

Ensure Security in Supply Chain with Blockchain Technology

by

Fairuz Tarannum
18101199

Nazibun Nafiz
18101109

Sumaya Khanam
18301278

Wasy Tabassum
18201048

Rudaba Adnin Kamor
18241004

A thesis submitted to the Department of Computer Science and Engineering
in partial fulfillment of the requirements for the degree of
B.Sc. in Computer Science

Department of Computer Science and Engineering
Brac University
September, 2022


© 2022. Brac University
All rights reserved.

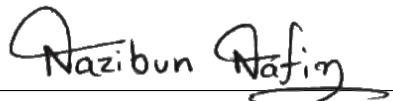
Declaration

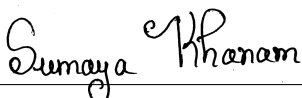
It is hereby declared that

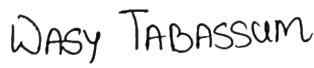
1. The thesis submitted is our own original work while completing degree at Brac University.
2. The thesis does not contain material previously published or written by a third party, except where this is appropriately cited through full and accurate referencing.
3. The thesis does not contain material which has been accepted, or submitted, for any other degree or diploma at a university or other institution.
4. We have acknowledged all main sources of help.

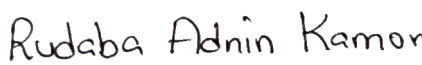
Student's Full Name & Signature:


Fairuz Tarannum
18101199


Nazibun Nafiz
18101109


Sumaya Khanam
18301278


Wasy Tabassum
18201048


Rudaba Adnin Kamor
18241004

Approval

The thesis titled "Ensure Security in Supply Chain with Blockchain Technology" submitted by

1. Fairuz Tarannum (18101199)
2. Nazibun Nafiz (18101109)
3. Sumaya Khanam (18301278)
4. Wasy Tabassum (18201048)
5. Rudaba Adnin Kamor (18241004)

Of Summer, 2022 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science on September, 2022.

Examining Committee:

Supervisor:
(Member)



Mr. Moin Mostakim
Senior Lecturer
Department of Computer Science and Engineering
Brac University

Thesis Coordinator and Co-Supervisor:
(Member)

Dr. Md. Golam Rabiul Alam
Associate Professor
Department of Computer Science and Engineering
Brac University

Head of Department:
(Chair)

Sadia Hamid Kazi, PhD
Chairperson and Associate Professor
Department of Computer Science and Engineering
Brac University

Abstract

Supply chain essentially means the network between the suppliers and distributors to produce and distribute products to the final consumers which comprises various activities, entities, databases and responsibilities. In this era of industrial revolution and computerized technology, industries are bound to incorporate modern and digitized versions of management systems to stay shoulder to shoulder with their competitors. Our goal is to modernize every step of the supply chain with implementation of blockchain technology so that there is almost no delinquency found in the whole operational flow. With the growth of new markets globally, companies need to be cautious if their current supply system is capable enough to fortify possible obstacles like counterfeit cash transaction, costly and inefficient data sharing, lack of source-to-store traceability, distrust among participants, little to no transparency, need of real time database system and unavailability of authenticated communication. Blockchain is an innovative and robust technology that has been proved to be very promising in increasing the efficiency of supply chain operations by enhancing customer service, removing trust issues or having to deal with suspicious stakeholders. The trick is to make all the entities use a shared and secured data record which amplifies transparency during transaction and reduces waste and cost. Many Global companies like IBM and Walmart are already bringing their whole supply chain system under the control of Blockchain. Our vision is to bring this development to the Bangladesh markets and automate the supply chain system which will be powered by blockchain. We have developed a full system including a client side application powered by Ethereum smart contracts where tasks will be automatically checked off after successful transaction, advanced shipment and distribution of products will be ensured and data will be managed transparently in every movement. Our aspiration is to explore all possible ways to maximize satisfaction in the supply chain management in Bangladesh so that we can cope up with global technology.

Keywords: Blockchain; Ethereum; lifecycle

Acknowledgement

Firstly, all praise to the Great Allah for whom our thesis have been completed without any major interruption.

Secondly, to our advisor Mr. Moin Mostakim and our co-advisor Dr. Md. Golam Rabiul Alam sir for their kind support and advice in our work. He helped us whenever we needed help.

And finally to our parents without their throughout support it may not be possible. With their kind support and prayer we are now on the verge of our graduation.

Table of Contents

Declaration	i
Approval	ii
Abstract	iii
Acknowledgment	iv
Table of Contents	v
List of Figures	1
1 Introduction	2
1.1 Research Problem	3
1.2 Research Objectives	4
2 Background Study	5
2.1 Blockchain	5
2.2 Idea of Logistics for Blockchain Technology	7
2.3 The architecture of the blockchain platform and how it works	9
2.4 Traditional Supply Chain Management	10
2.5 Blockchain Technology Integrated with Supply Chain	13
2.6 Smart Contract	15
2.7 How Smart Contracts Work	16
2.8 Challenges in implementing smart contracts	17
2.9 Templates and Parameters of smart contracts	17
2.10 Private and Public Key Generation	18
3 Literature Review	20
4 Methodology	25
4.1 System Overview	25
4.2 Proposed Model	27
4.2.1 Shipment	29
4.2.2 Distribution	30
5 Building The Application Powered By Ethereum Smart Contract	31
5.1 Building The Application Powered By Ethereum Smart Contract	31
5.1.1 Works that have been done so far	31
5.1.2 Smart Contract Implementation	31

5.1.3	Task Brief	31
5.1.4	Installing Dependencies, building the application and test . . .	32
6	Conclusion	39
	Bibliography	42

List of Figures

2.1	Proof of Work blockchain mining process	9
2.2	Flow of Blockchain Operation	10
2.3	Traditional vs Blockchain powered Supply Chain Management	11
2.4	The worldwide supply chain is made up of several transportation and logistical linking suppliers, manufacturers, and distributors.[4]	12
2.5	Cost savings due to blockchain in cross-border payments	14
2.6	How Smart Contract Works	16
2.7	Template, agreement and parameters.	18
2.8	Asymmetric Cryptography	19
3.1	Supply chain architecture based on blockchain technology	21
3.2	Template and agreement of smart contract	22
3.3	A transaction that transfers a tokenized asset (X) among users	22
3.4	Blockchain transformation phases.	23
3.5	Blockchain technology for supply chain	24
4.1	Flow of work	25
4.2	Secured transaction platform	26
4.3	Real-time tracking system	27
4.4	Suggested Framework	28
5.1	Private blockchain network Ganache	32
5.2	Metamask Wallet	33
5.3	Installing dependencies	34
5.4	Project Directory	34
5.5	Client view of application	35
5.6	Test passes(1)	36
5.7	Test passes(2)	37
5.8	Test passes(3)	38
5.9	Task being checked off	38

Chapter 1

Introduction

The expeditious response for the manufacturing industry and the supermarket company's effective consumer feedback can indeed be connected as the roots of the supply chain spirit. The entire supply chain process is rapidly being studied by a number of businesses from assorted industries. This section will work for the development of the supply chain as well as several given properties. The significance of collaboration within an external side of an organization has been acknowledged by companies since the 1980s, when supply chain management first achieved mist. Marketing is cognizant of that without the cooperation of their producers or even other supply chain competitors, they cannot effectively compete anymore. [29]. A supply chain is a thorough system for producing and delivering a product or service, computing the initial step of acquiring raw materials through the ultimate delivery of the good or service to end-users.

Supply chain managers face issues every day that demand for quick response and action. Variables affect these difficulties complexity and degree of intensity. There are several effective ways to address supply chain challenges and they range in complexity and seriousness. Regardless of the year, supply chain managers face a variety of challenges. Given the emphasis focused on strong and dependable supply networks today, such issues are becoming ever more pressing. Since proper corporate operations depend on efficient supply chains and also any issues will unavoidably have an impact on the front line. Monitoring client expectations, supervising suppliers, ensuring quality and long-term viability along with data access are a few of the critical problems that supply chain managers should deal with [1]. The framework and design of the supply chain are sophisticated in all industries. All sectors must improve their supply networks in order to boost production and revenue. Innovative approaches to improve supply networks are promised by new technologies. The use of blockchain in the supply chain has the potential to be negligible when we want to minimize administrative costs for ensuring forthrightness and legality. It can aid players in running a better supply chain by storing price, date, location, quality, certification, and other important data. The accessibility of this data within the blockchain can enhance material supply chain traceability, decrease losses due to fake goods and the gray market, increase visibility and compliance with regard to outsourced contract manufacturing, and could enhance a company's position as a pioneer in moral manufacturing. Smart contracts are nothing more than computer programs that execute when logical conditions are met and are stored on a

blockchain. They are frequently used to automate execution so that all parties comprehend the consequences without a need for an intermediary or any unnecessary time wastage. Furthermore, they can automate a workflow by operating on to the next phase if a set of logical conditions are satisfied. On the other hand, digital transactions can improve Bangladesh's overall security management, which is still mostly lacking.

1.1 Research Problem

As supply chain networks have become more and more widespread in the global economy, multiple bottlenecks have diminished the whole production process creating questions like; why are store shelves half empty? Why is the production of goods getting expensive day by day when we should cut back its costs? Why are the deliveries taking longer than they should? Why are customers not being able to buy what they want at the time of emergency? These factors are affecting the global network of manufacturers, suppliers, distributors, retailers, transport companies who work harmoniously to transport goods to the consumers doorstep. In short, there are so many steps from the product being prepared, to reach the final customers that it leaves plenty of opportunities to slow down the process, cascading arrays of problems for companies, vendors, agents and brokers [32].

Supply chain, already being a complex system, is getting more tangled with evolving customer requirements, geographically competitive environment, deploying new business models and so on. Moreover today's old technologies on which most supply chain managements depend on, has little to no capabilities to provide adequate security, manage risk factors, reduce production cost or even keep up with rapidly changing market necessities as they have shortage of real time tracking, digitized database, transaction transparency and many other shortcomings [22].

If we concentrate on security measures, handling and maintaining legal contracts have become a major complication on the way of coordinating with all the suppliers and stakeholders and gaining their trust. Lack of a secured transaction environment and failure to detect organizations that are involved in transporting duplicate products have also crippled the wheel of production and delivery [27]. Eventually customers will lose their trust in the companies which do not have proper quality control measures and stop using their product which will completely destroy a business and the sub-companies involved with it.

Our proposed system will bring about revolution in the environment of the industrial ecosystem. Blockchain based distributed ledger technology platforms have tremendous potential to change the nature of business globally, by growing consensus among business leaders and entrepreneurs and modifying business from accounting to operation [16]. Blockchain technology will ensure dynamic and fluid value exchange, transparency with pseudonymity, irreversibility of records, provide security and modern cryptography, reduce fraudulent activity, manage system risk, cut down transaction and transportation cost [27]. Blockchain portrays a promising future in 3 the performance of the supply chain of industries compared to many other methods applied so far.

We deployed a client side application powered by smart contracts which will enable people to enforce contractual business promises without human involvement. Pre-defined contract terms such as interest rate, payment method, currency rate, obligation and settlements are stated in the smart contract which is determined by the counterparties involved in the business transaction. Electronic scripts have the custody of all assets involved in a transaction [2]. Smart contracts, having no involvement of a third party, can eliminate the chance of error and manipulation and strengthen trust among business partners by ensuring automatically carried out terms.

1.2 Research Objectives

The research objective targets relevant issues in the supply chain and their respective perceived trends and stating the problem statement. Our objective is to create a full functioning platform for supply chain management whose security is ensured by blockchain technology. The challenges of shared information among every entity and trust issues in the supply chain are driving people towards blockchain technology which has the potential to upgrade the procedure for data exchange and transparency in logistics. The ultimate objective of this research are:

- To understand Supply chain management structure more profoundly
- Try to find solutions of the backdated framework of traditional supply chain like -
 - Safety issues and less transparency
 - Absence Of Collaborative Forecasting [27]
 - Meeting Customer Expectations
- To use the proper potential of the integration of supply chain and blockchain technology

Chapter 2

Background Study

2.1 Blockchain

Blockchain being a decentralized data management system, allows the users to store and exchange value without any third party. It was first designed for Bitcoin. It's a cutting-edge technology with the potential to upend existing economic and social structures and replace old trustless systems. It is based in a distributed ledger technology which verifies and approves transactions using the capabilities of a huge peer-to-peer network [9]. The network has immutable characteristics and users can trace every step of value exchange between parties which makes value exchange transparent. Cryptographic signature of records ensured data and transaction security more powerful. [9]

1. **Flexible value exchange:** The blockchain network is a permanent record of transactions that occur between individuals or between customers and businesses. The type of data kept in blockchain transactions is not restricted to a financial worth, such as the Bitcoin currency exchange, but can also include provenance of products and services, intellectual property rights, user identity data, carbon credits, asset ownership data, position data, and so on. There are various blockchain applications that are still in development. "In addition to transaction data, the blockchain platform can store supplementary state information, which is essentially key-value pairs that determine the state of the system" [31]. This feature of the blockchain value store makes blockchain technology highly adaptable to a variety of industries and applications [31].
2. **Shared control and adaptability:** No single entity or group has control over the blockchain ledger. Blockchain eliminates the requirement for trusted third parties to validate transactions because of its distributed database. It functions as a shared database that serves as a safe, verifiable, and single source of truth for all network members. "In essence, it eliminates the necessity for trust between parties" [11]. It raises transparency and, as a result, system confidence. Furthermore, a distributed database improves productivity by establishing common data formats, allowing for frictionless data sharing and process integrity across enterprises. The audit compliance and risk of error or fraud are improved since the transactions are reviewed in real time by network participants [25].

