REPUBLIC OF TÜRKİYE

ALTINBAŞ UNIVERSITY

Institute of Graduate Studies

Electrical and Computer Engineering

PROVIDE A NEW FRAMEWORK FOR BLOCKCHAIN BASED INTEGRATED AND RESOURCE CLASSIFICATION FOR THE CLOUD

Firas Hammoodi AL-MUTAR

PhD Dissertation

Supervisor

Prof. Dr. Osman Nuri UÇAN

Istanbul, 2022

PROVIDE A NEW FRAMEWORK FOR BLOCKCHAIN BASED INTEGRATED AND RESOURCE CLASSIFICATION FOR THE CLOUD

Firas Hammoodi AL-MUTAR

Electrical and Computer Engineering

PhD Dissertation

ALTINBAŞ UNIVERSITY

2022

The dissertation titled "PROVIDE A NEW FRAMEWORK FOR BLOCKCHAIN BASED INTEGRATED AND RESOURCE CLASSIFICATION FOR THE CLOUD" prepared by FIRAS HAMMOODI AL-MUTAR and submitted on 20/12/2022 has been **accepted unanimously** for the degree of PhD in Electrical and Computer Engineering.

Prof. Dr. Osman Nuri UÇAN

Supervisor

Thesis Defense Committee Members:

Prof. Dr. Osman Nuri UÇAN	Department of Electrical and Electronics Engineering, Altınbaş University	_____
Asst. Prof. Dr. Abdullahi Abdu İBRAHİM	Department of Computer Engineering, Altınbaş University	_____
Asst. Prof. Dr. Sefer KURNAZ	Department of Software Engineering, Altınbaş University	_____
Asst. Prof. Dr. Oğuz ATA	Department of Computer Engineering, Altınbaş University	_____
Prof. Dr. Hasan Hüseyin BALIK	Department of Computer Engineering, Yıldız Technical University	_____
Asst. Prof. Dr. Adil Deniz DURU	Department of Sports and Health Sciences, Marmara University	_____

I hereby declare that this dissertation meets all format and submission requirements of a PhD dissertation.

Submission date of the thesis to Institute of Graduate Studies: ___/___/___

I hereby declare that all information/data presented in this graduation project has been obtained in full accordance with academic rules and ethical conduct. I also declare all unoriginal materials and conclusions have been cited in the text and all references mentioned in the Reference List have been cited in the text, and vice versa as required by the abovementioned rules and conduct.

Firas Hammoodi AL-MUTAR

Signature

ABSTRACT

PROVIDE A NEW FRAMEWORK FOR BLOCKCHAIN BASED INTEGRATED AND RESOURCE CLASSIFICATION FOR THE CLOUD

Al-Mutar, Firas Hammoodi

PhD, Electrical and Computer Engineering, Altınbaş University,

Supervisor: Prof. Dr. Osman Nuri UÇAN

Date: December /2022

Pages: 86

Researchers in the manufacturing sector have recently shown an increased interest in the topic of cloud creation. Cloud generation is a customer-centric production strategy based on cloud computing, with the primary goal of providing access based on comprehensive service demand. The existing cloud architecture, on the other hand, has issues with a centralized network structure and operations. Basically, a centralized network offers insufficient flexibility, effectiveness, reliability, and security. In this study, the development of a decentralized network architecture for the cloud generation is made possible by blockchain technology. With Blockchain acting as a peer-to-peer network, a centralized peer-to-peer network might be created. The healthcare industry grew and became a significant actor in the provision of services. In recent years, patients have found remote observation services to be more beneficial. Healthcare practitioners create observation systems that diagnose and prescribe therapy in hospitals or clinics when patients are not actually present. Sensors are implanted in/on the bodies of patients. Wireless data interchange is possible across healthcare systems. Using characteristics from the blockchain, healthcare systems could be enhanced (e.g. distributed ledger, decentralized storage, and authentication). In this way, smart contracts automate the authentication and distribution of information, as well as participant criteria. When the number of users or other components increases, blockchains and smart contracts should maintain

quality service. Scalability, increased security, and optimal performance are all technical challenges of smart contracts based on blockchains.

Keywords: Blockchain, Peer-To-Peer, Smart Contract, Healthcare, Scalability, Security, Performance

TABLE OF CONTENTS

Pages

LIST OF TABLES

Pages

LIST OF FIGURES

Pages

ABBREVIATIONS

LANs	:	Local Area Networks
P2P	:	Peer-to-Peer
GUI	:	Graphical User Interface
APIs	:	Application Programming Interface
Dapp	:	Decentralized applications
PoW	:	Proof of Work
PoS	:	Proof of Stake
POA	:	Proof of Authority
BFT	:	Byzantine Fault Tolerant
PBFT	:	Practical Byzantine Fault Tolerant
BAACS	:	Blockchain as a Cloud Service
BaaS	:	Backend-as-a-Service
AMI	:	Amazon Machine Image
CM	:	Cloud Manufacturing
EVM	:	Ethereum Virtual Machine
OrBAC	:	Organization-Based Access Control
PAM	:	Principal Authorization Manager
RBAC	:	Role-Based Access Control
CH	:	Cluster Head
APIs	:	Application Programming Interfaces

CSA	:	Cloud Security Alliance
IDS	:	Intrusion Detection System
LAN	:	local Area Network
CSP	:	Content Security Policy
IDS	:	Intrusion Detection Systems
HSMs	:	Hardware Security Modules
MPC	:	Media Player Classic
UML	:	Unified Modeling Language
IDE	:	Integrated Development Environment
UI	:	User Interface
HSM	:	Hierarchical State Machine
SAAS	:	Software As A Service
IoMT	:	Internet of Medical Things
FHCs	:	Federated Hospital IoT Clouds
IoT	:	Internet of Things
ASE	:	Advanced Signature-Based Encryption

1. INTRODUCTION

Blockchain are a specific type of decentralized that enables individuals to trust each other to exchange transactions without depending on a middleman. Transactions are totally transparent, immune to tampering, and confidential. Previous transactions are immutably preserved, and a shared record is established. Not only have blockchains sparked interest in computer science and economics, but their potential influence has also sparked interest in other groups and businesses looking to capitalize on the previously stated qualities [1]. The cloud computing concept has grown in popularity in business since its beginnings. Some of the characteristics that have made business operations cloudy are scalability, ease, ubiquity, and high demand. The potential for cloud computing to deliver great benefits to industry and society has piqued the interest of the scientific community. The creation of user resources and their publication is based on the publishing source's request. Demand for resources guarantees that resources are allocated efficiently and cost-effectively. Investing in IT infrastructure does not require a great deal of money from individuals and businesses. . Customers use cloud-based resources and are charged based on usage. Cloud providers, on the contrary, can reuse resources as soon as a specific user relinquishes them[2].

Bitcoin and Ethereum are open-source blockchain systems that enable individuals to build an economic system with finances and a local currency to be transferred between accounts. Because the local units of exchanges are similar to tokens within any other system, they are referred to as coins, tokens, or cryptocurrencies. Cryptocurrencies are a manner of payment (or scrip) that can be utilized inside the system. Blockchains networks are basically connected to "peer-to-peer" nodes running the same software. Web3.js is a particularly useful software library that enables users to connect to these P2P networks through a web browser. JavaScript APIs provide a means to connect an app's front end (the GUI you see in a browser) to its back end (the blockchain). [3]. The blockchain technology introduced in 2008 enabled peer-to-peer payments in Bitcoin. To establish a digital currency that doesn't require trustworthy intermediaries and allows for non-duplicable digital assets, this concept integrated decentralized network principles with financial rewards. In an immutable network of peers, the blockchain stores transactions ordered by consensus in a replicated append-only data structure. A payment network's nodes act as independent validators of all transactions and are rewarded for securing the network financially, as opposed to previous systems [4].

1.1 PROBLEM

Healthcare and supply chain systems have not extensively explored blockchain technology to date. As the industry digitizes relentlessly, new insights are constantly presented, resulting in new research needs. Blockchain technologies need more time to be adopted, applied, and utilized to their full potential in supply chains and healthcare systems. Some of the consequences of blockchain technology adoption are currently unclear. These impacts could be seen from a technical, organizational, and, ultimately, economical perspective. For the area of implementation constraints and the discovery of causal links between them, further study is required. As a result, an empirical study is required to provide the framework for the successful adoption of blockchain technology. It's unclear if blockchain technology will be effective in the world economy since it relies on the parties' desire to use it. The deployment of blockchain in networks, in particular, involves challenges presented by the network environment, requiring more study in this area. The primary issue from the perspective of business management is what economic benefits it will offer in the big scheme of things. However, since blockchain innovation does not come without drawbacks, the problems should not be ignored implementing blockchain in healthcare and supply chain systems will present a variety of challenges. It may be useful to identify and overcome potential barriers early on in the implementation process by blending different perspectives and their links. Furthermore, it is unclear what impact specific hurdles have on implementation and how much they might offset in currently being discussed topics potential positive added value. Furthermore, this study's findings potentially assist to determine the applications based on blockchain in other industries.

1.2 RESEARCH QUESTIONS

This thesis describes the integration and scalability issues for decentralized applications, in addition to the main study topics which could be addressed as:

Problem Statement 1: the relationship integrated between blockchain and the cloud, which part of the blockchain network does a role in cloud computing.

Research Question 1: what solutions might blockchain bring to cloud computing security services?

Problem Statement 2: the benefits of cloud computing for blockchain performance issues, the evolution present, and research fields in merging the cloud and blockchain at main cloud providers, combining the two is a difficult task.

Research Question 2: what are derived from the various ways in which blockchain and the cloud can be combined? Because blockchain is a distributed service network and cloud computing is a separate service network.

Problem Statement 3: Using off-chaining, developers are inadequate to satisfy the privacy and scalability requirements of decentralized apps.

Research Question 3: What could developers do with off-chain technology to build decentralized apps that are more scalable and private?

1.3 CONTRIBUTIONS

Cloud computing is widely used to store data in blockchain research since it is such a common technology. In the design of decentralized applications, we see recurrent difficulties and solutions. The contributions to our study subject are as follows:

a) Describe the technology classification based on scalability, cloud computing, and data analysis. This paper illustrates how the proposed technological architecture is applied to cloud classification using a case study.

b) The study focuses on providing classifications for resources based on machine learning and cloud-based integrated.

c) The difficulty of scaling up with a high number of users still makes blockchain scalability, privacy, and performance challenging.

d) Create applications from beginning to end using key tools that have been developed to assist decentralized applications (Dapp).

1.4 PUBLISHED RESEARCH

Sections for such dissertation were analyzed and the results were published research in journals, and they also explain how and where specific papers affect this dissertation. The following list provides an overview of the author's scientific articles that include pertinent material:

[5] F. H. N. Al-mutar, O. N. Ucan, and A. A. Ibrahim, "Providing Scalability and Privacy for Smart Contract in the Healthcare System," *Optik (Stuttg).*, p. 170077, 2022.

[41] F. H. N. Al-mutar, A. A. Ibrahim, and O. N. Ucan, "a new framework is provided for blockchain-based integrated and resource classification for the cloud," *Appl. Nanosci.*, pp. 1–14, 2022

1.5 THESIS ORGANIZATION

This thesis's outline is divided into five chapters. Figure 1.1 depicts overview of the structure. The first chapter, which is an introductory chapter, establishes the basis for the required work. Chapter 2 gives background information on blockchains and verified operations. In Chapter 3, we create and present a blockchain-based resource integration and classification architecture. To study and analyze results that contribute to increased efficiency in the framework proposed. The solutions to Research Questions 1 and 2 can be obtained in these contributions. In Chapter 4, we identify particular scalability and privacy for Smart Contracts. These contributions respond to Research Question 3 by offering a solution. Chapter 5 explores the thesis's conclusions and makes suggestions for additional study.

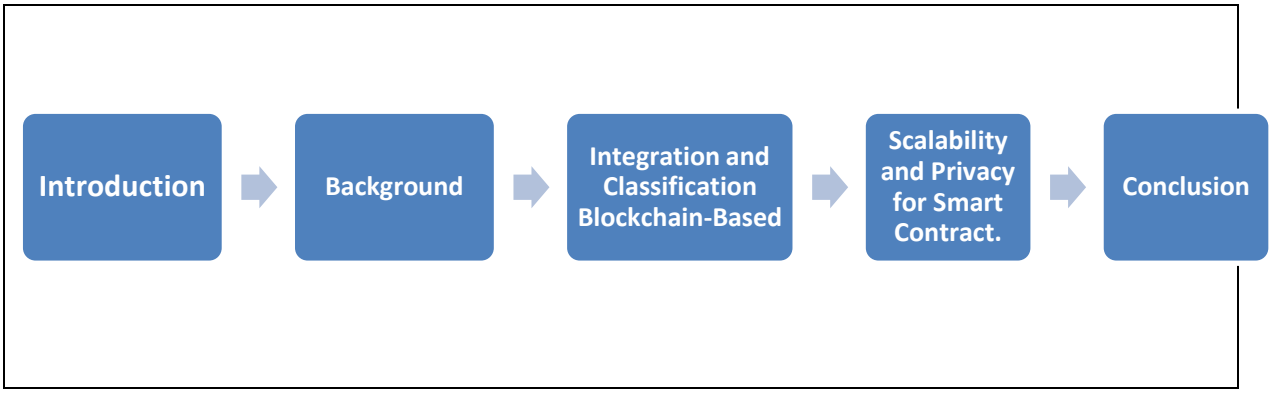

Figure 1.1: Thesis Organization

2. BACKGROUND

2.1 FUNDAMENTALS AND PLATFORMS OF BLOCKCHAIN

A blockchain is an immutable structure made up of a series of connected blocks that have been approved by peers in a peer-to-peer (P2P) network (miners). Since Bitcoin introduction, the popularity of blockchain has grown[6], an existing online currency that has no central authority to manage transactions and is maintained and validated peer-to-peer in a decentralized network by miners' blocks. Researchers have begun to understand bitcoin's widespread adoption and its decentralized block management concept, and working to focus their efforts for enhancement blockchain technique. So blockchain is considered a decentralized, distributed, non-manipulative structure that each peer-to-peer network participant owns[7][8].

2.1.1 Principal Characteristics of Blockchain

A blockchain has been designed and constructed of encrypted blocks. Blocks contain preceding block encryption hashes, timestamps, and trading data. It is impossible to change the block[9]. Transactions between separate parties are effectively recorded. It has developed a solution for cloud trust that uses a new technology called Blockchain to reduce cloud trust and enhance transparency for the problem of trusted third parties.

By enabling intelligent contracts, Atrium eliminates the need for a reliable third party to mediate disputes between parties. [10]. Smart contract can be accessed via a public atrium address. In the hash storage structure, a whitelist algorithm uses a key called the client address. Introduces the Saranyu system, which uses smart contracts[11]. Introduces the Saranyu system, which uses a distributed library to execute smart contracts to handle tenant and service accounts in cloud computing data centers and contains four services: authentication, authentication identity, licensing, and charge. The Saranyu system is based on the Quorum blockchain platform, which is well-suited to the development of distributed cloud architectures. Saranyu looks a lot like Atrium. Quorum accounts are divided into two categories: outsourced and smart. Saranyu is similar to Quorum's Dapp, which is based on the blockchain. Identifying tenant accounts and services is performed using the public portion of the public/private key pair. Other registered services can be used with Saranyu services, and if they are, the service will be reimbursed to the user.

