*Intelligent Automation & Soft Computing*
DOI: 10.32604/iasc.2023.025032
***Article***

Tech Science Press

# An Enhanced Security System Using Blockchain Technology for Strong FMC Relationship

**K. Meenakshi* and K. Sashi Rekha**

Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, India
*Corresponding Author: K. Meenakshi. Email: meennakshimeena@gmail.com

Received: 09 November 2021; Accepted: 10 January 2022

**Abstract:** Blockchain technology is a shared database of logs of all consumer transactions which are registered on all machines on a network. Both transactions in the system are carried out by consensus processes and to preserve confidentiality all the files contained cannot be changed. Blockchain technology is the fundamental software behind digital currencies like Bitcoin, which is common in the marketplace. Cloud computing is a method of using a network of external machines to store, monitor, and process information, rather than using the local computer or a local personal computer. The software is currently facing multiple problems including lack of data protection, data instability, and reliability. This paper aims to give the highest security for multiple user environments in cloud for storing and accessing the data in blocks. The users who are legitimate are only allowed for storing and accessing the data as like a secured block chain approach. As like the Blockchain which does not require a centralized system for transactions, the proposed system is also independent on centralized network interface. The decentralized system is developed in such a way to avoid counterfeiting. The system enables the fabricator to spend less or null resources to perform the validations for its direct operated stores. This ensures the product fabricator to avoid the circulation of its duplicate products. The customer as an end-user is also ensured to have only the genuine products from the fabricator. The Fabricator (F), Merchant (M) and consumer (C) forms an interconnected triangular structure without allowing any counterfeiting agents in their secured cloud chain. The proposed approach provides the stability in the security system of the cloud using the chaining mechanism within different blocks at each node. It takes roughly 4.7, 6.2, and 7.5 ms, respectively, to register each node in the proposed system for 5, 10, and 15 nodes. The overall registration time for each scenario is 11.9, 26.2, and 53.1 ms, despite the fact that each node's registration time was greatest for 10 nodes. By looking at the data, it's clear that the number of nodes is a function of time.

**Keywords:** Blockchain; bitcoin; customer; merchant; data protection; digital currencies; transaction

## 1 Introduction

Cloud computing is one of the well-defined developments that originated from large-scale distributed computing and aims to reduce consumers' workload. With falling hardware and infrastructure costs, connectivity around the globe, versatility with a fully automated operation, and ease of scalability, there are several benefits of cloud systems. Many companies are now embracing cloud-like computing, including IBM, Google, and Microsoft. Such apps exist from Amazon Web Services (AWS), Google Cloud Network, Google Software Engine and the Elastic computing platform. It offers a pay for use strategy and a responsive "just in time" IT architecture across the internet. While cloud computing offers many valuable resources, businesses are reluctant to implement in fear of being exposed. Security risks and the cloud's emerging problems are the main pitfalls [1].

Blockchain Innovation is at the heart of the industry as businesses pursue improved protection, privacy and greater efficiencies. Blockchain is a distributed digital archive of transactions that are cryptographically unbreakable without the assistance of a centralized authority. Participants or computers of the Blockchain technology are also known as nodes [2]. Blockchain offers a shared network in which everybody has a function to ensure data integrity. The data that is submitted to the Blockchain is secured with complex machine codes. Each block includes a hash, timestamp, and previous hash from the last block in the series. The data on the Blockchain is permanent and clear. Blockchain data contains a reliable record, and a network has been built that verifies users, removing privacy issues. In order for cloud infrastructure to expand, we will solve cloud storage security issues by combining with Blockchain technologies. It increases data stability, and also expands service efficiency and versatility through cloud data management [3].

Thousands of websites are hosted by the cloud in this Internet age. A server stack is needed to make the host site very expensive. These servers need to be traffic-free, tracked and constantly managed. More workers would have to be hired to organize and operate these repositories. Both data can be saved by data centers. Continued attempts to manage the server problem and personnel will detract us from the achievement of company objectives. We use cloud storage to escape this hectic upkeep. Cloud computing is a means to store, control and handle data from everywhere of the world by using a network of distributed servers. It is used instead of a local server or an actual computer [4]. Fig. 1 shows the layered cloud architecture.

Cloud networking resources, such as data storage and software, are offered to devices of the enterprise through the Internet. The integration of data centers, infrastructure and servers via the internet offers cloud computing with many advantages. These programmes are based on the rules on pay per use. Services are available internationally and cost substantially less, thereby facilitating staff teamwork. The cloud-based infrastructure is constantly revamped, making the cloud simple to access. The user of the service will also be in possession of the cloud documents. It has certain limits, too. Since cloud content is extremely flexible, securities, privacy concerns and susceptibility to attacks need to be taken into account. There are risks that the cloud gets its downtimes when there are a lot of people [5].

Cloud offers various offerings, which are primarily categorized into three distribution models. Software as a service (SaaS) is the first service that is like an application that is hosted by internet-wide users. As a single source for the apps operating in the cloud, the cloud service provider provides full programmes or initiatives that have several resources for each of the customers [6]. Cloud clients have no cloud infrastructure access. SalesForce.com and Google Mail are an important example of SaaS, as is AWS. Platform as a Service is the second service (PaaS). We will deploy our programming app and suites of languages on the platform via the cloud service provider [7].

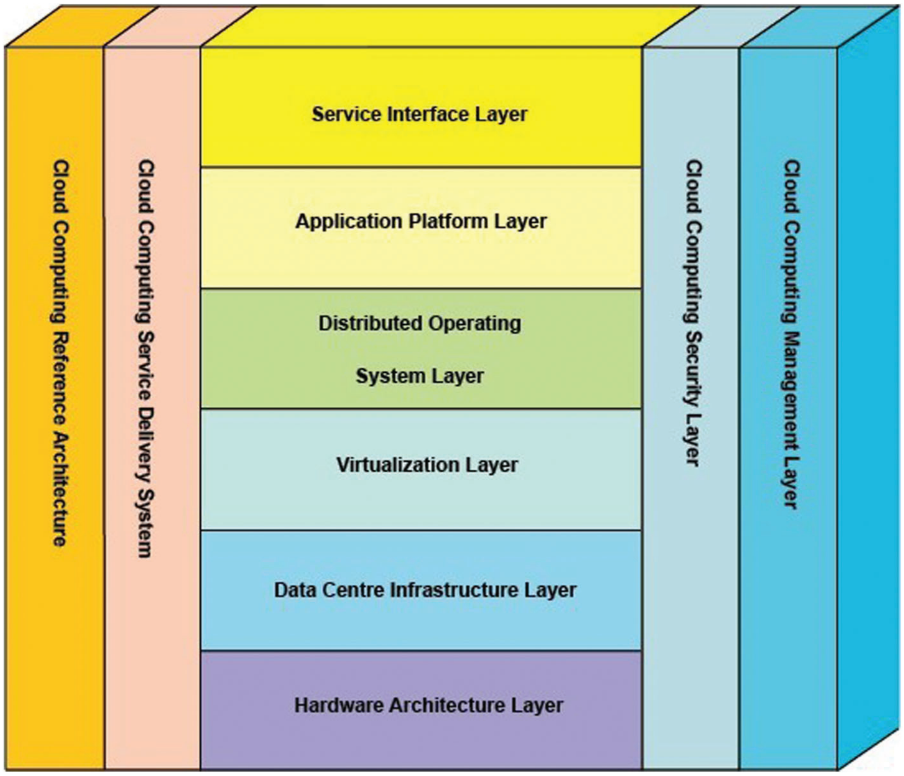

Cloud Computing Reference Architecture
Cloud Computing Service Delivery System
Service Interface Layer
Application Platform Layer
Distributed Operating System Layer
Virtualization Layer
Data Centre Infrastructure Layer
Hardware Architecture Layer
Cloud Computing Security Layer
Cloud Computing Management Layer

**Figure 1:** Layered cloud architecture

SaaS and PaaS vary from one another because SaaS holds the whole programmes in the cloud, where PaaS offers the application platform. The perfect explanation for PaaS is Google's search engine. The third service is IaaS, through which the customer may directly access the storage, transmission and other network services. Virtualization is used in IaaS, where physical services are spread to satisfy cloud customers' resource demand. The safest way of virtualization is to mount separate virtual machines and other VM's from the base hardware. They sell servers with a specific IP address to provide protection. The closest example of the IaaS is Amazon EC2, GoGrid.