3. **Scattered Network:** Without the use of a central intermediary, the blockchain network connects individual consumers to businesses. Within the blockchain's mentoring network, the digital payment data is shared in real-time. Every network member keeps a local record of transactions on their computers and sends data to other nodes [11]. It eliminates the need for trusted intermediaries like brokerage firms and centralized authority like banks to exchange value. It also eliminates friction in present transaction procedures by allowing for near-real-time value exchange while lowering expenses. Furthermore, the system is more robust because it eliminates a single point of failure in the event of a breakdown or conspiracy due to huge ledger replication among numerous participant nodes. It increases service quality, dependability, and availability [31], [30].
4. **Transparency combined with anonymity:** Every transaction value is available to every network participant with access permissions, making the blockchain-based transaction system extremely transparent. It makes it exceedingly difficult to carry out illicit transactions. However, while initiating a transaction, a network participant can choose what information about their identity they want to share with the rest of the network. Allowing for anonymity, each participant node in the network is given a digital signature called a private key, which serves as proof of identification and is used to validate transactions. The private key should not be shared with anybody else. It is used to stimulate public interest. For transactions, a key is a string of characters shared with others on the network.
5. **Record's mutability:** A consensus algorithm is used in blockchain to verify a set of transactions and add them to the blockchain as a block. It achieves consensus via the peer-to-peer network's power. A block of transactions is only posted to the blockchain after the majority of network participants have validated it. Any one party attempting to alter the ledger is unlikely to succeed because the modification must be validated by a majority. Additionally, each new block is linked to the preceding block, and when a new block is updated, all nodes in the network receive the most recent copy of the ledger. As a result, altering the prior block would be time-consuming and costly. It makes it difficult to modify records.
6. **Advanced encryption and protection:** To prove node identification and maintain data security, blockchain makes use of public key cryptography and digital signatures. This strategy protects identities and prevents hackers from tampering with data, lowering the chance of fraud or theft. The technique also prevents a single point of failure in the event of a compromise by eliminating centralized third parties [10].
7. **Logical programming:** Because blockchain transactions are digital, they can be linked to criteria specified in code. Only when specific predetermined requirements between the seller and the buyer are met can the computing logic be developed to allow value exchange. It makes it possible to automate, document, and regulate the transaction [11]. In blockchain technology, it is the foundation for smart contracts.

2.2 Idea of Logistics for Blockchain Technology

At many industries, distributed ledger technology remains in the solid evidence stage and there is currently no clear architectural approach. The main goal of the design for a vast scope of blockchain technology enabled application cases is to achieve peer - to - peer, consistent, and efficient operations. The basic operational components and design features of the blockchain technology are listed below.

1. **Ethereum:** Blockchain is essentially a network which stores a group of transactions and related data in a safe and transparent manner. All historical transactions and their values, as well as the time of block generation, are available to network participants at any time. A blockchain is a chronologically organized network of blocks, as the name suggests. Each new block contains information on the addresses that are eligible to receive the exchange value, as well as the preceding block's digital address (hash). If someone tries to change or tamper with transaction information in a block, the hash for that block will be changed, and it will no longer point to the hash of a previously verified block. As a result, blockchain can be audited in near real time, and interfering with records is difficult without reaching network consensus [24].
2. **Public blockchains and Private blockchains:** Anyone connected to the platform can partake in the confirmation extraction and processing and access a copy of the ledger thanks to Blockchain's decentralized and distributed and permissionless design. Nevertheless, because it failed to achieve processing economies of scale, this kind of governance was ineffective. The integrity of the trustless consensus process was compromised by the high probability of a single extraction group obtaining a dominance. Relative to bitcoin or public blockchains, private or permissioned blockchains have a distinct value proposition. Private blockchains work well when the integrity of either the audit trail is still not crucial but there is a need to standardize data sharing across industries for effective operations and a new market structure [24].

In either a transparent or anonymous blockchain, anyone can participate in any capacity. Anyone can approve new blocks throughout the mining process, but in a private or permissioned blockchain, network participation is restricted to a small group of predetermined stakeholders. The network can only analyze or mine data for certain individuals or groups. The cost of networking is still high since private blockchain still depends on trusted partners, despite the fact that it has no verification expenses. [24]

3. **Decentralized database:** The autonomous and secure database provided by blockchain technology is redefining how data is distributed online. The blockchain database allows data to be shared directly from machine to machine, in contrast to the current centralized internet systems like Gmail or Dropbox. Data sharing is rendered more secure and widespread although to encrypted communication protocols, that reduce the risk of data suppression by intermediaries much like administration. The distributed system can be used not only for data management; it can also be used to discreetly facilitate mobile casting for individuals all over the world. Such ballots can be recorded

and verified accurately. Blockchain technology has the potential to be widely used because of its secure and decentralized database [5].

4. **Mining and Authentication protocol:** The authentication mechanism provides a consultation process for confirming transactions and adding new blocks. It is a network security protocol. By guaranteeing data integrity through consensus and making the blockchain based intrusion detection system, it adds to the legitimacy of the blockchain. All miners receive and verify 10 minutes' worth of blockchain transactions thanks to the network's participants. Miners do the computationally daunting task of "creating a block, then constructing new, valid blocks and committing them to the shared blockchain ledger." The miners must engage in a randomization based on their processing power in order to get the chance to add the next to the chain. The miners try to overcome the challenging obstacle, and the first one to succeed broadcasts his achievement to everyone else. A majority consensus of more than 50% is required to accept and append a new block [24]. (See figure 2.1)
5. **Proof of stake:** Due to the high demanded processing power and the rewards-based system, the work verification network protocol is quite expensive for mine workers. In order to mine ledger operations, the blockchain community is migrating from the Public blockchain network protocol to the Proof of Stake network protocol. The proof of stake network protocol determines the miner of the new block in a predictable variety of ways depending on the position as in chain. There is no incentive towards introducing a new block.

The miners are simultaneously obtaining the processing expenses. Whereas less computing is needed when utilizing the proof of stake methodology, it costs less to achieve broad consensus [25]. It may have been possible to mix both different protocols in the future to develop a hybrid Proof of Work and Blockchain protocol in order to solve the issue of centralized control even though stakeholders with sizable stake ownership (in the Blockchain procedure) might endeavor to exemplify a consistency.

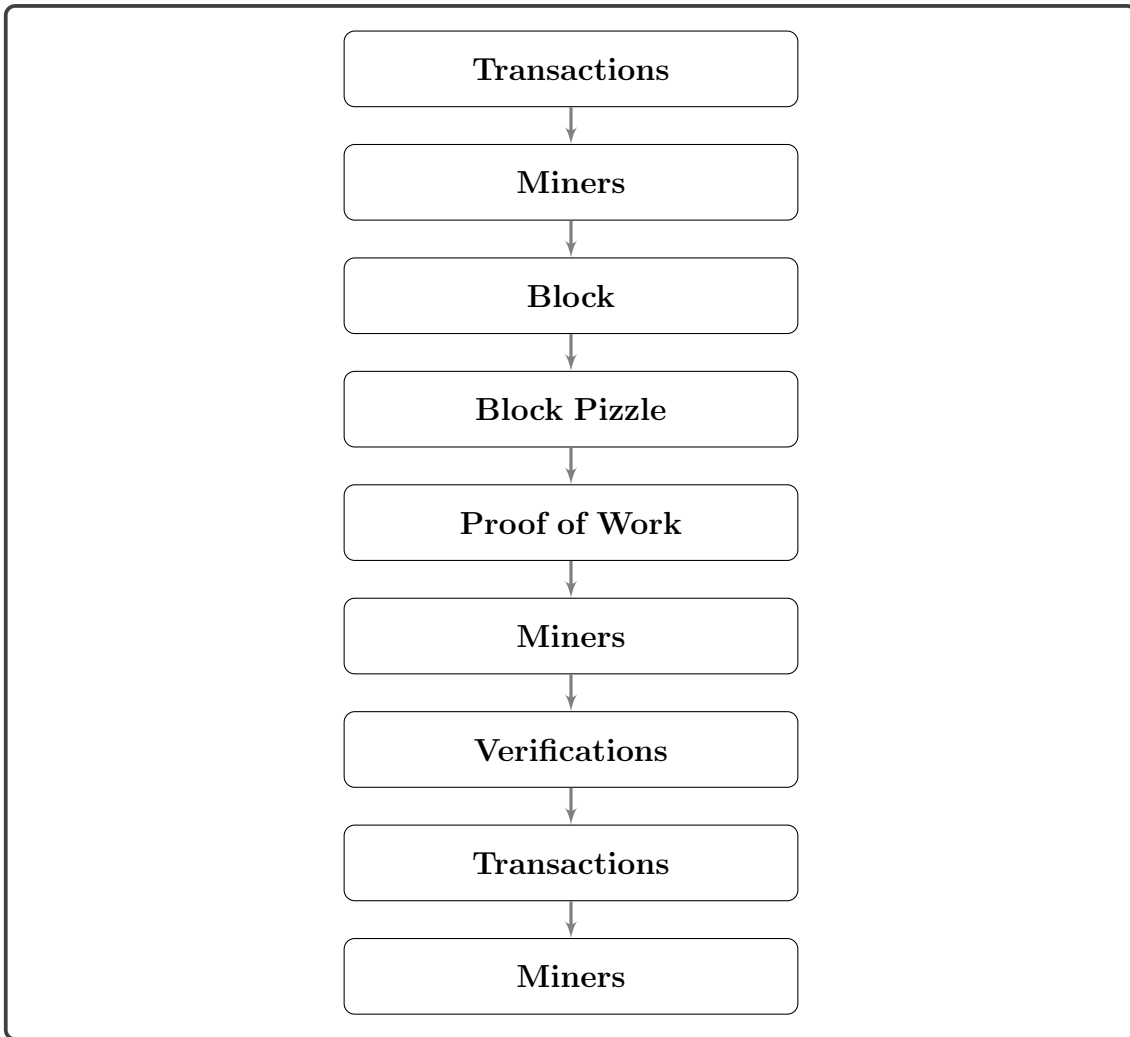


Figure 2.1: Proof of Work blockchain mining process

2.3 The architecture of the blockchain platform and how it works

There are various parts to the blockchain platform architecture. The complexity of the operation flow is increased by the implementation and interaction of various components. The following are the main components of the blockchain architecture: [31]

- The person’s public and private keys are maintained inside the Wallet. The primary interface for said blockchain system is an external system. According to the developers, users may ”suggest and accept encrypted documents that represent interconnected goods exported.” [31].
- On a peer-to-peer blockchain network, the Network Node represents a computer client. It has two ways of participating in transactional activity. It first houses a distributed ledger copy of historical transaction permanent records.
- Records are secure since the ledger, which is a collection all transactions, is duplicated across all nodes. The network is then broadcasted with such

a catalog of all transactions recommended by the wallet, which miners can validate and add as a new block.

- Every minute, a new block is generated by the cooperation framework comprising minors/validators by verifying the broadcasted transactions. A proof of operation issue is a technological riddle that's also incredibly difficult to solve, so miners fight to be the first to solve it. The winner receives 12.5 freshly formed dollars for generating a brand-new block, along with a small processing fee. After the miner uploads and publishes a block with one copy of the ledger, it is propagated all across the network [31].
- The deal is initiated from either a wallet that contains the unique identifier of an individual who initiated the transaction, as according to Farahmand's report, which was reported in the Intel Incorporated Scientific Journal. This operation is validated in the wallet ahead of being broadcast to all network nodes. The validated transaction is delivered to all complete nodes. To ascertain the future statuses of the connected accounts, the transaction is completed and validated (associated with assets). The live blocks of full nodes are where the new account states are kept. A full node is selected to submit their block to the blockchain. The live block is preserved and synchronized in the blockchain at the end of a period [31].

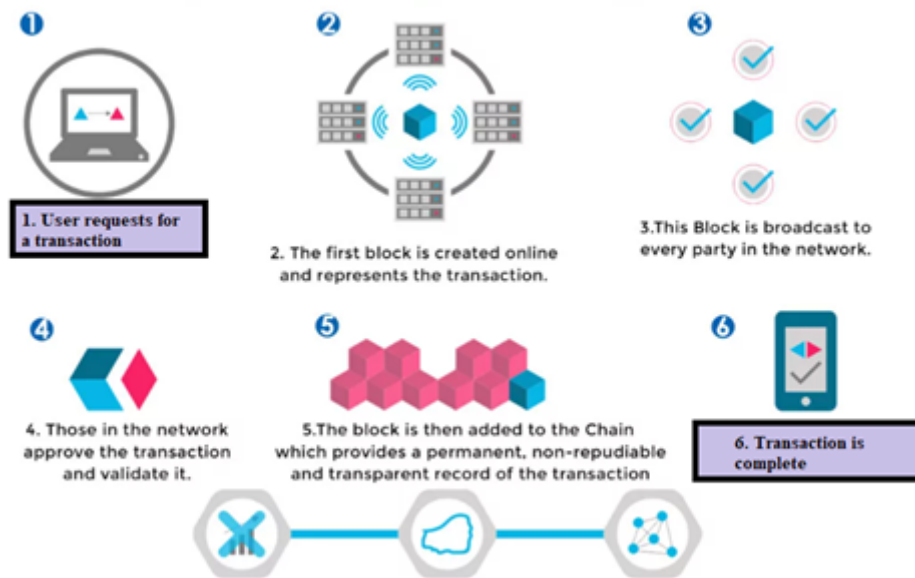


Figure 2.2: Flow of Blockchain Operation

2.4 Traditional Supply Chain Management

The supply chain is a system which connects a company as well as its supplier throughout order to manufacture and distribute a product to a client. It includes a variety of persons, organizations, communication, and asset actions. These initial stages of a supply chain are when materials are collected and acquired. The processes taken to convey a product or service from its originating location towards the

customer are generally referred to as a supply chain. This group contains producers, suppliers, warehousing, transport companies, fulfillment centers, and retailers. The supply chain encompasses all aspects like product design, advertising, administration, transportation, financing, and customer support. There are numerous supply chain links that need knowledge and expertise. The total costs and profits of a business can be reduced through efficient supply chain management. The damaged connection can be costly as well as problematic again for the rest of the chain.

