SUPPLY CHAIN OPTIMIZATION IN CEMENT INDUSTRY USING BLOCKCHAIN TECHNOLOGY

By

Rabeya Hamood

MSIS-20

Supervisor

Dr Imran Makhdoom

Department of Information Security

A thesis submitted in partial fulfillment of the requirements for the degree of Masters of Science in Information Security (MS IS) -20

In

Military College of Signals (MCS),

National University of Sciences and Technology (NUST),Islamabad, Pakistan.

THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS Thesis written by **Rabeya Hamood**, Registration No. **00000363294**, of **Military College of Signals** has been vetted by undersigned, found complete in all respects as per NUST Statutes/Regulations/MS Policy, is free of plagiarism, errors, and mistakes and is accepted as partial fulfillment for award of MS degree. It is further certified that necessary amendments as pointed out by GEC members and local evaluators of the scholar have also been incorporated in the said thesis.

Signature: _____

Name of Supervisor Dr Imran Makhdoom

Date: 22/8/23

Signature (HOD): _____

Date: 23/8/23

Signature (Dean/Principal) _____

Date: 24/8/23

Brig
Dean, MCS (NUS
(Asif Masood, Phd)

Declaration

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

_____

Dated:__Jul 2023 Author

(**Rabeya Hamood**)

Dedication

This thesis is dedicated to my parents and family, whose unwavering love and support have been the driving force behind my academic journey. Thank you for instilling in me the values of hard work, perseverance, and dedication. Your guidance and encouragement have been invaluable, and I am forever grateful for all that you have done for me.This thesis is a testament to all that I have learned from you and a dedication to your unwavering support.

Acknowledgments

I would like to express my gratitude to all those people who have helped me in completing my thesis report. Their support, guidance and help have been invaluable throughout this journey.

First I would like to thank my supervisor and co - supervisor for their guidance and expertise who has helped me whenever I needed help and encouragement. Their feedback and patience has been instrumental in collecting and gathering of data for this project. I am grateful for his dedication and commitment to my academic growth.

I would like to express my gratitude to the esteemed faculty members of my university for creating an intellectually stimulating academic environment. Their expertise, teachings, thought-provoking lectures, and engaging discussions have significantly expanded my knowledge and profoundly influenced my perspective in this field.

ABSTRACT

The research demonstrates how improved scalability and provenance of cement products are facilitated by the combination of Corda Blockchain and IoT sensors. The Corda ledger securely records each step, from the acquisition of raw materials through the delivery of the finished product, building an audit trail that cannot be changed. This openness promotes confidence among those involved in the supply chain and makes it easier to comply with legal requirements. The paper discusses the dangers and obstacles related to implementing Corda Blockchain and IoT sensors in the cement sector while highlighting the advantages. Scalability and data integrity are important factors to take into account. To guarantee successful deployment and wide adoption, mitigation tactics are put out.

Contents

List of Figures 9
List of Tables 10
1 Introduction 11
1.1. Background 11
1.1.1. Inadequacies of Present Technologies and the Justification for Blockchain 12
1.1.2. Architecture of Blockchain 13
1.2. Motivation 13
1.3. Problem Statement 14
1.4. Research Objective 15
1.5. Thesis Outline 16
2 Literature Review 17
2.1. Challenges in Supply Chain 17
2.1.1. Scalability 18
2.1.2. Interoperability 19
2.2. Utilizing blockchain Technology for the functions of supply chain Management 20
2.2.1. Benefits of blockchain in supply chain 23
2.2.2. Utilizing blockchain technology for critical Supply chain function 26
2.2.2.1. Chain of Custody 27
2.2.2.2. Supply chain stability 28
2.2.2.3. Supply chain redesign 30
2.2.2.3. Enchancing security 33
2.3. Applications of blochchain technology across various industrial sectors and in societal context 33
2.3.1. Financial Sector 34
2.3.2. Credit accounting and management systems with Blockchain technology 34
2.3.3. Technology Industry. 34
2.3.4. Manufacturing Industry 34
2.3.5. Logistics Industry 35
2.3.6. Power Sector 36
3 Blockchain Technologies 37
3.1. Different types of Blockchain technologies 37
3.2. Comparison of Blockchain Technologies 39
3.3. Benefits and Drawbacks of different Blockchain technologies 42
3.4. Consensus Algorithm 43
3.5. Smart Contract 43

4 Corda – An overview 44
4.1. Introduction 44
4.2. Key Features of Corda 47
5 Implementation & Results 48
5.1. Introduction 48
5.2. Environment Setup 50
5.3. Work Flow 53
6 Conclusion & Future Work 54
References 55

List of Figures

Figure 1.1. Basic Architecture of Blockchain 11
Figure 5.1. Network architecture Diagram 48
Figure 5.2. Project Structure 49
Figure 5.3 Nodes in Terminal 49
Figure 5.4 FrontEnd 50
Figure 5.5 FrontEnd Transaction Error 50
Figure 5.6 BackEnd Transaction Error 51
Figure 5.7. Transaction in Backend 53

List of Tables

Table 1 Advantages of Blockchain in Supply Chain 37
Table 2 In Different Sectors, Application of Blockchain 39
Table 3 Comparison of Different Blockchain Technologies..... 39
Table 4 Advantages & Disadvantages of Blockchain Technologies..... 42

Chapter 1

INTRODUCTION

1.1. Background

The cement business is the global construction industry's backbone, providing the necessary binding material for buildings, infrastructure, and numerous development projects. Despite its vital function, the cement supply chain has long faced several obstacles that have hampered its overall efficiency and effectiveness.

The cement supply chain has always been distinguished by a lack of transparency and traceability. It has frequently been difficult to pinpoint the origin of possible problems because to the fragmented information flow across stakeholders, including cement makers, suppliers, logistics companies, and end users. It has been difficult to streamline operations, cut costs, and guarantee consistent product quality because of this lack of visibility. The cement industry also encounters considerable challenges with regard to quality control during storage and shipping. Temperature, humidity, and weight are a few environmental factors that can seriously affect the integrity of cement. Without real-time monitoring capabilities, stakeholders have found it difficult to identify departures from ideal circumstances quickly, which could lead to quality degradation and unhappy customers.

Technology improvements in recent years have presented interesting answers to these supply chain inefficiencies. Two significant developments—Blockchain and Internet of Things (IoT) technology—have become game-changing technologies for streamlining the cement supply chain.

By recording each step of the supply chain process, Blockchain can improve transparency, traceability and scalability in the context of the cement business. Every movement and transfer, from the sourcing of raw materials to the delivery of the finished product, is securely documented, giving stakeholders access to a precise and impenetrable audit trail. Furthermore, the "smart contracts" capability of blockchain allows for the automation of contractual agreements, speeding procedures and eliminating the need for middlemen.

IoT-based sensors: The Internet of Things (IoT) technology combines internet connectivity with sensors and devices to enable data collection and sharing. IoT-based sensors can be integrated into cement bags, shipping containers, cars, and manufacturing machinery in the cement supply chain.

IoT sensors offer real-time information on environmental variables during transportation and storage, including temperature, humidity, and vibration. Stakeholders are able to proactively resolve possible problems that can compromise cement quality because to this ongoing monitoring. Early anomaly detection allows supply chain actors to quickly implement corrective measures, ensuring that the cement arrives at its destination in prime condition.

The supply chain for the cement industry has a great deal of potential to be transformed by the combination of blockchain technology and IoT-based sensors. Stakeholders may make data-driven decisions, optimize processes, and guarantee consistent product quality by implementing transparency, traceability, and real-time monitoring. Despite implementation difficulties, adopting these technologies presents the cement industry with a rare chance to increase productivity, cut costs, and create a supply chain ecosystem that is more robust and sustainable.

1.1.1. Inadequacies of Present Technologies and the Justification for Adoption of Blockchain

Although the current supply chain technologies have been useful over the years, they have some drawbacks and restrictions that may reduce the supply chain's effectiveness and transparency. The following are some of the main issues with current technologies that make switching to blockchain a viable fix:

1- **Lack of Transparency**: There is a lack of transparency in traditional supply chain systems because of the numerous middlemen and data silos that are frequently used. Due to this opacity, stakeholders find it challenging to have a complete picture of the full supply chain process, which causes delays and inefficiencies.

2- **Limited Traceability**: Due to the fragmented nature of data, it can be difficult to track the origin and movement of commodities across the supply chain. This restriction may make it challenging to pinpoint the origin of fraud, compliance violations, or quality problems.

3- **Data inconsistencies**: When multiple parties keep their own records, there may be differences in the data that might result in conflicting information and mistakes. In supply chain operations, these inconsistencies can cause delays and disagreements.

4- **Fraud Vulnerability**: Data tampering and fraud are possible with centralized systems. False items can enter the system through unauthorized changes to records and a lack of transparency in the supply

chain, resulting in huge financial losses and harming a brand's reputation.

5- **Ineffective Contract Management**: Manual procedures are used in traditional contract management, which causes delays and extra administrative work. The supply chain's overall speed and agility may be hampered by this inefficiency.
6- **Long Settlement Processes**: The settlement of financial transactions can be delayed by the multiple intermediaries and long clearance times associated with traditional payment systems. These delays may affect cash flow and impair the liquidity of the supply chain.
7- **Procedures for Complying with rules and Standards**: Complying with rules and standards can be a difficult and time-consuming procedure, particularly when many parties have varied reporting needs.

Blockchain technology presents an appealing remedy to fix these issues and enhance the supply chain in a number of ways:

1- **Enhanced Transparency**: All authorized parties may see transactions in real time thanks to the decentralized and unchangeable record of the blockchain. This openness increases stakeholder trust and lessens information asymmetry.
2- **Improved Traceability**: The immutable and accurate history of each transaction and movement within the supply chain is made possible by the tamper-resistant record-keeping of the blockchain. Effective traceability and origin of items are made possible by this feature.
3- **Consensus-Based Data**: All participants in a blockchain network must concur on data additions in order to ensure consensus and reduce data discrepancies.
4- **Enhanced Security**: The supply chain data's integrity is ensured by the cryptographic methods used in blockchain technology, which make data fraud and manipulation extremely difficult.
5- **Automation of Smart Contracts**: Based on predetermined criteria, smart contracts on the blockchain can automate the execution and enforcement of contracts. This simplifies commercial agreements and does away with the necessity for middlemen.

1.1.2. Architecture of blockchain

The architecture of blockchain can be understood by the figure 1.1 which explains the basic flow of blockchain:

- The data source module is used in "distributed and shared databases" to help build the blockchain. It guarantees that the data that blockchain users retrieve is accurate and undamaged.

The main characteristics of blockchain are data immutability, tamper-proofed storage with any form, and shareable data ledger through the "Application Programming Interface (API)".

• The "journey of a transaction in blockchain" is monitored, managed, enabled, and supported by the transaction module. It facilitates inclusion to the blockchain and helps validate transactions. Data transport occurs through smart contracts transaction gates.