Public cloud is the type of infrastructure that can be accessed by various business users that need a place to store their data, where each company user can have access to the provider. The cloud technology is democratically and free accessible, and can be used by more than one company depending on the capacity and memory space Cloud services provide cloud hosting and support for the clouds. Often a cloud service hosts the customer to take on reduced customer burden or save on costs for a limited duration. Microsoft Azure and other cloud-based applications are providing secure cloud infrastructure services. Although most large companies now purchase their IT technology on a more emergent unit basis, it is the private cloud that is the most powerful about the demand for the data, its security, and its management [8].

These consumers today have a subscription to the electric grid and the applications which are owned and deployed by us. The use of a cloud for storing information can be safe and costly. These cloud storage and bandwidth regulations are accounted for in the private cloud solution. The clients can maximize the user's access to the private cloud and can limit the users' abilities to access the private cloud. Eucalyptus is the perfect example of how a private cloud should function. The two models of cloud deployment complement and are merged to form a hybrid cloud. Hybrid cloud offers the mix of self-serve scale along with corporate controlled scale [9].

One of their main focuses is on company-owned and managed data centers, but they are relying on public cloud services to provide to provide computation. A security system using hybrid clouds will do a fantastic job defending an enterprise, but with the complexity of such a solution it would not be easy to handle. An online cloud firm, AWS, is an influential hybrid in the industry. A community cloud is a community sharing for the individual. It's like a user's personal cloud that he can access from other computers. A very small number of individuals may be individually taking charge of, administer, and run a company. An ultrafine cloud can be a valuable method for a school or a business field. The Facebook website is an example of a group cloud [10].

Cloud computing is a method that contains five core characteristics. On demand self-service is the manner in which a customer is able to have a storage option at any time to the user, instantaneously. For a stable distributed infrastructure, the network can provide single connectivity through the network, which can be conveniently reached with common frameworks to facilitate various kinds of clients. The framework is structured to have its workload spread between differing areas and servers, and then has such servers service the needs of multiple users and their demands. Measuring is where the services are measured (in meters) and maintained (in Celsius) by the metering capabilities.

Elastic scalability represents the ability for an organization to extend its processing capabilities and servers alongside their existing ones. The act of "auto scaling" is a means for the application to automatically obtain additional resources when the application's demand for resources outgrows its previous size. And though the cloud has several properties that are beneficial, there are also several defects that occur within the cloud. Any of these subjects are discussed as follows. Many of the cloud services have very strong encryption controls, and most can monitor where data will be transmitted or retrieved. However, in some situations loss of data does occur [11].

As more and more contents of celebrities' personal information are being revealed to the media, Apple's iCloud problem grew more serious. There is a fear that data handled online through mere internet connectivity somehow grants access to the user without the individual learning about it. The biggest issue for the corporations is that they are shying away from using the cloud and its resources. Most of the cloud providers are available 24/7, but some of the services are reserved for a timeout. They are out of the service right now for the time being for repairs. Recently some of the internet networks have been reduced to a small number of hours a day. Cloud consumers would be granted little control over the data that is stored in the cloud. Most cloud computing companies most of their power over IaaS (Infrastructure as a Service), where they have access to extend the available capacity, have control over where the virtual machines are housed, etc [9]. Fig. 2 shows the overview of Blockchain network.

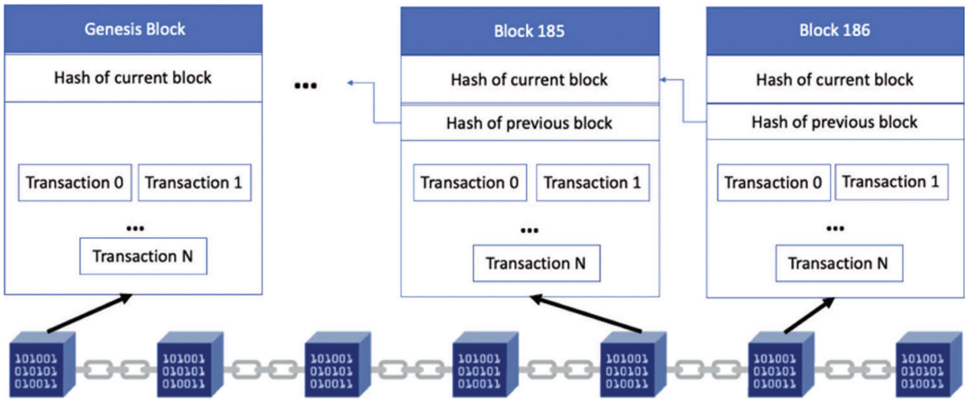


**Figure 2:** Overview of Blockchain network

Cloud access is largely reliant on the connectivity of the internet. For example, even if the entire world is already linked by networks, certain countries are still not connected to have an internet enough. The use of cloud computing simply doesn't "make sense" to those areas of the planet that don't have Internet access. In today's environment, no one needs to use cell data for computing programmes they are running. They want wireless networking, but they have no access. Even cloud services with more security and the defense are already in place. At times, the merchant is not responsible for any possible breach. There is no legal complication inherent with the cloud as data is processed in it in one country and used in other countries.

However, it's a good idea to keep an eye out for the maximum bandwidth. Speed alone isn't enough. The quantity of data that may be delivered simultaneously is known as bandwidth. In the event that you have a high internet speed but a low bandwidth rate, you will still struggle to access the cloud at the same time. Using the analogy of an expressway, the internet connection has a limited number of lanes with a high volume of traffic. Expanding the number of lanes or reducing the number of cars going by is necessary if the number of lanes is limited. For businesses with a large number of end users that want internet connection, having a lot of bandwidth is critical. To get the most out of your internet connection, you'll need extra infrastructure. Problems with your internet service provider or the manner you're accessing the internet might be causing the difficulty.

As a first step, your service provider may be experiencing an internal issue. If that's the case, your only option is to wait for an update on the status of your internet connection until it is fixed. Additionally, your internet connection may be an issue. It's possible that you're using a lot of data from numerous programmes and applications at once. Alternatively, there may be more customers on the network, which means that more data will need to be delivered, increasing the likelihood of a network slowdown. In addition to the rate of use, the network's infrastructure must also be taken into account. If so, what kind of connection do you have? If yes, how far away are you from the router in terms of distance? Which switches do you have quality? Always keep in mind that sending data across a distance has an effect. Getting closer to the router is preferable. To minimize the risk of data loss, it's best if your device is directly linked to the internet via an Ethernet cable.

With the launch of Bitcoin, Blockchain technology was implemented. Bitcoin is a kind of digital currency that was launched in 2008 with the pseudo name Satoshi Nakamoto. He created Bitcoin: A Peer-to-Peer Electronic Cash System, which provides direct transfer electronically between parties without any third parties. He is a white paper. This system is mostly used to resolve double spending, particularly the digital money design that allows for replication and spending more than once. This system is an electronic cash system. This problem is solved by tamper-resistantly connecting each transaction. The public directory is used to tamperproof link transactions. This leader helps a network to check the history of the deal, and to ensure that the coin was not used. Compared to Blockchain for Bitcoin, we may claim that Blockchain is a technology used in safe and secret transactions for several cryptocurrencies including Bitcoin.

Yet Blockchain is a transparent system for the supply of secrecy by Bitcoin. During online transactions Bitcoin is used for Blockchain transfer of records, rights and so on. Blockchain thus has a wider approach, whereas Bitcoin is confined to digital currency trading. Blockchain can be described as open, digitally signed transaction ledgers clustered into blocks. Each block includes a cryptographically generated hash value, which connects blocks to blocks, timestamps and transaction information. It is unable to change the concept of Blockchain results. It is a distributed, transparent ledger that can securely and permanently document transactions between the parties [12].

