paediatric-medicines.

[23] WHO Global Surveillance and Monitoring System for Substandard and Falsified Medical Products, "WHO Global Surveillance and Monitoring System for substandard and falsified medical products," Jul. 2023. [Online]. Available: https://cdn.who.int/media/docs/default-source/substandard-and-falsified/n5_2023_naturcold_en.pdf?sfvrsn=4ee41e9b_10

[24] E. Kelesidis, I. Kelesidis, P. I. Rafailidis, and M. E. Falagas, "Substandard/-Counterfeit Antimicrobial Drugs," *Clin. Microbiol. Rev.*, vol. 28, no. 2, pp. 443-464, Apr. 2015. [Online]. Available: https://pmc.ncbi.nlm.nih.gov/articles/PMC4402958/.

[25] M. Uddin, K. Salah, R. Jayaraman, S. Pesic, and S. Ellahham, "Blockchain for drug traceability: Architectures and open challenges," *Health Informatics Journal*, vol. 27, no. 2, p. 146045822110112, Apr. 2021, doi: 10.1177/14604582211011228.

[26] R. Raj, N. Rai, and S. Agarwal, "Anticounterfeiting in Pharmaceutical Supply Chain by establishing Proof of Ownership," *TENCON 2021 - 2021 IEEE Region 10 Conference (TENCON)*, pp. 1572–1577, Oct. 2019, doi: 10.1109/tencon.2019.8929271.

[27] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton, NJ: Princeton University Press, 2016.

[28] M. Swan, *Blockchain: Blueprint for a New Economy*. Sebastopol, CA: O'Reilly Media, Inc., 2015.

[29] A. M. Antonopoulos, *Mastering Bitcoin: Programming the Open Blockchain*, 2nd ed. Sebastopol, CA: O'Reilly Media, Inc., 2017.

[30] D. Tapscott and A. Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. New York, NY: Portfolio/Penguin, 2016.

[31] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292-2303, 2016. DOI: 10.1109/ACCESS.2016.2566339.

[32] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed. London, England: Pearson Education Limited, 2017.

[33] E. Androulaki et al., "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," in *Proceedings of the Thirteenth EuroSys Conference*, Porto, Portugal, Apr. 2018, pp. 1-15. DOI: 10.1145/3190508.3190538.

[34] L. Lamport, R. Shostak, and M. Pease, "The Byzantine Generals Problem," *ACM Transactions on Programming Languages and Systems (TOPLAS)*, vol. 4, no. 3, pp. 382-401, Jul. 1982. DOI: 10.1145/357172.357176. (While this is a foundational paper for BFT, modern blockchain consensus texts will cite it in context of specific BFT-based mechanisms used in blockchain). For a more direct blockchain consensus overview: X. Wang, F. X. Feng, Z. Gao, W. Wang and S. Chen, "A Survey on Consensus Mechanisms and Mining Strategy for Blockchain," *IEEE Access*, vol. 7, pp. 22320-22337, 2019. DOI: 10.1109/ACCESS.2019.2896106.

[35] N. Szabo, "Smart Contracts: Building Blocks for Digital Markets," 1996. [Online]. Available: `http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html`

[36] P. Thummavet, "Demystifying hyperledger fabric (1/3): Fabric architecture," *Medium*, Jun. 25, 2022. [Online]. Available: https://medium.com/coinmonks/demystifying-hyperledger-fabric-1-3-fabric-architecture-a2fdb587f6cb

[37]- P. Xiao, *Practical JaVa® programming for IoT, AI, and blockchain*. 2018. doi: 10.1002/9781119560050.

[38] S. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics and Informatics*, vol. 36, pp. 55-81, Mar. 2019. DOI: 10.1016/j.tele.2018.11.006.

[39] S. Underwood, "Blockchain beyond bitcoin," Communications of the ACM, vol. 59, no. 11, pp. 15-17, Nov. 2016. DOI: 10.1145/2994581.

[40] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," Applied Innovation Review, vol. 2, pp. 6-19, Jun. 2016. [Online]. Available: https://scet.berkeley.edu/wp-content/uploads/AIR-2016-Blockchain.pdf

[41] G. Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger," Ethereum Project Yellow Paper, 2014. [Online]. Available: https://ethereum.github.io/yellowpape

[42] F. Glaser, "Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain enabled Systems and Interorganizational Information Systems," in Proceedings of the 50th Hawaii International Conference on System Sciences (HICSS), Waikoloa Village, HI, USA, Jan. 2017, pp. 1543-1552. DOI: 10.24251/HICSS.2017.186.