Contract accounts are used to create tenants and services. Saranyu uses the private/public key to authenticate the renter each time he or she enters. Saranyu provides the agency as a smart contract with quotas for the maximum number of service features consumed by the recipient member, service feature recharge plans, and people with the authority to stop the agency. Saranyu is used to make licensing requests and carry out licensing processes. They will acquire the suspension and revocation license after receiving the two operations here. Saranyu does not accept digital money as a means of payment.

The solution is based on the ChainFS middleware technology[12], which employs cloud computing to protect cloud storage. ChainFS is also available in Atrium and S3F with fuse-based clients (user file systems) and uses Amazon S3 to evaluate cloud space and display low overhead in the ChainFS system. A client-based ChainFS system is a server with a blockchain that is hosted by an unreliable cloud. On two remote screens, Fuse customers engage with both parties.

2.1.2 Type of Blockchain

P2P networks can share information via blockchain, a non-centralized technique that uses blockchain to allow them to do so. Blockchains can be categorized according to their architecture and qualitative characteristics as permitted blockchains and unlicensed blockchains.[13]. In addition, blockchain is classified into private, public, and hybrid blockchains depending on numerous notions such as authorization and resource classification.

Table 2.1: Comparison Table for Platforms of Blockchain

Types	**Bitcoin** [6][8]	**Ethereum** [15]	**Hyperledger Fabric** [12]	**Hyperledger Burrow** [16]	**Ripple** [17]
Public	√	√	×	×	×
Private	×	√	×	×	×
Consortium	×	×	√	√	√
Consensus	**Bitcoin**	**Ethereum**	**Hyperledger Fabric**	**Hyperledger Burrow**	**Ripple**
PoW	√	√	×	×	×
PoS	×	√	×	×	×
PBFT	×	×	√	×	×
Tendermint	×	×	×	√	×
BFT	×	×	×	×	√
Capacity	**Bitcoin**	**Ethereum**	**Hyperledger Fabric**	**Hyperledger Burrow**	**Ripple**
7 tps	√	×	×	×	×
12 tps	×	√	×	×	×
Thousands tps	×	×	√	√	√
Forks	**Bitcoin**	**Ethereum**	**Hyperledger Fabric**	**Hyperledger Burrow**	**Ripple**
Support	√	√	×	×	×
Permission-less	**Bitcoin**	**Ethereum**	**Hyperledger Fabric**	**Hyperledger Burrow**	**Ripple**
Support	√	√ ×	×	×	×
Fee-less	**Bitcoin**	**Ethereum**	**Hyperledger Fabric**	**Hyperledger Burrow**	**Ripple**
Support	×	×	√	√	√

Techniques [14]. Depending on the kind, consensus method, smart contracts, amount of transactions, forks, unlicensed (permissionless) transactions, and unpaid fees. Table 2.1 lists

the several blockchain platforms that exist.

2.2 PLATFORMS OF BLOCKCHAIN

Digital currencies such as Bitcoin are increasingly being used with blockchain technology [18] gain in popularity. A blockchain is a decentralized, distributed, multi-party shared ledger that includes a linked data structure made up of several blocks of information. The header and the body are the two components that make up a block. The Merle tree root, the nonce, the time stamp, and the hash value from the preceding block are just a few of the details found in block headers. To link the front and back blocks, the block header uses the previous block hash value. The block body contains transaction data. [19]

According to the current application of blockchain, there are three types: (1) public blockchain (open, free entry, unlimited data access); (2) consortium blockchain (a blockchain managed by multiple organizations, where each organization can have multiple nodes; Only entities that are part of the system are able to access, write, send, and jointly record transaction data); and (3) private blockchain (a blockchain managed by multiple organizations, where each organization can have multiple nodes; transaction data only the organizations using the system will be able to read, write, send, and collaboratively record it) (a single organization controlling the writing power of a blockchain). The nodes of participating qualifications are carefully limited. Depending on whether access into a blockchain network requires authorization, we can divide them into permissioned blockchains and permission-less blockchains. A consortium blockchain and a private blockchain need a permission network, but a public blockchain operates without permission. The term "consensus algorithm" refers to the technique and procedure for achieving consistency among numerous nodes in a distributed system. The consensus algorithm solves the consistency problem. The consensus algorithm handles a wide range of issues, such as event sequences, transaction results, current master node elections, and so on. [20]Below are some common consensus processes seen in existing popular blockchain systems.

The Bitcoin system utilizes a consensus process known as "proof-of-work" (PoW)[21]. Master node must be chosen at random, and the PoW's unpredictable nature is determined by the unknown nonce in the block header. Until it discovers the nonce that solves the current challenge, each node in the network computes the hash of the current block header and tries to

write the value of the nonce. The proof-of-stake consensus method is more likely to be used in modern systems (PoS). It uses fewer computer resources and is more effective. Based on the weight established by the quantity of digital currency held in the wallet and the number of holding days, PoS modifies the complexity of the computer to conduct the hash computation. The bigger one of them weighs, the more likely it is that one of them has authority to create block[22].

Proof of Authority grants a limited number of "experts" the ability to package blocks, while ordinary users do not have this ability[23]. "Experts" must reveal their names and maintain their reputations, while regular people who wish to become "experts" must work hard to keep the blockchain in order. Existing "experts" vote on who should join and who should be kicked out.

The Byzantine Fault Tolerant (BFT) algorithm is the Byzantine problem's consensus algorithm. When the proportion of failed nodes does not exceed one-third of the total number of nodes, the Practical Byzantine Fault Tolerant (PBFT) technique, which Castro and Liskov first presented in 1999, may guarantee both integrity and availability. PBFT algorithm has a polynomial time complexity. Raft is a safe consensus algorithm. Raft is mostly used to manage log replication consistency. In the consortium chain, it is one of the most extensively utilized consensus algorithms[24].

Table 2.2: Comparison of Consensus Algorithms

	Transaction finality	Transaction rate	Trust model	Scalability
PoW	Probabilistic	Low	Untrusted	High
PoS	Probabilistic	High	Untrusted	High
PoA	Immediate	High	Untrusted	High
BFT and variants	Immediate	High	Semi-trusted	Low
Raft	Immediate	High	Semi-trusted	High

They have easy-to-understand scripts. Ethereum [19]Smart contracts are on the verge of achieving Turing completeness, which will allow them to move digital assets based on any preset rules.

According to Figure 2.1, a transaction is processed in the blockchain network. Hashing the transaction data allows the transaction initiator, such as patients and associated health professionals, to start a new transaction. Digital signatures for transactions are created by encrypting hashed data. Encryption of the data is done using the transaction initiator's private key. In order to process the transaction, the network is broadcast with the relevant digital signature and transaction data. A received transaction is validated by each validating node in the network. In order to achieve this, it is necessary to confirm the authenticity of the transaction initiator as well as the integrity of the transaction data. Its legitimacy is proven if the digital signature can be successfully decoded using the transaction initiator's public key. If the hash of the transaction data matches the hash of the data retrieved from the decryption procedure, the integrity has been confirmed. the legality of the transaction.

It is shown in the block and is carried across the whole network. After determining that the received valid transactions are indeed legitimate, a miner (a node that makes a block) builds a block out of those transactions. The consensus process for the blockchain network describes both the miner who creates a block and the steps involved in validating and attaching the generated block to the chain.

The three different consensus protocols used by blockchain are capability-based, computationally expensive, and voting-based. [24] The chosen miner generates the hash, sometimes referred to as the block's digital signature, and broadcasts it to the network. The block header and hashed value are first combined to create the block's hash. The date in the block header refers to the moment the block was created, whereas the version refers to the protocol version that was utilized. The transactions in the block data are sequentially pair-wise hashed to get the Merle root, which is a single hash result. Each validating node will include the block in their own copy of the ledger if it is valid. [24]

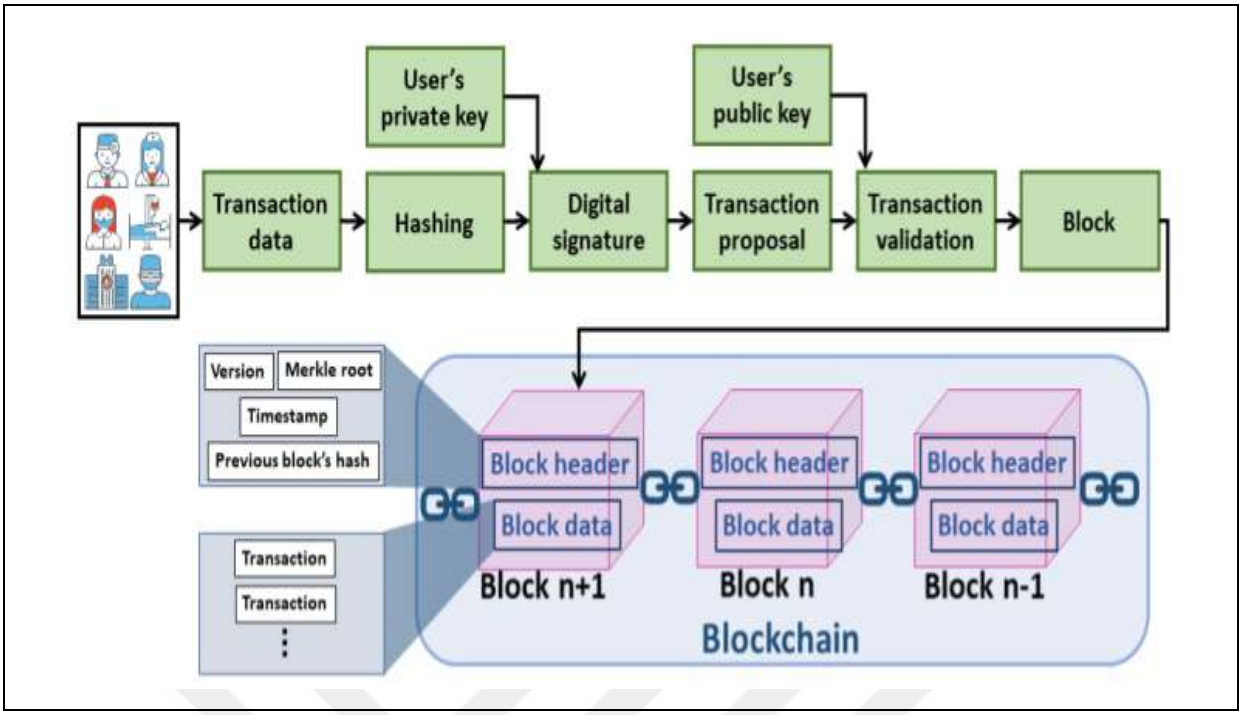

Figure 2.1: The illustration shows how a blockchain processes a transaction.

Blockchain networks can be hybrid, private, public, or consortium-based. Anyone can sign up and get unfettered access to transaction data on a public network. A private network, on the other hand, is one that is run by a single organization, where membership is restricted and data access is controlled by permissions. Since only authorized users can join the network and access control privileges are used to update and access the ledger, a private blockchain is perfect for the healthcare sector. A consortium blockchain is one where the network is controlled by a number of different businesses. A hybrid blockchain combines the advantages of both public and private blockchains and makes the ledger accessible to network members. Access is restricted for ledger changes, on the other hand. As was already mentioned, the blockchain's unique characteristics indicate that the healthcare sector holds a lot of promise for the technology. The following are some benefits of a blockchain-based healthcare system:

Provenance: The unalterable blockchain record makes it possible to create an audit trail, which boosts network confidence. It is possible to quickly trace the origin of any network fraud. The outcome is that malicious activity is deterred [23].

Protection against natural disasters: A database and its regional analogues might not be available. Hurricanes, floods, and forest fires are examples of natural disasters. Fault tolerance in this case can be improved by the globally replicated blockchain ledger. To identify illnesses that could be life-threatening, the local or closest copy of the ledger can examine patient

medical records in real-time. Inpatient precision medicine: The blockchain helps allied health workers diagnose and prognosis patients more accurately by giving them an uniform picture of all of their medical records [25].

2.3 INDUSTRY/MAJOR CLOUD SUPPLIERS BLOCKCHAIN APPLICATION STATUS

Most cloud computing platforms now include blockchain services and offer a BaaS delivery mechanism. The Blockchain as a Cloud Service (BAACS) model, which we briefly discussed in the introductory section, is known as BaaS. To shield the onerous network configuration work of the blockchain, CSPs use virtualization and container management tools like Red Hat OpenShift [25]Kubernetes [18]and Amazon Machine Image (AMI) images and instance templates[21]. Simple processes can be used to deploy a sophisticated blockchain network. Existing blockchain initiatives are encapsulated in most cloud computing platforms. Oracle, for example, encapsulates hyperledger fabrication[21]. Some businesses have not only absorbed existing blockchain projects but have also created their own blockchain projects. For example, Alibaba Cloud, for example, has Hyperledger Fabric, enterprise Ethereum Quorum, and its own Ant Blockchain [7]

2.4 ARCHITECTURE OF BLOCKCHAIN CLOUD MANUFACTURING (CM)

Figure 2.1 shows the fundamental elements of blockchain cloud manufacturing, which are based on those of current cloud manufacturing [27]. The blockchain cloud manufacturing architecture's components are all created to be straightforward, quick, and effective (For instance, if a new cloud provider joins the architecture). Another standout characteristic is the connection between customers and CM, which is made possible through a blockchain network. (P2P).

Several criteria are consequently taken into consideration for Blockchain, a peer-to-peer network that permits the integration of a significant number of networked workstations. Blockchain permits ledged and smart contacts for communications purposes. Considering that the system is decentralized, a single node failure does not render the entire system inoperable (i.e., the others can carry out their tasks on their own independently).

Flexibility: Each cloud manufacturing system can work on its own or in tandem. There are two sections to the proposed architecture. The user layer, often known as the CM's end-user layer,

starts first. However, this will only be briefly discussed because it is not the main goal of the book. The blockchain cloud manufacturing layer, which is the most crucial element of this design, is made up of the core layer, the P2P network layer (the blockchain network), and the cloud manufacturing layer [28].

2.5 CLOUD COMPUTING

Ben Noble is one of the creators of MarketBlok, a company that focuses on blockchain marketing and content. He formerly worked in the cloud computing services industry. He offers his thoughts on the blockchain in an article, claiming that this technology is a continuation of the cloud computing path:

The cloud computing industry has generated a $1 trillion ecosystem. However, this technology is only the beginning, and its refined form, the blockchain, has the potential to have a bigger impact.

The initial shift away from centralized control was made with cloud computing. For daily operations, businesses demand dedicated bandwidth, computing power, and data storage. The servers, on the other hand, required frequent maintenance, strong security, monitoring, and, of course, regular updates. Cloud technology was able to provide corporations with performance that exceeded hardware restrictions by distributing these servers across large networks.