As an input, a hash function may handle any length of string (numbers, letters, media files). Bit lengths can range from 32 bits to 128 bits to 256 bits, depending on the hash function being used, with the most common being 64 bits. In computing, this is known as a hash. As a side effect of using a hash algorithm, we get a hash like this. Bitcoin's Blockchain relies on a cryptographic hash function's feature for its consensus process in this scenario. To put it simply, a cryptographic hash is the digital fingerprint of a specific quantity of data. Transactions are fed through a hashing process, which produces a fixed-size output in cryptographic hash functions.

The Blockchain is a permanent digital directory that records economic transactions and programming them to preserve almost anything that has a meaning not merely in financial transactions. When applying Blockchain technology, no intervention is needed from the government and zero percent fraud is expected because of consensus confirmation. Instant transfers can be performed without paying processing costs by avoiding the presence of a third party. This increases financial quality. Notwithstanding all these benefits, Blockchain is unbelievably unpredictable and has many drawbacks. There are ways to widen the number of crimes committed by society because the user or node outside the network cannot find out about anonymous transactions [13]. A form of key management system known as a "public-key infrastructure" makes use of digital certificates to authenticate users and public keys to encrypt data. SSL and TLS, which both require PKIs, are widely used in Web communications.

## 2 Literature Review

The current encryption access control system based on the attribute is largely based on the single center. If you don't trust or maliciously challenge the center's authority, it may trigger a big leak. Some academics have suggested a multiple-authority attribute-based access control method for encoding the center's power in response to this issue. Various authorities are recommended to allocate attribute-based encryption schemes to users in the scheme, which would minimize the likelihood of the failure of a single central authority [4]. A multi-authority threshold for the fuse encryption of identities, without a central authority, enhancing multi-authority device security requirements is discussed in [10]. A decentralizing, multi-authority encryption system, without any core in essence is suggested in [8].

A system is developed in [14] to monitor access by multi-authorities and created a particular scheme to control access by multiple authorities. Not only does this scheme reduce the possibility of single malfunction triggered by a single authority, but it facilitates the upgrading of data users' attributes in a multi-authority environment. A secure and efficient monitoring mechanism is discussed in [15] for several authorities to guarantee access by a linear secret exchange, which significantly decreased the burden on the particular authority by many authorities. Blockchain technology is developed in [16] first and, until now, several Blockchain implementations have reached numerous industries, especially in areas where a trustworthy third party is necessary.

The Blockchain can be trusted internationally as its transparent and distributed framework. Since Blockchain technology is a valuable tool for wide-ranging cooperation without shared confidence between individuals [17]. Therefore, it can be used for dealing with transactions initially handled by intermediaries in many conventional centralization fields. A shared computing paradigm is suggested in [18] point-by-point that allows multiple stakeholders to store and handle data together while fully keeping the data private. This model dynamically handles personal data by removing the need for reputable third parties. A decentralized Blockchain in [19] is based on access management mechanism.

The Blockchain nodes validate the user's authority and apply a time dimension to the shared file encrypted with ciphertext policy attributes. A model is implemented in [20] for data sharing across Blockchain cloud providers. The model uses the benefits of intelligent contracts and processes to manage data access actions efficiently and to revoke access authorization for violations of access laws, in an unconfidently environment, to resolve the question of medical data sharing. A decentralized power management (BlendCAC) process in [12] efficiently secures the security of the broad IoT (Internet of Things) infrastructure for facilities, resources and information. A system is designed in [21] for monitoring, handling and implementing certain data sharing arrangements using intelligent contracts and Blockchain technologies.

A Blockchain based safe mutual mechanism is available in [11]. Scientists have widely agreed that the integration of Blockchain technologies and access management mechanism is an effective way to address the confidence issues that still occur today. Authentication in order to implement fine grain access control policies, provide privacy and protection assurances for starters, Blockchain technology is used in literature for storing the user's access control lists, Blockchain technology is used for biomedical and health care applications, and three smart access control contracts are implemented for the Internet of Things. However, the technology Blockchain has just appeared.

Most of the study into the decentralization of access control technology, such as literature, is still at the stage of growth, and few concrete plans exist. Many Blockchain-based technologies are being developed progressively. Any of the requests depend on authentication of transfers, such as digital currencies, stock exchange or financial assets. Some are trying to merge Blockchain with IoT, such as the storage of IoT system data. Other decentralized Blockchain apps include games, poker, voting online, car rentals etc. In this case, we would concentrate on an application for a supply chain, which is close to the sales information recording of our system [22]. The previous study on Blockchain-based supply chain management is discussed below.

In [16], the authors provide Blockchain with the architecture criteria for supply chain management. The authors pointed out that falsified goods are an essential concern that must always be understood by modern brands of international supply chains. Blockchain will exclusively track the movement of goods across the data records of the supply chain. The benefits and drawbacks of binding Blockchain RFID [15] supply chain technology are analyzed in [23] that cover the process of Blockchain information management. The author argues that the information stored on the Blockchain may be fully trusted provided the characteristics of the Blockchain.

In the case study, origin Chain is used for product traceability and the method applied. This framework applies product traceability by substituting Blockchain data storage for traditional centralized database. The main concept is to document the effects of the product research of the laboratory. A product ownership scheme, released in 2017, provides an Ethereum system that supplies a customer keeping certificate to guarantee that the goods have identification in the Blockchain and that they are combined with the RFID of products. However, the suggested agreement cannot ensure that the commodity that the vendor bought by the buyer is not fraudulent [14].

The substance falsified issue remains thus unresolved. In the market side, Seal Network integrates Blockchain technologies with Near Field Communication (NFC) to build a commodity verification platform. In this business, NFC chips are inserted into each object and used as a product certificate. The NFC data was submitted to the Blockchain of the organization. The use of NFC chips, however, is not sufficient for all product forms, fresh produce or small goods, for example. Moreover, buyers have to carry the goods from the retailers in this form of scheme and not directly from the suppliers and the consumers could understandably be worried about the merchants' faith. There is very little arrangement of data stored in the cloud. The stored information in the Blockchain is strongly ordered. The data can be tracked using each block's hash key [18].

Each block includes the hash key of the previous block and it is vital that the network stays monitored. The data in the block is checked and the nodes in the network can be reached. Cloud embraces firmness and can accommodate device load variability if necessary. With the support of a Distributed Boss, you can effectively navigate a vast number of events that lead to a range of intelligent contracts that guarantee the quality of service. Blockchain also guarantees anonymity for the user and will securely erase the record of the user from the system in order to avoid third parties from accessing details of the user. The cloud integration of Blockchain would also maintain trust for many companies and make it a on request service [24].

## 3 Research Contributions

In this paper, we propose to implement Ethereum architecture of Blockchain to record the ownership of products in Blockchain. Buyers don't have to rely on trusted third parties in order to know the component of the purchased product in full with the Blockchain's untraceability and transparency properties and to make sure no record is forged on the Blockchain [25]. In order to achieve safe and unforgettable anti-compression authentication, SMEs can implement the anti-counterfeit application system suggested in this paper and only need to pay a relatively low operating cost.

This system allows companies to increase the confidence of users over the brand and solves the problem of small and medium-sized enterprises, which cannot open direct stores and which cannot cooperate with large chain dealers [26]. In an overview of our system, the objective is to solve the brand certification issue, focusing on the expansion of sales channels and offering small vendors an opportunity to demonstrate the source of each component. This structure is only to pay the sum necessary for the creation and modification of its contract status. With the use of fully disclosed intelligent contractual data, everyone can easily prove the company's legitimate source and also provide evidence for the consumer to buy goods. For retailers, it can be proved whether they offer real goods by using this falsified Blockchain system and are unable to compete any longer with falsified goods sold at reasonable prices.

A decentralized cloud development model based on Hybrid Blockchain is built for this analysis. In this model, it is assured that both sides will reach a development arrangement between themselves and follow the cloud production process using a smart contract in the Blockchain network without the need for a third party. The breakthrough of this study was that decentralized programmes would use smart contracts with the aid of the hybrid paradigm on public Blockchain networks. The hybrid model has made production arrangements and coordination more open, economic and trustworthy. Agreements can be maintained on the Blockchain network at low cost without any cloud technology needing to be installed. In this model, correspondence, sharing of data and transfer of fees between the parties is presented on a public Blockchain Network. A decentralized framework was also developed and clarified how the Ethereum network of shared Blockchain networks can be developed through smart contracts.