Traditional supply management (SCM) is dispersed that provides a centralized point of control, while a blockchain-based SCM's public ledger allows stakeholders and parties to constantly update and be aware of the SCM's actual situation. A blockchain supply chain can let players record data on the price, date, location, quality, certification, and other pertinent factors so that the traditional supply chain can be managed more effectively. The connectivity of such a data inside the blockchain could indeed improve the tracking of a fabric supply chain, reduce the losses from the gray market and fake goods, increase transparency and conformance over outsourced settlement manufacturing, and conceivably perhaps enhance an organization's role of leader in moral production. Blockchain has a considerable ability to transform supply chain services, ranging from the beginning of the supply chain to re-engineering company operations for improved security and greater stability. Traditional SCM

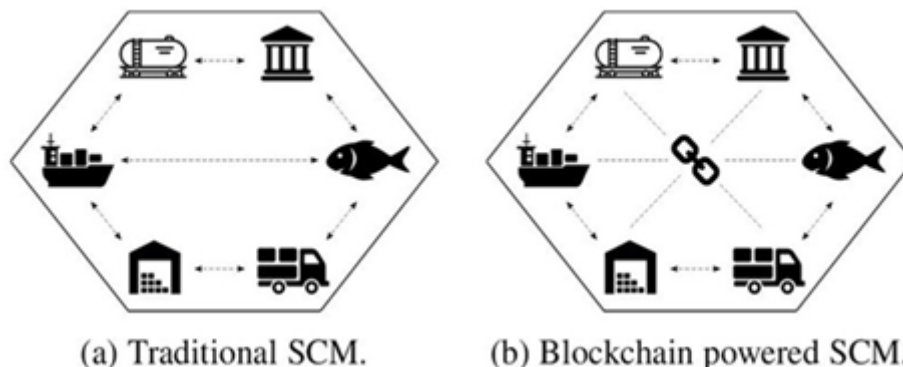


Figure 2.3: Traditional vs Blockchain powered Supply Chain Management

is driven by organizing, evaluating, executing, reporting, forecasting, and anticipating potential requirements based on past and present objectives and stakeholders in order to deal with any modifications, lags, or defects. Conversely, improving distribution networks, especially big chain lengths, can frequently be a technical problem. The supply chain shown in Figure 2.3 is the same for sources from all over the world. This supply chain is a broad, intricate structure with numerous sites for sourcing, manufacturing, and distribution.

Additionally, a multitude of methods of transportation will be provided to connect these objects together again and form a connected system. The traditional supply chain is highly complex due to the constantly changing client expectations, which further increases the hurdles and issues that arise. In contrast, the supply chain will encounter a variety of risks, such as supply interruptions, fluctuating global commodity prices, and more. The supply chain encounters some challenges as a result of its complexity [4]. The supply chain faces certain difficulties due to its complicated



Figure 2.4: The worldwide supply chain is made up of several transportation and logistical linking suppliers, manufacturers, and distributors.[4]

nature.

1. Lack of transparency and productivity in supply chain management

All participants' activities are becoming increasingly less "accessible" when there are more partners and operations in the wide system of supply chains. Since transparency refers to the network's shared access to information about the supply chain cycle, it is essential in a supply chain network. When data is sent between crucial parties and when data is lost or distorted for whatever reason, this network suffers from a major lack of transparency. Traditional supply chains are paper-intensive, making transparency difficult to develop and maintain.[2]

2. Trust in SCM is a source of concern

Many stakeholders are involved in the supply chain, which has a complicated processing chain that is strongly embedded in the physical world and is unable to respond to changing market needs efficiently and cost-effectively. A strong foundation of trust among the network's participants is required for a successful supply chain network. For inspection and evaluation, participants must rely heavily on external brokers, which raises operating expenditures and reduces effectiveness.

3. Product efficiency and security cannot be tracked in SCM

The supply chain system includes tasks including manufacturing, staff and inventory management, logistics, and sales. Customers want to know how the things they're buying are made, including the manufacturing process, location, raw material production, activities, supplier details, and quality assurance and detection of any internal problems. They are, however, unable to monitor the efficiency of all processes at any one time or location. As there were no internationally connected platforms, consumers were unaware of their products' existence, raising worries about product safety across the supply chain.

4. **SCM monitoring is insufficient in real-time**

The supply chain would be confronted with a variety of risks as a large-scale, dynamical interaction, including supply disruption and changes in the cost of raw materials globally. As a result, having access to all real-time operations activities is a crucial source of confidence among many stakeholders. Therefore, monitoring the entire product lifecycle in the supply chain network is essential.

5. **Managing and administering contractual agreements in supply chain**

It is impossible to physically maintain all types of contracts, such as financial contracts, ownership certificates, and business contractual arrangements. The legal staff may experience difficulties in safely sending documents to certain other participants.

6. **Coordination and transaction issues in SCM**

Because of the inaccurate information in SC, coordination and transaction concerns arise, eroding trust among SC partners. As a result, a platform should be established, consisting of a database for recording transaction information that enables two parties to conduct direct transactions utilizing their distributed ledgers without the need of a centralized third party, resulting in more transparent transactions.[26]

2.5 **Blockchain Technology Integrated with Supply Chain**

Blockchain adoption is expanding as numerous businesses and startups work together to develop and test proofs of concept for diverse use scenarios. Blockchain technology enhances therapeutic potential, profitability, and confidentiality in multiparty commercial activities like supply chains through fine-grained security jurisdiction of the decentralized system. Right now, anyone who retains their separate interpretation of events in their respective compartments. These are typically redundant and inconsistent with the scenario at hand. The ledger optimizes profitability by having an appropriate electronic record and higher product characteristics, accelerates interaction between stakeholders by eliminating lag time and facilitating integration, and leads to better performance by distributing uniform data layouts. Blockchain adoption is increasing as numerous businesses and startups work together to develop and test proofs of concept for diverse use cases.

1. **Decreased transaction costs:** Catalini and Gans illustrate how transaction verification and networking for the value exchange of services in a dynamic ecosystem are affected by blockchain technology in relation to two crucial costs. Blockchain does away with the role for intermediaries in the resolution of dispersed activities. Verification packages are provided by these intermediaries. Using blockchain technology in cross-border payments will eliminate the requirement for third-party financial institutions, cutting bank transaction costs. The cost of networking is reduced by combining the blockchain

ledger with tokens, allowing the creation of a decentralized marketplace to be crowdfunded. Individuals are motivated to commit resources to the platform's growth by the tokens. It eliminates the need for an expensive central actor to build and manage the platform. Individuals are motivated to commit resources to the platform's growth by the tokens. It eliminates the need for an expensive central actor to build and manage the platform.

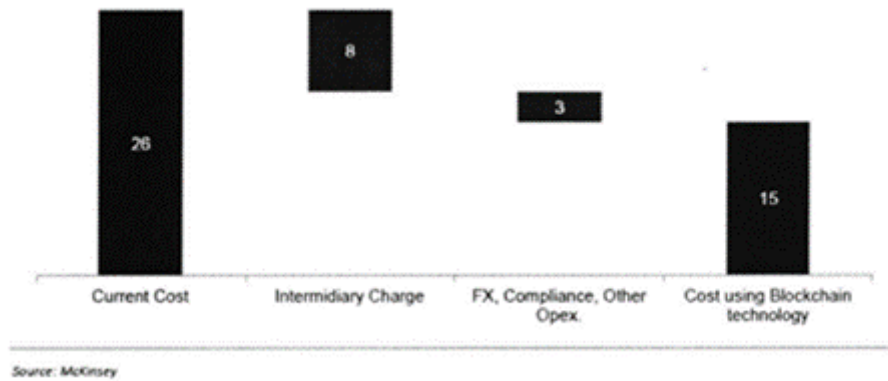


Figure 2.5: Cost savings due to blockchain in cross-border payments

2. **Fraud reduction:** User-initiated transactions can be rigorously verified using blockchain technology. The user's identity is checked each time a transaction is initiated, letting the transaction proceed if the user is eligible. Blockchain increases privacy while minimizing fraud risk. Furthermore, thanks to blockchain-based digital transaction verification, the quality of items and services provided may be tracked. It makes it easier to validate the features, lineage, stability, or existence of any property held on the blockchain as a currency, providing its trustworthiness, possession demonstration, and authenticity. In a nutshell, blockchain technology helps existing intermediaries reduce fraud by providing verification services.
3. **Distributed resilience and control:** No one corporation or agency has influence over the blockchain database. Blockchain does away further with stipulation for purchasing guidelines by authorized external parties due to its distributed database. Through the removal of the need for trust, it fosters trust between parties. It raises transparency, which strengthens the legitimacy of the system. A distributed database also boosts efficiency by providing standardized data formats that facilitate data sharing and process integrity across businesses.
4. **Transparency:** Every network member with access permissions has access to every transaction value, making the blockchain-based transaction system incredibly transparent. It makes carrying out illegal transactions extremely tough. A network participant can choose what information about their identity they want to disclose with the rest of the network before starting a transaction, allowing pseudonymity. To do this, each network participant is issued a private key, which acts as proof of identification and is used to validate transactions. Nobody else should have access to the private key.

5. **Programmable logic:** Blockchain transactions can be connected to criteria described in code because they are digital. The computing logic to support value exchange can only be built when precise pre-defined requirements. Transactions become digitized, recorded and regular because of this foundation.
6. **Security with cryptography:** Blockchain safeguards identities and prevents data manipulation, reducing the risk of fraud and theft. In the case of a breach, the approach also eliminates a single point of failure by eliminating centralized third parties.

2.6 Smart Contract

A contract is a reciprocal deal involving two or more parties in which one party promises to execute a certain task in exchange for a desired benefit. This promise is a written commitment in particular words that is legally enforceable as a binding legal understanding. Contracts have always been an important part of managing commercial relationships since they define the terms and conditions under which transactions are conducted. To buy products or services, customers must agree to these conditions. The consumer has faith that the online retailer or platform will provide honest services in return for their investment. Contrarily, the merchant depends on the financial institution or credit card provider to assume the risk of missed payments. The level of authentication for both stakeholders towards this value exchange is quite limited. The payment process is premised on the client's payment history and the trader's company reputation, each of which is validated by an unbiased person or entity. All stakeholders may seek settlement through the civil system's judiciary in the event of a breach of agreement or confidence. This pledge is a deal that is made in writing and is enforceable at law as a contractual contract. Agreements have traditionally played a significant role in the administration of professional activities since they specify the policies and terms under which trades will occur. Customers must accept these policies in order to purchase goods or services.

A smart contract is a compilation of pledges represented in electronic information, as well as the methods through which the counterparties implement agreements legally, computer scientist Nick Szabo coined the phrase "smart contract" in 1996. Smart contracts are cryptographically signed business terms negotiated upon by two or more parties, with the details of the agreement in coding language. The smart contract is "smart" because it can independently self-execute comprehensive and multi transactions, which is beyond the scope of any individual entity. The settlement procedure is sped up, computerized, and made simpler. Additionally, it compromises the credibility of business alliances and equalizes all stakeholders in the globalized era. On this distributed blockchain ledger, which offers an immutable operating system, smart contracts are created. Everyone on the network is able to audit the tamper-proof chronological records and examine the equivalent documentation of the smart contract's movements. It promotes transparency in the veracity and moral fiber of smart contracts.

2.7 How Smart Contracts Work

The main objective of smart contracts is to advance a market-driven economy by empowering individuals to do transactions with outsiders without the intervention of credible external parties. By integrating assets into blockchain transactions using programmable logic, contractual promises can be verified and settled without the need for human involvement.

1. **Predefined terms of contract:** A commercial transaction's counter parties agree on the desired results for each side. Variable interest rate, payment currency, currency rate, and other terms are specified. There are additional restrictions and settlement directions. Smart contracts are put in charge of both the digital and tangible properties associated with a deal by developing digital scripts. These smart contract scripts are recorded at a specific address in the blockchain. When the contract is launched on the blockchain, this address is determined.
2. **Events:** A transaction started by any party or any external feedback obtained might be considered an event. The smart contract is executed on the blockchain when an event defined in the script occurs.
3. **Execute and value transfer:** On the shared, duplicated, and unchangeable blockchain ledger, the smart contract is performed. The transfer of value is dictated by the contract's predefined terms. When an event occurs, a transaction is delivered to a predefined address, and the script's clauses are implemented.
4. **Settlement:** The asset's values are resolved by making appropriate transfers to the intended receivers. The transfers are authorized by agreed terms. The blockchain ledger, essentially acts as a traceability and irrevocable legal record, refreshes when affiliated participants' accounts do. On the network, transactions involving virtual currencies like bitcoins are immediately processed through wallet transactions. Account adjustments on the ledger would be in compliance with off-chain resolution requirements for assets handled off-chain, such as stocks and currencies. The blockchain ledger may need to be watched closely by legislature like policymakers and supervisors. It would help the documents to be harmonized.