Companies can now access their offices from anywhere and even hire people who work remotely. The block can now be considered the second wave of evolution in the computing framework. The Blockchain creates a network by utilizing a distributed head office system that is highly secure, democratic, and unbreakable. This infrastructure can lead to the development of non-hackable systems and networks that are transparent and reliable. Miners are a group of people who participate in blockchains. Miners are in charge of approving transactions and solving challenging mathematical challenges. In exchange for a digital currency reward, miners offer their computer processing power to the network. The network of miners takes part in the process of generating new blocks. The network's miners are the nodes that store and process data.

Miners provide their computing power to the network for three purposes:

a) Keep a duplicate of the block on hand.

b) Transaction confirmation and processing

c) Put smart programs and contracts into action.

One of the most well-known blockchain technologies that enables users to access blockchains is the Ethereum Virtual Machine (EVM). EVM (Ethereum Virtual Machine) gives consumers the tools they need to create decentralized apps (Dapps). The Ethereum Blockchain serves as the host for these programs.

Decentralized applications (Dapps) are separated into little pieces, such as torrents, and run on several computers rather than on a single server. Because no single computer possesses all of the pieces, the software cannot be hacked or crashed.

Unlike cloud computing, decentralized blockchain does not necessitate the use of massive servers. A network of nodes, such as Ethereum, can perform the same functions as these huge servers. Blockchain technology, in fact, distributes network processing power all across the world.

The blockchain's high potential for using computing power around the world refutes the argument that digital currency is worthless or that its price is a bubble. The fact is that digital currency is a better and more secure instrument that may help people gain access to information technology and other applications. Using the blockchain, we can create a network of volunteers to provide cyber protection. The China bloc appears to be shaping the exciting future we are about to embark on.

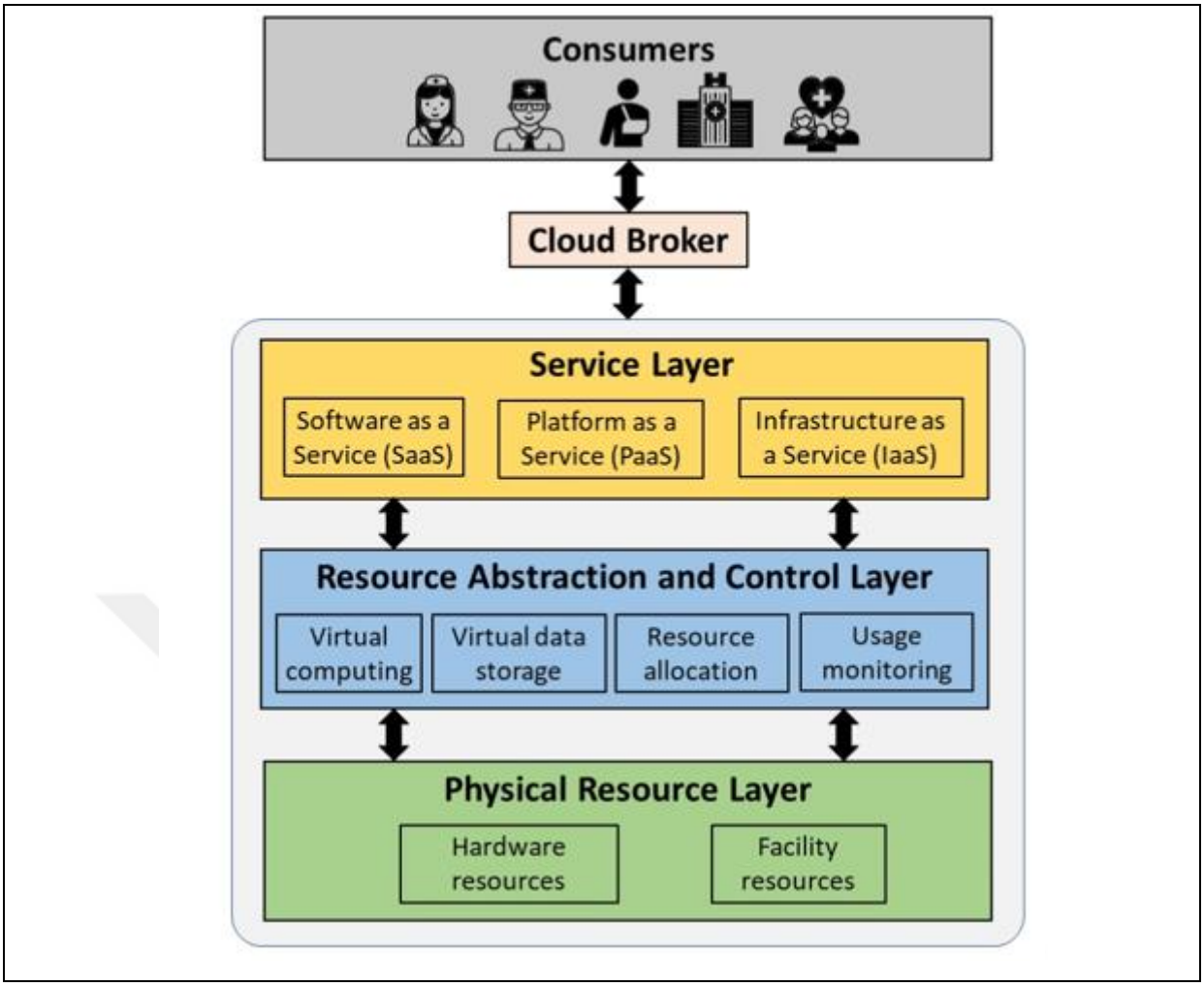

Figure 2.2: An Overview of the cloud system architecture.

There are three different types of cloud networks: The public cloud offers unrestricted access to systems and services to the general public, but it is less secure.

A private cloud is safer than a public cloud since only users who work for the firm that runs the cloud have access to the systems and services. A private cloud that is used by many different companies is called a community cloud. In order to offer greater flexibility, a hybrid cloud mixes public and private cloud services.

The private cloud can be used to manage sensitive and confidential work while managing routine operations on the public cloud. The healthcare system shifted from client-server to cloud computing as cloud computing became more widespread. Client/server-based healthcare systems' problems with dispersed health records and high total cost of ownership are resolved by the cloud.

2.6 CLOUD DISTRIBUTED RESOURCE CLASSIFICATION USING NON-BLOCKCHAIN

By using method, resource categorization can be spread without subjecting end users to centralized controls. A distributed resource management solution built on the OrBAC methodology, SmartOrBAC[29][30] uses the cloud (organization-based resource classification). SmartOrBAC [26] improves on the current OrBAC [26] in context-aware concerns, allowing it to adapt to cloud environments' limited resources.SmartOrBAC divides the resource classification process into various functional layers.

Confined layer: The objects and subjects are contained in this level, which is the most constrained. This resource classification layer can handle activities that require more computing power.

The organization layer is in charge of determining the organization's rules as well as the responsibilities and rights of the different parts of the organization.

The organization layer enables various companies to concur to engage with one another by using the Principal Authorization Manager (PAM).

Resource classification methods should be simple since the cloud's limited power and storage make it impossible to maintain security measures that need a lot of processing and communication. SmartOrBAC, on the other hand, does not provide a lightweight method for circumventing OrBAC's cloud context adaptation constraints.

Capability-based resource classification is one of the cloud resource management techniques that lets one company grant resource authorisation to another (CapBAC). A token, key, or ticket that allows access to a computer system's entities or objects serves as an example of a capacity. [32] In order to respond to real-world circumstances, the token should also be unchangeable and obvious. It could also be seen as a group of privileges that endow the individual with the token. Another subject interested in extracting specific information from an object is CapBAC. As a result, they must transmit a token in order to request processing. The object then determines the subject's (requester's) permission level, which was previously granted in order for the request to be processed. The distribution of resource classification procedures are made simpler by this streamlined authorisation. There are three different resource classification systems: decentralized mechanisms, contextualized and centralized mechanisms—were put into place for the Internet of Things. [27]

The writers went over each mechanism's advantages and disadvantages. Furthermore, because of its scalability and interoperability, the distributed approach is better suited to cloud systems. This method, on the other hand, lacks dynamicity and is not classified as context-aware management. The authors [28] developed cloud resource management with CapBAC, a component of the European FP7 Cloud@Work project.

Compared to centralized approaches like RBAC, this resource management promotes delegation and provides more flexibility. However, the CapBAC has significant flaws, such as a lack of fine-grained resource classification and a lack of context consideration. Additionally, it needs to provide capabilities to all parties concerned with the large-scale system authorization process.

In Table 2.3, token-based cloud resource classification techniques are compared. Resources are classified, blockchain types, transaction mechanisms, and other crucial aspects of the techniques are compared. Requesters can grant or restrict access to cloud resources using these tokenization resource classification techniques in compliance with the owner's policy. On the other hand, these tokenization techniques do not automatically enforce resource classification rules. Additionally, several of these frameworks require tokenization in order to work, which means that in order to cancel a token or request a new resource, one must contact the owner, which takes time. It is feasible to embed resource classification policies in a smart contract, which would then automatically implement the policies to limit resource entitlements and flag unwanted behaviors, preventing transaction latency for resource classification using tokenization techniques in cloud systems.

Table 2.3: The Following table compares various token-based resource classification schemes.

Reference	Resource Schematic	Type of Blockchain	Principal Elements of the Transaction-Model Used
FairResource [29]	Attribute-based AC	Public	- It broadcasts a user's Token/Smart contract transaction via the P2P network using wallets. - The privacy of the users is protected via a pseudonymous method.
CloudChain [30]	ACE Authorization model	Private	- In this token/smart contract, authentication is accomplished using the ACE principle. - It uses the OSCAR idea to provide complete security.
Outchakoucht et al. [31]	General-AC	Public	Token/Smart contract - A reinforcement learning method is used to create autonomously and self-adjusting resource classification rules.
Xue et al.	General-AC	Private	- In the blockchain header, resource policies are stored. The owner can view the visitors' resource privileges using the token, which serves as a policy file.
Maesa et al. [32]	Attribute-based AC	Public	-The XACML policy model uses it for implementation. Token. To apply AC policies via blockchain, Policy Administration Point (PAP) and Policy Enforcement Point (PEP) are employed..
BlendCAC [33]	Capability-based AC	Private	Tokens and certificates were implemented using a JSON schema.
Fotiou et al. [34]	Role-based AC	Public	Token/ Smart contract - It used the Ethereum-based ERC20 standard to create token-based resource categorization.

2.7 BLOCKCHAIN-BSASED POLICY-HEADER-BASED RESOURCE CLASSIFICATION

This method allows for the integration of resource classification policies into the local blockchain's policy header, giving the network's owner authority over all incoming and outgoing transactions.. Patil et al. developed blockchain technology. [35]For smart greenhouse farms, we devised a secure, lightweight solution. All sending and receiving transactions on private local blockchains are managed using policy headers in this system.

Furthermore, this technique groups cloud nodes into clusters from which any cluster head can be chosen. Cluster chiefs are in charge of the overlay network. Because the owner has set a resource management list in the policy header, local blockchain miners can validate and approve any transactions that arrive from the overlay network. They employed a policy header, which constantly updates its policies and transfers these policies to newly created blocks, to bypass the PoW mechanism's high-cost computation. This system does not always follow its resource classification policies, while having robust security measures in place to ensure confidentiality, integrity, and availability.

Dorri et al. [42, 43] showed a smart house with three levels of cloud storage, an overlay network, and a smart home as a component of a straightforward blockchain solution for cloud security. The resource categorization policies are kept in the policy header of a private (local) blockchain in this system to secure device authorisation and execute the owner's resource policy. A sophisticated piece of hardware called a miner or controller is installed in every home. It controls a private blockchain and sends resource management and monitoring data to the cloud to protect communications both within and outside the house. The miner employs this technique to manage the smart-home layer, which contains all prohibited devices (controller). Because of this, no PoW consensus is required for block validation, and if the broadcasted key is reliable, devices in other connected houses can use it to complete transactions. On the other hand, the controller disqualifies the shared key and tells the devices if the devices are no longer required access to the resource. This framework has a number of transactions that deal with resource management, storage, and monitoring, among other things. Due to the overlay network's integration of consumer devices, cloud storage, and smart homes, it resembles a peer-to-peer network. Each cluster in this network elects a cluster head (CH) to oversee the blockchain, which is made up of the network's nodes.

2.8 INFRASTRUCTURE OF CLOUD FOR BLOCKCHAIN

Cloud computing structures ought to have availability, performance, scalability, security, and alerting capabilities. Application programming interfaces (APIs) that permit builders to customize cloud computing services, in addition to massive information garage and analytics tools, ought to all be included. As it contains a few carrier ingredients with those qualities, the infrastructure of the AWS cloud is taken into account. These service add-ons' six categories are, among others, virtualization, integration, security, storage, analytics, and notification. They might be included in a number of well-known cloud infrastructures, including Google Cloud, Microsoft Azure, and IBM Cloud. [44].

Clients can increase or decrease computer resources (such memory, memory, and computing power) to meet their demands thanks to the flexible cloud computing solution provided by the virtualized service component. This service component assigns users to virtual servers, enabling them to develop and deploy software, set up networking and security parameters, and control storage on cloud computing servers. An API for building web server programs that are compatible with cloud computing is provided by the integration service component. Between two apps or systems, APIs act as a link. The API can be used by programmers to create software that communicates between two applications by sending signals and messages back and forth. The integration service component enables programmers to build unique APIs for blockchain applications [45]. Using the cloud storage function of the cloud hosting feature, users can store and retrieve things and data in the cloud. Additionally, it provides incredibly scalable, open, and effective data storage. The database technology used in the storage service component is designed to manage enormous volumes of data. It is built on key-value and document database architectures, both of which are capable of handling massive volumes of data[36].

As a support for blockchain applications and a repository for metadata, the storage service component can be used (that is, information about the data).Large volumes of transaction data must be divided into two categories since each block in a blockchain has limited storage capacity. Both the original transaction data and its hash can be saved off-chain (outside of a block)[47]. The initial transaction data can be kept in an off-chain database. The block's hash value, which is used to link the pertinent large-sized transaction information kept outside of the block and in cloud storage, can be used to assess the immutability of the transaction data. Solutions for applying artificial intelligence algorithms in real-time to analyze blockchain data are part of the analytics service component. This component captures, processes, and analyzes

real-time streaming data and provides a cloud data warehouse for huge data storage and analysis [48].

The notification service component in distributed cloud systems provides communications between users, managers, and even other service components. Users are able to queue messages and process them later using this service component. Communication between apps and between apps and people is also feasible. Events-driven serverless apps, microservices, and distributed systems can all connect with one another via applications. The application-to-person communication function of cloud computing states that messages can be distributed widely to other users via SMS, mobile push, and email. Developers can run code using the notification service without deploying or managing cloud servers. The only thing needed from the programmers is to produce the code and send it to the notifications service package, which scales the resources needed for cloud technology to run it. [49].

2.9 BLOCKCHAIN CLOUD MANUFACTURING

This part is divided into three main levels: the core layer, the peer-to-peer (P2P) or blockchain network, and cloud manufacturing systems. The following provides a description of these levels:

2.9.1 Core Layer

To secure information in transit, CSA standards advocate using a combination of IDS, IPS, and firewall virtual LANs. User information leaks based on permitted networks and the use of basic infrastructure are also covered in the guidelines. CSAs advise using these tools in conjunction with management strategies. To enable visibility and traffic monitoring on virtual networks, a CSA-like hybridization of virtual and traditional physical devices is used.