## 4 Proposed System

We deliver a comprehensive and irreproducible Blockchain-based system for counterfeiting products. In order to store the related updates on new sales in Blockchain that is open to everyone, the fabricators can use this method. The cumulative profits that are probable by the merchant are obvious to the customers, as is the number of items left by the merchant. The customer may automatically conduct supplier-side verification using the functions given by our device, and this authentication cannot be performed. Fig. 3 shows the overview of the proposed model.

In our model, there are three important models that we need to consider as follows.

Fabricator: In the case of the merchant, the tasks offered include inserting new addresses of the merchant for contracts, adding the amount of goods to be delivered by the merchant or gathering information about the merchant to restore the current revenue status. On the side of the customer, the goods sold by the distributor can be checked and the consumer can check whether the product has been traded or whether the current status is verified. The consumer's public key certificate has still been checked of the product.

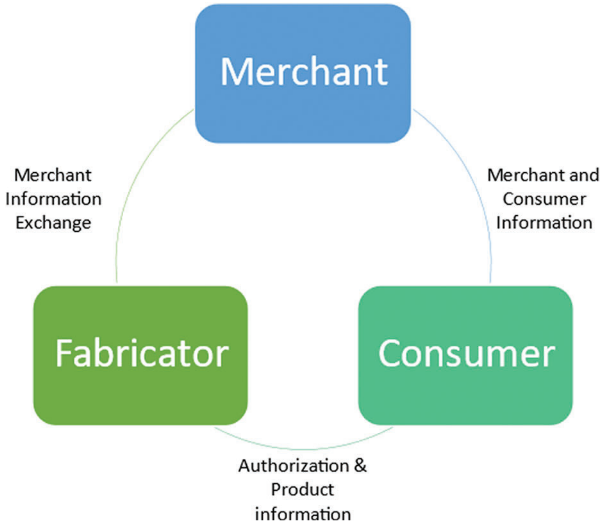

Merchant
Merchant Information Exchange
Merchant and Consumer Information
Fabricator
Consumer
Authorization & Product information

**Figure 3:** Proposed model

An intriguing element is that the Blockchain may be utilized as an authentication provider. Imagine you can verify yourself with government agencies, banks, airlines and other services with only one identity utilizing Blockchain technology. Using their key-pair, people register themselves identification on the Blockchain. This registered identity is a piece of information that comprises hashes of numerous identity related properties. For example, their name, government registration number, fingerprint recognition or other personally identifiable information. After that such a user may go to a recognized party, which checks the hashes earlier registered on the Blockchain and let the recognizing party "sponsor" that piece of information as the truth on the Blockchain. Other parties which trust the particular recognizing party may now trust the identity on the Blockchain and utilize it as an authentication or identifying technique. This situation involves a hurdle as it still requires a confidence between various parties of the advertisers and parties that identify them as a trustworthy sponsor which still isn't optimal. It is nonetheless a wonderful concept and an excellent start.

Merchant: The merchant can use the functions of the device to encrypt the verification data using a private key, while the user may use the public key of the merchant to check if that is what the merchant is. Following the acquisition and sale, the dealer states the address of the purchaser in the fabricator's contract to receive the details. The dealer is permitted to view information about his goods, such as sales lists and the amount of stock he owns.

Customer: On the part of the merchant the consumer will check whether the merchant has a sales connection with the fabricator and also if the stock of the merchant has not been sold out yet. The fabricator should show that their name is compatible with their address and the customer can receive individual purchasing reports and standing of their product in the case of a well-preserved contract address. Fig. 4 shows the flow design of proposed system.

In our design, the suppliers are responsible for transmitting merchant details, including the number of goods the merchant may sell and the address of the merchant. Following the approval by the Fabricator, the Merchant may receive a certain number of registration rights for the goods he may sell under the deal. The trader stores the customer address through the mechanism in the contract to end the deal when the consumer buys the commodity. Fig. 5 shows the authentication process of the proposed system.

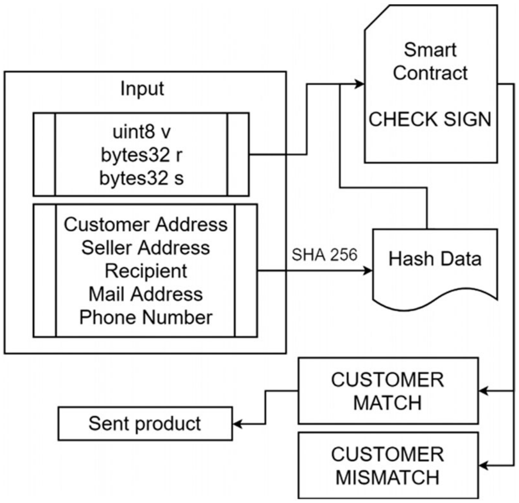


**Figure 4:** Flow design of proposed system

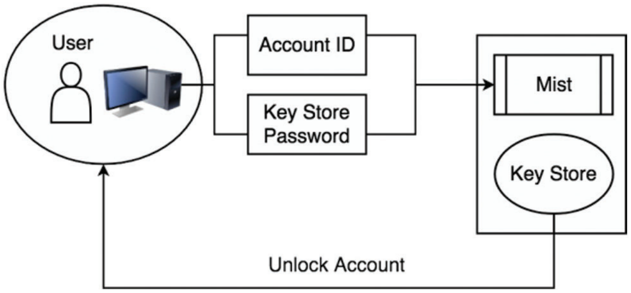


**Figure 5:** Authentication process

Consumers may use the framework to check specifically for a deal with the merchant and the unselling of goods. Upon purchase, the customer will notify the manual producer that the product needs to e-mail and encrypt it using a private key from the consumer. The fabricator collects and uses the encrypted files and public key to returning it to the user. When the information is in accordance with the information of the customer, the merchant sends the goods to the consumer and finishes the purchasing process.

## 5 System Design

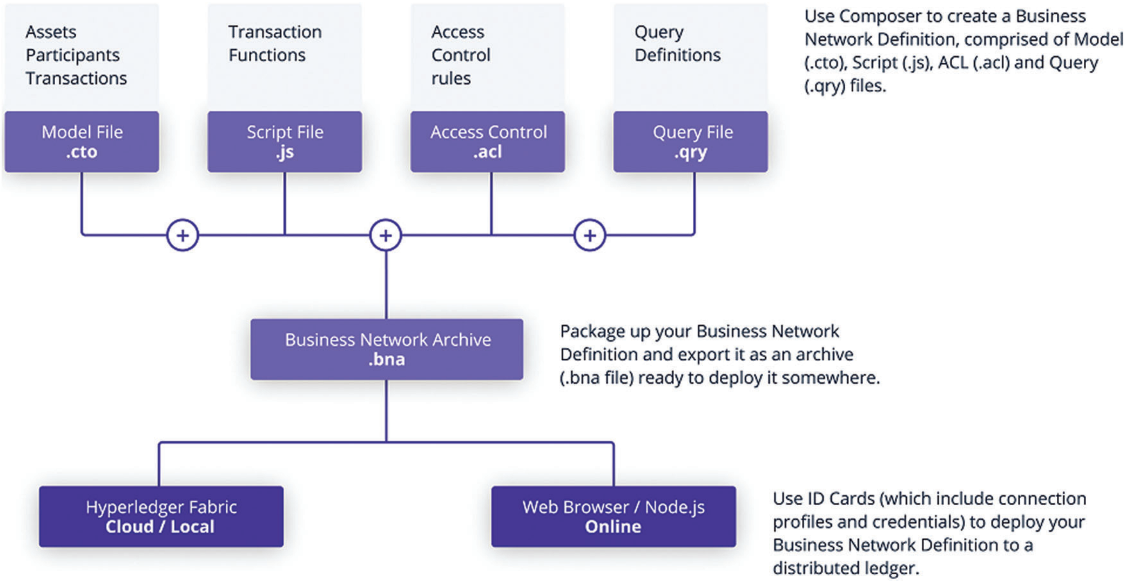
This implementation has been carried out in Google Cloud Platform (GCP). A Blockchain node can be identified as a Blockchain network system. The node class is graded according to the mission it executes. There are various types of nodes. Mining nodes still render the Blockchain bricks. These nodes only search whether the block in the process of mining can be added to the list. Mining nodes cannot hold blocks; only blocks are generated and inserted into the chain. Incorporated network blocks where complete nodes verify the Blockchain are released. Regulation of the complete node holds and transfers block copies to all nodes of the network. Their duty is to verify transactions during publication before genesis is stopped.