[43] S. Saberi et al., "Applications of Blockchain Technology in Supply Chain Management," International Journal of Production Research , vol. 62, no. 12, pp. 3456–3473, 2024.

[44] I. Lee and K. Shin, "Blockchain technology in supply chain management: Innovations and applications," *Business Horizons* , vol. 67, no. 3, pp. 231–242, 2024.

[45] D. Tapscott, A. Tapscott, and Hyperledger White Paper Working Group, "An introduction to Hyperledger," report, 2018. [Online]. Available: https://8112310.fs1.hubspotuserc
na1.net/hubfs/8112310/Hyperledger/Offers/HL_Whitepaper_IntroductiontoHyperledger.pdf

[46] "Introduction — Hyperledger Fabric Docs main documentation." `https://hyperledger-fabric.readthedocs.io/en/release-2.5/whatis.html`

[47] Hyperledger, "Hyperledger Architecture, Volume 1," Hyperledger Foundation, 2017. [Online]. Available: https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledg

[48] Hyperledger Fabric Documentation. The Linux Foundation. Accessed May 20, 2025. [Online]. Available: https://hyperledger-fabric.readthedocs.io/

[49] M. S. Al-Rakhami and M. S. Al-Mashari, "A Review of Hyperledger Fabric: A Permissioned Blockchain for Enterprise Applications," *Sustainability*, vol. 13, no. 10, p. 5775, May 2021. DOI: 10.3390/su13105775.

[50] D. Ongaro and J. Ousterhout, "In Search of an Understandable Consensus Algorithm," in *2014 USENIX Annual Technical Conference (USENIX ATC 14)*, Philadelphia, PA, Jun. 2014, pp. 305-319. [Online]. Available: https://www.usenix.org/conferenc
sessions/presentation/ongaro

[51] K. K. S. Kumar, A. K. G. J, S. K. Panda, and J. J. P. C. Rodrigues, "Blockchain Technology for Pharmaceutical Supply Chain Management: A Comprehensive Review," *IEEE Transactions on Engineering Management*, pp. 1-17, Early Access, 2023. DOI: 10.1109/TEM.2023.3265259.

[52] T. T. T. Nguyen, T. H. T. Le, and H. M. La, "A Blockchain-based Traceability System for Pharmaceutical Supply Chain," in *2019 IEEE International Conference on Systems, Man and Cybernetics (SMC)*, Bari, Italy, Oct. 2019, pp. 2604-2609. DOI: 10.1109/SMC.2019.8914499.

[53] P. Thummavet, "Demystifying hyperledger fabric (3/3): network traffic handling, service discovery, and operations service," *Medium*, Dec. 10, 2021. [Online]. Available: https://medium.com/coinmonks/demystifying-hyperledger-fabric-3-3-network-traffic-handling-service-discovery-and-operations-f9a2046b4067

[54] Li, Dun & Han, Dezhi & Xia, Benhui & Weng, Tien-Hsiung & Castiglione, Arcangelo & Li, Kuan-Ching. (2022). Fabric-GC: A Blockchain-based Gantt Chart System for Cross-organizational Project Management. 10.48550/arXiv.2207.09249.

[55] Chacko, Jeeta Ann & Mayer, Ruben & Jacobsen, Hans-arno. (2021). Why Do My Blockchain Transactions Fail? A Study of Hyperledger Fabric (Extended version)*. 10.48550/arXiv.2103.04681.

[56] "Medium," *Medium*. https://medium.com/@aldredbenedict/using-3rd-party-root-cas-in-hyperledger-fabric-3cafa91d126023151.

[57] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[58] H. H. M. Hussien, S. H. Abbas, R. A. Bakar, M. A. Salahuddin, and N. Suryana, “Blockchain technology in the healthcare industry: Trends and opportunities,” *Journal of Industrial Information Integration*, vol. 17, pp. 100125, 2020.

[59] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An overview of blockchain technology: Architecture, consensus, and future trends,” in *Proc. IEEE Int. Congr. Big Data*, 2017, pp. 557–564.