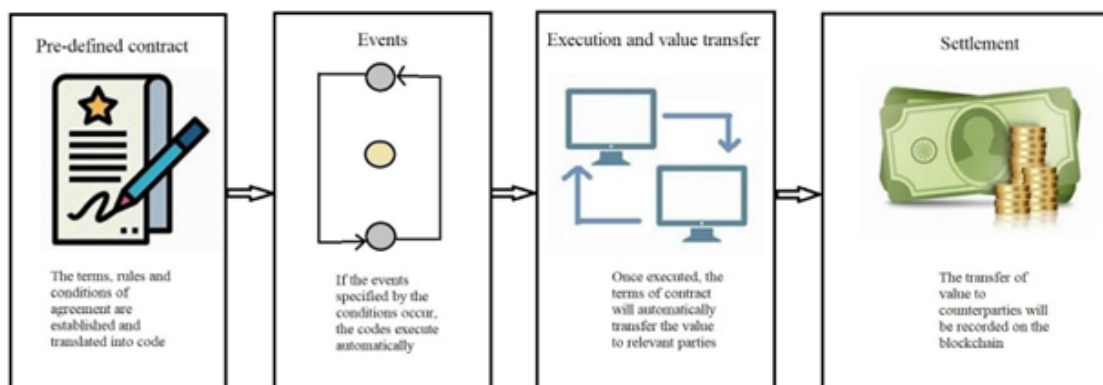


Figure 2.6: How Smart Contract Works

2.8 Challenges in implementing smart contracts

Although smart contracts have certain favorable circumstances, significant technical challenges need to be solved prior to them being extensively used. Some of the challenges are described below:

1. **Complex business ecosystem:**

For smart contracts to operate precisely and consistently within a given time frame, all control operations carried out by the code must be embedded into the same platform. Due to functional or physical limitations of the platform, certain actions might not always be successful. Strict oversight is necessary to accomplish the value exchange. Second, it can be challenging to recognize all contract conditions discussed at the beginning of a business deal due to the complexity of the industry. Contracts are frequently inaccurate in the actual world, and situations change after an agreement, necessitating contract amendment. Smart contracts lack procedures that allow parties to update their contracts even when both sides agree.

2. **Threat of hacking:**

The security concerns with the code are the major obstacle to the widespread use of smart contracts. A \$53 million sum was stolen from the coffers of the DAO, a venture capital fund based on blockchain technology. Modifications to the programming were needed in order to recover the cash. The DAO has portrayed itself as a smart contract that is created from irreversible computer code and operates independently of outside interference which also has the potential to slow down the network, disrupt operations, and, worst of all, result in significant financial losses. Because blockchain transactions are difficult to reverse, users have more faith in the blockchain record.

3. **Contract Code:**

The contemporary business infrastructure would need to change fundamental responsibilities in order to employ smart contracts in real commercial settings. Administrators must either begin to recognise such codes themselves or focus exclusively on a foreign entity to do so, much as lawyers must learn how to write contracts in a software program. It can require more time and be complicated for legal practitioners without previous programming abilities to develop and authorize a smart contract. The new smart contract enabled contractual relationship model differs from traditional contract law and dispute resolution concepts. Before the generation of smart contracts can become easier and more reliable, significant progress in web application development will be required.

2.9 Templates and Parameters of smart contracts

Conventional blueprints known as "smart contract templates" serve as the basis for intricate, mandatory contracts for corporate bonds. Extensive sets of necessary pa-

perwork may be bolstered with the characterization of design parameters that are crucial for regulating the functionality of the smart contract script.

A template is a digital representation of a legal instrument that has been made publicly available by a standards organization, such as the International Swaps and Derivatives Association (ISDA).

An agreement is a fully-functional blueprint that includes any custom legal document and conditions. At this point, legal documents and parameters are frequently customized as a result of negotiations between the parties. An agreement's legal text and parameters will be generated from the template but need not be similar.

Three factors may make determining the set of code parameters more difficult:

1. Texts usually contain parameters; these parameters are typically spatially recognized with the aid of an UI.
2. A few of the materials specified in the contract as "parameters" might not have an impact on how the smart contract code works and hence wouldn't be procured.
3. There are instances where a parameter can be declared, given a quantity, and then utilized.

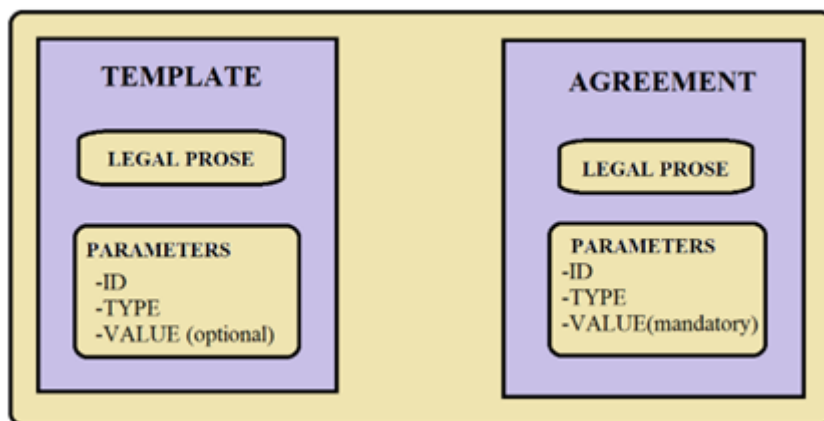


Figure 2.7: Template, agreement and parameters.

2.10 Private and Public Key Generation

Asymmetric cryptography is used to design public and private keys. It allows users to digitally sign operations in order to confirm their legitimacy. It will be clear how and why it is more reliable when opposed to traditional symmetric cryptography. To begin, symmetric cryptography encodes a piece of data that can also be decoded using a key. The receiver must have the key to decode the information in order to send it. However, sending the key over the internet poses a security risk. In asymmetric cryptography, encoded script can be decrypted using both public and private keys. The private key can be linked to a password that the user shouldn't divulge, and

the public key to a widely known username. This key pair can also help us send payments to specific instances, protecting the information from being detected by other nodes. The way it operates is that a piece of information or data can be opened by the public key if it has been hashed by the private key, and likewise. This process is employed to generate a digital signature that enables other nodes to confirm that the information's sender and writer are identical. As a result, since everyone has a copy of the public address, any node can confirm any transaction. The only nodes that will be capable of verifying and deciphering the data, however, will be those to which we employ this mechanism to send transactions.

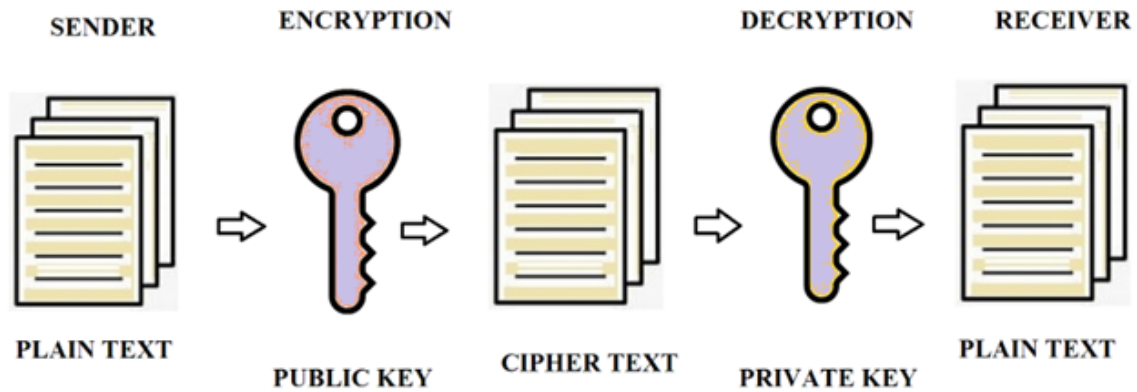


Figure 2.8: Asymmetric Cryptography

Chapter 3

Literature Review

As blockchain technology is getting prominent day by day, people started to see why moving to this decentralized network will benefit them in every possible way. Already carpooling companies like Lazooz and ArcadeCity are operating solely based on blockchain infrastructure where only peer-to-peer interactions between drivers and passengers are required without any third party involvement. Today's tech giants like Facebook, Uber, Google, Twitter, Airbnb are moving their traditional platform towards decentralized shared economy by deploying various distributed social networks applications like Synereo, Akasha or Steem.io into blockchain [12] Multinational retail corporations like Walmart have moved their entire ecosystem of food supply towards blockchain for better traceability, immutability, and transparency. Walmart collaborated with IBM to create a system on Linux Foundation's Hyperledger Fabric which compels every vegetable supplier to enhance food safety and hold the liability for any sort of unscrupulous behavior [18].

Agarwal [2] resented a model on how blockchain technology will bring about transparency and smoothness in every level of supply chain operation and secure sensitive data of the stakeholders. It documents the timestamps and record of product flow starting from raw materials to end customers. The system is based on a hybrid ledger where a distributed network is applied. Only the stakeholders who are involved in a transaction can access the private ledger where private transaction's information is stored whereas everyone can access the public ledger where tracking information of shipped products and hash value of private transactions are recorded. Hence each node has a copy of the ledger and together they authenticate and verify the security of the database stored in the blockchain. The Figure 3.1 shows their Hybrid model.

Zhang [22] explains how blockchain integration in the supply chain system will revolutionize the entire business environment. The paper portrays the current issues related to supply chain management systems along with the chain architecture of blockchain information including security and transparency, as well as the actual items that can be considered for transactions. While blockchain simplifies the process by eliminating the need for physical identification, it can also be used by miners to perform unlawful transactions (in verifying contracts, not gaining access to the contents). The supply management system in this period is based on brutal stakeholder trust, transparency, obsolete data sharing methods, as well as varied value exchanges with decentralized architecture and logically centralized.

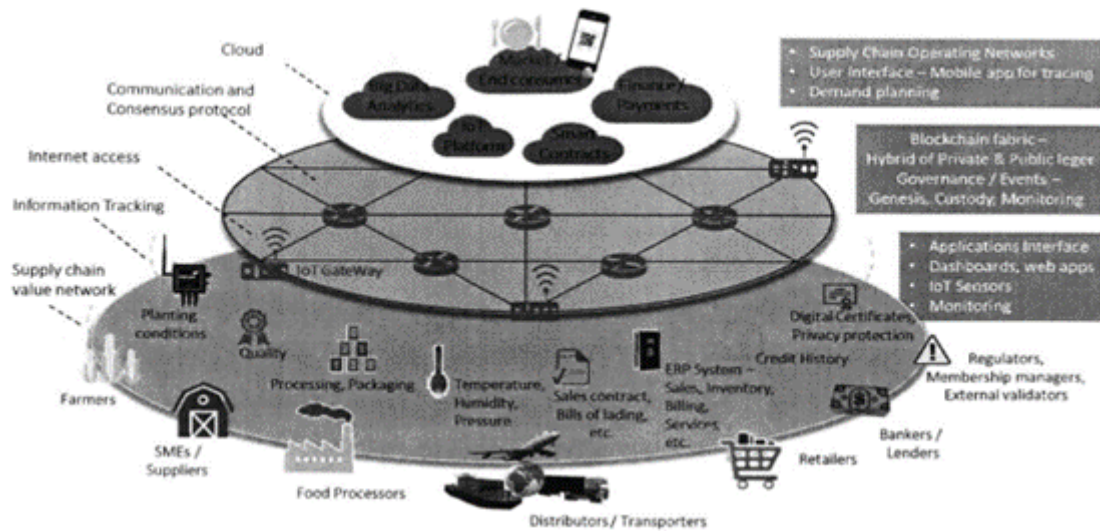


Figure 3.1: Supply chain architecture based on blockchain technology

Korpela et al [13] described how a digital supply chain (DSC) is integrated into blockchain. DSC collaboration is a method of digitizing a multi-partner system in which the main corporations act as a hub for all other companies involved in the supply chain. They used the QFD method to examine how effective blockchain is on supply chain operation which showed that blockchain has a high support mechanism for data integration but cannot solve end-to-end integration through data model even though standard data model is required for DSC integration. Furthermore, they devised the concept of Cloud integration, which will provide a cost-effective business procedure and expand DSC's opportunities.

IPDC has launched the concept of a digitized program dubbed "IPDC-Orjon" for the first time in Bangladesh [21]. Orjon being a large supply chain financing ecosystem program aims at bringing together the stakeholders of any small or micro-business. Their focus is to utilize a shared blockchain database and implement a digital credit program to reduce operational cost and improve loan tracking.

Clack et al [8] provide templates and agreements for smart contracts based on legal documents. They discover operational parameters in legal papers, their design environment, including how parameters are becoming more sophisticated, how common standardized code is being used more frequently, and how long-term research is being conducted. They even proposed a model which is given in Figure 3.2.

El Maouchi et al [15] presented a decentralized, transparent, and traceable supply chain which he named the "TRADE" system where numerous stakeholders can be involved in the supply chain. Customers will also access the database to check their desired items, according to the requirement. Auditability and trustworthiness of the suppliers is also verified and recorded at each step.