The data is forwarded to all other network nodes after authentication to ensure trust in the blockchains. It would not be difficult to crack it if there are more nodes in a more decentralized network. Based on the number of trades made by an entire node, a node may be considered a Super Node. Super Nodes are still involved and bind the majority of the total nodes in the network to make them appear. Light nodes are identical to complete nodes, but only a part of the complete block is included in them. You just have the previous transaction blocker to verify the Blockchain to notify the remaining nodes of the network. Light nodes are synonymous with and not as powerful to the parent node, i.e., the complete node.

When certain circumstances occur, a smart contract, a decentralized programme, will carry out its business logic. Digital rights management protected content may be unlocked and other sorts of data manipulation, such as altering the name on a property title, can be accomplished through the execution of smart contracts. For example, a smart contract may be used to enforce privacy protections by permitting the selective release of privacy-protected data to satisfy a particular request. It doesn't matter if all parties are on the same page when it comes to executing a multi-party procedure, because smart contracts may speed up the process regardless. However, when events spiral out of control and there is no mechanism to stop or unwind unexpected behaviour, this capability can exacerbate the damage they do.

In general, bitcoin miners make money in the form of bitcoin, although they frequently use fiat currency to cover their running costs, such as power and rent. Miners' currency exchange activity has a significant impact on the price and profitability of crypto currencies. Because of the technological difficulties required in the shift to proof of stake, there is a discussion that it is nearly impossible for Bitcoin to move to proof of stake, which would greatly disadvantage people who have put the most work into bitcoin currently present. Bitcoin's creator of Swiss crypto currency broker, Bitcoin Suture material, thinks that a proof-of-stake mechanism is inevitable for Bitcoin in the future.

If an entire node is compromised and the manipulated data is stored, the light node will catch and discard this Blockchain as false and send a Blockchain that is meant to retain the full node details. Since they do not have more data capacity, they lead to decentralization of the network and to a decreased cost of long distances than complete nodes. When inserting a block in the Blockchain, all nodes in the network must validate this block as true. Consensus algorithms are something of a protocol that manages the Blockchain network nodes in order to settle on a transaction order and to filter incorrect transactions. There is more than one transaction and the other for receiving a reward from the transaction to be written. Fig. 6 shows the implementation model using GCP.



Use Composer to create a Business Network Definition, comprised of Model (.cto), Script (.js), ACL (.acl) and Query (.qry) files.

Package up your Business Network Definition and export it as an archive (.bna file) ready to deploy it somewhere.

Use ID Cards (which include connection profiles and credentials) to deploy your Business Network Definition to a distributed ledger.

**Figure 6:** Implementation model using GCP

Consensus algorithms were designed to solve the problem of judgement. The miners are also hard to achieve a consensus, since the Blockchain network is distributed without a central authority. The consumer power of this proof-of-work consensus model is strictly proportional to the overall computing power of the system. The primary goal of the consensus models is the removal of dishonest nodes, namely truthful nodes. To log all transactions, a node must be selected in the decentralized network. One-way is a random node collection, but is prone to attack. If a user or node wishes to enter transactions, so they must prove they are not vulnerable to attacks on their networks. The consumer must face the difficulty of solving a dilemma.

Computational issues by attaching a node to the Blockchain are solved to get the reward. This network node is used to calculate the cryptographic hash function SHA-256 using a block header and a nonce. The miners are prone to alter the nonce in order to get different hash values. The miners can measure the value equivalent to or below a consensus value. The miner is passed into all other nodes in the network, when a miner reaches the target values, and all other nodes must check that the hash value is true to one another. If the data update is authorized, the other miners will be linked to it. Parallel to the target value found by multiple miners, valid blocks may sometimes be formed. In these cases, block divisions are created and are called competing forks.

Central and pairwise clustering are the two most common forms of clustering. Feature-based clustering, also known as central clustering, is a kind of this technique. Feature-based clustering, such as the K-means algorithm, is one such method. Because it can handle a broader range of input formats, pairwise clustering is a more generic and adaptable method to clustering. The preferred technique of clustering is dominant sets, a pairwise clustering approach that extends the concept of maximum clique to weighted networks. Metric embedding isn't necessary because it works with pairwise similarities. There are tens of thousands of transactions occurring every second within the Blockchain network. Studying common patterns in these increasingly many transactions is essential if we are to effectively manage and organize them. It's possible that grouping these rising numbers of transactions may reveal transactions that have common traits, as well as anomalous ones.

This study proposes a novel way for resolving security and integrity concerns at the device level, which is called the suggested model. For security and monitoring purposes, it is a linked list of the virtual existences of the actual network members. The chain of nodes is constructed on the present structure of the classic Blockchain. Traditional consensus algorithms have a different objective and a different consensus algorithm than this one. With this chain, devices' digital IDs are linked together, making it extremely difficult to fake or attack them.

The data to be maintained in a distributed structure is stored in stable contracts in this programmes. Saving all information in a stable contract would be a very expensive option to achieve a truly distributed structure. A data collection with a non-distributed solution is thus feasible. In the application, it will be a cost-effective approach to archive data into a local database that does not break agreements. The core idea of the programmes is that reliability can never be undermined. Stable contracts that guarantee process confidentiality, store and run key process information. However, a variety of specific information is processed in local databases with numerous methods during the execution of the process. This knowledge is detailed: A job design log, stable contract addresses, network capabilities, and much more. This knowledge can be viewed as a workaround to be processed on a central server.

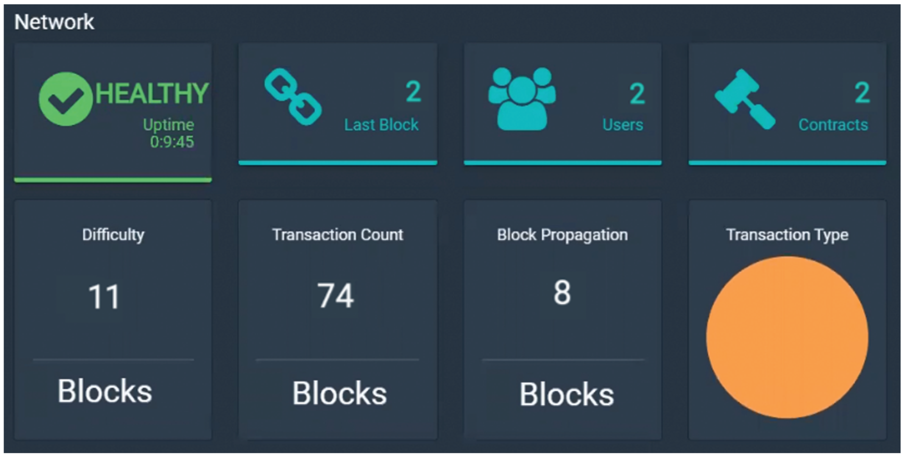
It is standard practice to use a device's digital signature and digital identity to authenticate the device. Blockchain technology is used to improve hardware security and integrity, digital identification, and authentication in this article. Extrinsic attributes like as memory attributes, software characteristics, PUF specifications, etc. based on each device's manufacturer requirements will be hashed and analyzed to generate a unique identifier (UID), which will be stored in the Blockchain for access to this database reasons. Devices' virtual presence in an independent ledger is represented by the chain of blocks. It's all about establishing an independent database to identify, analyze, delete, and add new switches and routers using a private form of Blockchain. There are links between each node's UID and each of its blocks in this linked list.