[60] “ZKFABLedger: Enabling Privacy preserving and Regulatory Compliance in Hyperledger Fabric,” *IEEE Journals & Magazine | IEEE Xplore*, Apr. 01, 2025. https://ieeexplore.ieee.org/document/10839283

[61] Hyperledger Foundation, “Hyperledger Caliper Documentation,” *Hyperledger Caliper*, 2023. https://hyperledger.github.io/caliper/

[62] IBM Developer, “Benchmarking Hyperledger Fabric using Caliper,” *IBM Developer*, 2023. https://developer.ibm.com/articles/benchmarking-hyperledger-fabric-using-caliper/

[63] Hyperledger Foundation, “Hyperledger Caliper User Guide,” *Hyperledger Caliper*, 2023. https://hyperledger.github.io/caliper/v0.4/

[64] T. H. Lee and C. K. Tham, “Performance Analysis of Blockchain Systems: A Survey,” *IEEE Access*, vol. 7, pp. 14167–14188, 2019. https://doi.org/10.1109/ACCESS.2019.289

[65] Oracle, “What is Docker?,” *Oracle Cloud Infrastructure*, May 2024. https://www.oracle.com/africa-fr/cloud/cloud-native/container-registry/what-is-docker/

[66] M. Crosby, Nachiappan, P. Pattanayak, S. Verma, and V. Kalyanaraman, ”Blockchain technology: Beyond Bitcoin,” Applied Innovation, vol. 2, pp. 6–10, Jun. 2016. [67] A. M. Antonopoulos, Mastering Bitcoin: Programming the Open Blockchain, 2nd ed. O’Reilly Media, 2017. [68] Hyperledger. ”Hyperledger Fabric Documentation: Security Model.” Accessed Jun. 24, 2025. [Online]. Available: `https://hyperledger-fabric.readthedocs.io/en/release-2.2/security_model.html` [69] S. H. K. Narayanan, S. P. R. A. M, and E. G. Julie, ”A comprehensive review on blockchain technology,” in 2021 5th International Conference on Computing Methodologies and Communication (ICCMC), 2021, pp. 1163-1169. [70] S. Nakamoto, ”Bitcoin: A peer-to-peer electronic cash system,” 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf [71] M. S. Ferdous, M. J. M. Chowdhury, M. A. Hoque, and P. A. Colman, ”Blockchain in healthcare: A systematic literature review,” in Advances in Computers, vol. 117, Elsevier, 2020, pp. 1–62. [72] R. C. Merkle, ”A digital signature based on a conventional encryption function,” in CRYPTO ’87: Advances in Cryptology, 1988, pp. 369–378. [73] X. Wang, Z. Feng, and Z. Zhang, ”A survey on blockchain security,” Journal of Communications and Information Networks, vol. 3, no. 1, pp. 1-21, 2018. [74] National Institute of Standards and Technology, ”Secure Hash Standard (SHS),” FIPS PUB 180-4, Aug. 2015. [75] W. Stallings, Cryptography and Network Security: Principles and Practice, 8th ed. Pearson, 2020. [76] G. G. D. L. Torre, S. G. Taliani, and E. G. P. M. Fadda, ”Blockchain-based traceability in the pharma supply chain,” in 2020 IEEE International Conference on Technology and Entrepreneurship (ICTE), 2020, pp. 1-6. [77] D. Johnson, A. Menezes, and S. Vanstone, ”The elliptic curve digital signature algorithm (ECDSA),” International Journal of Information Security, vol. 1, no. 1, pp. 36–63, Aug. 2001. [78] Hyperledger. ”Hyperledger Fabric Documentation: Endorsement policies.” Accessed Jun. 24, 2025. [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.2/endorsement-policies.html [79] Hyperledger. ”Hyperledger Fabric Documenta-

tion: Private data." Accessed Jun. 24, 2025. [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.2/private-data-arch.html [80] E. Androulaki et al., "Hyperledger Fabric: A distributed operating system for permissioned blockchains," in Proceedings of the Thirteenth EuroSys Conference, 2018, pp. 1–15. [81] T. Kanstrén, "Merkle Trees: Concepts and Use Cases - CoinMonks - Medium," Medium, Mar. 30, 2022. [Online]. Available: https://medium.com/coinmonks/merkle-trees-concepts-and-use-cases-5da873702318