Jensen et al [19] TradeLens is built on the IBM Network, which has been built on Ethereum Blockchain in which members ("Trust Anchors") will have to be au-

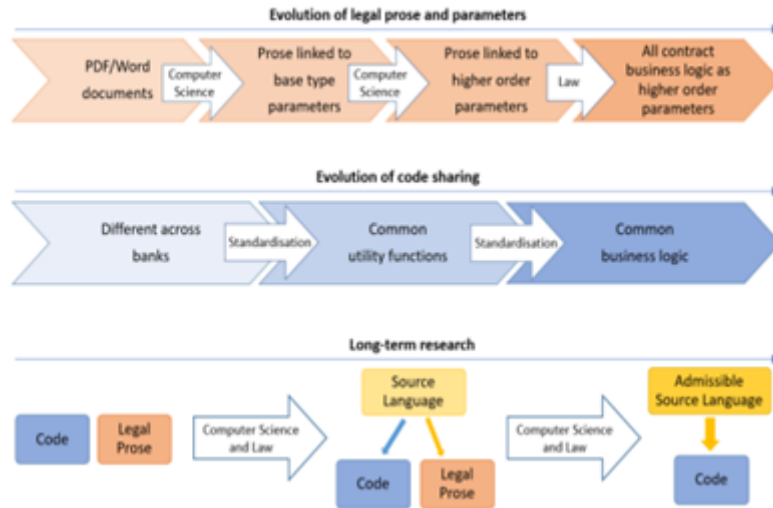


Figure 3.2: Template and agreement of smart contract

thenticated by encrypted fingerprints and are known to the network.

Idrees et al [28] Private blockchain: Because of the small number of participating nodes-consensus occurs quickly-and scalability, which allows the number of nodes to be altered according to demands, private blockchains exceed public blockchains in terms of computation speed. With the aid of smart contracts, McGonagle et al. [17] found that conducting descriptive study required a thorough explanation of the technique used to collect data as well as the methodology for assessing the research evidence.

Christidis et al [7] explored the effect and ease of deployment of smart contracts in a decentralized blockchain platform. Transactions between many parties can still be obtained by a manufacturer who has long exited the network without any user interactions. The "auditable trail of information" is shared inside a single database that may be automated utilizing IoT. However, some disadvantages include the fact that any third party may detect transaction patterns and determine their hash, and hence the identity of the participant. The Figure 3.3 below portrays their framework.

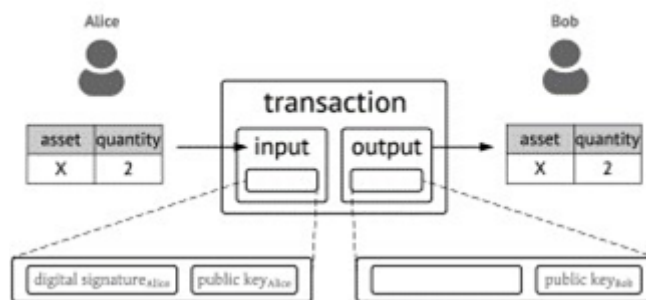


Figure 3.3: A transaction that transfers a tokenized asset (X) among users

Dobrovnik et al [14] stated in his model that the blockchain framework in a supply

chain passes through several (usually four) transformation phases, making it usable despite the assets missing third-party confirmation or verification of ownership transfer. Single-use, localization, substitution, and transformation are the 4 stages shown in Figure 3.4.

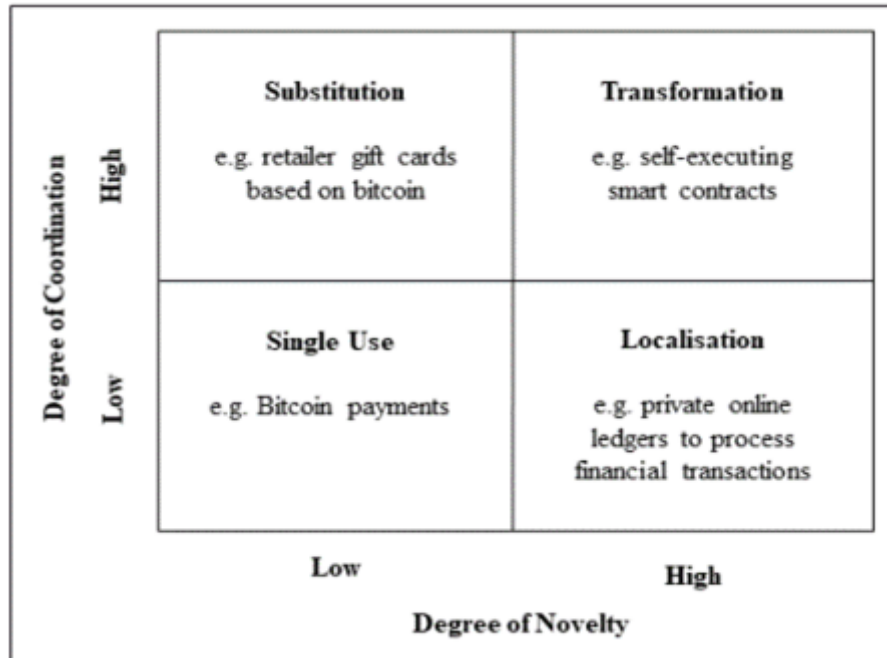
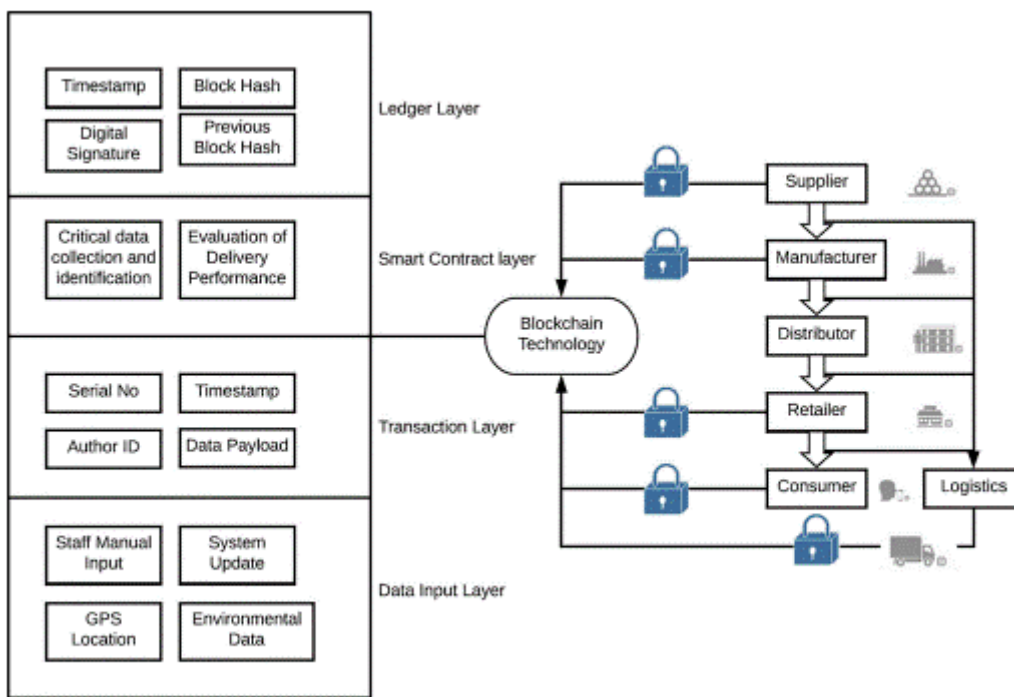


Figure 3.4: Blockchain transformation phases.

Queiroz et al [20] explored the benefits of blockchain in Supply Chain Management (SCM) as well as the obstacles that come with integrating blockchain technology into SCM. They are expected to cause major disruptions and issues across a wide range of businesses. This research focuses on examples of blockchain-SCM integration, emphasizing the need to rethink business structures in order to include blockchain technology. According to Apte et al [6] a blockchain is a decentralized system that maintains an record of online transactions that cannot be manipulated after an occurrence, and blockchain has the potential to completely transform the present supply chain management system. The advantages and downsides are discussed in the editorial.

Dhruman et al [27] suggested that blockchain and smart contracts can solve the problem of having less trust and fear in safely managing legal papers. All legal contracts are securely kept digitally on the blockchain server and are visible to all parties in the supply chain. Through the ownership certificate, it assists manufacturers in gaining faith in the raw material supplied by the source. i.e Automobile manufacturers have access to all ownership certificates for all items used in the manufacturing of a vehicle. Their applied framework is visible in Figure 3.5:

Moradi et al [3] shared: With the fast expansion of computer networks over the last decade, computer security has become a critical concern. In recent years, various soft-computing-based techniques for the development of intrusion detection systems have been developed.



Source(s): Author

Figure 3.5: Blockchain technology for supply chain

Chapter 4

Methodology

4.1 System Overview

Our workflow is shown below at the figure 4.1:

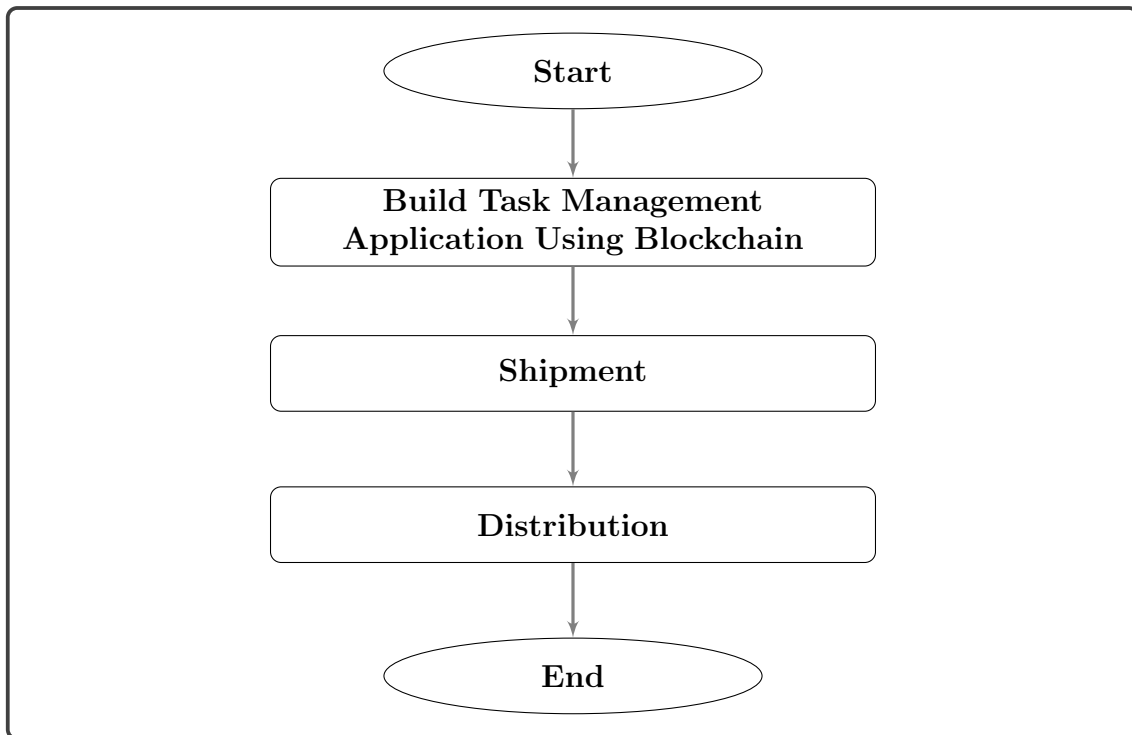


Figure 4.1: Flow of work

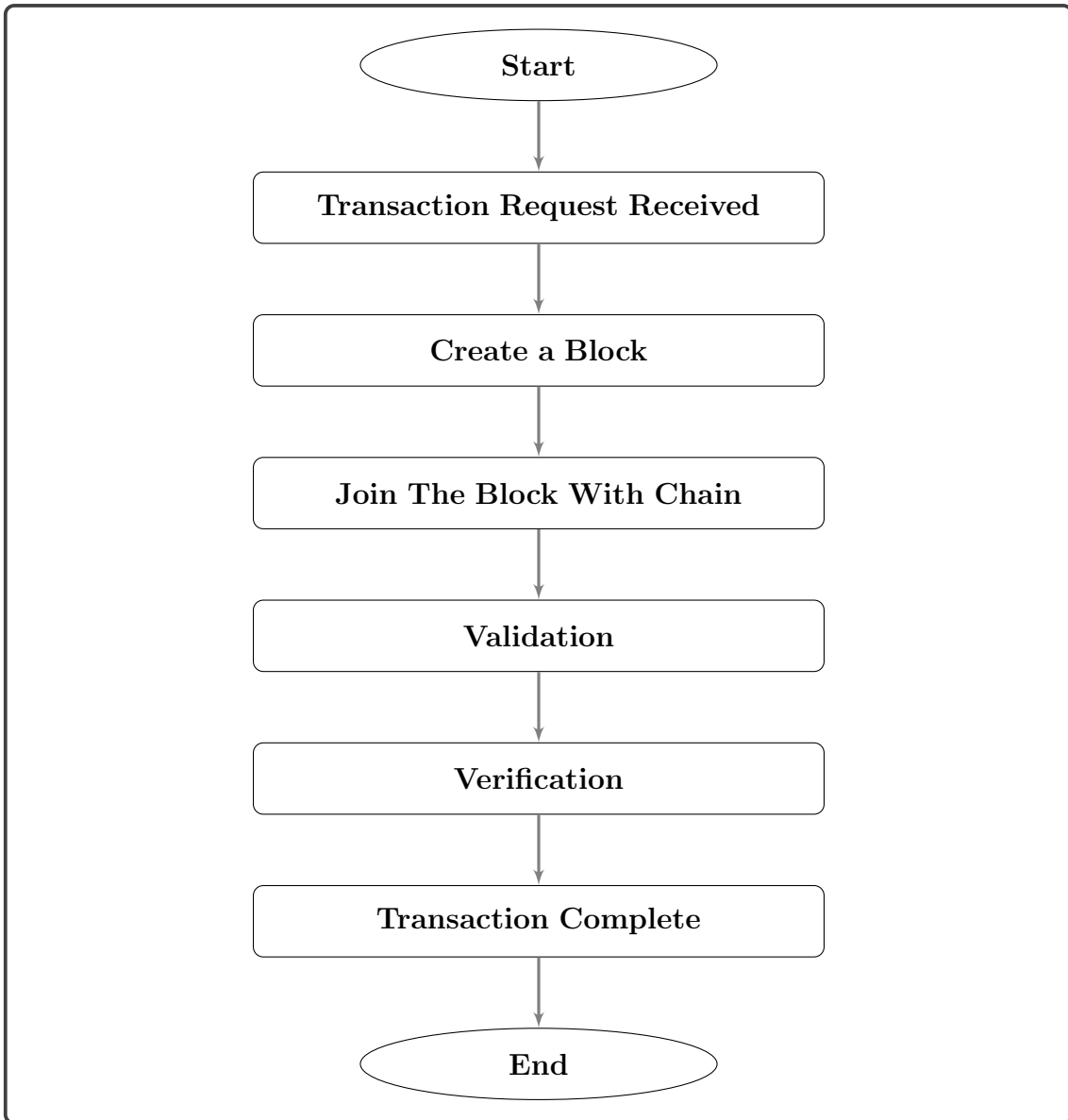


Figure 4.2: Secured transaction platform

Figure 4.2 depicts a blockchain based transaction system. Consensus is the mechanism by which a blockchain transaction is approved. To validate transactions, nodes compare chains. The longest chain is the valid chain. This transaction is irreversible as well. Meaning the data of transaction cannot be altered or even deleted.