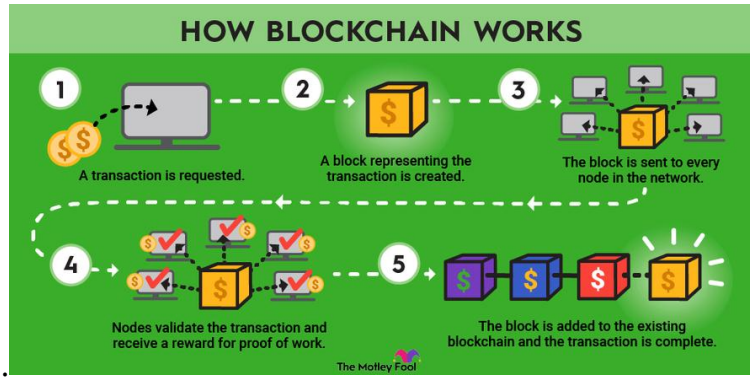


Figure 1.1 Basic architecture of Blockchain

- The blockchain is used to create the information flow across the SC as well as shared visibility of transactions. A block of transactions is bundled together and sent to every node. Be aware that after a transaction has been sent to the blockchain, it is nearly hard to reverse or cancel it.
- Module for creating blocks: Blocks can be seen as the miners' own data structures. They contain data and transaction details that are copied to all network nodes. By giving the hash values and connections of the preceding block, the block creation module facilitates the insertion of additional blocks to an already-existing SC. "Chronological blocks" are used to hold transaction sequences, and they make it simple to identify and trace blocks that contain incorrect transactions.

Almost no data on the blockchain can be changed because of the architecture.

1.2. Motivation

Research is being carried out to utilize the advantages of blockchain in Supply chain. However, the scope and integration face many challenges.

1- **Inefficiencies in the Supply Chain**: The cement industry's supply chain is intricate and involves a number of parties, including manufacturers, manufacturers' suppliers, logistics service providers, and construction firms. Real-time visibility may be lacking in traditional supply chain management

systems, which can result in delays, a surplus of inventory, and higher expenses.

2- **Scalability**: The cement industry operates on a large scale, comprising numerous suppliers, extensive production facilities, and extensive transportation networks. The volume of data and transactions produced by such a large and complicated ecosystem may be too much for traditional supply chain systems to handle. Scalability becomes a crucial issue as the sector develops and cement demand rises on a global scale.

3- **Lack of Transparency and Traceability**: Due to a lack of transparency and traceability, it is challenging to pinpoint the cause of issues or disruptions in the supply chain. This may cause delays, inefficiencies, and difficulty fixing quality problems.

1.3. Problem Statement

The cement industry faces numerous challenges in its supply chain, including inadequate tracking and monitoring of products. These issues result in delays and lower customer satisfaction. One potential solution to these problems is the use of blockchain technology in conjunction with IoT devices to create a secure, transparent, and automated supply chain system and preserve the data integrity. However, there is a need of research on the implementation of blockchain and IoT in the cement industry supply chain. Therefore, the aim of this study is to investigate the potential benefits and challenges of implementing a blockchain-based supply chain system with IoT devices in the cement industry, and to propose a framework for its successful implementation.

1.4. Research Objective

- To develop a mechanism that demonstrates the potential of blockchain and IoT integration in the cement industry supply chain and overcomes the issue of scalability.
- To propose a methodology for verifying the integrity of cement sacks, including detecting any tampering, theft, or removal of cement from the sack.
- To investigate the integration of IoT devices with blockchain technology to create a more secure and efficient supply chain management system.

1.5. Thesis Outline

- **Chapter 1**: A brief introduction is given. The problem statement is highlighted followed by the

motivation behind this research. Also research objectives are listed too.

- **Chapter 2**: It gives a detailed Literature review of supply chain, its challenges and Drawbacks also its advantages.
- **Chapter 3**: A detailed description of Blockchain, Its comparison between its technologies, advantages and disadvantages, consensus Algorithms etc.
- **Chapter 4**: Moving on to the Blockchain technology which is used for the project and its features as well as a detailed workflow how corda works.
- **Chapter 5**: Proposing a prototype for supply chain of cement.
- **Chapter 6**: It gives the conclusion and some future work.

Chapter 2

LITERATURE REVIEW

2.1. Challenges in Supply Chain

Although the technology itself is ground-breaking, there are numerous restrictions and difficulties with its use. When it comes to retrieving and committing records, blockchain is much slower. Additionally, it necessitates a considerable increase in computational resources, and the scalability of those resources is a major worry. Additionally, any systems engaging with the Blockchain must be interoperable. A comprehensive study of hurdles to blockchain adoption in supply chains are briefly but thoroughly discussed.

2.1.1. Scalability

Scalability is the capacity of a system to respond and function even after the size of the input is increased to meet user demand. Scalability approaches are divided into on-chain, off-chain, side-chain, child-chain, and inter-chain categories to address scalability-related difficulties. The technologies for scalability are categorized according to the quantity of transactions, block interval time, data storage, and data transport. We divide scalability solutions into four categories: (i) on-chain scalability; (ii) off-chain scalability; (iii) scalability based on consensus mechanisms; (iv) scalability based on distributed acyclic networks.

- On-chain scalability

In order to implement on-chain solutions, Blockchain must undergo structural or fundamental change, which necessitates a change to the protocol's governing principles. In situations where there is a split in the community due to the emergence of factions that approve or reject the proposed update, this is referred to as a hard fork or controversial hard fork.

- Off-chain scalability

Off-chain approaches are referred to as second layer scalability solutions since they use additional protocols that are constructed on top of the primary Blockchain. With this method, transactions are handled privately between the engaging parties and off-loaded off the main Blockchain. It offers the benefits of decreased MainNet congestion, higher throughput, lower transaction costs, and space

savings.

- Consensus mechanism based Scalability

Scalability problems are addressed by optimizing the operation of the consensus algorithm in Consensus Mechanism based Scalability. Major players in this space include VeChain, which uses Proof of Authority, ARK.io, LISK, bitshares, EOS, and steemit, which use Delegated Proof of Stake, Ripple and Stellar, which use Federated Byzantine Agreement, NEO, which uses Delegated Byzantine Fault Tolerance, Libra, zilliqa, and Hyperledger.

- Distributed Acyclic Graph-Based Scalability

Blockchain differs from Distributed Acyclic Graph-Based Scalability. It is yet another well-known application of distributed ledger technology. Transactions don't follow any particular process; they work independently and asynchronously. The system keeps track of transaction records using a topological ordering data structure. In contrast to Blockchain, DAG distributed ledger technology does not have the same scalability problems. IOTA, Byteball, NANO, and Hashgraph are a few examples of solutions in this group.

2.1.2 Interoperability

Although blockchain technology is being adopted more widely, this is being hampered by the isolation of Blockchains in their individual "silos" caused by a lack of interoperability standards. A hyper-connected world may be possible if collaboration and cross-chain interaction problems among public, private, and consortium Blockchains are solved. The functionality of consensus models, transactions, and contracts all require common capabilities and feature sets that blockchain systems must embrace and share. Three categories can be made out of the proposed solutions for Blockchain interoperability: (i) Notary Schemes, (ii) SideChain relays, and (iii) Hash Locking

- Notary Schemes

A trusted third party known as a notary acts as an intermediary in notary schemes to witness and confirm the state of the interconnected Blockchains and facilitate operations. In this category, Liquid utilizing Federated Pegged Sidechain is a major solution.

- SideChain/relays

Many interoperability solutions involve relay schemes. Among them are ChainLink, Cosmos, and Polkadot.

- Hash Locking

Although it has several functional limitations, hash locking is the most feasible method for blockchain interoperability. Some of its primary solutions include ARK Core Series and Interledger Protocol (ILP).

2.2. Utilizing blockchain technology for the functions of supply chain management.

Every industry's foundation is made up mostly of the huge SCM sector. Traditional SC systems, on the other hand, are not flexible and transparent enough to meet the escalating needs and demands of the future, which results in extremely high overhead costs in terms of fraud management, administration, expenses, and mistake handling.

2.2.1. Benefits of using blockchain in supply chains

Blockchain is suggested as a solution to manage records in the Industry 4.0 era through a distributed consensus process. Its characteristics of cost reduction, disintermediation, transparency, authenticity, trust, and security, as well as its effective operations and decreased waste, have the potential to alter SCM. Additionally, blockchain-supported transactions are all more transparent, efficient, and safe. Thus, it is generally accepted that blockchain's distributed nature aids in reducing risks in the SC related to piracy, hacking, vulnerability, expensive adherence to governmental regulations, and contractual disputes. With the use of smart contracts, blockchain also makes it possible for real-time order settlement and industrial task automation. Blockchain also guarantees that ripple effects in SC are minimized, lessening the disruption brought on by shifting paradigms. Table 1 shows some of the benefits of blockchain implementation in Supply Chain.

Benefits of Blockchain in Supply Chains	Details
Enhanced Data Management	Enhances the security and integrity of data saved;
	Makes it easier to calibrate data dispersed across several supply chains.
	- Enables real-time capturing of information throughout the supply chain.
Improved Transparency	- Enables monitoring the progress of products via the supply chain process at each stage.
	- Increases visibility and insights by automating data analysis tasks.
	- Offers end-to-end transparency depending on access hierarchy and permission levels.
Faster Response Time	- Creates a dynamic, real-time supply chain that maximizes resource use.
Efficient Smart Contract Management	- Allows for personalized and unique contracts for different supply chain roles, ensuring efficient coordination.
	- Supports the design of processes for effective business operations.
	- Improves visibility and does away with the necessity for middlemen during contract execution.
Improved Operational Efficiency	- Accelerates supply chain procedures from beginning to end, cutting down on delays.
	- Recognizes problems early on and fixes them, increasing process resilience.
Disintermediation	Reduces reliance on intermediaries by enabling uninterrupted and direct transactions.
	- Increases confidence among all parties and speeds up transaction times.
Data Immutability	- Uses a consensus approach to ensure tamper-proof records for all data updates.
	- Supports intellectual property protection and streamlines registration procedures within the supply chain environment.
Intellectual Property Management	- Strengthens the security and dependability of all supply chain transactions.

Table 1 Advantages of Blockchain in Supply Chain

2.2.2. Utilizing blockchain technology for critical supply chain functions

With the use of blockchain technology, several of the key processes including Supply chain reengineering, security, resilience, provenance, process management, and product management may be altered.

2.2.2.1. Chain of custody provenance

The study of the traceability ontologies and limitations on the Ethereum blockchain allows for the granular provenance of physical items that are manufactured and delivered through intricate, interorganizational, or globally spanning SCs. By providing certifiability, traceability, verifiability, and tractability of product information, as well as assurances of origin and authenticity and integrity along the whole SC stretching across borders, SC provenance is supplied. It has been the main use of blockchain in the supply chains for diamonds. Blockchain and IoT technologies have been used to implement the "Hyperledger Sawtooth" project in particular. Blockchain-based SC provenance architecture that saves all necessary data, guarantees role-based access to the data, and encrypts the data securely.

2.2.2.2. Supply-chain Stability

By minimizing the effects of interruptions, using a proactive and preventative approach to risk management, and offering multilayer protection for SC networks, blockchain technology helps SCs be more resilient. Blockchain's hierarchical layout makes it easier to identify the organizational and network risks connected to any SC.

2.2.2.3. Supply chain redesign

Blockchains improve the traceability, privacy, and visibility of SC, allow for process automation, do away with middlemen, and enable real-time tracking—all of which are essential components of SC reengineering. An SC that has been correctly reengineered can synchronize tracking data across all business domains. Additionally, using smart contracts can help cut down on the time and expense needed, supporting SC reengineering.