To give additional security to cloud resources, advanced ACPS cloud protection systems have been developed. A number of security services for CSP resources have been developed by ACPS developers, including network protection against user and CSP information threats. Tenant attacks can also be avoided by monitoring the virtual machines (VMs) running on the host platform. In addition, ACPS allows you to review virtual machines. The host platform divides ACPS into distinct models. The interceptor model is in charge of detecting any unusual behavior on the host. The alarm recording module records any suspicious activity and stores it in the alert repository.

The evaluator, which is a stimulus for the stimulus module's activity according to the security policies, evaluates the registered activities. At the time of installation, ACPS calculates the checkmate for essential infrastructure, including the network. The status of the infrastructure influences how the control computations for the objects are looked at. An alert will be provided to the assessor in the event of any anomaly. During the check-in period, the cloud points' control approval is constantly monitored. Use the IP table and alerts logged in the pool to prevent attacks on the ACPS network architecture using the mechanism provided in the network.

ACPS protects against VMs and information attackers additional to network security and other critical infrastructure. A crucial feature of ACPS is that movement between VMs is invisible and undetectable. No communications from the system are filtered by the interceptor module in order to avoid detections. It is done regardless of whether the attack activity is confirmed. To neutralize the assault, enough time to notice the monitoring system, the initial system authorization is announced. Eucalyptus was used to implement the ACPS prototype, and OpenECP is now available for cloud systems. CyberGuarder, a cloud computing security technology, protects virtual networks by using virtual network devices deployed.

In addition, between the virtual bridges is a two-layer VPN tunnel that separates virtual networks. Without the aid of a centralized server, data is sent between VMs peer-to-peer. Although cloud data is retained in the central node to monitor traffic between VMMs.Software for monitoring network traffic. Traditional network security methods, such as intrusion detection systems (IDS), are utilized to protect virtual network applications. CyberGuarder also protects virtual machines by evaluating application integrity and monitoring citation systems. The findings of the experiments suggest a 10% rise in Cyberguarder installations and a 5% increase in energy consumption.

To protect against cybercrime, Wu et al. [37]created a model of a virtual network. The proposed model is represented by the Xen hopper. The suggested model configures the virtual network using the XEN hypervisor bridge and path. It connects directly to the VM via an Ethernet virtual bridge in XEN bridge mode. The physical network is then connected to the bridge. The P2P route type creates a connection between the virtual machine and management domain 0. (Management domain 0).

Table 2.4: The Blockchain Network's Components[38].

Part	**Accountability and Objective**	**Core Modules**
Block of chained data	It is in charge of supplying the chained data blocks to the rest of the system. as well as similar techniques, that are utilized for the system.	Hash Algorithms, and Asymmetric Encryption
Network part	It specifies the dispersed networking techniques and denotes peer-to-peer data transmission.	Data Forwarding, Peer , and Data Management
Agreement part	Also known as the handshake or consensus part. It facilitates network communication by allowing for decentralized communication.	Proof of the Work, the Stake, and the Delegated
Motivation part	It is in charge of giving the network a sense of drive by providing a reward for more blocks, or, to put it another way, driving the network.	Crypto Data.
Contact part	Using different scripts, algorithms, and smart contracts, it is in charge of acting as activators for static data.	Script and algorithms. -

It lets devices connect to and use traditional cloud computing services, allowing for ubiquitous cloud computing access and the use of traditional cloud computing services. Mobile devices, on the other hand, have restricted resources compared to traditional computer platforms. Low processing power, storage space, electricity, and Internet connectivity make it impossible to compute and store applications that must run on mobile devices. This constraint serves as the incentive for a new computing paradigm known as MCC, which expands actuator capabilities by transferring storage and computationally expensive activities from the actuator to the cloud.

By utilizing cloud service computing and storage procedures, drive devices may now conduct heavy computation and compact storageThe MCC paradigm allows users to access and control their apps and data straight from the drive device rather than moving to a typical computer. However, MCC, like traditional cloud computing, has security vulnerabilities that are preventing its mainstream adoption. This section provides a quick overview of the MCC paradigm's core security challenges and the broader method of addressing them.

Because the MCC functions similarly to a typical cloud cloud, all of the security concerns stated in Section 3 also apply to it. The shortage of resources on propulsion devices, on the other hand, prevents regular cloud security certification. It's worth noting that the cloud security solutions will not change until the end. Client-side (drive device) security solutions necessitate a lightweight version that can be executed on drive devices. Security software, privacy, authentication, and data security are all concerns at MCC.

2.9.2 Security Software of The Driver

Stimulus devices, like regular computing devices, are subject to malicious programming. Examples of harmful software that can affect an operating system's software include worms, viruses, and Trojan horses. Traditional security software, such as antivirus and intrusion detection systems, cannot be run constantly on bootable devices. As a result of identity theft, security software or devices may be compromised. Powerful cloud security solutions that identify intrusions and deliver hazardous code can also be operated using the basic idea of computing evacuation.

2.9.3 User Privacy

The trigger device, especially with location-based services, might be a source of location leakage. This is a severe privacy issue, and if the attacker knows where people are, things might get considerably worse. By masking the user's geographical location, the notion of hiding location can be utilized to safeguard the privacy of the user's location.

2.9.4 Authentication

Another challenge with resource-driven devices is authentication. Passwords are typically employed for MCC authentication due to the limited limitations of text input, which might lead to vulnerable theft over time. For secure authentication, dynamically generated credentials can be employed. Due to the drive device's minimal computing power, credential generation might be attributed to a third party.

2.9.5 Data Security

Actuators cannot perform complex calculations of large-key cryptography methods due to their low processing power. MCC necessitates some type of encryption with low storage, processing, and transmission requirements. Alternatively, to protect the user's data, the intensive

calculating, encryption, and decryption operations might be delegated to a trusted third party. The recommendations for CSA data security and key management are as follows. Businesses and consumers, or a reputable encryption service, must handle key management. The greatest alternative for maintaining and securing essential things is to choose trusted vendors. Off-the-shelf technology should be used whenever possible. An individual or group must maintain the key domain.Rather than using dedicated cryptography techniques, it is preferable to employ common algorithms. SecCloud is a storage security protocol developed by Wei and colleagues that safeguards both the computation done on the data that users submit to the cloud. SecCloud uses encryption to gain access to protected storage.

The user, the cloud, and the trusted third party all have keys generated by combining two straight lines (with cyclic additions and multiplication groups). Data is stored using CSP. A reliable third party verifies the information (in m divided by the number of messages) (called the authentication agency). Data is encrypted and sent to the cloud using a session key. By using Bilinear Deffie-Hellman, the session key determines both the user and the cloud. In determining the partition in the cloud, data decryption, signature authentication, and storing are used.

Computational security protects against partial computations and the use of erroneous data, lowering the cost of computing. It also ensures that the data is kept in the correct cloud division. SecCloud secures computing by employing the Merkel hash tree. By reconstructing the Merkel tree, the approval agency was able to verify the computational results. The validator employs the probabilistic sampling method rather than building the entire tree to reduce computational redundancy .To keep data secure in the cloud, the author of 98 employs a combination of recognized and specialized procedures, as well as the extra proposed steps.

The suggested method gives the customer the option to select from a range of values from one to ten to decide the level of secrecy, availability, and integrity necessary (1–10). These metrics are employed to assess the SR of user data. The data is split up into one of three possible divisions inside the provided cloud according to the SR value. A desired partition has levels of public, private, and restricted access. SR value exceeds the sum of the three public partitions' subvalues, as well as the eight data points allotted to the limited access partition. Before being transferred to the Mac, the data will be encrypted with 128-bit SSL encryption. Searching for encrypted data is also possible with the index. Data and indicators are transmitted to the cloud and stored there based on the requirements.

The owner of the data and the cloud allow downloading based on user authentication. There is no need to authenticate data on public partitions. Both directions of SSL data must be transmitted. By enabling data verification accuracy, the authors of [52] suggested a practical method for guaranteeing the quality, integrity and accessibility of cloud-based data. The suggested method verifies cloud data without having specific knowledge of the data spectrum. The above is accomplished using muddled code and homomorphic symbols. The user computes the homomorphic token in advance, and the data is divided and stored in excess across cloud servers.

A challenge consisting a random data block index is given to the cloud in order to verify the data. A cloud calculates the response and distributes it to users, who then compare the received result to pre-calculated tokens to make a decision. The suggested system also configures error localization by identifying the server that is performing the incorrect activity. Additionally, the proposed layout supports inserting, deleting, changing, and adding data blocks. Integrated assaults, Byzantine failure, and collusion server attacks are all protected by the proposed cloud storage method. In addition to clearing correction codes, the authors in [39]used the concept of re-encrypted proxy to provide resident and data security.

As described in [40], FADE is a protocol that includes key management as well as data privacy and integrity. FADE is a lightweight cryptographic technology that employs both symmetric and asymmetric techniques. Shamirs (K) are used in the symmetric key to increase the key's trustworthiness.FADE is a trusted third party that works with a group of KM management keys. The symmetric key used to encrypt K is called S. KMs gave ei a public/private key combination that shows di and uses S encryption. A policy assumes that the access policy is valid based on a P file. An application sends P to the KM request to form a key pair in order to deliver data. The public and private keys associated with P and KM are paired.

The user encrypts the file at random by producing K and then encrypting K using S, which is primarily public key encryption provided by KM. The integration key is also used to calculate the MAC. Downloads the packet encryption spectrum from the cloud, using P to decrypt all cloud data and S to transfer it to KM for RSA decryption. Decrypt F once you've decrypted S and the other keys. FADE supports the cancellation policy. After the policy expires, KM uses secure writing to clear the relevant key and P, rendering the information unavailable and hence securely erased.

Data encryption prior to cloud outsourcing ensures data privacy, but it comes with drawbacks. Restrictions apply in circumstances where data is exchanged within a group and/or transportation is required. User invalidations can override this environment, necessitating data re-encryption and key alterations to prevent data leakage to the user. To enable group data sharing security and access control, Liu et al. presented a time-based re-encryption proxy (ABE). Data is securely delivered to this group of users using the specified technique (TimePRE), and transactions with unauthorized users are prevented.

TimePRE does not require data owners to be online and does not generate a new encryption key for undesirable users, unlike other proxy encryption solutions. CSP automatically cancels TimePRE when the user's time period expires. Using a pre-shared master key between the data owner and the CSP, the CSP can re-generate the key. The use of ABE for access control ensures that a set of identity features are used to identify users. TimePRE employs ABE to identify users by combining eligible time periods with other characteristics. The proposed strategy protects the group's data by ensuring its privacy and availability. It does not, however, pay attention to data security.

3. INTEGRATION AND CLASSIFICATION BLOCKCHAIN-BASED

The internet of things (IoT) paradigm is quickly evolving. Controlling the Cloud's vast worldwide expansion, in reality, creates significant security and privacy concerns. Cloud systems are protected by standard resource categorization procedures. These methods, however, depend on centralized administration, which poses issues with sustainability, single failure points and secrecy. Scalability, cloud processing, analytics, and technical design are all topics covered in this chapter along with the technology classification. A case chapter was utilized to demonstrate how the suggested technical design is applied to the cloud classification to obtain the technical classification. We also provide cloud-based integrated and resource categorization utilizing machine learning. This chapter is based on our paper[41] .

3.1 INTRODUCTION

Due to its advantages over traditional methods, such as cost savings, decentralization, efficient processes, and waste reduction, as well as accessibility, authentication, trust, and security, blockchain has the potential to revolutionize supply chain management. All blockchain-based transactions are additionally more transparent, cost-effective, efficient, and safe [55]. This has led to the widespread belief that the distributed nature of blockchains aids in the control of smart contract risks such as infringement, hacking, vulnerability, costly conformity with legislative requirements, and contract disputes. Through the use of smart contracts, blockchain can also aid in the automation of industrial operations and real-time order settlement [56]. By controlling the client order process, blockchain technology might be able to improve order efficiency, traceability, and visibility. The "proof of concept algorithm" for blockchain, which ensures accountability, dependability, and efficiency, allows for asset management. Pilot ideas like decentralized autonomous organizations were put into practice to replace the antiquated management structure with automated governance. However, security concerns forced them to be dropped. In order to enable optimal integration with business operations and reduce security concerns, adoption and deployment of blockchain technology should be carried out gradually. To transition to automated governance from the outdated management system, pilot projects like highly autonomous associations have been implemented. They had to be abandoned, nevertheless, due to security reasons. Blockchain technology adoption and implementation should be done gradually in order to allow for the best integration with corporate operations and to decrease security concerns.

3.2 RELATED-WORK

Load balancing or removing jobs from overloaded blockchain machines and allocating them to low-loading blockchain machines is vital to comprehend in the cloud, and a distributional solution is always required, because one or more blockchain maintenance jobs are always required. It is neither practicable nor cost-effective to meet only some of the minimum standards by being active and inactive. It is obvious that centralized assignment of work to certain blockchains is unfeasible due to the magnitude and complexity of these systems. The load balancing that is proposed for the service provider is required for proper management of service provider resources.

One of the most important algorithms in the field of load balancing and response time reduction is the machine learning algorithm. In 2005, Karaboga proposed an optimization technique based on the population under investigation's intelligent behavior. The intelligent behavior of the investigating machine learning population prompted this innovative meta-exploratory method. The proposed optimization algorithm is a numerical function. The capacity to search globally in the machine learning cloning technique, which has been realized by adding the neighborhood source generation mechanism, is a benefit of the algorithm. In this dissertation, we aim to improve the task classification method by using a machine learning strategy to balance the load and decrease response time.

In[42], a machine learning-inspired approach called load balancing is used to create a load balance between blockchain devices in order to maximize power. The suggested technique balances jobs in blockchain machines according to priority, resulting in the shortest possible wait time for tasks in the queue. In two phases, an improved cost-based method for effective mapping of activities to cloud resources was developed. They employed an algorithm to organize tasks by priority after improving the nest algorithm to prioritize tasks.

The technique starts with a random population matrix in [43] a heuristic workflow classification algorithm based on group optimization of tasks inspired by animal group behavior, such as the collective movement of birds and fish. The algorithm is made up of two parts. The major component is created, which includes utilizing a heuristic approach to find the relevant resources and then using a task group optimization method to accurately map these resources to the tasks. [44] The resource discovery method and resource allocation to accomplish workflow tasks are the two primary phases of an optimal workflow classification algorithm whose overall structure is based on a tree.

The use of this approach resulted in a considerable reduction in CPU consumption[44]: The [45] genetic-fuzzy optimization approach for task classification has been redesigned to enhance Hadoop framework resources. However, the task vector chosen has a significant impact on prediction efficiency. [46] Suggested a particle swarm optimization technique for cloud task classification that reduces processing time. With a larger number of tasks, this algorithm converges faster. Because the lack of diversity in particle cluster optimization algorithms contributes to ectopic convergence in the job classification problem, a hybrid particle cluster optimization method with diverse operations is employed to prevent ectopic convergence.