However, a clustered programmes will be unwanted to run when adhering to a key point. It creates significant long-term issues whether the application is associated with an individual or an entity in terms of protection and continuity. Different applications for cloud computing can be a useful method for now. In the private exchange between the parties in particular, this approach would be very realistic.

Every server in the Bitcoin network is required to solve a challenge as part of the proof of work confirmation method. Once an issue is solved, a new block may be added, as well as the miners are rewarded with bitcoin for their efforts. The nodes seem to be the administrative center of the network and check the validity of each block's transactions. Data is put onto the Blockchain once a block of transactions has been confirmed. The proof-of-stake consensus protocol was developed as an alternative method to the proof-of-work protocol because of concerns about scalability and environmental sustainability.

## 6 Results and Discussion

In terms of validity and performance, the proposed model is tested in two headings. As for the applicability, unlike other distributed cloud industrial applications, there are certain restrictions to how the model can be implemented on a public Blockchain network. With respect to consistency, analyses of how mediators are excluded and how a trust atmosphere can be provided have been carried out. An analysis of how cloud development processes can be run on a public Blockchain network has been carried out. Users can share work resources in a decentralized system without a central framework on a cloud development system via the built app. Fig. 7 shows the dashboard in GCP.



Network

HEALTHY
Uptime
0:9:45

2
Last Block

2
Users

2
Contracts

Difficulty
11
Blocks

Transaction Count
74
Blocks

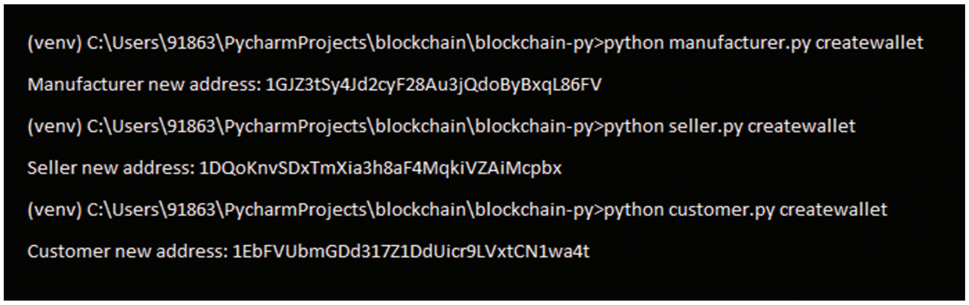
Block Propagation
8
Blocks

Transaction Type

**Figure 7:** Implementation of Blockchain-dashboard in GCP

The distinction with this framework is that transactions are made on Blockchain from conventional cloud development applications. By using a public network, anybody without any registration or affiliation was allowed to use the programmes. The private Blockchain protection can be protected in public Blockchain networks through encryption methods. Internal Blockchain network secrecy transfers in public Blockchain networks are not feasible. This role enhances the transparency of transactions in the application. This programmes is supposed to operate on the network of shared blockchains. However, the public Blockchain network does not hold such required information but it is saved in the local database. This database derives support from another database.

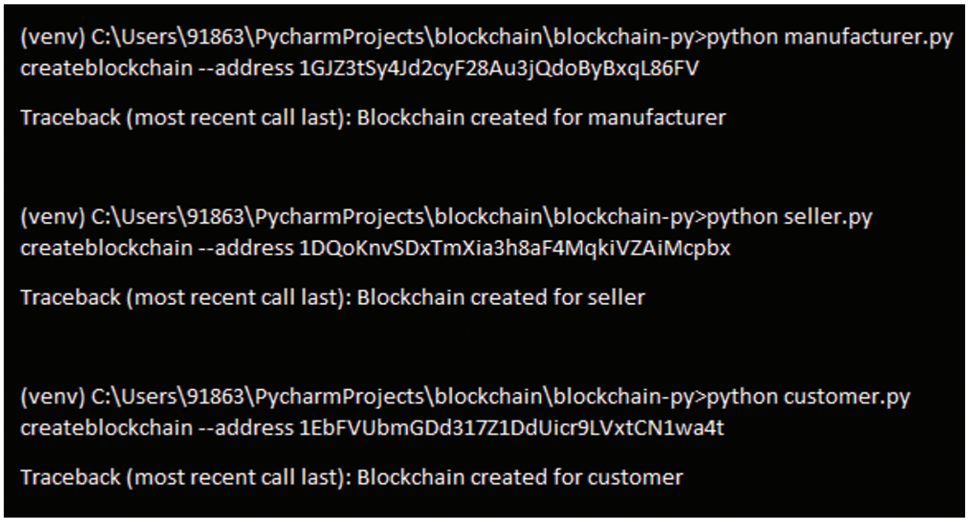
This repository may be a central or distributed server. What is essential here is not to store any information that needs a hosting charge on the public Blockchain network. Detailed knowledge like product design should be transferable to the framework, unique messages across multiple networks, resource knowledge. These channels may be private server or cloud-based computing areas. The transfers of information outside the Blockchain network do not breach the arrangement between the parties. The data size is highly significant in the Ethereum network, there is a transaction cost. The Ethereum network information can include only fundamental information from the arrangement between the participants. The current Blockchain network is used when selecting the public Blockchain network and there is no requirement for extra costs. Fig. 8 shows the creation of unique wallets for FMC.



```
(venv) C:\Users\91863\PycharmProjects\blockchain\blockchain-py>python manufacturer.py createwallet

Manufacturer new address: 1GJZ3tSy4Jd2cyF28Au3jQdoByBxqL86FV

(venv) C:\Users\91863\PycharmProjects\blockchain\blockchain-py>python seller.py createwallet

Seller new address: 1DQoKnvSDxTmXia3h8aF4MqkiVZAiMcpbx

(venv) C:\Users\91863\PycharmProjects\blockchain\blockchain-py>python customer.py createwallet

Customer new address: 1EbFVUbmGDd317Z1DdUicr9LVxtCN1wa4t
```

**Figure 8:** Creation of unique wallets for FMC

Thus, users can use the new network without Blockchain investment. Using the public Blockchain network, users only receive one payment per practical implications. There is an administrator of the proprietary Blockchain or decentralized consensus networks. Unique individuals control these networks. In preparation for the system to meet an operating expense continually thrive. However, no extra cost to the network's sustainability is included in this application. Fig. 9 shows the creation of Blockchain for FMC individually.



```
(venv) C:\Users\91863\PycharmProjects\blockchain\blockchain-py>python manufacturer.py
createblockchain --address 1GJZ3tSy4Jd2cyF28Au3jQdoByBxqL86FV

Traceback (most recent call last): Blockchain created for manufacturer


(venv) C:\Users\91863\PycharmProjects\blockchain\blockchain-py>python seller.py
createblockchain --address 1DQoKnvSDxTmXia3h8aF4MqkiVZAiMcpbx

Traceback (most recent call last): Blockchain created for seller


(venv) C:\Users\91863\PycharmProjects\blockchain\blockchain-py>python customer.py
createblockchain --address 1EbFVUbmGDd317Z1DdUicr9LVxtCN1wa4t

Traceback (most recent call last): Blockchain created for customer
```