2.2.2.4. Enhancing security

In the services it offers, blockchain supports authentication, confidentiality, privacy and access control, data and resource provenance, and integrity guarantee. Additionally, it enables the development of a framework for risk control analytics to investigate the relationship between business, information, and

engineering as well as to gather analytics-related viewpoints on digitalization in SC. Due to its capacity to scale up to meet demands, blockchain can offer effective risk management even in large production enterprises. Due to its improved cybersecurity and performance, blockchain is far more secure than conventional IoT systems or conventional security services. When blockchain technology is incorporated, the following mechanisms are improved, perhaps creating a more secure SC:

- **IoT security**: A centralized network of digital integration makes up the conventional IoT system. Blockchain enables a consensus method for dynamic data storage, secures end-to-end data transfer, and offers product traceability and monitoring, all of which contribute to the high security of IoT systems. Algorithms based on rules and hierarchy-based consensus all contribute to enhancing IoT device security and enhancing transaction speed. Additionally, because it offers a decentralized platform for data sharing and data verification as well as an immutable ledger structure, blockchain is less vulnerable to manipulation and identity frauds by nature.
- **Intrusion detection system:** Blockchain assists in the development of collaborative intrusion detection systems, which allow product codes to communicate with one another and share information during their entire path. By using blockchain technology, which helps to secure the integrity and transparency of data storage, a risk related to code tampering and security can be eliminated.

2.3. Applications of blockchain technology across various industrial sectors and in societal contexts

By leveraging shared, protected, distributed, and permissioned transactional ledgers, blockchain technology has the potential to address problems, clear the way for further study, and eliminate bottlenecks. These characteristics have made it inescapable and a pioneer in the research across several industrial industries. Interchain management, project management, relationship modeling, new product creation, and interchain coordination are all made easier by blockchain in a variety of global industries. Blockchain also spurs innovation in value offerings and business models, particularly among startups and business owners. A fresh variety of applications, the availability of open source software, and the elimination of third parties would all support blockchain's goal of fostering industry innovation. If blockchain is purposefully used to solve SC problems, it can produce enormous benefits. In SCs throughout numerous industries and sectors, we have discovered numerous blockchain applications and implementations that could improve societal welfare. We include a few of the major industries and their

societal and industrial implications below.

2.3.1.1.Financial Sector

Due to the rise of bitcoin and cryptocurrencies, blockchain technology, which has its roots in banking, has been widely adopted in the financial industry. Blockchain technology has the potential to revolutionize share trading, streamline cross-border payments, enhance identity management, and make it easier to manage money in the financial industry. Blockchain technology can be used by the financial sector and the government to develop a new virtual money for the community, but correct legislation and stringent oversight are necessary for a successful deployment. For SC financial systems, it can be utilized to support "sophisticated fractional calculus models." The rise of cryptocurrencies has an impact on society and everyday life. Future transactions could be supported by a variety of virtual currencies, both domestically and internationally.

2.3.1.2.Credit accounting and management systems with blockchain technology

Credit transactions with encryption enabled are more secure, take less time and money to track, automate credit monetization, and make the execution, verification, and recording of the credit journey transparent and searchable. According to reports, the "Belt and Road Blockchain Consortium" has employed blockchain as a quick and effective mechanism to move money for China's One Belt One Road plan across borders of more than 56 countries. Another illustration is the AgriDigital platform, a "closed blockchain application" that enables quicker and more secure post-delivery payment.

2.3.1.3.Technology Industry

Identity management and strong cybersecurity pose the largest threats to the technology sector, but they can be overcome by connecting the technological platforms with blockchain. Although increasingly employed across all industries, cloud, Industry 4.0, and IoTs are vulnerable to security concerns because of their centralized nature. The security and scalability of the cloud network would be increased with the incorporation of blockchain technology. The centralization of IoT platform architecture also increases the risk of a single point of failure. Blockchain enables decentralized Internet of Things (IoT) systems, in which both technologies work together to create a strong and intelligent technology. There is a need for an independent system that could facilitate real-time data sharing with total transparency due to many causes like globalization, human error, and regulatory inefficiencies.

Blockchain can assist in the design and implementation of a sustainable SCM using its decentralized

and ultra-secure structure because traditional ERP solutions are vulnerable to single point failures, corruption, and hacking. In an industrial system, blockchain can be utilized to determine causal links. The entire process can be automated using blockchain and "Industrial IoT" (IIoT).

2.3.1.4.Manufacturing Industry

Blockchain utilizes a cross-enterprise framework that supports a higher level of information sharing to assist in integrating the transition to shared and distributed systems in manufacturing ecosystems. Integration of blockchain technology enables firms to develop adaptable and scalable enterprises at a reduced cost in a more secure, efficient, and well-controlled manner. By offering real-time transparency and cost savings, it also raises a company's profit and competitiveness. Additionally, it facilitates the incorporation of agile manufacturing techniques, enables product customization, intelligent automation, and enhances employee empowerment. Examples of blockchain integration in the manufacturing industry can be seen when a corporation links a chemical signature or tokens in the underlying database systems to resolve concerns with counterfeit items in additive manufacturing.

2.3.1.5.Logistics Industry

For the purpose of integrating and connecting all business activities (finance, banking, IoT, SC, production, insurance) in the context of a shipment, lockchain can be implemented in the cargo shipping industry. Blockchain guarantees disintermediation, reduced transaction costs, and cost-effective enforcement in maritime SCs. Assuring minimal delays in real-time transactions, transparency of transactions from remote locations, increased vigilance for data confidentiality, and transaction validation are all possible with integrated and networked merchant ships. By setting up projects, people, information, payments, and communication in safer, wiser, and more effective ways, blockchain can also revolutionize the maritime sector. Smart contracts and blockchain technology can be used to handle shipments, automate payments, detect infractions, and improve the effectiveness of the SC as a whole.

2.3.1.6.Power Sector

By facilitating transparent, secure, and effective electrical energy transactions, blockchain has the potential to revolutionize the energy industry. A flat trading and decentralized system with direct communication between dispersed agents is made possible by blockchain, which also aids in the establishment of transactional energy systems. By separating the trading process into two stages—the call auction stage and the continuing auction stage—it makes it possible for a decentralized and

distributed accounting method to meet the present requirements of participant's dispersed needs in the energy market. By utilizing a peer-to-peer blockchain network for energy systems, customers will have access to cheap, high-quality energy at all times while simultaneously saving money and democratically connecting various energy supplies.

Sector	Scalability	Data Privacy	Interoperability	Auditability	Product Traceability	Processing Speed	Transparency	Disintermediation
Finance	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Healthcare	Yes	Yes	Yes					
Manufacturing	Yes	Yes	Yes	Yes		Yes		
IoT	Yes	Yes	Yes	Yes	Yes	Yes		
Social Service	Yes	Yes	Yes	Yes		Yes		
Shipping	Yes	Yes	Yes	Yes	Yes	Yes		Yes
Agriculture & Food	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Sector	Scalability	Data Privacy	Interoperability	Auditability	Product Traceability	Processing Speed	Transparency	Disintermediation
Education	Yes	Yes	Yes	Yes				
E-commerce	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 2: In different sectors, Application of Blockchain

This offers value by outlining current blockchain advancements and exploring the possible uses of the technology in a range of industries, including healthcare, banking, technology, energy, agriculture, trade, and shipping.

Chapter 3

BLOCKCHAIN TECHNOLOGIES

Blockchain technology is a distributed ledger that securely logs transactions over a network of computers. It is decentralized and decentralized. Blockchain was first introduced as the underlying technology underpinning the cryptocurrency Bitcoin, but it has since developed and found several uses in a range of sectors.

A blockchain is fundamentally a series of blocks, each of which comprises a group of verified transactions. Since these blocks are connected using cryptographic methods, the recorded data is guaranteed to be accurate and unchangeable. An outline of the main elements and characteristics of blockchain technology is provided below:

- **Decentralization**: Blockchain functions in a decentralized fashion, in contrast to conventional centralized systems that depend on a single authority. It disperses the transaction data among numerous network nodes (computers), strengthening security and preventing single points of failure.
- **Consensus Mechanism**: To confirm the legitimacy of transactions and add them to the ledger in a blockchain network, consensus procedures are utilized. The widely used Proof of Work (PoW), Proof of Stake (PoS), and Delegated Proof of Stake (DPoS) consensus algorithms each have a different strategy for reaching consensus.
- **Immutability**: Data is essentially unchangeable once it is stored on a blockchain. Because the consensus system is cryptographic, changing previous records in a block would involve changing subsequent blocks, which is computationally impossible. This constancy ensures data integrity and prevents tampering.
- **Transparency**: All network users can see transactions made on a blockchain. The blockchain is fully transparent and auditable since each participant has a copy of the entire ledger.
- **Security**: is excellent thanks to the cryptographic architecture of blockchain technology. Public-key cryptography is used to safeguard transactions, and the network's decentralized structure

lowers the possibility of hacking and illegal access.

- **Smart Contracts**: Self-executing programs known as "smart contracts" automatically enforce an agreement's terms when certain criteria are satisfied. They make it possible for automated, trustless transactions, which frequently do away with the need for middlemen.
- **Transparency**: of blockchain transactions notwithstanding, some blockchains provide privacy measures that shield sensitive data using cutting-edge cryptographic methods. Private transactions and zero-knowledge proofs are two examples.
- **Interoperability**: As the blockchain ecosystem develops, it becomes increasingly important that various blockchain networks interact together. Solutions for interoperability are designed to facilitate smooth data transfer and communication between various blockchains.
- **Scalability**: Because they can only process a certain number of transactions per second, traditional blockchains like Bitcoin and Ethereum have problems growing. Sharding and layer-2 protocols are two scaling techniques that try to increase blockchain scalability.

Researchers and developers are exploring the possible uses of blockchain technology beyond finance and cryptocurrencies as it continues to grow. Blockchain is being aggressively adopted by sectors like supply chain, healthcare, logistics, and identity management to increase transparency, security, and productivity in their processes. As the technology develops, it is anticipated that it will have a bigger impact on how different areas of our digital world will develop in the future.

3.1. Different types of Blockchain Technologies

- Ethereum

Decentralized platforms like Ethereum (ETH) allow for the creation and deployment of smart contracts and decentralized applications (dApps). It popularized the idea of programmable blockchain, enabling programmers to build unique tokens and carry out challenging tasks on the blockchain.

- Bitcoin

The first and most well-known blockchain-based cryptocurrency is called Bitcoin (BTC). With no need for middlemen like banks, it functions as a peer-to-peer digital cash system, enabling safe and borderless transactions.

- Ripple (XRP)

Blockchain technology called Ripple (XRP) is intended for quick and inexpensive cross-border transactions. Targeting the financial sector and international remittances, it promises to make rapid and affordable money transfers possible everywhere.

- Hyperledger Fabric

The Hyperledger project of the Linux Foundation has created Hyperledger Fabric, an enterprise-grade blockchain platform. With increased privacy and scalability, it focuses on building private, permissioned blockchain networks for corporate applications.

- Cardano (ADA)

It is a third-generation blockchain platform created to solve the scalability, sustainability, and interoperability issues that were present in earlier blockchain systems. It intends to give smart contracts and decentralized applications (dApps) a more stable and scalable foundation.

- Stellar (XLM)

Stellar is a blockchain platform created primarily for quick and affordable international trade and asset issuance. It targets financial institutions and promises to make money transfers and remittances quick and easy.

- PolkaDot (Dot)

A multi-chain blockchain technology called Polkadot (DOT) offers interoperability between several blockchains. It improves the ecosystem's overall scalability and usefulness by enabling connections between various blockchain networks, information sharing, and asset transfers.

- VeChain (VET)

It is a blockchain network that focuses on supply chain management and the confirmation of product authenticity. It offers a visible and tamper-proof record of product information, guaranteeing the goods' legitimacy and traceability.

- Tezos (XTZ)

Through on-chain governance, Tezos, a self-amending blockchain platform, enables stakeholders to update and change the protocol. Without the need for hard forks, it strives to increase network consensus and develop over time.