This article focuses on reducing completion time while also maximizing resource utilization.[47]: Based on the classification of jobs in the cloud computing environment, a new model is being developed to reduce switching time between resources and increase blockchain performance and throughput. [48]compares and contrasts various approaches to resource classification in the cloud computing environment; the scenarios discussed are examples of hybrid or heuristic algorithms for allocating cloud computing resources.

The process of transferring jobs from overburdened blockchain machines to underburdened blockchain machines is known as load categorization. The overall performance of the system running the program can be affected by load classification. Load categorization algorithms can be broken down into two types[42]:

Static load classification algorithms[49]: when estimating source needs, decisions on load classification will be taken at compile time. The current algorithm's advantage is merely linked to performance and overhead because no constant monitoring of nodes for performance statics is required. When the load fluctuation for the surrounding computers is low, Statium methods function well. As a result, these strategies are ineffective in network and cloud computing situations where the demand fluctuates.

Dynamic load classification methods make modifications by distributing network load among running nodes; they make distribution decisions based on current load information[12].

Holeh et al. [50]look into static load classification techniques in trees with a fixed total load. Hu et al. propose an effective data migration strategy for identifying incoming dynamic loads by computing the Euclidean Lagrangian multiple of the transferred weight in Reference Gennad et al. [50]offer an early MPI-Scatterv to allow master-slave load categorization, as well

as calculate and distribute data using linear scheduling algorithms that take optimization into account.

Reference [50] introduces the probabilistic load categorization technique of the new era in network computing. The current algorithm's major goal is to achieve load categorization while reducing reaction time. The job load classification approach for network computing is provided in reference one. This algorithm selects resources based on their most recent status and the shortest time to completion. The primary goal of this method is to classify loads and reduce response time. Reference [42] introduces the job load balancing approach for network computing. On the basis of local characteristics, hierarchical load categorization methodologies and related algorithms are explored. In the first place, this method is preferable to local classification.

After that, there will be a high hierarchical classification. The current concept's key advantage is that it reduces the number of messages transferred between network resources. This approach generates a hierarchical architecture that is decoupled from the network architecture. Similarly to the preceding article, Reference [44] describes a task load classification model in a network setting under the title "Dynamic Load Classification in Network Computing." In the same way as the prior reference, it describes the system model. This strategy's primary characteristics are as follows: (1) a superior method of shifting local responsibilities to reduce communication costs; and (3) the strategy is sporadic, with local decision making.A network can be converted into a tree using this system. No matter the intricacy of the network topological structure, this system can turn it into a tree. This tree will be used by the system to classify the load. Reference [48] presents a comparison of distributed load categorization techniques for cloud computing. The current study looks at three potential load balancing approaches in large-scale super-systems. First, using Blockchain and local actions, nature-inspired algorithms could self-organize and achieve global load categorization. Second, random sampling of the system area can be used to engineer self-organization, revealing how the load is spread over all nodes. Third, the system can be modified to improve the efficiency of job placement on blockchains.

As scientists explore for distributed methods to manage the size and complexity of such systems, they have recently focused a lot of scholarly emphasis on nature-inspired networking and computing models. To create load categorization algorithms, the following guidelines can be put into use:

It specifies what workload data should be collected, when it should be gathered, and where it should be collected. Commissioning Policy: Determines when load classification processes should begin. Based on their accessibility status, resources are classified as "blockchain" or "task recipient."

Location Policy: Finds the best partner for the blockchain or receiver based on resource policy outcomes. Tasks that must be transferred from overburdened resources to the least useful resources are defined by the selection policy the properties of load classification methods [5] can be used to further categorize loads into two groups: centralized and distributed loads, and program level and surface loads.

Reference [13]introduces the routing load classification policy for network computing systems. This strategy employs computer network routing techniques to determine the neighborhood and search of the majority of computers, effectively dividing the application workload. This approach is intended to disperse the workload of concurrent application tasks over a network of computers. The route algorithm is designed for environments with many heterogeneous processors and multiple jobs in parallel applications. When it comes to large-scale systems, absolute runtime minimization isn't the main goal of the load classification technique. The cost of communication that is incurred as a result of load redistribution is also an important consideration. In the reference, In the reference, In the reference, As a revolutionary architecture for computation offloading in the network, Yogubi offers a hierarchy load classification paradigm [14]. There are bottlenecks in this model. Reference [51] introduces the mathematical model of the cloud computing architecture that employs the bee colony optimization technique. A machine learning cloning mechanism is used for web services on dispersed web blockchains.

Because task classification in the cloud computing environment is dynamic, it's challenging to come up with a good solution that minimizes task execution time, input task execution time, and resource bit load balancing.The number of requests entering the system is increasing at a faster rate than the source[48][50]. The features of requests that have been entered into the environment from the beginning, such as arrival time, execution time, and necessary memory, are unclear and continually changing. The cloud computing ecosystem is made up of a variety of different resources.

It has network features such as bandwidth, traffic, and so on. Sources: the source of some hardware and software features such as load volume, the amount of free memory in the system,

and so on. Based on the Ant Colony Optimization Algorithm (LBACO) [12]Conley et al. (2001) presented a categorization for cloud jobs. The current method's fundamental policy is to classify the entire system in an open manner. In addition, the policy aims to reduce downtime as much as possible. In this research, the characteristics of the ant method were used to classify tasks. A classification system based on genetic algorithms [6]was introduced by Sarov Banerjee et al. (2002).

The ant colony method, which is based on the behavior of birds and fish, was proposed by Kennedy et al. (2011). The particle swarm algorithm is a solution space search that requires matching a number of parameters.

To achieve load balancing in machines, Babu et al. (2003) employed a heuristic technique. The proposed technique displayed the priority of jobs in the machine queue based on the minimal waiting time. They've witnessed a considerable reduction in waiting time and a significant improvement in execution time [8][13] [15][52].

Task classification is critical for scientific operations, but it is also a difficult task to master. Traditional distributed computing systems have already looked at task classification. In a fault-tolerant power condition, it is managed. Reference [50] presented a task classification technique for ensuring data robustness in computing settings. In RAID structured storage systems, in [6] presented an energy-aware workload classification technique.

At the cloud computing scale, In [52] looks at multi-core computational accelerators and the MapReduce programming style for high-performance computing. They looked at system design alternatives and job classification-aware capabilities in accelerator-based distributed systems for large data processing. They improved the MapReduce scheduling paradigm by allowing runtime to make use of several types of computational accelerators by matching runtime workloads with adaptive mapping of MapReduce workloads for accelerators in blockchain contexts.

As a result, none of them focuses on lowering processing costs and reducing the time it takes to move data between data centers and the Internet. As the importance of cloud computing grew, new data management systems such as Google File Systems (GFS) and Hadoop were created. Data is hidden in the infrastructure, which gives users minimal control over it. Web search applications were considered when developing GFS. Some study makes advantage of cloud computing. For the data center, the Cumulus project [8] has presented a scientific cloud

design. The Nimbus tool[15], which can be clustered directly inside the cloud and has already been used to build clouds for scientific applications, can also be clustered directly inside the cloud.

Because there are rapid connections between nodes, such as Ethernet, and the processing time is not much longer, moving data within a small cluster is not a huge concern. As a result, the cloud science workflow system is made up of distributed apps that must be deployed across multiple data centers through the Internet.

[53]Reference In terms of cost, recent research has looked at a number of data and computing-related applications. They created a nonlinear programming approach to reduce data recovery time and costs associated with cloud-based data operations. The usefulness of reclassification using cloud resources to boost work completion reliability is investigated in reference[15]. Classifications are created at the start of a project or when using network resources, whereas cloud resources are only used for reclassification after a job is completed.

They use task packages, which include a significant number of individual jobs, in their research; this work model is used in a variety of engineering and scientific programs. They presented a new reclassification approach termed "reclassification using clouds for dependable completion" and tested it on three well-known mental methods. To decrease data transportation in cloud computing, reference [12]presented a matrix-based k-middle clustering approach. As a result, reducing data transmission and cost does not imply a reduction in processing expenses or transfer time.

In this study, to reduce data transmission time and processing costs, we apply the pso approach to classify application data. In reference[16], the problem of selecting an application is studied from two separate and often opposing perspectives: that of the system supplier and that of the user. Users want to maximize the system's execution of

their individual requests without having to worry about the requests' repercussions. As a result, the manufacturer's goal is to improve system performance while also allowing for equitable resource allocation and consumption patterns as established by decision makers. While consumers are likely to seek the same request strategy, the responsible system may encounter a dynamic environment that includes changing requirements, changing consumption habits, and changing decisions based on business objectives. To solve this problem, they present a

genetic algorithm-based optimization framework for selecting distributed applications in heterogeneous contexts (GA).

In fact, the job assignment has been determined to be entirely NP [17]Since task determination is a complete NP problem, genetic algorithms have been used to track tasks[17]. However, genetic algorithms may not be the most effective way. According to the reference [24]the particle optimization method is able to obtain a higher classification than the genetic algorithm. According to the reference [7]the particle optimization algorithm outperformed the genetic algorithm in the scattered system. In most circumstances, the quality of the PSO algorithm solution is greater than the genetic algorithm in most circumstances, but it also launches faster.

As a result, we solve the task classification problem using the particle swarm optimization method. This essay's goal is to reduce total execution and transfer time. Because the service provider was expected to serve many users' applications at various times and from various locations. Task classification is one of the cloud computing industry's most difficult issues. As a result, categorizing these jobs for execution in a cloud computing environment can be a more efficient and flexible way.

PSO and evolutionary algorithms have been used to develop a number of meta-exploratory task categorization algorithms[47][48][50]. The relevant work on PSO will be discussed because the suggested job classification is based on the PSO algorithm.

A job classification algorithm has been suggested by Ali Al-Memari and Fatemeh Omar[6]. The Cuckoo's Algorithm The PSO algorithm was included in this proposed approach to generate optimal task classification in the cloud computing environment is needed to finalize jobs in the shortest amount of time while utilizing the least amount of resources.

A classification algorithm based on the PSO algorithm has been suggested by Solmaz Abdi, Seyed Ahmad Motamedi, and Saeed Sharifi [5]. The current algorithm's main ideas are that there are tasks and that the processors are stored in ascending order. Jobs are defined using one-to-one mapping once tasks and processors have been classified. The Fastest Job Processor (SJFP) algorithm is then used to construct the PSO algorithm's starting population. By combining the simulated irradiation technique with its rapid randomized global search classification approach in the cloud computing environment, Shaobin Zhan and Hojiang Hu [54] proposed an updated job classification algorithm based on the PSO algorithm. The results

of experiments suggest that this technique can minimize the average startup time and boost the rate of resource availability.

Wisalakshi et al. Civanadam [8]suggested a task classification that included PSO and elitism. The practice of selecting better people with better orientation is known as elitism. Elitism is significant since it offers a number of options for resolving the problem. Because elitism eliminates the loss of the best solution identified, PSO performance can be quickly improved. Resource classification has undergone a lot of development in order to increase cloud computing effectiveness. The majority of these studies improve costs, waiting times, scale, resource usage, execution times, and packet delivery times from the source to the destination and back. However, other critical factors like dependability, availability, classification success rate, speed, and scalability are not taken into account. One of the reasons these challenges go unaddressed is their complexity.

GHPSO (Genetic Hybrid Particle Optimization) based on Quality of Service (QoS) a system for categorizing applications for cloud resources has been introduced[70]. The genetic algorithm's intersection and mutation are implemented in GHPSO's Particle Swarm Optimization (PSO) method. According to the simulation results, GHPSO performs better than the traditional particle swarm technique. A model for task categorization was created in reference [61]. A low position value rule-based particle swarm optimization approach was proposed to reduce processing costs. Based on experimental information from a comparison of the intersection, leap, and local search PSO algorithms. According to the test results, the PSO algorithm is more appropriate for cloud computing.

3.3 CREATING A CLOUD-BASED BLOCKCHAIN ARCHITECTURE

To ensure the long-term survival of supply chain blockchains, which make use of a number of technologies, the cloud-based blockchain is required (see Figure 3.1). Service components are located at the infrastructure layer. The cloud services that are employed are determined by the requirements of each supply chain blockchain application. A platform layer sits on top of the infrastructure layer, including sublayers for APIs, blockchain frameworks, and container technology.

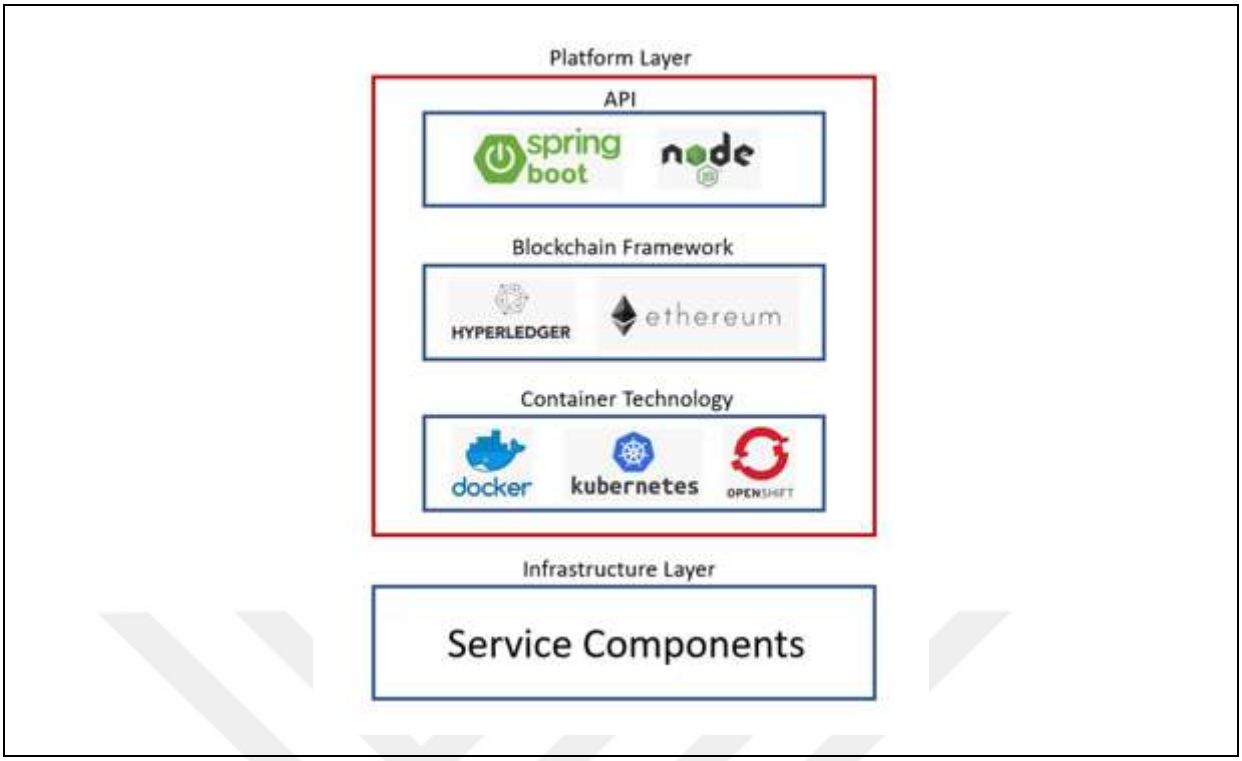

Figure 3.1: Cloud-Based blockchain architecture.