**Figure 9:** Creation of blockchain for FMC individually

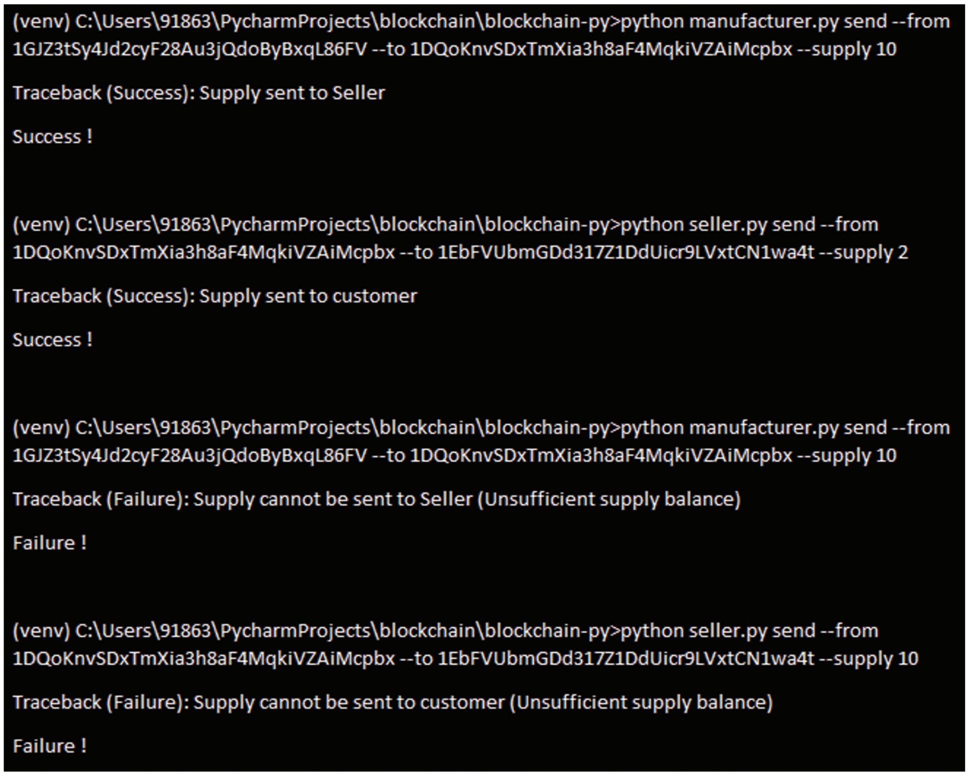
The operation of the proposed system has the following steps: Authentication Procedure: The user must select which account to login before connecting to the device. As long as Auth has started, user accounts are linked to the Auth accounts, the user can pick the account, which is attached to the Auth product code account list. The user must then enter a secure file that contains the private key in the KeyStore file. Finally, the user will pick the specific details from the contract address and press the Save button.

When we need to maintain the authenticity of a message and the sender's legitimacy, we may utilize keys stored in our application's keystore to sign the payload. When we're running a server and need to use HTTPS, we'll often use a keystore. The server retrieves the private key from the keystore and provides the public key and certificate to the client during an SSL handshake. It follows that the client must submit its public key and certificate in order to authenticate itself in a mutual authentication scenario. Because the default keystore doesn't include a key for encrypted channels, we'll need to set up the appropriate ways to utilize one. Using a class, we may alter our keystore format if it differs from the default. We may, of course, utilize these keys for other purposes. Public and private keys are used to sign and decrypt data, respectively. These functions can also be performed using secret keys. A keystore is a place where we may keep our keys safe and secure.

Trade public records: The information on vendors is entirely public for the purpose of transparency. Our system offers intelligent search for contract details that allows you to return each merchant's vendor's list, buyer list and other retailer records. Using Blockchain technology, it is possible to create a data structure with intrinsic security. Using cryptography, decentralization, and consensus principles, it ensures that transactions are secure. Each block of data in most Blockchain or distributed ledger technology (DLT) comprises a transaction or bundle of transactions. All the previous blocks are linked together in a cryptographic chain, making it almost hard to tamper with any of the new ones. There is a consensus process in place to ensure that all transactions in the blocks are correct and truthful. Members of a distributed network can participate in decentralization through the use of Blockchain technology. All transactions are recorded and there is no single point of failure. However, certain essential features of security differ between Blockchain and other systems.

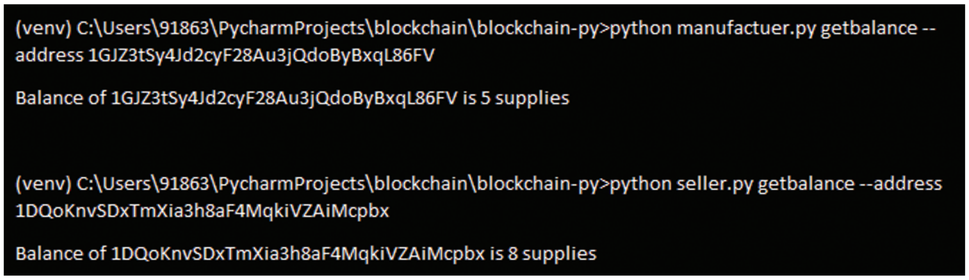
Attaching the merchant's information: In our scheme, including the inclusion of new merchant's addresses and even the addition of a range of items from a single merchant, enables producers to monitor merchant's information in this way. The smart contract software first tests if the developer is the purpose setter. If it is right, the software shall create a vendor structure and set the maximum number of goods to be sold to the merchant, this can subsequently also be updated. Additionally, a strong transaction ledger may be maintained with the help of a reliable consensus mechanism in the Blockchain implementation. Reliability ensures that the system always responds the same way to a transaction's status. According to one example, the "stable" status of one transaction can be stated by one node on a network "A stable condition should be reported by all other nodes on the network if they are asked and reply truthfully. All nodes or processes finally agree on a choice or a value because of liveness. "eventually" refers to a point in the future", it suggests that a sufficient period of time may be required to reach an agreement. It guarantees that a transaction ledger is strong so that only valid transactions are accepted and become permanent by combining persistence and liveness. Fig. 10 shows the supply distribution for FMC.

Unique User Goods Share Provision: When clients prove identification and the account to which it is being transmitted. The merchant shall first check if the identification is right and then decide whether the details about the consumer goods have been used in the smart contract. For a statement, this feature checks whether the fabricator is the setter. If not, through adjusting the value the function would return. Fig. 11 shows the supply balance variation for FMC.



```
(venv) C:\Users\91863\PycharmProjects\blockchain\blockchain-py>python manufacturer.py send --from
1GJZ3tSy4Jd2cyF28Au3jQdoByBxqL86FV --to 1DQoKnvSDxTmXia3h8aF4MqkiVZAiMcpbx --supply 10

Traceback (Success): Supply sent to Seller

Success !


(venv) C:\Users\91863\PycharmProjects\blockchain\blockchain-py>python seller.py send --from
1DQoKnvSDxTmXia3h8aF4MqkiVZAiMcpbx --to 1EbFVUbmGDd317Z1DdUicr9LVxtCN1wa4t --supply 2

Traceback (Success): Supply sent to customer

Success !


(venv) C:\Users\91863\PycharmProjects\blockchain\blockchain-py>python manufacturer.py send --from
1GJZ3tSy4Jd2cyF28Au3jQdoByBxqL86FV --to 1DQoKnvSDxTmXia3h8aF4MqkiVZAiMcpbx --supply 10

Traceback (Failure): Supply cannot be sent to Seller (Unsufficient supply balance)

Failure !


(venv) C:\Users\91863\PycharmProjects\blockchain\blockchain-py>python seller.py send --from
1DQoKnvSDxTmXia3h8aF4MqkiVZAiMcpbx --to 1EbFVUbmGDd317Z1DdUicr9LVxtCN1wa4t --supply 10

Traceback (Failure): Supply cannot be sent to customer (Unsufficient supply balance)

Failure !
```

**Figure 10:** Supply distribution for FMC



```
(venv) C:\Users\91863\PycharmProjects\blockchain\blockchain-py>python manufactuer.py getbalance --
address 1GJZ3tSy4Jd2cyF28Au3jQdoByBxqL86FV

Balance of 1GJZ3tSy4Jd2cyF28Au3jQdoByBxqL86FV is 5 supplies


(venv) C:\Users\91863\PycharmProjects\blockchain\blockchain-py>python seller.py getbalance --address
1DQoKnvSDxTmXia3h8aF4MqkiVZAiMcpbx

Balance of 1DQoKnvSDxTmXia3h8aF4MqkiVZAiMcpbx is 8 supplies
```

**Figure 11:** Supply balance validation for FMC

Contract document of the buyer: the merchant can insert the consumer account in the intelligent contract when the merchant and consumer transaction is made. Each merchant has a merchant structure and the merchant places the customer addresses in the region of the owner of the merchandise. In comparison, the merchant's commodity owner domain can only be given access privileges set by the vendor.