- EOS (EOS)

Scalability and quick transaction processing are priorities for the EOS blockchain platform. It is appropriate for large-scale dApps because it uses a delegated proof-of-stake (DPoS) consensus process to provide faster throughput and lower latency.

- IOTA (MIOTA)

Blockchain platform IOTA (MIOTA) was created for the Internet of Things (IoT) environment. It utilizes a novel Tangle structure as opposed to a conventional blockchain, offering an ecosystem that is

scalable and cost-free for IoT devices to exchange data and value.

- Corda

Corda is an open-source blockchain platform created with business use cases in mind. In order to meet the demands of companies and financial institutions, R3 developed Corda, which places a strong emphasis on privacy, scalability, and interoperability. Through its distinctive "notary" method, it enables direct peer-to-peer transactions while guaranteeing that sensitive data is transmitted only with necessary parties. For intricate financial arrangements, supply chain management, and other corporate procedures requiring a high level of security and anonymity, Corda is especially well suited.

3.2. Comparison of Blockchain technologies

Technology	Consensus Mechanism	Scalability	Smart Contracts	Interoperability	Privacy	Use Cases and Features
Ethereum (ETH)	Proof of Work (PoW)	Moderate	Yes	Limited	Limited	programmable blockchain, decentralized apps (dApps), and token production
Bitcoin (BTC)	Proof of Work (PoW)	Limited	No	Limited	Limited	Peer-to-peer exchanges and digital currencies
Ripple (XRP)	Ripple Protocol Consensus	High	No	Limited	Yes	Financial sector, remittances, and international payments
Hyperledger Fabric	Pluggable Consensus	High	Yes	Yes	Yes	solutions for business blockchain, private networks, and permissioned networks

Technology	Consensus Mechanism	Scalability	Smart Contracts	Interoperability	Privacy	Use Cases and Features
Cardano (ADA)	Ouroboros Proof of Stake	High	Yes	Limited	Yes	Smart contracts, scalability, sustainability
Stellar (XLM)	Stellar Consensus Protocol	High	No	Limited	Limited	Transacting internationally and issuing assets
Polkadot (DOT)	Nominated Proof of Stake	High	Yes	Yes	Yes	Blockchain interoperability and chain-to-chain communication
VeChain (VET)	Proof of Authority (PoA)	High	No	Limited	Yes	Verification of product authenticity and supply chain management
IOTA (MIOTA)	The Tangle	High	No	Yes	Yes	Data and value transfer via the Internet of Things (IoT), including cost-free transactions
Corda	Pluggable Consensus	High	Yes	Limited	Yes	Enterprise blockchain for privacy-focused applications, supply chain management, and complex financial arrangements

Table 3: Comparison of Different Blockchain Technologies

3.3. Benefits and Drawbacks of different Blockchain technologies

Technology	Advantages	Disadvantages
Ethereum (ETH)	- A sizable decentralized apps (dApps) developer community.	- Problems with scalability caused by expensive transaction costs and extended processing times.
	- A blockchain that can be programmed to support smart contracts and unique tokens.	- Proof of Work (PoW) consensus mechanism.
Bitcoin (BTC)	- Created the first decentralized payment system and digital money.	- Limited scalability which leads to higher transaction fees and slower confirmation times.
	- A peer-to-peer ledger that is transparent and secure.	- Proof of Work (PoW) consensus mechanism.
Ripple (XRP)	- Cross-border transactions that are quick and affordable, boosting remittances.	- Centralized validators raise concerns about decentralization.
	- Aimed at financial organizations for efficient international money transfers.	- Relies on a unique consensus protocol, Not fully permissionless

Technology	Advantages	Disadvantages
Hyperledger Fabric	– Appropriate for business apps with a privacy-focused design.	- For maintaining the network it Requires a consortium or membership
	- Modular architecture that is adaptable to individual company requirements.	- Higher complexity in implementation.
Cardano (ADA)	- Blockchain protocol that has undergone peer review and scientific investigation.	- Slower development due to a rigorous peer-review process.
	- Put an emphasis on scalability, governance on-chain, and sustainability.	- Limited number of developed dApps
Stellar (XLM)	- Created for international trade and asset issuance.	- Limited smart contract capabilities
	Integration with the current financial infrastructure has been made simpler.	- Relatively lower adoption
Polkadot (DOT)	- Promotes communication between various blockchains.	- Complex architecture

Technology	Advantages	Disadvantages
	- Allows autonomous blockchains to safely link and exchange data.	- Immature ecosystem with fewer active dApps and users.
VeChain (VET)	- Improves supply chain management and the assurance of product authenticity.	- Mainly focused on supply chain use cases
	- Assures immutability and transparency for certified product data.	- Limited adoption and awareness outside of specific industries.
IOTA (MIOTA)	- A lightweight architecture appropriate for IoT devices and fee-free transactions.	- Vulnerabilities in the Tangle structure
	Fast and scalable data and value transfers are made possible by The Tangle.	- Security issues and development challenges.
Corda	- Designed for supply chain management and complicated financial agreements.	- Limited adoption and recognition compared to major public blockchains.
	- Privacy-focused, only sharing information through notaries with parties who need it.	- Specific use case focus may limit broader adoption.

Table 4: Advantages and Disadvantages of Blockchain Technologies

3.4. Consensus Algorithms

A consensus protocol is essentially a set of guidelines that each participant must abide by. Blockchain requires a distributed consensus method since it is a distributed system without a single source of trust, hence everyone must concur on its present state. Due to scarcity, more control over a limited resource results in more control over how the blockchain functions. Blockchains have been designed with a variety of unique consensus mechanisms, such as Proof of Work (PoW), Proof of State (PoS), Delegated Proof of State (DPoS), Proof of Elapsed Time (PoET), Practical Byzantine Fault Tolerance (PBFT), Directed Acyclic Graph (DAG), Proof of Authority (PoA), Tendermint, Ripple, Scalable Byzantine Consensus Protocol (SCP), Proof of Band, depending upon their requirement.

3.4.1 Proof of Work (POW)

PoW chooses a problem that can only be guessed at. When creating and validating a full block, for instance, the challenge is to determine a nonce value such that the difficulty must match the output of a hash function that uses the transaction data and the nonce value as inputs. Currently, every node in the network is making random guesses at various nonce values until one node eventually finds the nonce value that corresponds to the difficulty. In order to successfully create a block to link to the blockchain and earn an incentive mining reward, which is money, a mining node must invest a lot of computational resources in it and solve the problem more quickly than others.

3.4.2. Proof of Stake (POS)

The second-most popular consensus approach, PoS, requires fewer calculations to mine than PoW. PoS eliminates the time and energy consumption issues that PoW has because finding a nonce requires electricity, and finding a nonce requires miners to take some time. To be selected as the next block creator in a PoS network, nodes must stake some money. The creator of each chosen block will get the transaction fees related to that block. A block winner will forfeit their stake if they attempt to add an invalid block. The blockchain's "world computers" migrate from the PoW to the PoS consensus algorithm in the first stage of the Ethereum 2.0 upgrade.

3.4.3. Delegated Proof-of-Stake (DPoS)

In DPoS, every token holder has the ability to cast a number of votes for delegates and to assign voting

authority to other users. The number of tokens a token holder has determines how much voting power they have. Then, in order to protect the network, the delegates are in charge of validating transactions and blocks. Token holders in DPoS are permitted to vote on who to mine new blocks and reward only the best miners, unlike PoW and PoS, which reward the miners with the biggest computing power or tokens. One blockchain system that makes use of the DPoS algorithm is EOS.

3.4.4. Proof of Elapsed Time

PoET was created by Intel Corporation to offer a different method of choosing a block miner. Each potential validation node in PoET demands a randomly generated waiting time that is produced on a reliable computing platform, such as Intel's SGX. The first node to finish waiting for the allotted amount of time is the validation winner and is able to add the new block. Every node can have a chance to win thanks to the trusted computing platform.

3.4.5. Practical Byzantine Fault Tolerance (PBFT)

The goal of Byzantine Fault Tolerance (BFT) is to find a suitable consensus while resolving the well-known general problem that some generals are dishonest. BFT is optimized by the consensus algorithm known as PBFT [16]. In PBFT, the blockchain system will come to consensus on the blockchain's present state as long as the number of malevolent or hostile nodes is fewer than one-third of all the nodes. The security of a blockchain system increases with the number of nodes. PBFT is now used by Hyperledger Fabric.

3.4.6. Directed Acyclic Graph (DAG)

In contrast to previous consensus procedures, DAGs are composed of vertices and edges (the paths linking them). The edges and vertices are acyclic because they do not loop back on themselves and are directed since they all point in the same direction. In the structure, each vertex stands for a transaction. Here, there is no concept of blocks, and adding transactions is not dependent on mining. Each transaction is constructed on top of another rather than being gathered into blocks. Still, when a node submits a transaction, a little PoW operation is performed. This confirms that earlier transactions are legitimate and prevents network spam. The DAG consensus algorithm is used by IOTA.

3.5. Smart Contract

A further admirable feature of blockchain is the ability to write very objective computer code that

specifies how a process will be managed and what actions will be taken when an event occurs, in addition to providing a distributed, unalterable record of all the different events that have occurred. Breaking the constraints of Bitcoin was one of the objectives of the smart contract proposed in Ethereum. The concept of a smart contract is computer code that is developed to react to specific kinds of important events. The smart contract does not have to be legally binding or include more than two parties.

Smart contracts, often referred to as chaincode, are used to integrate rules and decision-making into blockchain processes and transactions.

• Ensure that transactions are automated and that they all adhere to the same regulations.

• Utilize a blockchain.

The smart contract, which is the foundation for enterprise blockchain applications, will alter the way we conduct business. Smart contracts can be created by anyone without the use of middlemen. The smart contract offers independence, effectiveness, efficiency, and cost savings.

Chapter 4

CORDA - AN OVERVIEW

4.1. Introduction

R3, a group of top financial institutions and tech firms, established the Corda platform for distributed ledger technology (DLT). In order to manage complicated transactions and contracts, it offers a safe and scalable solution tailored to the demands of corporations and enterprises. Contrary to conventional blockchains, Corda's architecture is designed with data secrecy and privacy as a top priority. Each transaction is shared only with the persons that need to know about it, which is a novel strategy used to ensure that sensitive information is only accessible to those who need it. Corda is a good fit for

applications that demand strong privacy and adherence to legal regulations thanks to this capability.

"CorDapps," or smart contracts, are supported by Corda for development and execution. These contracts may be read by developers of all skill levels because they are written in well-known programming languages. By automating agreement enforcement and streamlining company procedures, smart contracts on Corda minimize manual intervention and operational inefficiencies.The performance and scalability of Corda are two of its standout qualities. It is appropriate for enterprise-level use cases that require quick and dependable transaction processing because it offers high transaction throughput without sacrificing security.

The architecture of Corda places a strong emphasis on interoperability, enabling seamless integration with current networks and systems. This makes it possible for companies to use blockchain technology without having to completely redesign their present infrastructure. The platform makes use of a novel consensus method that depends on a community of "notaries" to verify and reach consensus on particular transaction data. This strategy guarantees transaction immutability and finality while avoiding the resource-intensive mining operations frequently connected to conventional blockchains.

Numerous different sectors and use cases find usage for Corda. It has demonstrated to be very helpful in a variety of fields, including trade finance, supply chain management, insurance, healthcare, real estate, and financial services.

With privacy, scalability, and interoperability to solve the complexity of enterprise-level transactions, Corda is a strong and adaptable distributed ledger platform. Businesses looking for secure and effective

blockchain solutions will find it an appealing option because to its emphasis on data confidentiality and smart contract capabilities.