[82] Chronicled, "The MediLedger Project," 2020. [Online]. Available: https://www.mediledger.co
[83] U.S. FDA and IBM, "Blockchain for Drug Traceability Pilot," 2017. [Online]. Available: https://www.fda.gov [84] PharmaLedger Consortium, "PharmaLedger Project: Final Deliverable," 2023. [Online]. Available: https://www.pharmaledger.eu
[85] K. Werbach and N. Cornell, "Contracts Ex Machina," Duke Law Journal, vol. 67, no. 2, pp. 313–382, 2017. [86] H. Wang, Z. Xu, and S. Li, "Design of a Blockchain-Based Drug Traceability System," International Journal of Information Management, vol. 52, 2020. [87] M. Angraal, H. Patel, and H. Rajkomar, "Data Sovereignty in the Cloud Era," Journal of Medical Internet Research, vol. 23, no. 6, 2021. [88] A. Kumar, P. Tripathi, and M. Dutta, "Blockchain-Based Drug Traceability Framework," Journal of Supply Chain Management, vol. 14, no. 2, pp. 101–114, 2021. [89] C. Esposito et al., "Blockchain for Cold Chain Logistics in Vaccine Delivery," IEEE Access, vol. 8, pp. 107719–107736, 2020. [90] R. Hussien, S. Yasin, and M. Alaboudi, "Medical Record Management using Blockchain," Healthcare Informatics Research, vol. 25, no. 4, pp. 263–270, 2019.

Appendix A

Installing Prerequisites (Docker, Go, Git, etc.)

1. Open PowerShell in Administrator mode.
2. Enable Windows Subsystem for Linux (WSL):

```
dism.exe /online /enable-feature /featurename:Microsoft-Windows-
    ↪ Subsystem-Linux /all /norestart
```

3. Enable Virtual Machine Platform:

```
dism.exe /online /enable-feature /featurename:
    ↪ VirtualMachinePlatform /all /norestart
```

4. Set WSL 2 as the default version:

```
wsl --set-default-version 2
```

5. Install Ubuntu 20.04 LTS from the Microsoft Store.
6. Install Windows Terminal (recommended for managing multiple shells).
7. (Optional) Install the WSL2 Linux kernel update:
   - `https://wslstorestorage.blob.core.windows.net/wslblob/wsl_update_x64.msi`
8. Launch Ubuntu once to initialize and integrate with Windows Terminal.
9. Update and upgrade Ubuntu packages:

```
sudo apt update && sudo apt upgrade
```

10. Download and install Docker Desktop for Windows:
    - `https://desktop.docker.com/win/stable/amd64/Docker%20Desktop%20Installer.exe`
11. Enable Docker for Ubuntu in Docker Desktop:
    - Go to `Settings > Resources > WSL Integration`
    - Enable `Ubuntu-20.04`
    - Click `Apply & Restart`
12. Verify Docker installation:

```
docker --version
docker-compose --version
```

13. Install `curl` (if not already installed):

```
sudo apt-get install curl
curl --version
```

14. Check and install Go (Golang):

```
go version
```

If not installed:

```
sudo wget https://golang.org/dl/go1.16.3.linux-amd64.tar.gz
tar xvf go1.16.3.linux-amd64.tar.gz
sudo mv go /usr/local
export PATH=$PATH:/usr/local/go/bin
export GOPATH=$HOME/go
export PATH=$PATH:$GOPATH/bin
```

15. Verify Go installation:

```
go version
```

16. Check and install Git:

```
git --version
sudo apt install git
```

1.2.2 Downloading Fabric Samples

1. Create a working directory:

```
mkdir -p $HOME/go/src/github.com/
cd $HOME/go/src/github.com/
```

2. Download Fabric samples and Docker images:

```
curl -sSL https://bit.ly/2ysbOFE | bash -s
```

Note: This installs Fabric version 2.3.2.

1.2.3 Using the Test Network as a Starting Point

1. Navigate to the test network directory:

```
cd ~/go/src/github.com/fabric-samples/test-network
```

2. Clean up previous network (if any):

```
./network.sh down
```

3. Start the test network:

```
./network.sh up
```

4. Check running Docker containers:

```
docker ps -a
```

1.2.4 Analyzing Network Files and Key Scripts

- `network.sh`: Main script to bring the test network up or down, create channels, and deploy chaincode.
  - `./network.sh up` – starts the network
  - `./network.sh down` – cleans the network
  - `./network.sh createChannel` – creates the default channel
- `scripts/`: Contains helper scripts used for certificate generation, peer/channel setup, and other automation tasks.
- `organizations/`: Contains MSP, TLS, and crypto configuration for each organization.