The API sublayer gives programmers the tools they need to create supply chain applications, such as sourcing, procurement, delivery, inventory management, and insurance claims. Using API sublayer apps and the integration service component at the infrastructure layer, programmers can interact with cloud infrastructure and connect to it. The API sublayer also regulates system interconnection. Both Spring Boot and Node.js are used as application programming tools in this API sublayer. Blockchain technology is applied in the layer of the supply chain blockchain framework. To this sublayer both Ethereum and Hyperledger belong. The API sublayer also regulates system communication. Application programming frameworks in this API sublayer include Spring Boot and Node.js. An extensive range of industrial applications can benefit from modular architecture. Ethereum is a platform for decentralized applications that runs on a public distributed blockchain network of computers. Examples of decentralized applications include voting, global supply networks, payment options, and financial systems.

3.4 SUPPLY CHAIN MANAGEMENT DATA ANALYTICS ARCHITECTURE ON THE CLOUD WITH BLOCKCHAINS

The supply chain management using blockchains on the cloud data analytics architecture is shown in Figure 3.2, and it includes the processes for gathering, storing, processing, and consuming data.

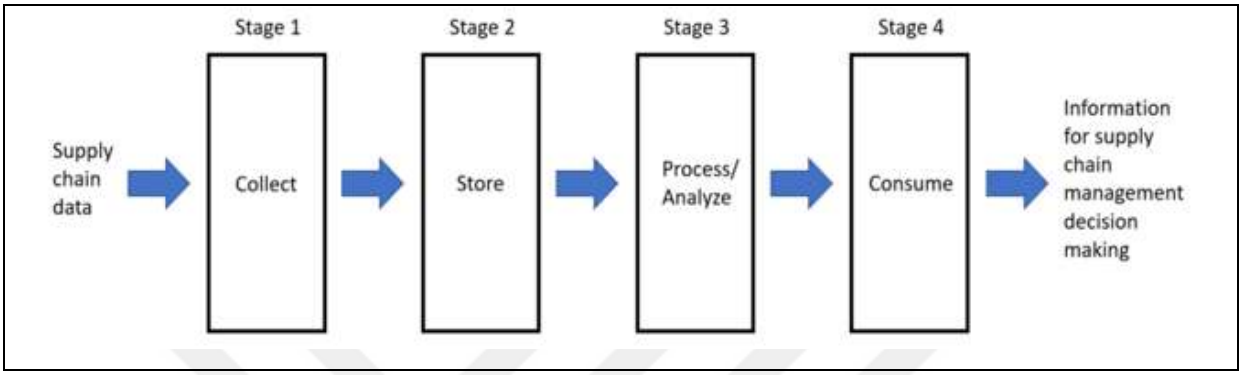

Figure 3.2: Blockchain in the cloud has been used to create a data analytics architecture for supply chain management.

Blockchain in the cloud has been used to construct a data analytics architecture for supply chain management. Structured data refers to information that has been put into a form that can be stored in a relational database. Codd created the relational technique to eliminate unnecessary data [71]. A relational database is a system for storing data that is based on the relational paradigm. Relational databases' structured data can be modified using the standard language known as Structured Query Language (SQL). Semi-structured data constructs a structure based on organizational characteristics and the usage of identifiers or tags rather than using a preset data format. Semi-structured data is typically described using IDs or tags from extensible markup languages (XML). Quasi data cannot be stored in relational databases or analyzed with SQL, regardless of the fact that it does not fit into any relational paradigm. This semi-structured data requires additional modification before it can be used or analyzed. Text, photos, audio, and video are just a few examples of unstructured data. It is impracticable for SQL to process them and produce a structure or semi-structure because they do not follow any data model.

Obtaining and putting supply chain data into a database or data lake are part of the second stage. Typically, unstructured data is preserved in a data lake, a storage facility that maintains both structured and semi-structured data in its original formats.

The third stage of the supply chain requires retrieving and processing the previously saved data. There could be involvement from operations like data transformation, aggregation, and cleansing. Almost all data analysis happen at this level. In the interim, data patterns can be found using machine learning algorithms. For the supply chain management, stock reordering levels can be developed, for instance, by using machine learning to examine past sales data.

The fourth step is where the analytical findings from the stage before are consumed. Or to put it another way, the analysis's results are offered to help the reader understand. This time-consuming stage could involve creating charts, tables, and dashboards using business intelligence and visualization software to deliver the results to supply chain stakeholders.

3.5 SUPPLY CHAIN MANAGEMENT USING MACHINE LEARNING AND BLOCKCHAINS IN THE CLOUD

We'll show you how we work in this area. We assume the software has already been transmitted to the cloud vendor, who makes allocation decisions offline. There are three steps to our procedure.

a) Using the job parameters included in each blockchain structure, we obtain the attributes of each blockchain structure.

b) The blockchain structures must now be added to the server. The implementation algorithm must take into account both the server's resource capacity and the blockchain structures' resource requirements. At the hypervisor level, this is done. The goal of the blockchain structure for server implementation is to reduce the number of servers utilized in order to conserve energy. A novel approach to solving the implementation problem, also known as the optimization problem in this procedure, has been developed.

c) Last but not least, the server's blockchain structures must be assigned to the server's CPU cores. For this, we devised a procedure. The bandwidth of a physical core may be used by the blockchain architecture. As a result, one core can handle many blockchain structures at the same time. The blockchain structure planner in our architecture is in charge of coordinating the execution of physical core-wide blockchain structures. This planning takes occur at the level of the host operating system on the actual servers. The blockchain structure planner only employs the blockchain structure specification for data segmentation

and trust management. The task data contained in the blockchain structures, for instance, is unknown to the planner.

Blockchain structure insertion stage on the server is referred to as "implementation." The step of allocating the blockchain structure to cores is referred to as "assign."

Bee-genetic algorithms are thought to allocate a subset of blockchain structures to a database. The attributes of the blockchain structure must be observed when blockchain structures are assigned to base cores. The assignor of the blockchain structure to the kernel, for example, is not permitted to divide it by more than the same maximum number of levels. We initially partition blockchain structures into a smaller number of cloud users since some blockchain structures may only have one application. For segmentation, we explored two options:

Intensive segmentation is the first step.

A. A well-balanced segmentation. This is how compact partitioning is done.

A blockchain structure with a utilization of 1.5 and a value of m = 3 is divided into three sections, each of which is worth 0.5.

Then, depending on the decreasing amount of utilization values, the segments of information and data in blockchain structure databases are categorized. Finally, we use machine learning to assign the partitioned pieces to the cores. The following is how these algorithms based on the cloud pattern are used. The proposed methods segment the data in a sequential manner. Keep in mind that the sections are listed in chronological sequence. We choose the kernel that has the sparest space after allocating the current section at each assignment step.

If the proposed algorithms are unable to allocate the current segment, move on to the next section in the sequence. Because these algorithms distribute the amount of use as trust management to the cores or the desired data in the databases, the cloud technique is used. In terms of utilization, balanced cores reduce the server's power consumption. This is due to the fact that idle data does not fail. The proposed methods produce a number that represents the number of errors. The sum of all the fractions of the blockchain structure that the assignment technique has been unable to allocate to the cores is the degree of assignment error I u.

We'll use a simple example to help you understand this argument. Assume we wish to assign three blockchain structures to a dual-core database with a utilization rate of 0.6. The mistake in the assignment is equal to 0.6. The allocation fails (I u = 0.6) despite the entire application

of blockchain structures being smaller than the existing processing power of several processors (1.82). A zero error rate (p i. U = 0) indicates that all blockchain structures placed on the server can be used successfully and without limits.

The cloud architecture includes tools for developing, training, and deploying machine learning for supply chain management using blockchains. Figure 3.3 depicts the stages of construction, training, and deployment.

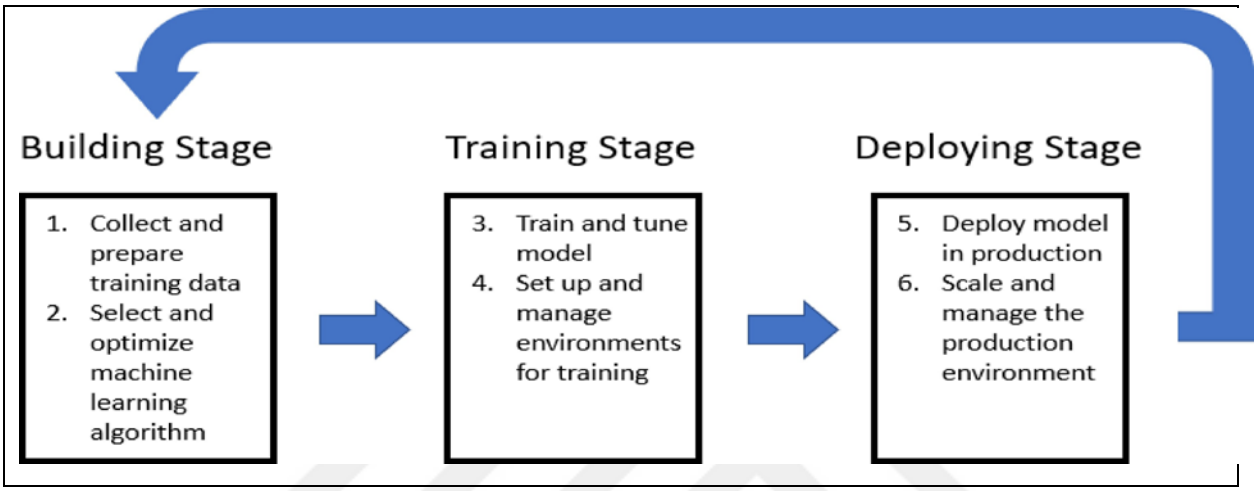

Figure 3.3: Machine learning can be built, trained, and deployed.

3.6 SUPPLY CHAIN MANAGEMENT USING BLOCKCHAINS IN THE CLOUD TO INTEGRATE MACHINE LEARNING AND DATA ANALYTICS

The integration approach suggested by Yeung, Wong, Tam, and So [26] can be utilized to manage supply chains in the cloud utilizing blockchain. As demonstrated in Figure 3.4, this tactic entails utilizing machine learning to discover insights while performing data analytics.

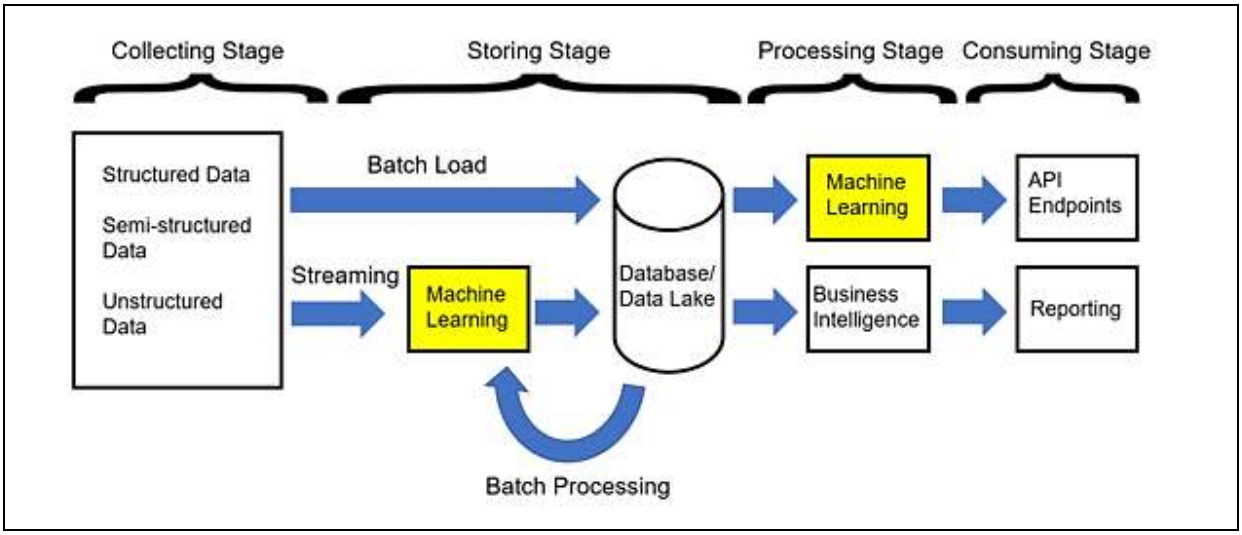

Figure 3.4: Machine learning is being integrated into data analytics.

This problem is expressed as a mathematical linear formula in this section. We'll look at how the tools and algorithms can aid in the implementation process. The goal is to keep the overall power of the servers to a minimum.

$$TP(x) = \sum_{i=1}^{M} P_i^{Blockchain}(x), \tag{3.1}$$

$$\sum_{i=1}^{N} h_i x_{ij} \leq H \qquad \forall j \in [1 \dots M], \tag{3.2}$$

$$\rho_i^u \leq 0 \qquad \forall i \in [1 \dots M] \tag{3.3}$$

$$\sum_{i=1}^{M} x_{ij} \leq 1 \qquad \forall i \in [1 \dots N] \tag{3.4}$$

Where TP (x) represents the total power of the databases for task X and $P_i^{Blockchain}(x)$ represents the power of the first database for task X.

It's worth noting that Equation (2) indicates the memory limit, which states that the overall memory demand of the blockchain structures assigned to each blockchain should not exceed the database's memory limit. The impacts of usage limits on the optimization issue are shown in Equation (3). The output of the hybrid algorithms discussed in this method, which was indicated as the process for allocating blockchain devices to cores, is the basis for this calculation. The last constraint (Equation 4) demonstrates the no-increment requirement, which

states that any blockchain structure can only be assigned to one blockchain. It is preferable to combine the goal functions and all constraints into a single function that may be employed as a proportional function for the optimization issue under the notion of linear numerical optimization. In the following sections, we will introduce a single fit function that includes the optimization problem. Under the notion of linear numerical optimization, it is preferable to combine the goal functions and all restrictions into a single function that may be utilized as a proportion function for the optimization issue. As shown in the following sections, we will introduce a single fit function that includes the optimization problem.

$$fittness(x) = TP(x) + \alpha \sum_{j=1}^{M} \rho_j^{mem}(x) + \beta \sum_{i=1}^{N} \rho_i^{u}(x)$$

So that

$\rho_j^{mem}(x)$is the compensation function defined by Equation (5), which is used to determine if a value is satisfied from a memory standpoint.
It's worth noting that if the second and third sections of Equation 5 are both zero, then the val ue of X meetsall time and memory limitations.
Otherwise, there will be some missed deadlines or memory errors.

As well as Compensation coefficients are used to direct investigations in order to develop valid procedures. The number of compensation functions is controlled by these coefficients, which are determined by the breadth of the objective function and the importance of violating each constraint. In a software system, for example, when the loss of a few deadlines (3.6) acceptable, the factor can be given a lower value.

$$\rho_j^{mem}(x) = max\ (0, \sum_{i=1}^{N} h_i x_{ij} - H)$$

The blockchain machines' loads will be combined. Some of the many types of blockchain machines are overloaded blockchain machines, underloaded blockchain machines, and trusted management blockchain machines. Each set has a number of blockchain machines Work from one of the overloaded blockchain sets was removed depending on the load and tasks available on the under-loaded blockchain machine to identify where one of the few low-loaded vector machines should be located. This work is referred to as a "bee," and low-load blockchain machines are referred to as the "bees' destination," based on the dispersion pattern of the parent-

child genetic system. The information that the bees (tasks) update is stored in the blockchain machine.