4.2. Key Features of Corda

4.2.1. Ledger

1. A distributed ledger is a fact database that is shared, copied, and synced among numerous users on a network.
2. Participants are referred to as nodes, and their vault has a copy of the ledger.
3. Depending on the facts it shares, each node has a distinct perspective of the ledger.
4. Before a fact can be committed to the ledger, the nodes that share it must come to an agreement.
5. Any on-ledger information that two nodes share are always displayed in exactly the same form.

There is no central repository for data in Corda. Every node keeps a database of facts—things it is aware are true based on interactions—that it knows to be true. For instance, if Alice lends Bob some money and there are nodes on the network representing Alice and Bob, Alice and Bob will both maintain the same record of the details of that loan. Alice and Bob are the only nodes that ever see or store this data if Alice and Bob are the only parties to the loan.

4.2.2. States

An immutable object known as a state represents a truth that one or more nodes are aware of at a certain instant in time. States can be used to express any kind of information or truth. A financial instrument, Know Your Customer (KYC) information, or identity details are a few examples. States are unchangeable; they cannot be altered. State sequences are used by Corda to trace the development of facts. One of the participants in the state creates a new state if a fact changes, designating the old state as historic.

Every node on the network keeps a vault up to date. This is the node's database, which is used to keep track of both the node's most recent and previous participation states.

4.2.3. Transactions

The only way to alter the Corda ledger is to add new transactions; it cannot be edited. By consuming current input states and producing new states, a transaction updates the ledger. The transaction consumes the "historic" states.

Every state is unchangeable and cannot be altered. An UTXO (unspent transaction output) model is what this is.

- Any number of inputs, outputs, and references of any kind may be included in a transaction. Different sorts of states representing various financial products, such as cash or bonds, might be included in transactions.
- By producing a transaction without inputs, issue states are created. None of the new states will take the place of any current ones because none are designated as "historic".
- Create transactions without outputs to exit states. The consumed states are not replaced by any new ones as a result of this.
- Consolidate or divide fungible assets. For instance, they might create a $7 cash state by combining a $2 state and a $5 state.
- Trades are atomic. Either all recommended changes to the transaction are accepted, or none are.

The two most common forms of transactions are:

- Transactions for changing the notary for a state.
- For all other transactions, general transactions.

4.2.3.1. Transaction backchains

A node can confirm that each input was produced from a legitimate sequence of transactions using transaction backchains. Walking the chain is what is meant by this. You can reissue states if you need to break this chain for any reason, such as to improve performance by limiting the number of transactions the node needs to examine or to maintain the privacy of earlier transactions.

Input state references are linked together over time to form backchains. The outputs of earlier transactions can be used as the inputs for new transactions thanks to input state references.

References to input states include:

- The hash of the input's creation transaction.
- The backchain's index of the input in the prior transaction's outputs.

4.2.3.2. Transaction Validity

It takes more than just getting the necessary signatures to put a transaction on the ledger. Moreover, it

must be:

Valid: All required parties must sign the proposed transaction and every transaction in the backchain of the proposed inputs in order for them to be legally binding.

Unusual: None of the inputs to the proposed transaction have been used by any previous committed transaction. A notary decides whether something is unique.

The outputs of the transaction are invalid and will not be accepted as inputs into subsequent transactions if it collects all the necessary signatures without complying with these requirements.

4.2.4. Smart Contract

By converting the contract terms into code that runs automatically when the terms are met, smart contracts digitize agreements. This implies:

- The parties are not required to have faith in one another to uphold the terms of the agreement.
- External enforcement is not necessary.
- It is always agreed upon how to read the contract.
- The network's nodes each have a copy of the contract code. Before the contract is signed, the network's participants must agree that all of its requirements have been met.

Contracting Corda gives it the following special characteristics:

- It can only be updated and replaced, not changed.
- Once implemented, the outcomes cannot be changed.

4.2.5. Flows

Point-to-point communications, as opposed to a worldwide broadcast paradigm, is used by Corda networks. Network members must determine what information needs to be communicated, to which counterparties, and in what order in order to update the ledger.

Corda uses flows to automate the procedure so that you don't have to explicitly specify these stages. A flow is a series of instructions that shows a node how to carry out a particular ledger update, like issuing an asset or concluding a deal.

RPC calls are used by node operators to tell their node to begin a particular flow. The flow abstracts

away from the node operator all networking, I/O, and concurrent concerns.The context of these flows governs all behavior on the node. Contrary to contracts, flows do not execute in a sandbox, allowing nodes to engage in networking, I/O, and the use of randomness sources while a flow is in progress.

Because Corda offers a library of flows to handle typical operations, developers do not have to rewrite the logic for everyday procedures like:

- Notifying and documenting an event.
- Accumulating counterparty node signatures.
- Checking the sequence of transactions.

4.2.6. Consensus

Before you can add a proposed transaction to the ledger, there must be agreement that it is legitimate. To achieve agreement, trust, and security across decentralized networks, blockchains require consensus processes. Popular mechanisms like proof-of-work and proof-of-stake could be known to you.

Corda is unique. By demonstrating that a transaction is both legitimate and unique, consensus can be reached.

The proposed transaction and each transaction in the backchain that produced the inputs to the proposed transaction are subject to validity consensus tests that:

- Every input and output state's contracts agree to the transaction.
- There are all the necessary signatures on the transaction.
- This is known as "walking the chain."

For instance, if a node suggests a transaction to transfer a treasury bond, the transfer of the bond is only legitimate if:

- The central bank issued the treasury bond in a legal issuance transaction.
- Every subsequent exchange in which the bond was transferred was also legal.

4.2.7. Notaries

The notary is a distinctive consensus service offered by Corda. By ensuring that each transaction only contains distinct input states, it avoids double-spends. One or more notaries who function as a notary

cluster make up a notary service. The notary's responsibility is to make that each transaction has a distinct set of input states. Once the cluster confirms that a proposed transaction's input states have not already been used by another transaction, it obtains the signature of the cluster. The notary cluster will next decide whether to:

- If it is determined that each input state is unique, sign the transaction.
- If any of the input states match those that were seen in a prior transaction, reject the transaction and indicate a double-spend attempt as having taken place.

Every state has a designated notary cluster, therefore the cluster will only notarize a transaction if it is the designated notary cluster of every state that the transaction is being received from.

4.2.8. Vault

A Corda vault is a database that houses all of the ledger's information that is pertinent to a node. The database keeps track of states that have been consumed and not consumed. From a commercial standpoint, this entails keeping track of all the transaction states that you, as the node owner, can spend as well as all the spent states from transactions that concern you. It functions similarly to a bitcoin wallet, keeping track of your spending and available funds. Any transaction kept in the vault can have a descriptive text note attached to it.

4.2.9. Nodes

A Corda node has a distinct network identity and runs in the Java Virtual Machine (JVM) runtime environment. JVM runtime environments offer a reliable platform for running and deploying Java programs, including Corda services and CorDapps.

The architecture's fundamental components are:

- A layer of persistence for data storage.
- A network interface that allows nodes to communicate.
- An RPC interface for communicating with the owner of the node
- The service hub, which enables calls to internal node services from flows.
- A CorDapp interface and provider for adding CorDapps to the node.

Chapter 5

IMPLEMENTATION & RESULTS

5.1. Introduction

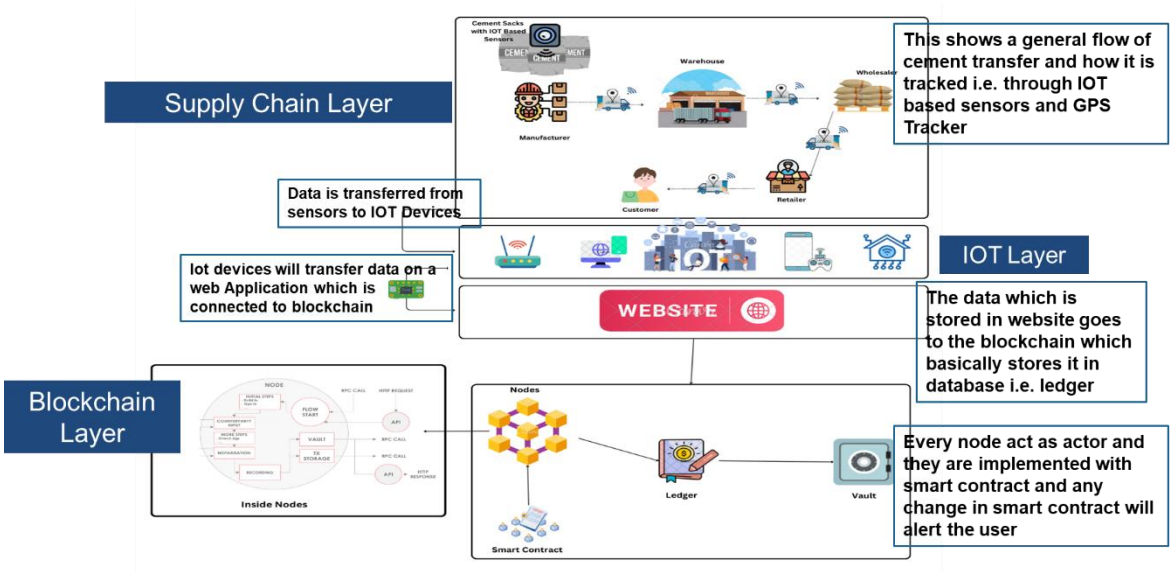


Figure 5.1: Network architecture diagram

This study presents a prototype for the novel methodology to maintain the integrity of data in cement industry while using the blockchain technology Corda. The proposed architecture is for the tracking of supply chain of cement it can also be used for multiple purposes. Our prototype basically has four actors i.e. Manufacturer, Wholesaler, Retailer and customer. But for this prototype we have only shown the transactions between Manufacturer and wholesaler. The same goes for the rest of the actors.

5.2. Environment Setup

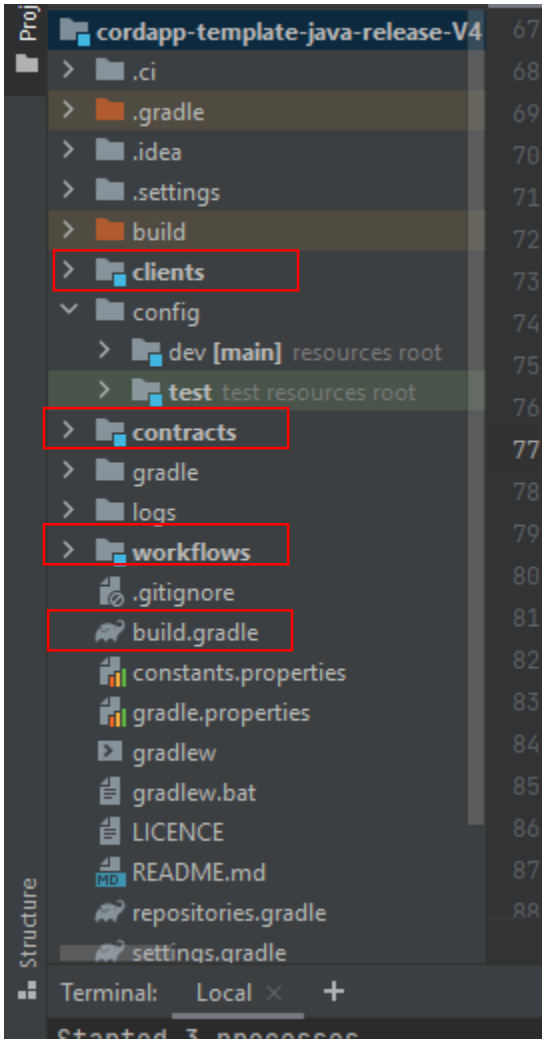
We used Corda version 4.9 Community edition, which was implemented on Intellij version 2020, to create this prototype. Java JDK 8 was used to create the project because it works with Corda 4.9. Additionally, Gradle was used to manage the project's build and dependencies. These technological decisions were chosen to guarantee the prototype's compatibility with the Corda ecosystem, ease of development, and seamless integration.