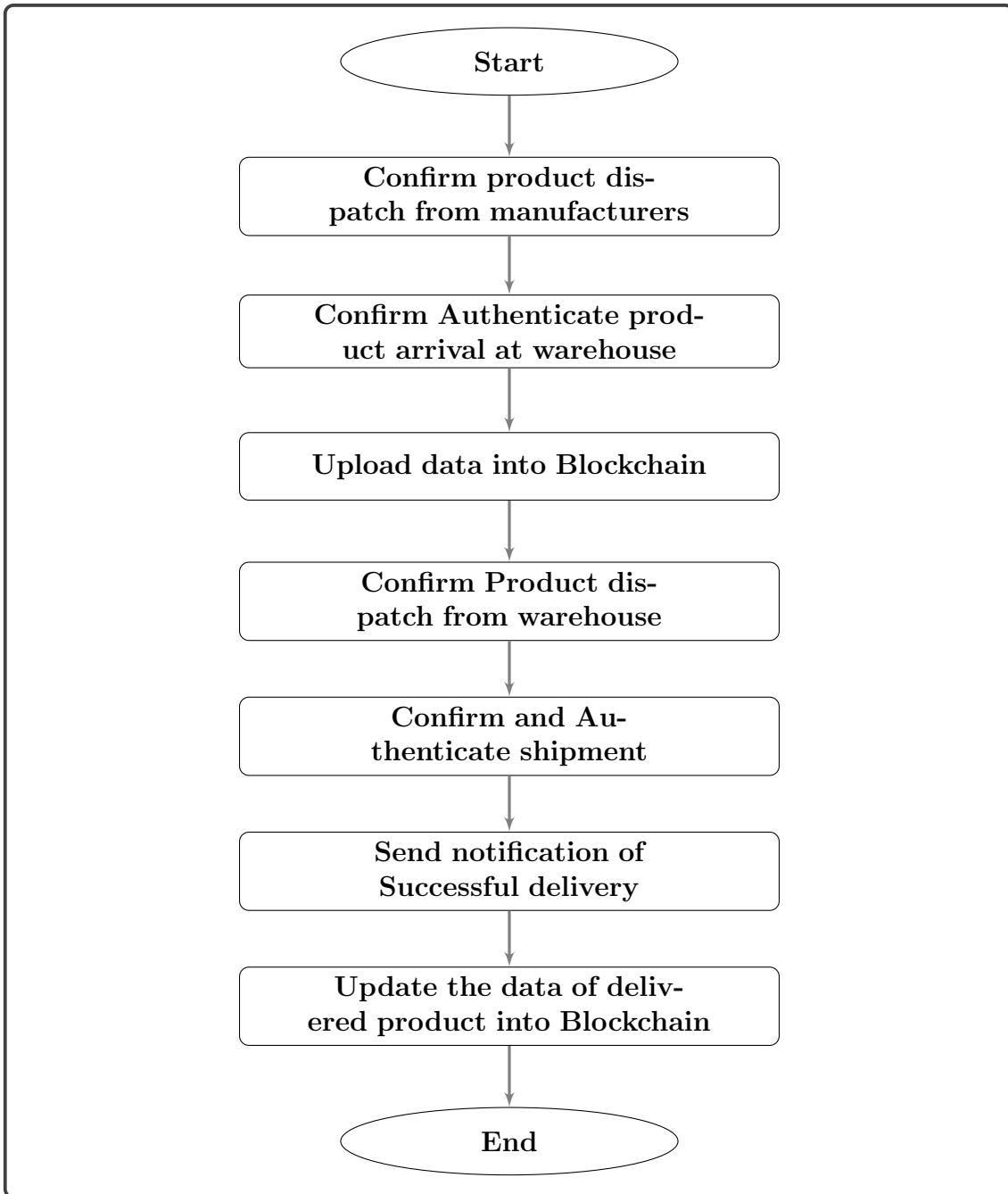


Figure 4.3: Real-time tracking system

Figure 4.3 shows the steps of product tracking, starting from the manufacturers to the end delivery. Blockchain allows business partners to track and trace real-time product data. Multiple parties can deal directly over a peer-to-peer network using blockchain technology, eliminating the need for a central authority to verify transactions.

4.2 Proposed Model

This figure 4.4 shows the suggested framework for leveraging blockchain and smart contracts to automate the current supply chain for items made of paper and pens,

making the data storage and access control impenetrable. The suggested technique

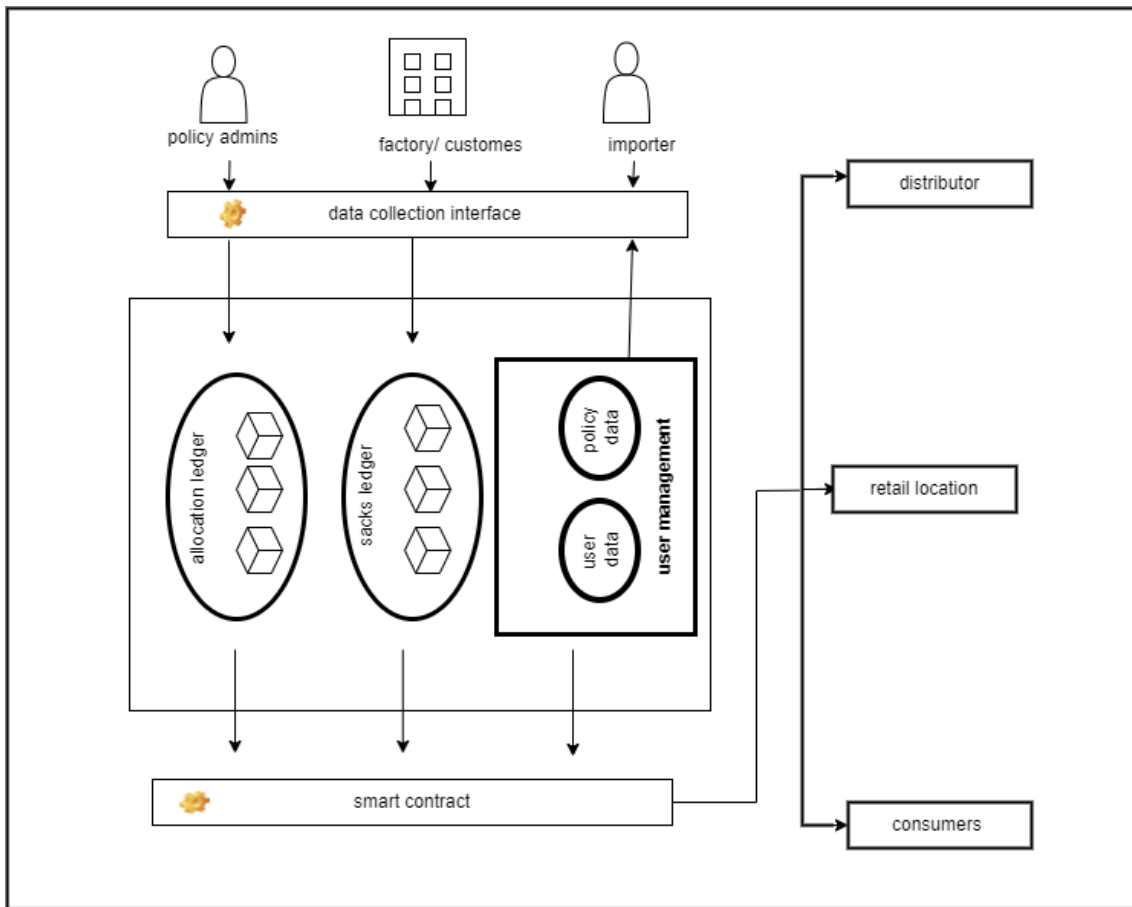


Figure 4.4: Suggested Framework

gathers, stores, and manages each product’s vital product information over the duration of its life cycle using a decentralized distributed system that makes use of blockchains.

The suggested technique gathers, stores, and manages each product’s vital product information over the duration of its life cycle using a decentralized distributed system that makes use of blockchains. Each product consequently obtains a safe, shareable record of exchange that contains thorough information about all the products. Each of these parties makes a substantial contribution to the system by uploading vital information about the goods and their current condition to the blockchain network. Since the blockchain data design inherently ensures data integrity, we decided to use it in the proposed approach. There have been numerous reports of data alterations in the current supply chain system. As a result, our primary objective is to ensure supply chain data authenticity in order to stop data manipulation. The high-level users (policy admins , factory, and importers) are able to provide goods to the appropriate end users, manage end-user data, and access new product records. Policy administrators have the ability to control end users of the supply chain and distribute goods in accordance with international norms. The system solely uses the allocation data in order to handle end-level user data read requests. Users and blockchain-based data ledgers can now communicate with one another using smart contracts. Once we post our contract into the blockchain, the code cannot

be changed. Users can perform a transaction by simply sending it to a contract's address. The contract will then be changed as necessary at that point. The contract may be able to transmit and receive messages, maintain a balance in its account, read from and write to its private storage, or even construct other contracts depending on the transaction it receives. The smart contract must verify users before it can read relevant data from the proper ledgers. The right data from the smart contract is delivered to end-level users in accordance with their user credentials and allocation ledger. In the given blockchain-based supply management system only highly privileged users can generate new products, record allocate products to respective end-level users and manage end-level users credentials. Where policy admins can allocate products according to the requirements and manage users. In our proposed distribution system, two main operations are shipment and delivery of the finished products to middlemen and consumers.

4.2.1 Shipment

In the shipment segment, the product is given to the proper delivery person. Consumers are assigned against retailers and retailers against distributors. To connect all these types of users at the supply chain policy level admins are the key users deliverymen are used for transporting shipments from one to other parties.

Algorithm 1 Pseudo Code for Shipment

```

a ← 1
Consumer:
    productUnit == allocate_to_consumer(list_of_product_units,
                                        PU_consumer[a])
    b ← 1
    Retailer:
        if consumer[a] is paired with the retailer[b] Then
            Retailer_unit == allocate_retailer(product_unit,
                                                PU_retailer[b])
        c ← 1
        Distributor:
            if retailer[b] is paired with the distributor[c] Then
                Distributor_unit == allocate_distributor(retailer_unit,
                                                         PU_distributor[c])
    Delivery_unit == assign_delivery_man(PU_delivery_man[c],
                                        distributor_unit)
    Carried_good[c] == verify_carry(PR_delivery_man[c], delivery_unit)

```

In this section, the product units are assigned to the 'a'th consumer. A previously allocated product unit is assigned to a certain retailer, who then gets assigned to a specific distributor, and the product unit for distributors is accepted by a deliveryman for delivery following the delivery man's authentication, and the items are eventually carried by the confirmed deliveryman. As a result, a collection of items is transported to various dealers by an authorized delivery man.

4.2.2 Distribution

In this part at first the 'c'th is getting authenticated using his private key . Then the 'c'th delivery man will again get verified and the products will be shipped by him to the retailer . Basically each time the product is shipped to anybody, the receiver needs to get verified before receiving the product . So the retailer and the consumer also needs to get verified with their individual private key before receiving the product from the respective delivery man [23]

Algorithm 2 Pseudo Code for Distribution

$c \leftarrow 1$

Distributor:

Received_good[c] == verify_deliver(PR_distributor[c],
Carried_good[c])

Delivery_unit[c] == assign_delivery_man(PU_delivery_man[c],
Received_good[c])

Carried_good[c] == verify_carry(PR_delivery_man[c], delivery_unit)

$b \leftarrow 1$

Retailer:

if retailer[b] is paired with the distributor[c] **Then**

Received_good[b] == verify_deliver(PR_retailer[b],
Carried_good[c])

$a \leftarrow 1$

Consumer:

if is paired with the distributor[c] **Then**

verify_receive(PR_consumer[a], Received_good[b])

Chapter 5

Building The Application Powered By Ethereum Smart Contract

5.1 Building The Application Powered By Ethereum Smart Contract

5.1.1 Works that have been done so far

So far research papers have produced smart contract and defined secured transaction systems using the blockchain platform. But we have come up with an innovative idea to use smart contracts to build an automated blockchain application where all the tasks will be handled with proof and transparency. We attempted to build a complete system of client side application which will be powered by Ethereum smart contracts where tasks will be automatically checked off after successful transaction. Transparency can be ensured properly through this measure. This automated process will take the supply chain system into another level.