The timer should begin the trust management portion of the burden if the decision is to become a trust management burden. To execute load trust management, we need to detect overloaded blockchain machines, demand (load required), low-loading blockchain machines, and supply. We must evaluate the tasks in order to decide which blockchain machine is ideal for the eliminated task queue.. Tasks that were removed before overloaded block machines were detected may be useful in discovering the current task's incorrectly loaded blockchain machine. This food finder is now the watch bee for the next mission. This process will continue as long as the work of trust management is effectively fulfilled. We have explained and demonstrated the special way of its development and diagnosis in several areas. In this chapter, the detection procedure in relation to cloud computing and blockchain in the context of machine learning patterns should be exactly like this. Acted upon following that, we presented the proposed topic in its entirety, in accordance with the needs of the problem related to the cloud system and bees, based on the genetic pattern, so that the results would be clear to us according to the topic of the next chapter, which is implementation.

With the use of numerous various data models, this work aims to improve the diagnostic and forecast accuracy of a two-state classification problem associated to speed improvement. For this reason, only high-performing data from the test sample space is used, while inefficient data is sought and ignored. The performance of each data set for a "test sample" is determined in this case using samples from the training data set that are close to the test sample. This allows the data to vote for the best-performing test sample.

Data mining and the bee pattern on it are used to predict the number of samples in the training set close to the new sample in order to assess the effectiveness of a set of bee data for a new sample in the training data set. By contrasting the actual label with the label predicted by the genetic pattern, it is possible to assess the accuracy or performance of data near to the new sample. If the system's diagnostics and performance fall within the preset range, the system's diagnostics and performance will be significantly improved. If the data in this system isn't unique to this new instance, the prediction will be removed from the data prediction suite. To assess performance, the KNN approach is utilized. This approach makes use of a number of close samples.

The class with the most views among the k samples determines the new sample prediction class. As proximity criteria, direct distance, square of direct distance, step distance, and so forth can all be employed. The new sample's surrounding samples are the k samples with the shortest distance in this example.

We consider multiple layers based on the considered basis and accessible data in such a way that the layer with the highest detection accuracy and the least amount of time and effort wins. We consider existing data as if it were fresh data, allowing us to select the desired layer or sample depending on the target's unique characteristics and the sample's special characteristics. We discover and eliminate unneeded layers based on this option.

3.7 CASE STUDY

The case study approach is well-documented and acknowledged across the academic literature as a useful tool for examining phenomena that have not yet been investigated, as indicated by Di Vaio, Varriale, and Alvino [74]. Case studies can be used to assess particular characteristics while isolating occurrences from their environment [75] [76].

Because of the confidentiality agreement, this unique blockchain on cloud design with machine learning embedded into data analytics for supply chain management has no equivalent precedents. Investigation's theoretical underpinnings included technology scalability and massive data processing and analysis.

3.8 IMPLEMENTATION OF SUPPLY CHAIN

Following the receipt of an order notification and a shipping request, Maersk organizes the shipment and determines the most practical route for a cargo ship to take between the port of origin and the port of destination. The shipment's schedule, route, and required paperwork (such the bill of lading, letter of credit, and forwarder's certificate of carriage) are communicated to the parties involved (e.g., the bank, the supplier, the port authorities, and the buyer). As seen in Figure 3.5, the blockchain-based platform with machine learning is primarily intended for the detection and evaluation of marine risk. This detection is made possible by a machine learning system that makes use of computational and statistical analyses of previously assigned routes and historical dangers. Learning or growing as a result of experience is a cycle that leads to more precise forecasts. Using huge data from previously assigned routes and historical danger zones,

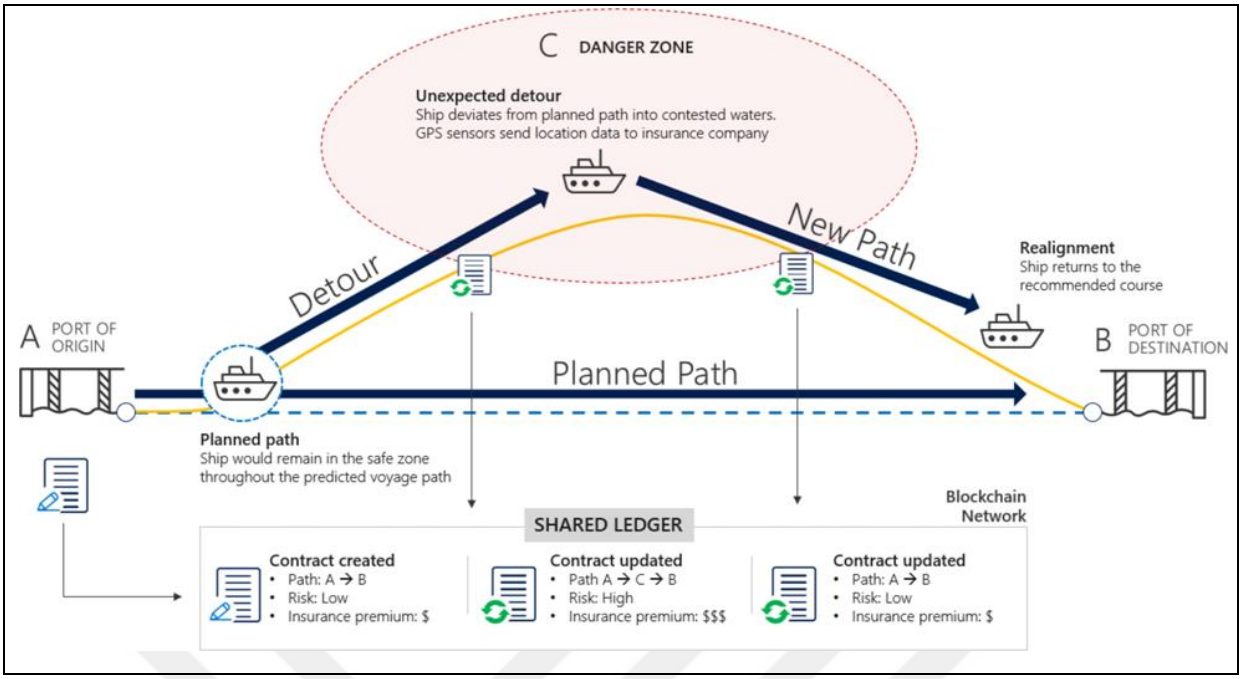

Figure 3.5: Assessment of marine danger in real time. Cheaper insurance premium

3.9 SIMULATION

The implementation, technique, and data analysis are all covered in depth in this chapter. This chapter will broadly discuss how cloud computing is categorized based on the blockchain architecture using the explanations provided in the previous three chapters as a foundation. The proposed approach is then evaluated against several techniques for gathering the required data.

A general system based on adjustments for the desired system is evaluated in the initial phase for a general state based on security and cloud environment users. A general condition is regarded as a cloud environment in this system, depending on the changes that are considered for the system, according to the security formulation and based on formula 4-1. Any parameter that isn't part of this framework isn't acceptable.

$$\alpha = unifrnd\left(-gamma, 1 + gamma, size(x_1)\right) \quad (1) \tag{3.7}$$

This parameter is based on changes that extend across both the horizontal and vertical axes. The next phase will be to define the final limit for the proposed system, based on which the cloud environment will be able to protect data in terms of security. For development based on genetic patterns and neural networks, all of these are defined as parameters and formulas.

$$y_1 = \alpha .* x_1 + (1 - \alpha) .* x_2 \qquad (2) \tag{3.8}$$

$$y_2 = \alpha .* x_2 + (1 - \alpha) .* x_1$$

$$y_1 = \max(y_1, varMin) \qquad (3)$$

$$y_1 = \min(y_1, varMan)$$

$$y_2 = \max(y_2, varMin) \qquad (4)$$

$$y_2 = \min(y_2, varMan)$$

Parameters outside of this structure are regarded as threats within this structure. In this regard, and based on the recommended adjustments for the proposed system, a final classification based on numerous data points should be completed at the conclusion to establish the overall efficiency of the task. After all of these processes are completed, a structure is created for the simulation pattern of this general curve, which depicts the entire cloud environment.

$$x_1(k+1) = x_1(\mathrm{k}) + \left(\mathrm{a} * x_1(\mathrm{k}) - \mathrm{b} * x_1(\mathrm{k}) * x_2(\mathrm{k})\right) * \mathrm{dt} \qquad (5)$$

$$x_2(k+1) = x_2(\mathrm{k}) + \left(-\mathrm{c} * x_2(\mathrm{k}) + \mathrm{d} * x_1(\mathrm{k}) * x_2(\mathrm{k})\right) * \mathrm{dt}$$

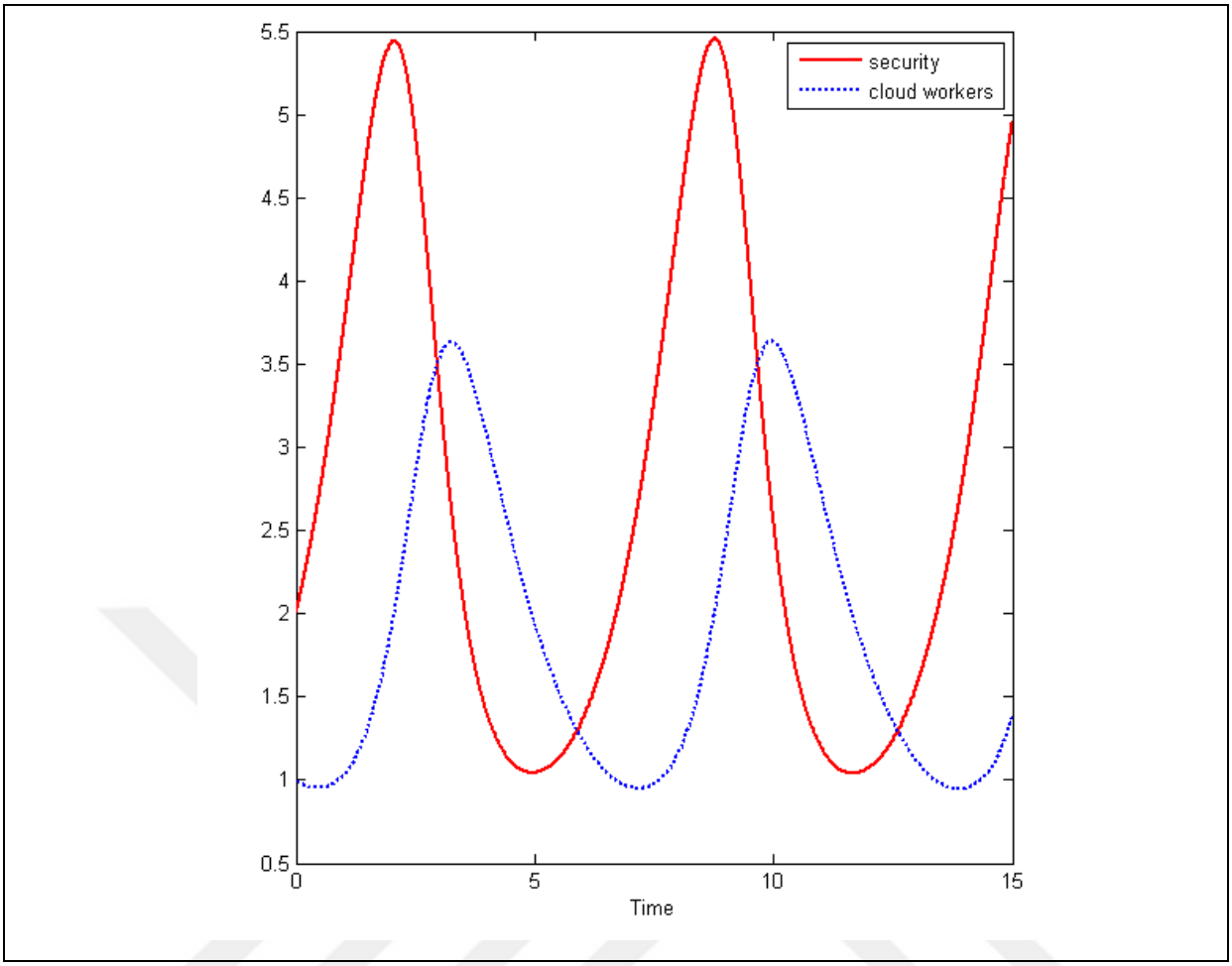

Figure 3.6: Security Detection and adaption in the cloud environment are the basis for this general pattern.

The red diagram in Figure 3.6, on the other hand, depicts the proposed system's security structure in terms of dimensions and general characteristics. In reality, the security structure in this section demonstrates how any modifications in various cloud frameworks affect Formula 4-5. This is a broad foundation for the cloud environment, not a specific security goal.

In reality, the image indicates that there is a complete pattern for detecting distinct factors that extends outside the cloud environment based on the modifications.

The generic and hypothetical framework for a cloud environment is described based on the security and cloud models, according to the explanations provided in formulas 1 to 4. Figure 3.7 depicts this broad structure.