After setting up Git for Windows, we started by cloning the Corda sample project that we had

downloaded from the Corda website. We then opened the project in Intellij, and Gradle was used to build it. This series of steps was taken in order to follow official development procedures and make use of the materials offered by the official documentation. Frontend is created in HTML using springboot APIs.

5.3. Work Flow

The basic files which were used for the prototype are as follows:

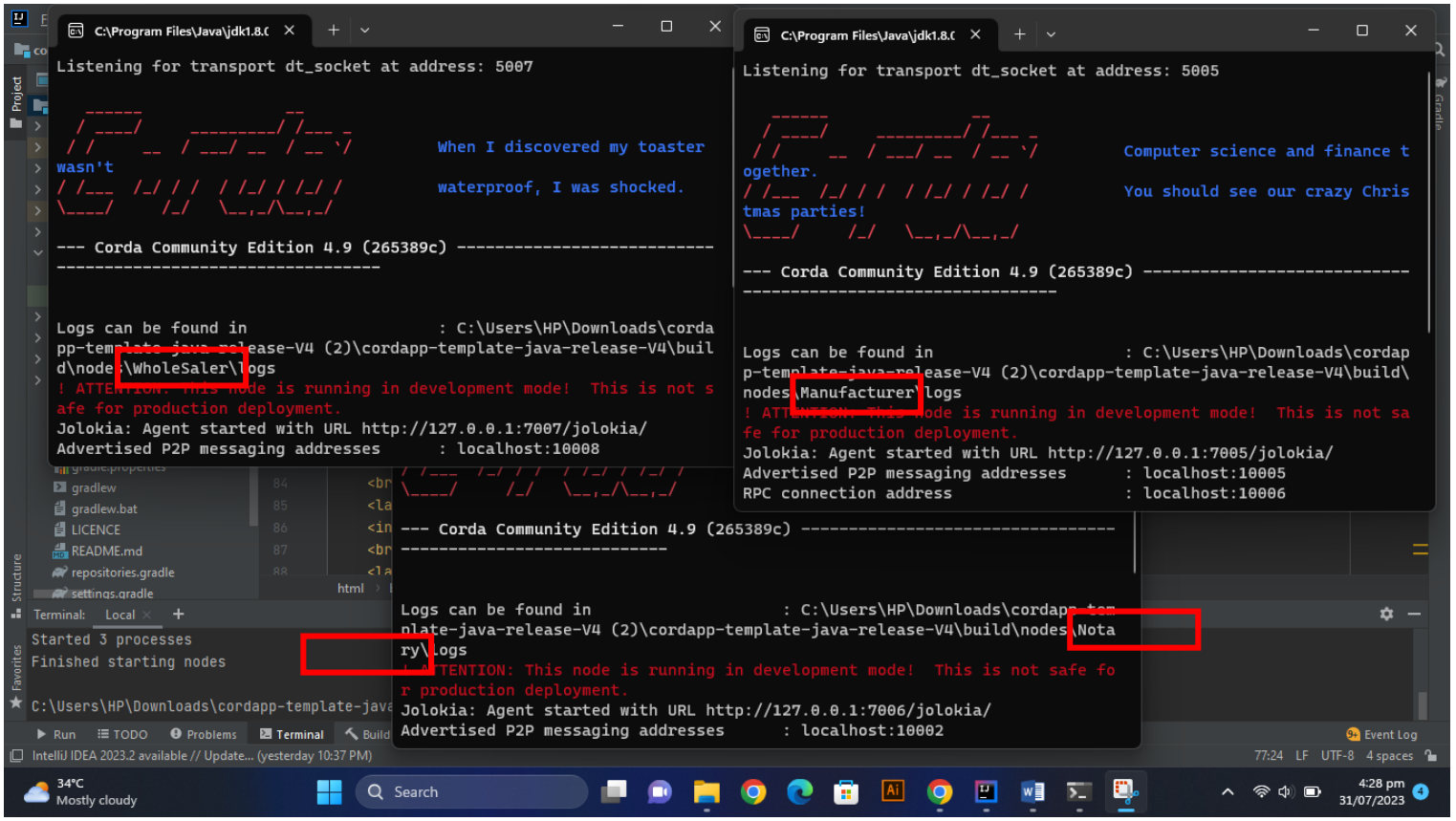


We first build the project and after that run nodes by following commands:

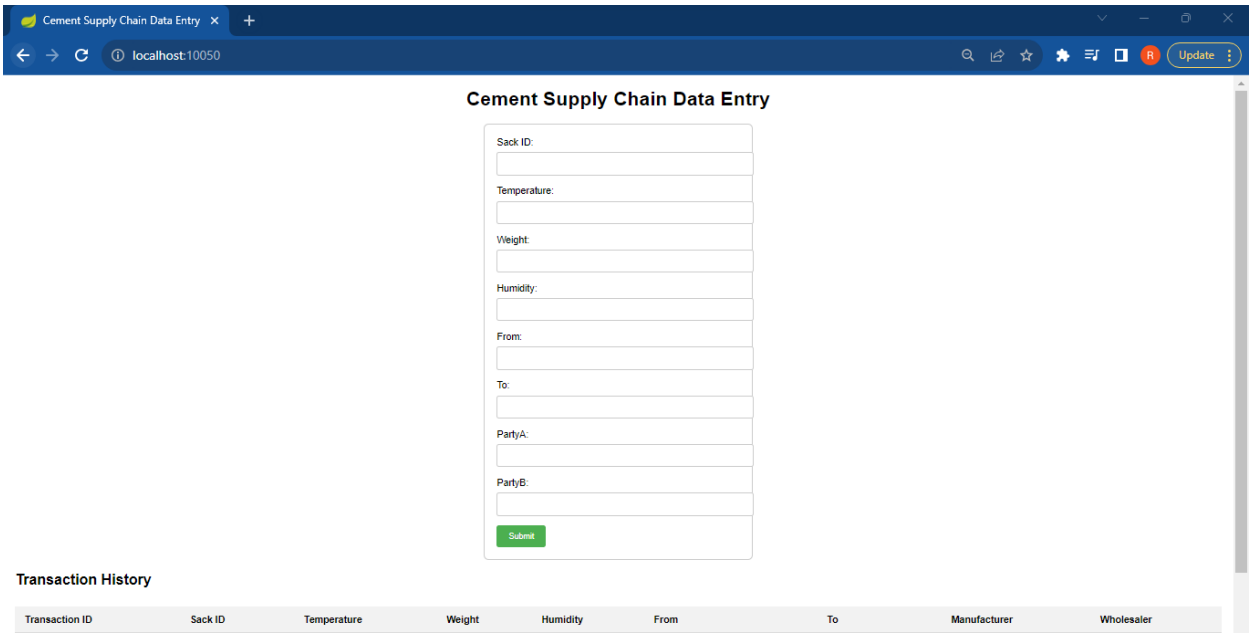
- gradlew DeployNodes
- .\build\nodes\runnodes

The actors we have are actually our nodes which we defined in Corda – An overview chapter so

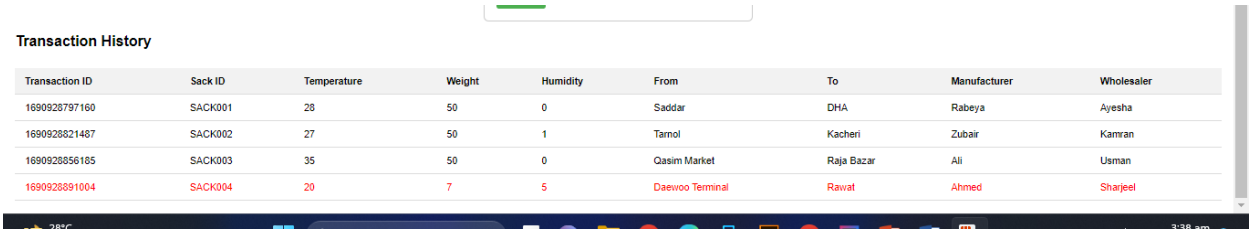
after running nodes, a terminal will open for each node along with notary.



For the use of client a front end is designed. And it is accessible on local host 10050. So http://localhost:10050 will open the client web application



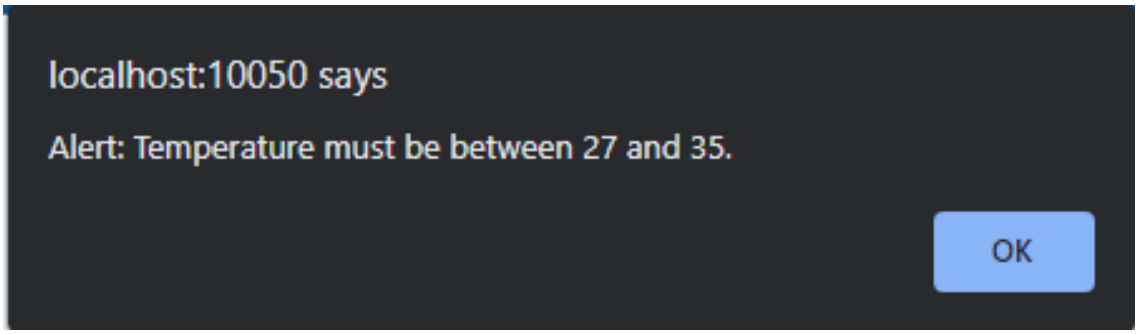
Now Let's see the transactions

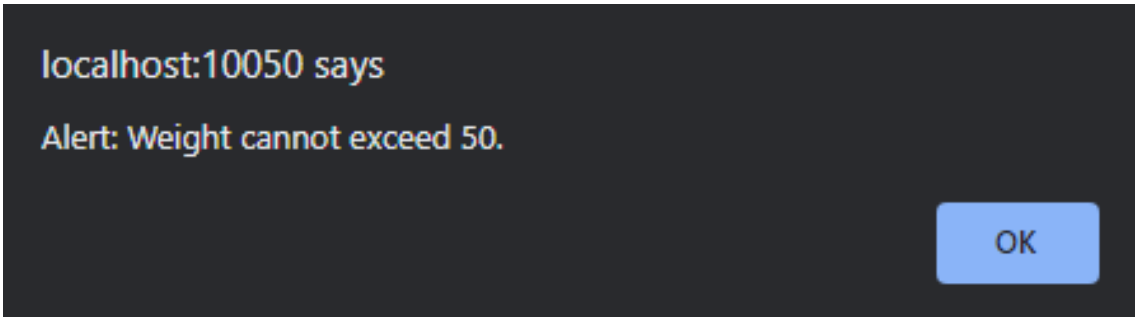


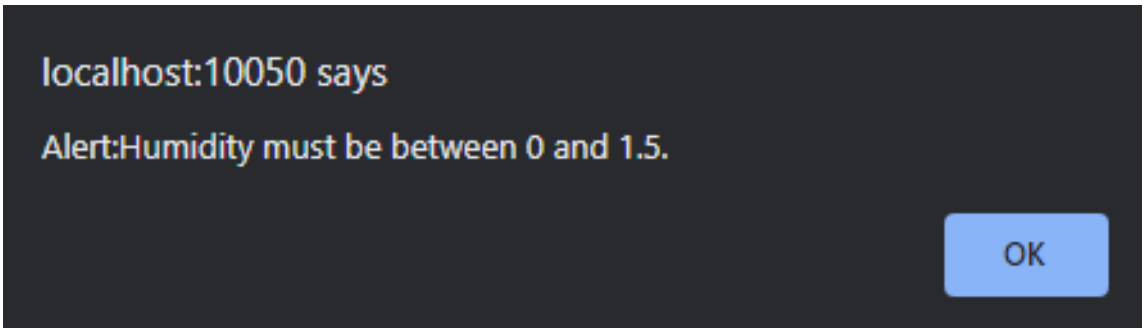
Transaction History

Transaction ID	Sack ID	Temperature	Weight	Humidity	From	To	Manufacturer	Wholesaler
1690928797160	SACK001	28	50	0	Saddar	DHA	Rabeya	Ayesha
1690928821487	SACK002	27	50	1	Tarnol	Kacheri	Zubair	Kamran
1690928856185	SACK003	35	50	0	Qasim Market	Raja Bazar	Ali	Usman
1690928891004	SACK004	20	7	5	Daewoo Terminal	Rawat	Ahmed	Sharjeel