5.1.2 Smart Contract Implementation

We have picked a to-do list application to demonstrate our integration of smart contracts with supply chain management. This application will read and write data to and from the blockchain and run business logic to control how it behaves. Through this procedure, we would create our Ethereum smart contracts in Solidity, a JavaScript-like programming language. All the codes that build up the smart contract are unchangeable. No one can alter or update any of the code after the smart contract is launched into the blockchain for which it is secured and trustworthy. They serve as an interface for both running business logic and accessing and writing data from the blockchain. They can be accessed by anyone with access to the blockchain because they are publicly accessible.

5.1.3 Task Brief

We will develop a client side application for listing the tasks that communicate with the blockchain directly. We will connect our application to a single Ethereum node in order to view the Ethereum blockchain. The to-do list's code will be created as a smart contract in Solidity, which will then be uploaded to the Ethereum blockchain.

We'll also use an Ethereum wallet to connect to the blockchain network using our individual accounts in order to communicate with the to-do list application.

5.1.4 Installing Dependencies, building the application and test

5.1.4.1 Ganache Personal Blockchain

This mimics the characteristics of a personal blockchain account. For Ethereum development, we will use Ganache as our own blockchain as it can launch smart contracts, create applications, and carry out tests thanks to it. It can be used in Windows, Linus and MAC. After we have installed Ganache, we have a private blockchain network in our hands. A list of accounts connecting to the network and some information about the server Ganache is operating on may be seen here. 100 ether have been credited to each account.

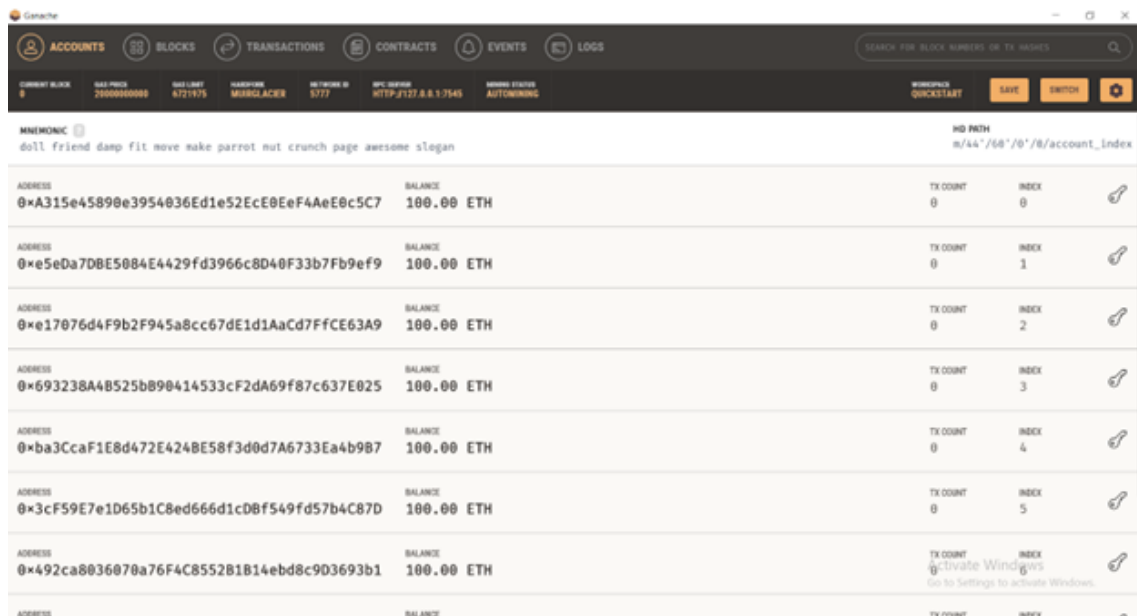


Figure 5.1: Private blockchain network Ganache

5.1.4.2 Node.JS

After setting up a private blockchain, we must set up the ecosystem for creating smart contracts. The Node Package Manager, included with Node.js, is the first dependency we require.

5.1.4.3 Truffle framework

In order to develop the smart contract using the programming language Solidity, we must now install the Truffle Framework. Furthermore, we will be able to compile the smart contract into bytecode, and then execute them on the Ethereum Virtual Machine (EVM). Using truffle we will be able to write tests against smart contracts, deploy smart contracts to the blockchain, work with a development console and also develop a client side application.

5.1.4.4 Metamask Ethereum Wallet

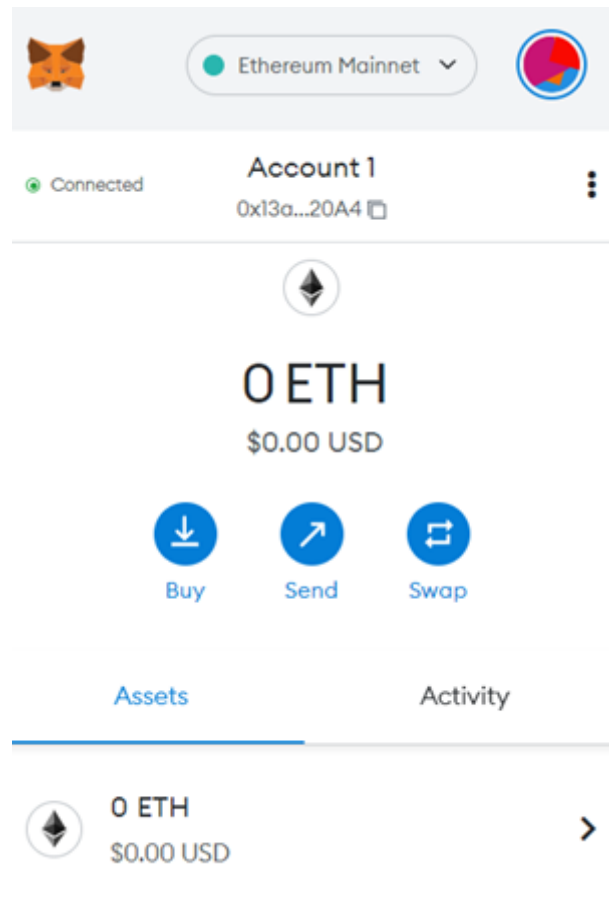


Figure 5.2: Metamask Wallet

5.1.4.5 Project Set-Up

First we will create a project directory through command prompt and initialize the truffle project. To install some development dependencies that the project will require we will also create a package.json file.


```
CAWINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.19044.1826]
(c) Microsoft Corporation. All rights reserved.

C:\Users\hp>mkdir eth-todo-list
C:\Users\hp>cd eth-todo-list
C:\Users\hp\eth-todo-list>truffle init
✔ Preparing to download
✔ Downloading
✔ Cleaning up temporary files
✔ Setting up box
Unbox successful. Sweet!

Commands:
  Compile:      truffle compile
  Migrate:      truffle migrate
  Test contracts: truffle test

C:\Users\hp\eth-todo-list>touch package.json
Touching package.json
C:\Users\hp\eth-todo-list>
```

Figure 5.3: Installing dependencies

After bootstrapping all project dependencies and installing them from cmd with command “npm install”, we can create the project directory shown below:

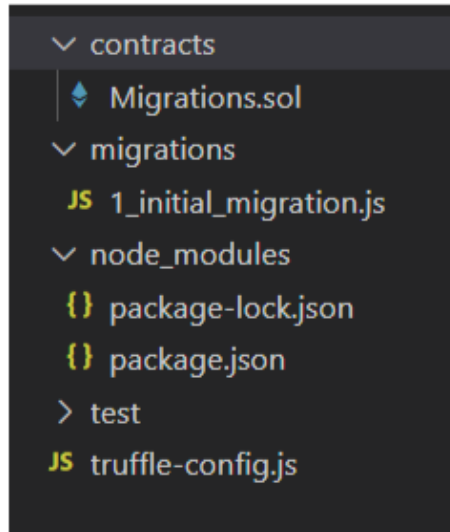


Figure 5.4: Project Directory

All smart contracts reside in the contract directory. In the migration directory all the migration files are found. We can compare them with other web development frameworks that we use regularly. To update the state of blockchain by deploying smart contracts, we need this migration.

In the `node_modules` directory, all the node dependencies are installed and we can test our smart contract in the test directory. Main configuration files can be found in the Truffle config file. This will handle network configuration for our truffle project. There is a smart contract in the migration file. It handles our migrations when we want to deploy new contracts to the blockchain. In the aforementioned directory we will create a new file called which we need to declare the smart contract and write all the code for the smart contract.

We build a smart contract called `TodoList`, which is then surrounded by curly braces

and all of the smart contract code will reside there. We are targeting to keep the track of the tasks in the list numerically. The algorithm for creating the task is:

Algorithm 3 Pseudo Code for creating new task

Connect \rightarrow (*blockchain*)

taskCount = 0

Input:

`initialize_id`

`initialize_content`

`bool_completed`

`mapping(uint \rightarrow task)`

Output:

`taskCount` ++

`_content`

`False`

End();

We initialized the task id, text and a boolean function to track if the tasks have been completed or not. Here mapping works like hashing where task id can retrieve the task using the sequence of listing. Task count is a state variable. We can access the value of this variable outside of smart contracts. Before deploying the smart contract into the blockchain, we will run a migration script. Without it, we cannot deploy new contracts into blockchain because blockchain is immune to any change, as we stated earlier.

We also need to design the frontend of the application where Web3 will be incorporated. This way our application will be able to talk to the blockchain. We developed HTML codes and CSS for user interface.

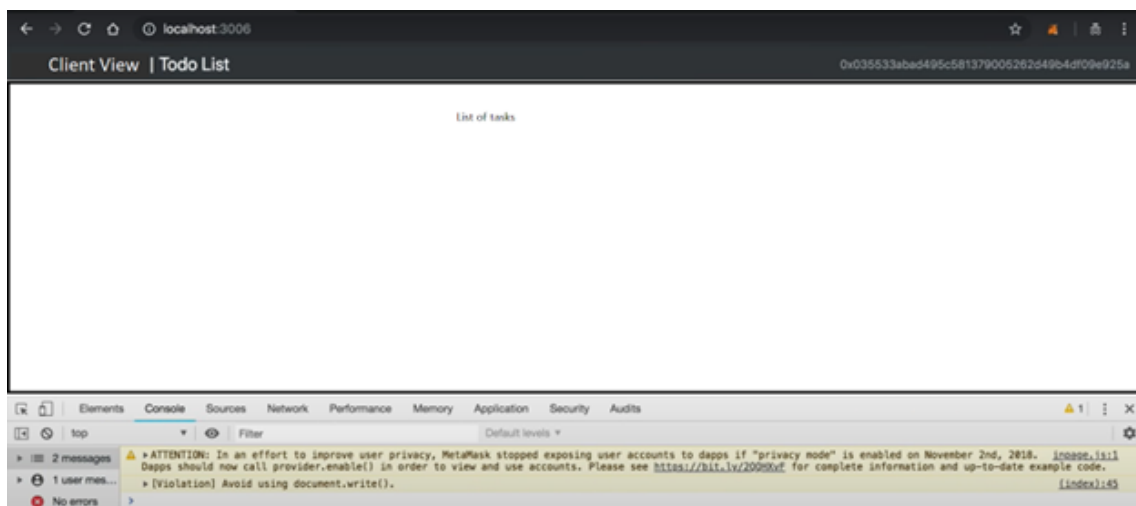


Figure 5.5: Client view of application

5.1.4.6 Testing

As Ethereum blockchain code is immutable, we need to discard the codes and deploy a new copy if there are any issues. It will have a different address than the previous one. All the tests will be written in javascript.

First we will test if the smart contract has been deployed properly and confirm the fact that we are being able to retrieve the tasks from the task count. To check the deployment, we need to check if the address of the contract is not null, undefined or zero. Then by comparing task id with task count and matching the task content, we can confirm the task listing.