Transactions submitted by users trigger the execution of smart contracts by the Blockchain nodes. For every smart contract function call, there is an associated destination function, a payload containing input values, and the submission signature. This means that any node in the Blockchain network can submit a transaction to the whole network, which will be broadcast to all other nodes. It is at some time throughout the transaction that the executable programme in the target smart contract is executed by each individual node. An updated Blockchain will be created if this transaction is successful. A smart contract may reject the transaction as a failure if the input is deemed invalid by the smart contract.

Authenticity review: Authenticity check is one of our system's most critical components. Users will use their address for themselves in our scheme. The address is specified for the last 20 bits of the public key of the recipient. In order to alter the current Ethereum contract, the customer must sign the agreement using his private key and digital signature. As long as the private key of the user is secure, no means would be available to alter the identity of the user. Our framework enables people to use their digital signature to sign if necessary, to authenticate the presence of each other. Authentication information of the customer often offers a feature to validate each other.

## 7 Conclusion

The application constructed will run through a continuous living network in a distributed way. There is no need to use a single version of software created in this architecture. The users on the Ethereum network will concurrently use different models. The updated edition of the code allows users to upgrade their software with new agreements, whether they wish to benefit from the changes. Benefiting from the open source programmes, users can continue using the framework for multiple iterations by changing the codes to their tastes. A software that can be constantly created and available at any moment, independent of the individual or organization, will be very exciting. The edition sold by the organization must be used in core applications. The company's life will be up to the background of the deals to be made. This paper seeks to provide optimal protections for the collection and access of data by blocks in various cloud user environments. Legitimate users are only authorized to store and view data as a protected block chain solution. Like the Blockchain, which doesn't need a central transaction mechanism, the proposed network interface is also autonomous. It takes roughly 4.7, 6.2, and 7.5 ms, respectively, to register each node in the proposed system for 5, 10, and 15 nodes. The overall registration time for each scenario is 11.9, 26.2, and 53.1 ms, despite the fact that each node's registration time was greatest for 10 nodes. By looking at the data, it's clear that the number of nodes is a function of time. To prevent counterfeiting, the decentralized system is created. The method allows the producer to invest fewer or zero money to verify directly run shops. Besides all of this, it poses important concerns for consumers in private networks that the network is dominated by one individual or entity. Furthermore, a private network entity must be responsible for the server resources. A composite structure has been chosen for these purposes. Users will make production arrangements and payments between each other without any intermediary with this model. In this study, an example framework aims to clarify the use of Blockchain technologies in cloud production and it is aimed at throwing light on future studies. For potential jobs, stable contracts may be created and the system can specifically be incorporated with other services, including such Sales as a service.

**Funding Statement:** The authors received no specific funding for this study.

**Conflicts of Interest:** The authors declare that they have no conflicts of interest to report regarding the present study.

## References

[1] S. Alansari, F. Paci and V. Sassone, "A distributed access control system for cloud federations," in *IEEE Int. Conf. on Distributed Computing Systems*, Atlanta, GA, USA, pp. 2131–2136, 2017.

[2] B. Kaynak, S. Kaynak and Ö. Uygun, "Cloud manufacturing architecture based on public blockchain technology," *IEEE Access*, vol. 8, pp. 2163–2177, 2019.

[3] J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-policy attribute-based encryption," in *IEEE Symp. on Security and Privacy*, Berkeley, CA, USA, pp. 321–334, 2007.

[4] M. Chase, "Multi-authority attribute based encryption," in *Theory of Cryptography Conf.*, Berlin, Heidelberg, Springer, pp. 515–534, 2007.

[5] H. G. Do and W. K. Ng, “Blockchain-based system for secure data storage with private keyword search,” *IEEE World Congress on Services*, Honolulu, HI, USA, pp. 90–93, 2017.

[6] C. V. Murthy, M. L. Shri, S. Kadry and S. Lim, “Blockchain based cloud computing: Architecture and research challenges,” *IEEE Access*, vol. 8, pp. 205190–205205, 2020.

[7] G. Magyar, “Blockchain: Solving the privacy and research availability tradeoff for EHR data: A new disruptive technology in health data management,” *IEEE 30th Neumann Colloquium*, Budapest, Hungary, pp. 135–140, 2017.

[8] A. Lewko and B. Waters, “Decentralizing attribute-based encryption,” in *Annual Int. Conf. on the Theory and Applications of Cryptographic Techniques*, Tallinn, Estonia, pp. 568–588, 2011.

[9] T. T. Kuo, H. E. Kim and L. Ohno-Machado, “Blockchain distributed ledger technologies for biomedical and health care applications,” *Journal of the American Medical Informatics Association*, vol. 24, no. 6, pp. 1211–1220, 2017.

[10] H. Lin, Z. Cao, X. Liang and J. Shao, “Secure threshold multi authority attribute based encryption without a central authority,” *Information Sciences*, vol. 180, no. 13, pp. 2618–2632, 2010.

[11] C. Lin, D. He, X. Huang, K. K. Choo, A. V. Vasilakos *et al.,* “BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0,” *Journal of Network and Computer Applications*, vol. 116, no. 3, pp. 42–52, 2018.

[12] R. Xu, Y. Chen, E. Blasch and G. Chen, “Blendcac: A smart contract enabled decentralized capability-based access control mechanism for the IoT,” *Computers*, vol. 3, no. 39, pp. 1–12, 2018.

[13] S. Wang, X. Wang and Y. Zhang, “A secure cloud storage framework with access control based on blockchain,” *IEEE Access*, vol. 7, pp. 112713–112725, 2019.

[14] K. Yang and X. Jia, “Attributed-based access control for multi-authority systems in cloud storage,” in *IEEE 32nd Int. Conf. on Distributed Computing Systems*, Macau, China, pp. 536–545, 2012.

[15] J. Wei, W. Liu and X. Hu, “Secure and efficient attribute-based access control for multiauthority cloud storage,” *IEEE Systems Journal*, vol. 12, no. 2, pp. 1731–1742, 2016.

[16] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” *Bitcoin*, vol. 8, pp. 1–15, 2008.

[17] J. Ma, S. Y. Lin, X. Chen, H. M. Sun, Y. C. Chen *et al.,* “A blockchain-based application system for product anti-counterfeiting,” *IEEE Access*, vol. 8, pp. 77642–77652, 2020.

[18] G. Zyskind and O. Nathan, “Decentralizing privacy: Using blockchain to protect personal data,” *IEEE Security and Privacy Workshops*, San Jose, CA, USA, pp. 180–184, 2015.

[19] M. Jemel and A. Serhrouchni, “Decentralized access control mechanism with temporal dimension based on blockchain,” in *IEEE 14th Int. Conf. on E-business Engineering*, Shanghai, China, pp. 177–182, 2017.

[20] Q. I. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du *et al.,* “MeDShare: Trust-less medical data sharing among cloud service providers via blockchain,” *IEEE Access*, vol. 5, pp. 14757–14767, 2017.

[21] K. Liu, H. Desai, L. Kagal and M. Kantarcioglu, “Enforceable data sharing agreements using smart contracts,” *arXiv preprint arXiv:1804.10645*, pp. 1–8, 2018.

[22] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, X. Zhang *et al.,* “BBDS: Blockchain-based data sharing for electronic medical records in cloud environments,” *Information*, vol. 8, no. 2, pp. 1–16, 2017.

[23] P. J. Lu, L. Y. Yeh and J. L. Huang, “An privacy-preserving cross-organizational authentication/authorization/accounting system using blockchain technology,” in *IEEE Int. Conf. on Communications*, Kansas City, MO, USA, pp. 1–6, 2018.

[24] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, J. Wan *et al.,* “Smart contract-based access control for the internet of things,” *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1594–1605, 2018.

[25] S. Murugan, T. R. Ganesh Babu and C. Srinivasan, “Underwater object recognition using KNN classifier,” *International Journal of MC Square Scientific Research*, vol. 9, no. 3, pp. 48–52, 2017.

[26] Y. Nagesh and G. Prakash, “Secure and efficient block chain based protocol for food beverages,” *International Journal of MC Square Scientific Research*, vol. 10, no. 3, pp. 16–27, 2018.