The transaction in red shows that there is an error in readings and if the readings are changed means the sack is opened or the cement is taken out or something else is inserted in the sack. This Alert can be seen too which is as follows:



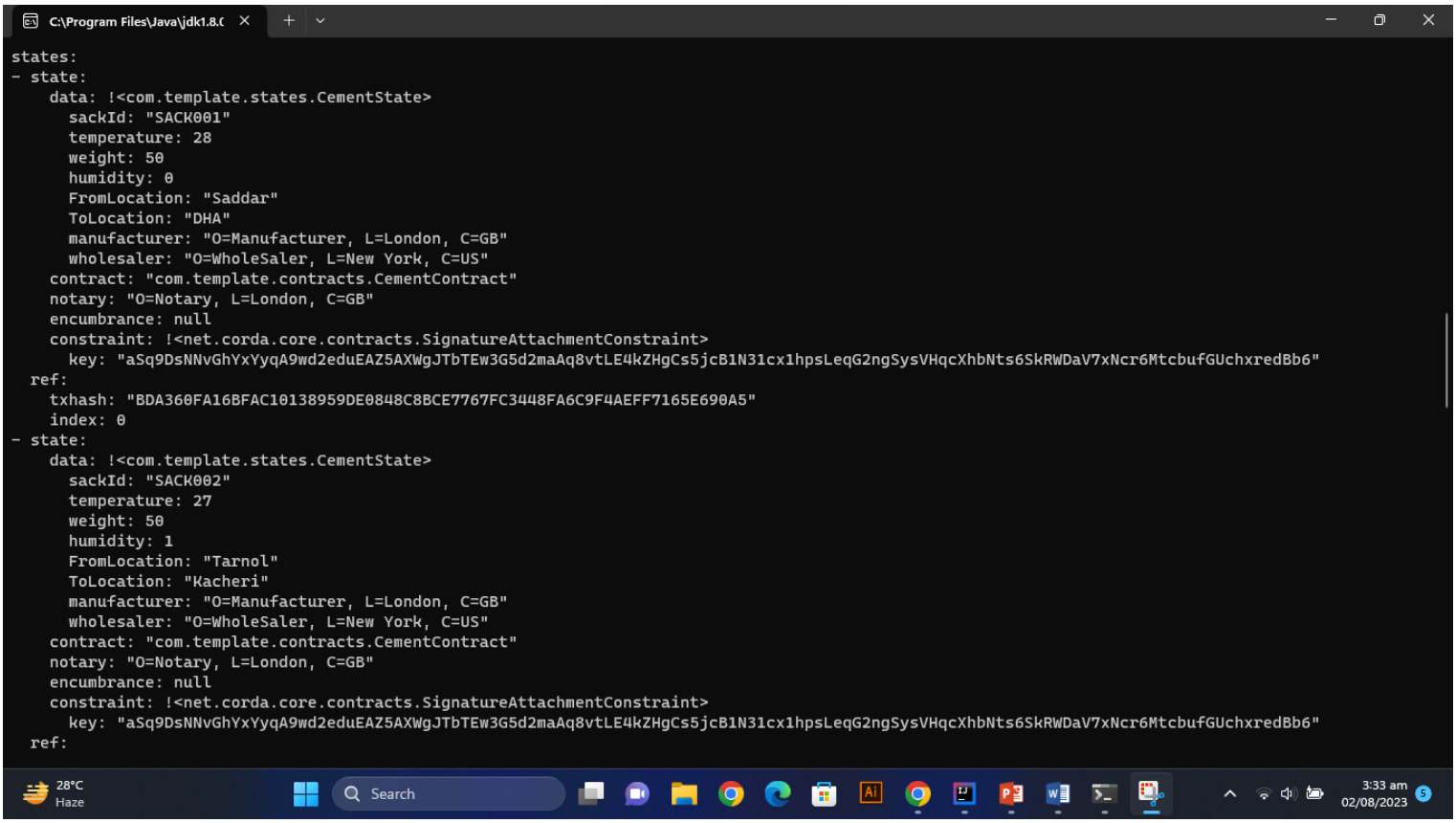




This alert will also send to backend that there is some change in values:

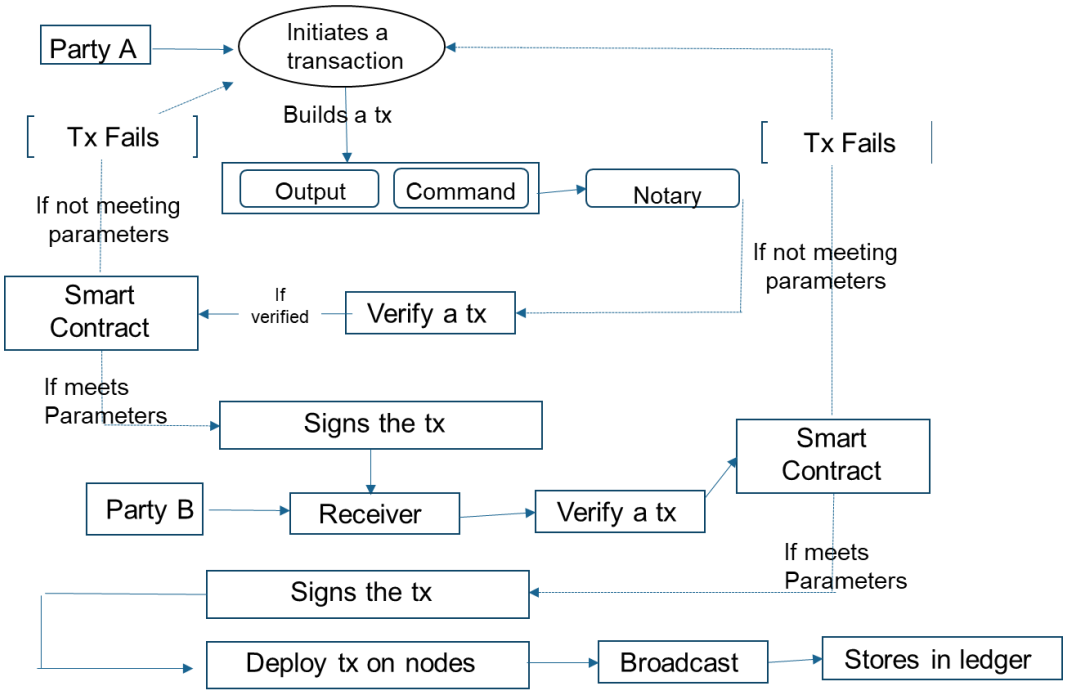
```
Starting
[ERROR] 03:03:58+0500 [Node thread-1] internal.Verifier. - Error validating transaction 9595DF67B52C4B27220B62A44C7A46E4DD716AD6B64EDD92E5C0C5F0AAD58CBC. {actor_id=internalShell, actor_owning_identity=O=Manufacturer, L=London, C=GB, actor_store_id=NODE_CONFIG, fiber-id=10000005, flow-id=39ae1bc7-7d23-4737-bdd7-27c45eb2c40f, invocation_id=004d0ec9-f606-4917-a381-68e875a96771, invocation_timestamp=2023-08-01T22:03:58.009Z, origin=internalShell, session_id=48afe1f5-7e59-499c-8f0e-c057d78ac1dc, session_timestamp=2023-08-01T22:00:10.979Z, thread-id=172}
[ERROR] 03:03:58+0500 [Node thread-1] internal.Verifier. - Error validating transaction 9595DF67B52C4B27220B62A44C7A46E4DD716AD6B64EDD92E5C0C5F0AAD58CBC. {actor_id=internalShell, actor_owning_identity=O=Manufacturer, L=London, C=GB, actor_store_id=NODE_CONFIG, fiber-id=10000005, flow-id=39ae1bc7-7d23-4737-bdd7-27c45eb2c40f, invocation_id=004d0ec9-f606-4917-a381-68e875a96771, invocation_timestamp=2023-08-01T22:03:58.009Z, origin=internalShell, session_id=48afe1f5-7e59-499c-8f0e-c057d78ac1dc, session_timestamp=2023-08-01T22:00:10.979Z, thread-id=172}
```

Also this data is stored in ledger in backend which is as follows:

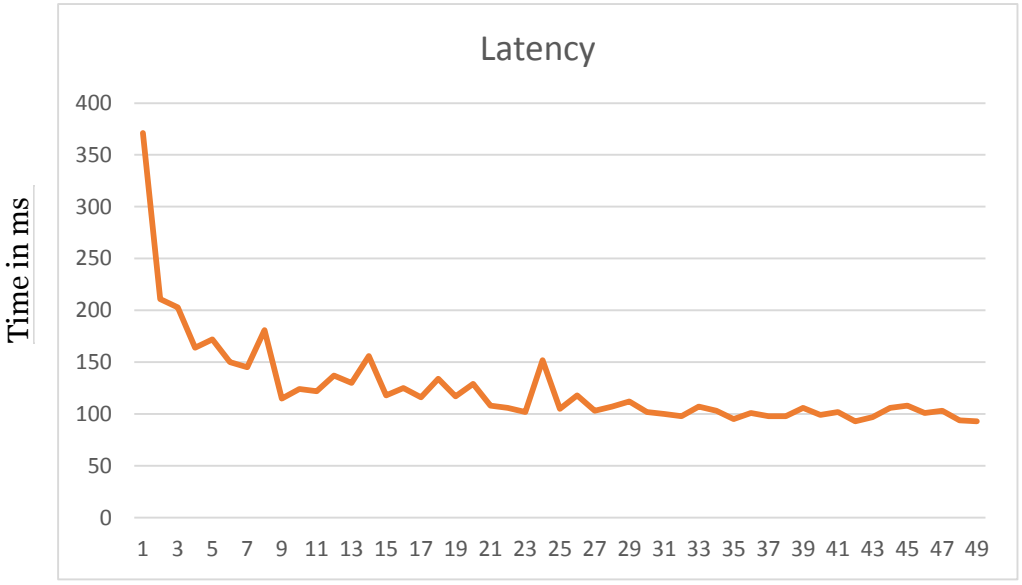


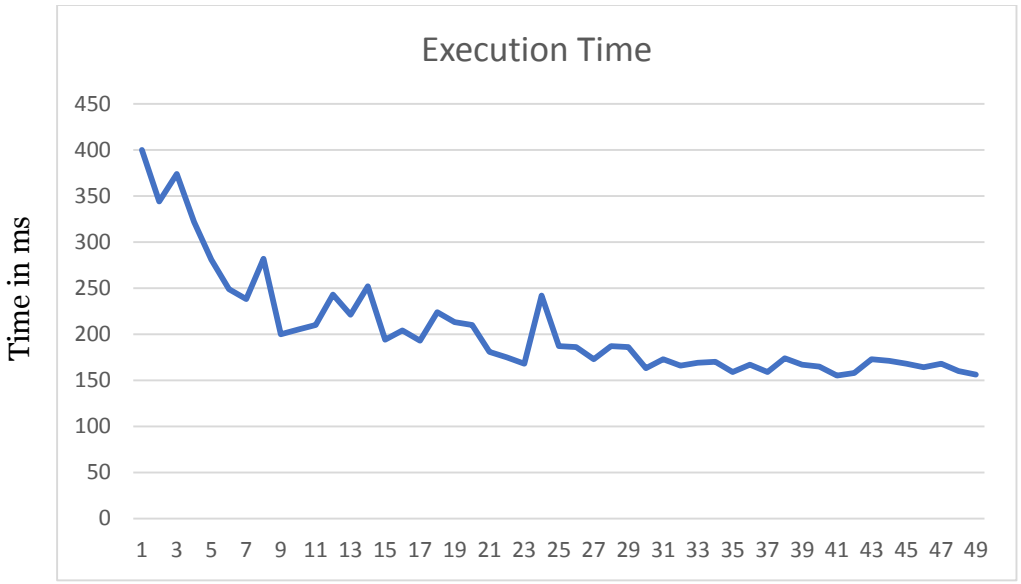
So this shows that transactions which are done are constantly stored in backend. So when in real time when the sensors will give data every second this prototype will store the data in Vault.

Implementation Flow



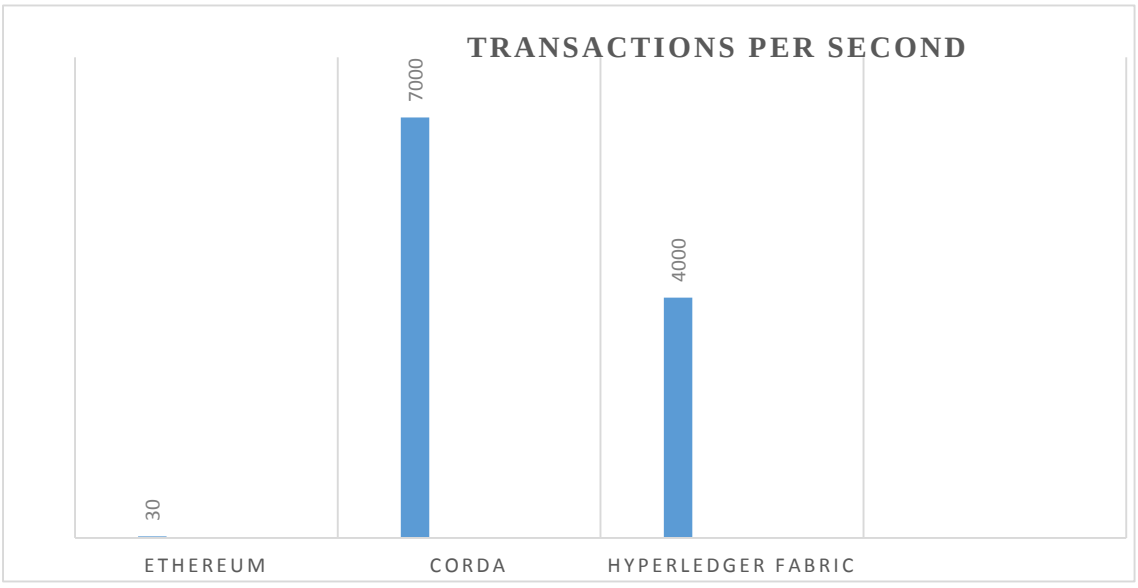
Performance Analysis





Comparative Analysis

In comparative analysis we can see that corda has highest number of transactions per second which is approximately 7000-8000 whereas Hyperledger fabric has 4000 transactions per second and Ethereum has lowest rate of transactions which is 40-50 transactions. This shows that Corda has huge capacity of accepting transactions which can increase the scalability of Blockchain Technology.



Security Analysis

Security-Related Benefit	Corda	Ethereum	Hyperledger Fabric
Privacy and Confidentiality	Selective data sharing	Limited privacy features	Private channels, access control
Fine-Grained Access Control	Granular control over data access	Limited access control	Fine-grained access control
Network Identity	Uses X.509 certificates	Public key cryptography	Identity solutions, certificate authorities
Immutable Transactions	Cryptographic hashing ensures immutability	Hashing and consensus mechanisms	Consensus mechanisms, cryptographic hashing
Secure Smart Contracts	Java and Kotlin languages	Solidity, Vyper languages	Various programming languages
Secure Channels	Private channels for secure communication	Public transactions by default	Private channels, secure communication
Secure Interoperability	Interoperability with existing systems	Interoperability initiatives	Interoperability solutions

Chapter 6

CONCLUSION AND FUTURE WORK

6.1. Conclusion

In order to solve the inherent difficulties and inefficiencies in the conventional cement supply chain, this study offers a transformational strategy. The initiative intends to improve transparency, traceability, real-time monitoring, and data-driven decision-making, ultimately improving the cement supply chain, by fusing Blockchain technology with IoT sensors.

The study has repeatedly called attention to the shortcomings of current technology, such as their lack of transparency, poor traceability, inconsistent data, and susceptibility to fraud. These flaws highlight the requirement for a more sophisticated and creative solution that can revolutionize the supply chain for the cement industry.

A strong solution to these problems is provided by the combination of blockchain technology with IoT sensors. A precise and impenetrable audit trail is produced by using blockchain technology, whose decentralized and unchangeable database provides transparent recording of all supply chain transactions. The incorporation of IoT sensors enables proactive interventions to protect product quality and integrity by providing real-time monitoring of environmental conditions during transit and storage.

The project has shown the potential benefits of the suggested approach, such as greater scalability, increased transparency, smart contracts for automating contractual agreements, and proactive quality control. The cement industry's stakeholders may streamline operations, cut costs, and provide customers with higher-quality products by adopting these technologies.

Additionally, the research has addressed possible risks and obstacles related to the use of Blockchain with IoT in the cement sector, including the need for established protocols, initial investment costs, and data privacy concerns. To guarantee their widespread adoption and successful execution, mitigation techniques have been put forth.

In conclusion, the research demonstrates how the supply chain for the cement industry could be revolutionized by fusing blockchain technology with IoT sensors. The suggested method has the

potential to develop a more reliable, secure, and transparent ecosystem, encouraging cooperation and sustainability among those involved in the supply chain. The cement industry may position itself as a competitive participant in the global market by adopting this transformative strategy, generating growth and profitability while satisfying the requirements of an industry landscape that is continually changing.

6.2. Future Work

We intend to implement the prototype on an actual cement bag, incorporating a barcode and budget-friendly IoT sensors. This approach holds promise as a significant step forward for our project. The cement bag will be designed to include a barcode label, serving as a unique identifier to link each bag with its digital record on the blockchain.

The selection of budget-friendly IoT sensors is a crucial aspect of our implementation. These sensors will be embedded within the cement bag during its manufacturing process. We will configure the sensors to monitor relevant environmental conditions, such as temperature and humidity. Ensuring low power consumption will be a priority to extend battery life and reduce maintenance efforts.

References

- Jabbar, S., Lloyd, H., Hammoudeh, M., Adebisi, B., & Raza, U. (2021). Blockchain-enabled supply chain: analysis, challenges, and future directions. Multimedia Systems, 27, 787−806.
- Dutta, P., Choi, T.-M., Somani, S., & Butala, R. (2020). Blockchain technology in supply chain operations: Applications, challenges and research opportunities. Transportation Research Part E: Logistics and Transportation Review, 142, 102067.
- Guo, H., & Yu, X. (2022). A survey on blockchain technology and its security. Blockchain: Research and Applications, 3(2), 100067.
- May Altulyan et al. “A unified framework for data integrity protection in people- centric smart cities”. In: Multimedia Tools and Applications 79 (2020), pp. 4989− 5002.
- Fred Cohen. “A cryptographic checksum for integrity protection”. In: Computers & Security 6.6 (1987), pp. 505−510.
- Haddad, H., Obeid, A., & Zantout, R. (2020). Supply chain optimization using blockchain technology: A systematic review. Journal of Cleaner Production, 259, 120883.
- Mohapatra, S. K., Padhy, R., & Biswal, M. P. (2020). Blockchain in supply chain management: A comprehensive review. Journal of Cleaner Production, 256, 120428.
- Lu, J., Lin, Z., Huang, J., & Gao, J. (2020). Application of blockchain technology in supply chain management: A comprehensive survey. Journal of Industrial Information Integration, 17, 100123.
- Shi, W., Hao, S., & Shen, Y. (2021). A blockchain-based secure and efficient supply chain finance scheme. IEEE Transactions on Industrial Informatics, 17(2), 1327-1335.
- Mofokeng, T., van der Merwe, A., & Visser, J. K. (2021). Blockchain-based food supply chain traceability: A review of implementation challenges and opportunities. Sustainability, 13(1), 197.
- Kouhizadeh, M., Sarkis, J., Govindan, K., & Abbasi, M. (2021). Blockchain technology for improving traceability in logistics processes: A case study in the automotive industry. Transportation Research Part E: Logistics and Transportation Review, 153, 102227.
- Huang, Y., Qian, Y., Chen, H., & Lu, Y. (2021). Blockchain technology in transportation and logistics: Applications, challenges and future perspectives. Transportation Research Part E: Logistics and Transportation Review, 150, 102205.
- Li, X., Liu, L., & Shao, S. (2019). Blockchain technology in supply chain management: A review. International Journal of Production Research, 57(7), 2119-2135.

- Joan Daemen and Vincent Rijmen. “A survey of hash functions”. In: IEEE Trans- actions on Computers 51.7 (2002), pp. 917−929.
- Joe Kilian. “A survey of digital signature schemes”. In: ACM Computing Surveys (CSUR) 30.1 (1998), pp. 31−96.
- Mohammed A AlZain, Ben Soh, and Eric Pardede. “A new approach using re- dundancy technique to improve security in cloud computing”. In: Proceedings Ti- tle: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec). IEEE. 2012, pp. 230−235.
- S Sathiamoorthy, J Li, and K Gopalan. “Erasure coding for data integrity in cloud storage”. In: International Conference on Information and Network Technology. IEEE. 2010, pp. 1−6.
- X Chen, Y Tian, and Y Li. “Data replication techniques for ensuring data integrity in cloud computing”. In: IEEE Transactions on Services Computing 8.2 (2015), pp. 243−255.
- Ali Vatankhah Barenji et al. “Toward blockchain and fog computing collabora- tive design and manufacturing platform: Support customer view”. In: Robotics and Computer-Integrated Manufacturing 67 (2021), p. 102043.
- Shreshth Tuli et al. “Fogbus: A blockchain-based lightweight framework for edge and fog computing”. In: Journal of Systems and Software 154 (2019), pp. 22−36.
- Gbadebo Ayoade et al. “Decentralized IoT data management using blockchain and trusted execution environment”. In: 2018 IEEE International Conference on Information Reuse and Integration (IRI). IEEE. 2018, pp. 15−22.