Algorithm 4 Pseudo Code for testing 1 (deployment and list tasks)

```
Connect→(blockchain)
Connect→(accounts)
if deployment == successful then
  check if:
    address is not null;
    address is not 0;
    address is not defined;
if lists_task == successful then
  check if:
    id of the task is equal to the sequence of task;
    content of the task is the name of the task;
    task completion is false;
    first task is set as number 1;
End();
```

This test passes successfully:

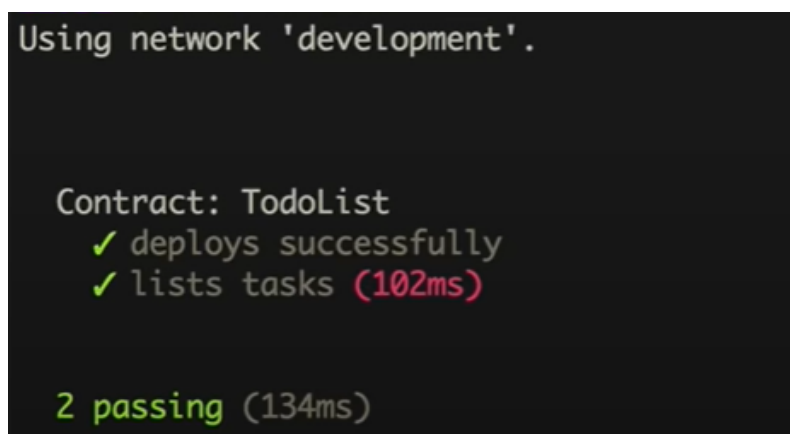


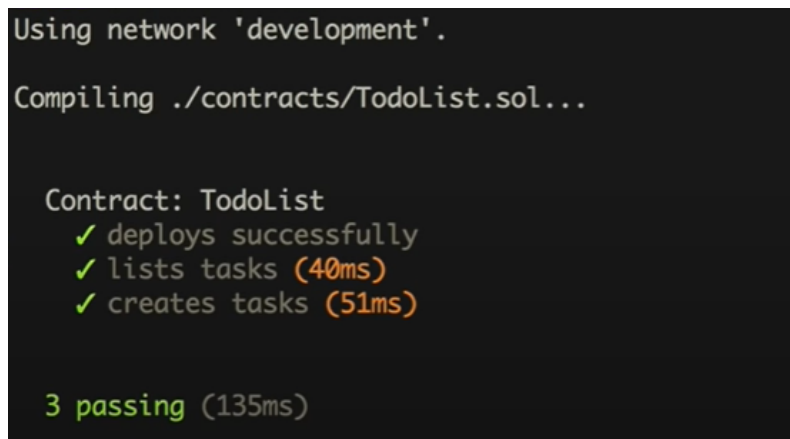
Figure 5.6: Test passes(1)

Now we will test if the task creation is successful. Whenever a new task is created, external customers can subscribe to the events that are triggered. We can create tests to inspect data to make sure that the events are triggered anytime a new task is created.

Algorithm 5 Pseudo Code for testing 2 (task creation)

```
Connect→(blockchain)
Connect→(accounts)
if create_Task == successful then
  create new task;
  check task count for new task;
  check if:
    event is getting triggered;
    event id is 2;
    event content is the name of new task;
    event completion is false;
End();
```

This test also passes successfully: Finally we have to confirm if the task completion



```
Using network 'development'.
Compiling ./contracts/TodoList.sol...

Contract: TodoList
  ✓ deploys successfully
  ✓ lists tasks (40ms)
  ✓ creates tasks (51ms)

3 passing (135ms)
```

Figure 5.7: Test passes(2)

function works by checking the boolean function to become true after the transaction is completed.

Algorithm 6 Pseudo Code for testing 2 (task completion)

```
Connect→(blockchain)
if task_complete == successful then
  task is completed;
  task completion function is true;
  check if:
    event is getting triggered;
    first task is completed and event id is 1;
    event completion is true;
End();
```

This test also passes properly:

```
Contract: TodoList
  ✓ deploys successfully
  ✓ lists tasks
  ✓ creates tasks (51ms)
  ✓ toggles task completion (116ms)

4 passing (258ms)
```

Figure 5.8: Test passes(3)

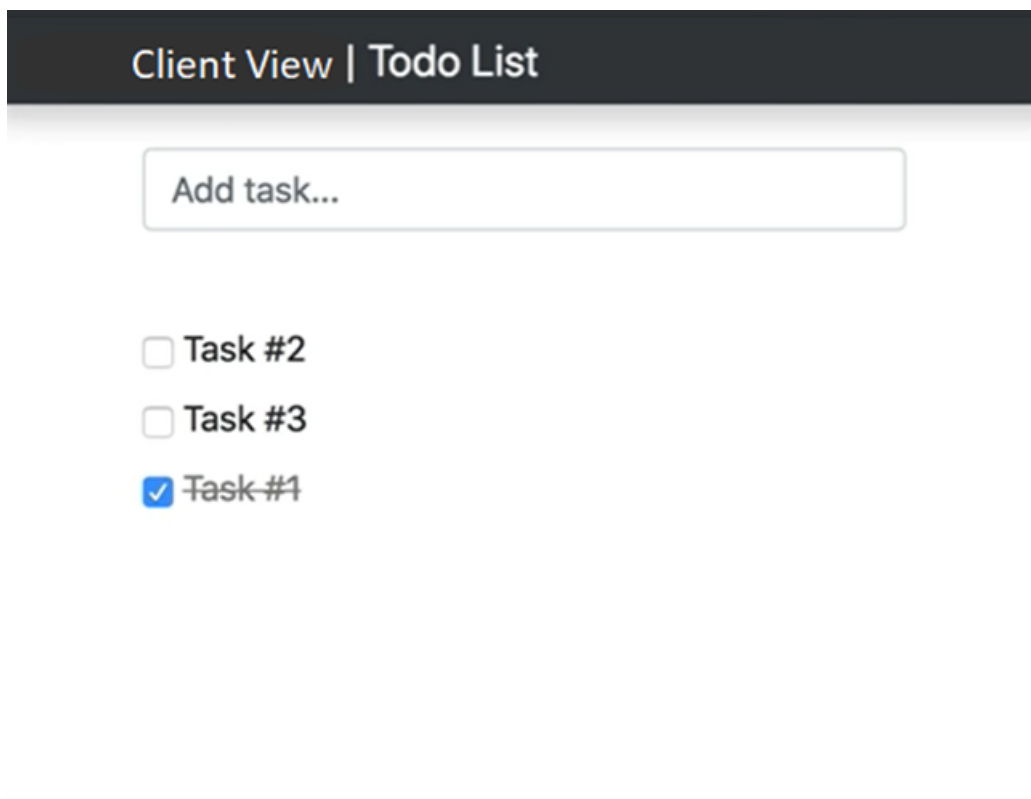


Figure 5.9: Task being checked off

Chapter 6

Conclusion

In today's times, traditional supply chain management methods are insufficient. Large amounts of paperwork, a lack of trust, incompatibility, and unstructured data (booklet, succeed) all limit business growth. So, for a better experience, we've proposed a model that ensures security, transparency, faster product movement, tracking, and consumer interaction. The ledgers supplied by blockchain assist us in maintaining a shared and safe database flow throughout the whole system, which is a very significant detail to note. We've proposed a cost-effective and time-saving automated mining method. To reduce the danger of any component failing, security measures such as intrusion detection are implemented. Several businesses across a variety of industries have recently begun to investigate the entire supply chain process. This section will look back at the beginnings of the supply chain as well as some current triumphs. Since corporations realized the benefits of incorporating blockchain with their organizations beyond their own in the 1980s, interest in supply chain management has gradually grown. Businesses are becoming more and more aware that they can no longer compete successfully without the support of their suppliers and other supply chain partners. Above all, with the expansion of new geographic areas, businesses must assess if their present supply system is capable of mitigating potential threats such as counterfeit currency transactions.

Bibliography

- [1] R. R. Lummus and R. J. Vokurka, “Defining supply chain management: A historical perspective and practical guidelines,” *Industrial Management and Data Systems*, vol. 99, no. 1, pp. 11–17, 1999. DOI: 10.1108/02635579910243851.
- [2] S. Agarwal, *Blockchain technology in supply chain and logistics*, 2014. [Online]. Available: <https://dspace.mit.edu/handle/1721.1/118559>.
- [3] M. Moradi and M. ZULKERNINE, “A neural network based system for intrusion detection and classification of attacks,” Feb. 2014.
- [4] D. Garcia and F. You, “Supply chain design and optimization: Challenges and opportunities,” *Computers and Chemical Engineering*, vol. 81, Mar. 2015. DOI: 10.1016/j.compchemeng.2015.03.015.
- [5] A. Wright and P. De Filippi, “Decentralized blockchain technology and the rise of lex cryptographia,” *SSRN Electronic Journal*, Jan. 2015. DOI: 10.2139/ssrn.2580664.
- [6] S. Apte and N. Petrovsky, *Will blockchain technology revolutionize excipient supply chain management?: Published in journal of excipients and food chemicals*, 2016. [Online]. Available: <https://jefc.scholasticahq.com/article/910-will-blockchain-technology-revolutionize-excipient-supply-chain-management>.
- [7] 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.
- [8] C. D. Clack, V. A. Bakshi, and L. Braine, *Smart contract templates: Foundations, design landscape and research directions*, 2016. DOI: 10.48550/ARXIV.1608.00771. [Online]. Available: <https://arxiv.org/abs/1608.00771>.
- [9] A. Tapscott and D. Tapscott, *How blockchain will change organizations*, 2016. [Online]. Available: <https://sloanreview.mit.edu/article/how-blockchain-will-change-organizations/>.
- [10] B. Dickson, *Blockchain’s brilliant approach to cybersecurity*, 2017. [Online]. Available: <https://venturebeat.com/business/blockchains-brilliant-approach-to-cybersecurity/>.
- [11] N. Hackius and M. Petersen, “Blockchain in logistics and supply chain: Trick or treat?,” Oct. 2017. DOI: 10.15480/882.1444.
- [12] S. Jagati, *What blockchain means for the sharing economy*, 2017. [Online]. Available: <https://hbr.org/2017/03/what-blockchain-means-for-the-sharing-economy>.

- [13] K. Korpela, J. Hallikas, and T. Dahlberg, “Digital supply chain transformation toward blockchain integration,” Jan. 2017. DOI: 10.24251/HICSS.2017.506.
- [14] M. Dobrovnik, D. Herold, E. Fürst, and S. Kummer, “Blockchain for and in logistics: What to adopt and where to start,” *Logistics*, vol. 2, p. 18, Sep. 2018. DOI: 10.3390/logistics2030018.
- [15] M. el Maouchi, O. Ersoy, and E. Zekeriya, “Trade: A transparent, decentralized traceability system for the supply chain,” May 2018. DOI: 10.18420/blockchain2018_01.
- [16] P. Misra, *5 ways blockchain technology will change the way we do business*, 2018. [Online]. Available: <https://www.entrepreneur.com/article/309164>.
- [17] C. D. Clack and C. McGonagle, “Smart derivatives contracts: The ISDA master agreement and the automation of payments and deliveries,” *CoRR*, vol. abs/1904.01461, 2019. arXiv: 1904.01461. [Online]. Available: <http://arxiv.org/abs/1904.01461>.
- [18] P. D. Filippi, *Walmart’s foray into blockchain, how is the technology used?* 2019. [Online]. Available: <https://cointelegraph.com/news/walmarts-foray-into-blockchain-how-is-the-technology-used>.
- [19] T. Jensen, J. Hedman, and S. Henningsson, “How tradelens delivers business value with blockchain technology,” *MIS Quarterly Executive*, vol. 18, pp. 221–243, Dec. 2019. DOI: 10.17705/2msqe.00018.
- [20] M. Queiroz, R. Telles, and S. Bonilla, “Blockchain and supply chain management integration: A systematic review of the literature,” *Supply Chain Management: An International Journal*, vol. 25, Feb. 2019. DOI: 10.1108/SCM-03-2018-0143.
- [21] S. B. Report, *Ipdc rolls out blockchain-based supply chain finance platform*, 2019. [Online]. Available: <https://www.thedailystar.net/business/news/ipdc-rolls-out-blockchain-based-supply-chain-finance-platform-1837315>.
- [22] J. Zhang, “Deploying blockchain technology in the supply chain,” in *Computer Security Threats*, C. Thomas, P. Fraga-Lamas, and T. M. Fernández-Caramés, Eds., Rijeka: IntechOpen, 2019, ch. 5. DOI: 10.5772/intechopen.86530. [Online]. Available: <https://doi.org/10.5772/intechopen.86530>.
- [23] S. Ahmed, M. Islam, M. Hosen, and M. Hasan, “Blockchain based fertilizer distribution system: Bangladesh perspective,” Jan. 2020, pp. 1–5. DOI: 10.1145/3377049.3377116.
- [24] C. Catalini and J. Gans, “Some simple economics of the blockchain,” *Communications of the ACM*, vol. 63, pp. 80–90, Jun. 2020. DOI: 10.1145/3359552.
- [25] A. Rosic, Blockgeeks, and M. Baggetta, *Proof of work vs proof of stake: Basic mining guide*, 2020. [Online]. Available: <https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/>.
- [26] D. Ghode, R. Jain, G. Soni, S. Singh, and V. Yadav, “Architecture to enhance transparency in supply chain management using blockchain technology,” *Procedia Manufacturing*, vol. 51, pp. 1614–1620, Jun. 2021. DOI: 10.1016/j.promfg.2020.10.225.

- [27] D. Gohil and S. Thakker, “Blockchain-integrated technologies for solving supply chain challenges,” *Modern Supply Chain Research and Applications*, vol. 3, May 2021. DOI: 10.1108/MS CRA-10-2020-0028.
- [28] S. M. Idrees, M. Nowostawski, R. Jameel, and A. K. Mourya, “Security aspects of blockchain technology intended for industrial applications,” *Electronics*, vol. 10, no. 8, 2021, ISSN: 2079-9292. DOI: 10.3390/electronics10080951. [Online]. Available: <https://www.mdpi.com/2079-9292/10/8/951>.
- [29] G. McAllister and D. Rombough, *Major issues facing supply chain managers*, 2022. [Online]. Available: <https://blog.procurify.com/2021/03/02/4-major-issues-facing-your-supply-chain-manager/>.
- [30] V. Grewal-Carr and S. Marshall, *Blockchain Enigma. Paradox. Opportunity*. Deloitte.
- [31] R. Kandaswamy, R. Valdes, and D. Furlonger, *The evolving landscape of blockchain technology platforms*. [Online]. Available: <https://www.gartner.com/en/documents/3626317>.
- [32] *Supply chain issues: 'there really are problems everywhere,' even for small companies*. [Online]. Available: <https://www.cbsnews.com/newyork/news/supply-chain-issues-port-delays-trucking-railroads-warehouses-worker-shortage/>.