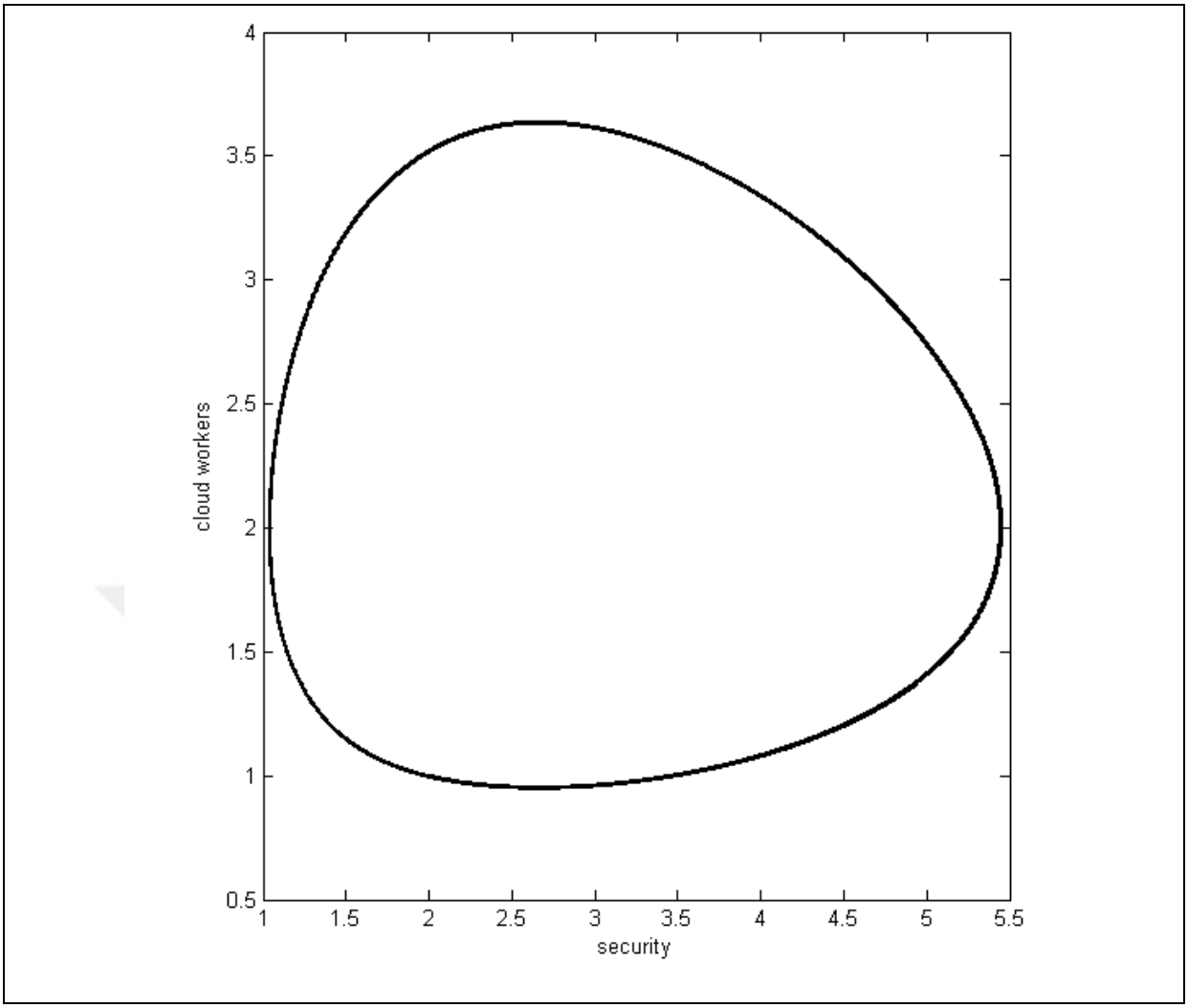

Figure 3.7: The Relationship between security and cloud computing

The link between current data and cloud security is illustrated in Figure 4-2. The proposed system's general structure is shown in this structure, which is based on these assaults. The extent of our reviews, the in-depth examination of blockchain categorization challenges in cloud computing, and the focus on the most recent solutions offered in the papers in the aforementioned research all differ significantly. We've also put together a table that compares the different techniques. In addition, we briefly explore blockchain-based categorization challenges in mobile cloud computing, as well as general tactics that can lead to a solution.

In the cloud environment, classifications based on the blockchain framework are carried across many physical sites and cloud facilities based on a variety of factors like migration, equipment failure, load balancing, energy efficiency, and hardware/software rating. Many blockchain-based classification challenges addressed in the previous sections are caused by blockchain-based classification migration. As a result, categorization considerations based on a high

blockchain architecture are required. Below is a list of strategies that are classified as blockchain frameworks in the Responsible Migration Management framework.

In the accessible results, there is also a comparison of the detection rate based on a specific knowledge of the entropy of the data. The proposed approach to this research has the maximum detection rate based on the available identifiers, as is shown in the proposed method in each interval and model that is imagined for the article.

Figures 3.8, 3.9, and 3.10 show the simulation results. Each table's first two columns contain user identifiers (1 to 15) and provider identifiers (1 to 3). Figure 3.8 displays the percentage averages of CPU utilization, RAM memory usage, resource consumption, the ratio of on-time payments to total payments, and the historical value of the user session latencies, which are a measure of connection stability. Figure 3.9 shows typical (historical) user input along with typical values from outside data sources (F1, F2, F3, and F4). The sum of the data points from the ten simulations for each external data source yields these figures, which represent the historical average. Based on the data from the preceding Figure, Figure 3.10 displays the values of the Objective and Subjective Credibility Indicator.

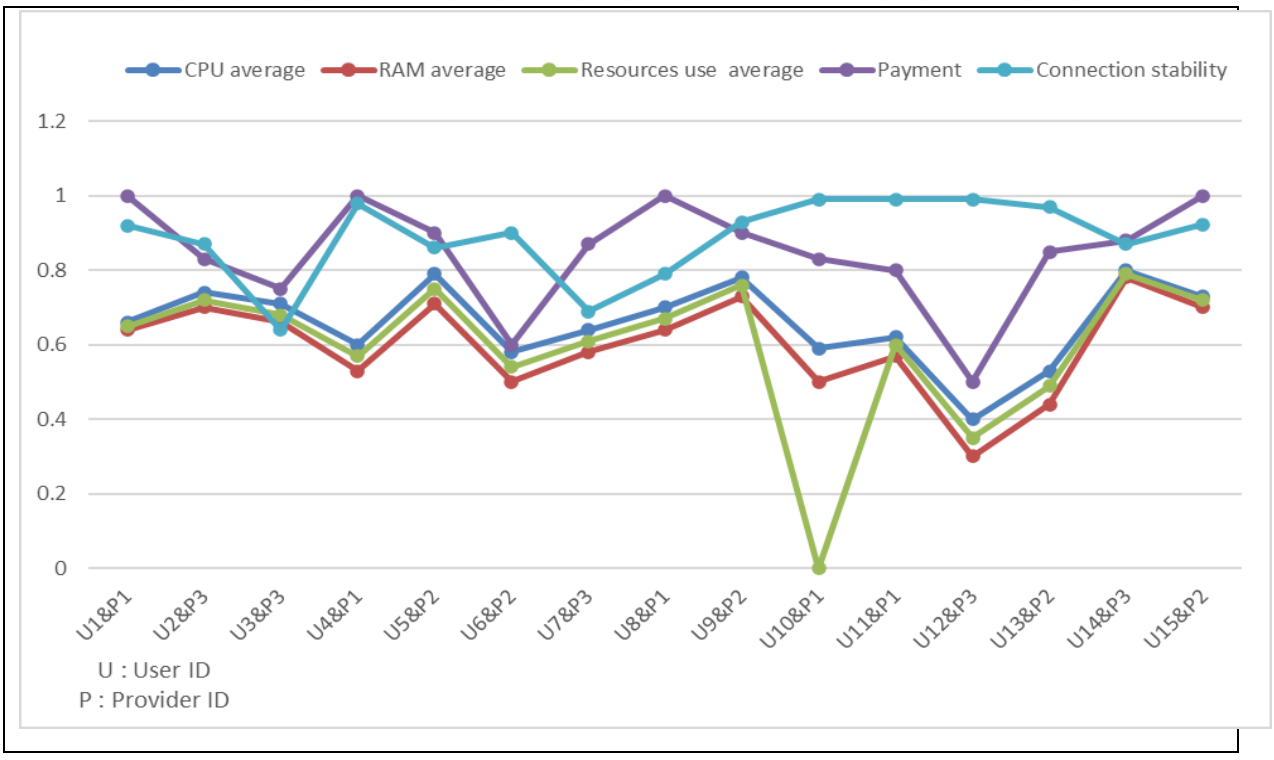

Figure 3.8: Cloud Providers provide statistics on user sessions.

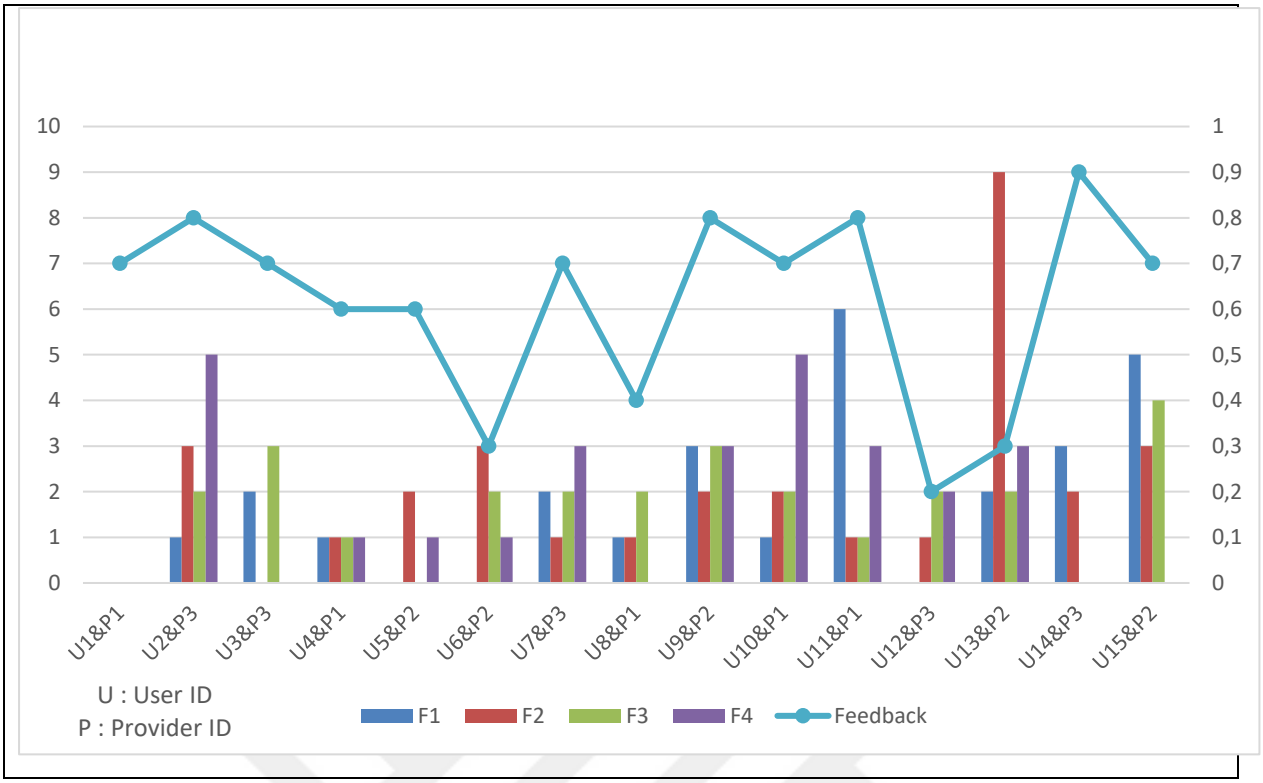

Figure 3.9: External data sources were used to compile this report.

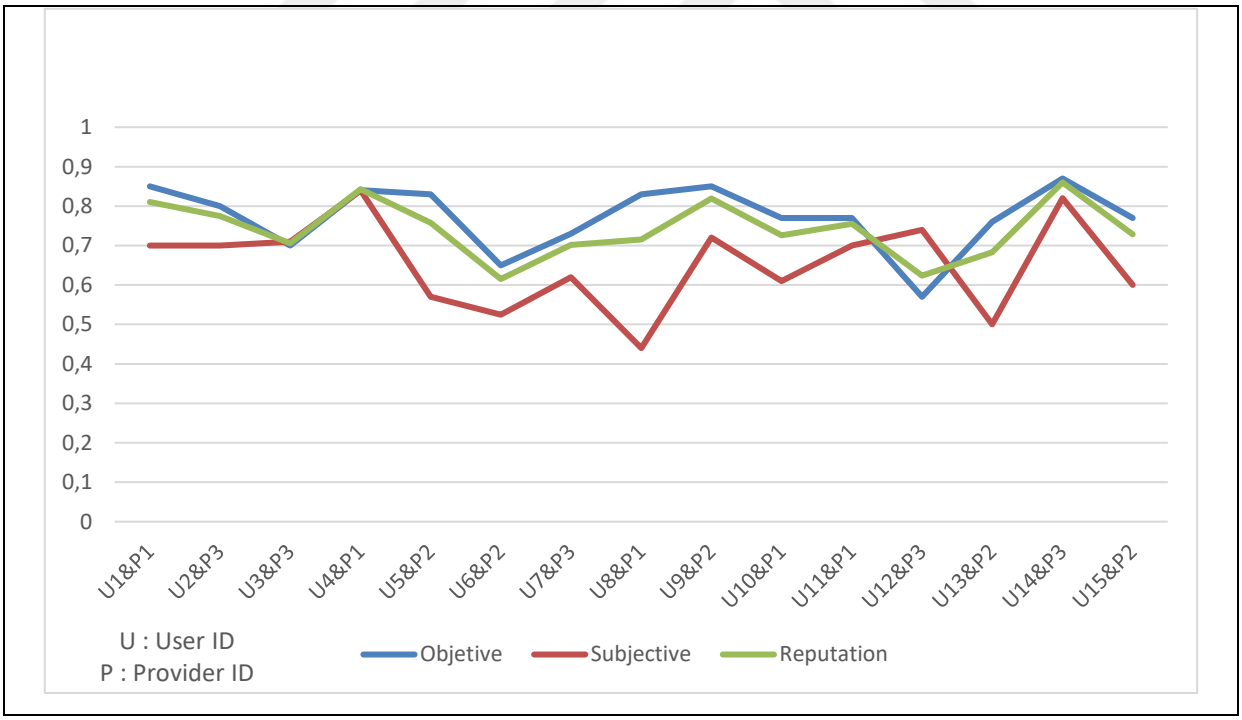

Figure 3.10: Results and repute of indicators.

Additionally, each user's reputation score is displayed in Figure 3.10. Finally, Figure 3.9 illustrates the users' reputation values. The users' identifiers (U1 to U15) are coupled with the providers' identifiers on the x axis of Figure 3.9, which displays the distribution of users at the

providers (P1 to P3). Each user's reputation values are displayed on the y axis, which range from 0 to 1, with 1 being the best. The figures show that User 14 (U14), who utilized Provider 3's services, has the highest reputation value of all users, with a value that is almost 85%.

When compared to the other users, U14 has the greatest average resource usage (Equation 6) and hence this number is related to historical average computing resource utilization (Figure 3.8). It also completes the majority of monthly or annuity payments on time, as illustrated in Figure 3.8, and has outstanding connection stability. User 14 also had a high overall average of provider feedback ratings, despite having a total of five unresolved complaints from external sources, as shown in Figure 3.9. As a result, this user has an equal balance of objective and subjective behavior, as seen by his objective credibility indicator of 0.87 and subjective credibility indicator of 0.82. Figure 3.9 displays the values for user 12 (U12), who also utilized provider 3's services.

Fortunately, the blockchain's immutability and decentralization help classify cloud resources, assisting in overcoming the drawbacks of centralized AC. Furthermore, the independent implementation of AC policies by the smart contract may reduce the requirement for third parties. Researchers have recently created blockchain-based cloud resource classification systems that can give or restrict resources. In order to guarantee that requesters had access to the resources they required, they also developed resource classification policies. These rules can be included in tokens as blockchain transactions or smart contracts, or they can be found in the block header as a policy file. Cloud resource management issues were partially resolved by blockchain technology, but new ones were also brought about.

Privacy considerations arise in a public blockchain, since cloud devices have limited resources and all network participants may see transactions. On the other side, a private blockchain enhances privacy by enabling user limitation and participant authentication. Because it is not a truly decentralized network, accountability is not guaranteed. As a result, you may use this article as a reference to select a blockchain platform for your cloud application.. The following are the study's most major unresolved problems:

Data leakage: By leveraging digital signatures and data encryption to preserve data privacy, blockchain technologies improve the security of cloud services. However, the majority of the proposed effort will involve analyzing user data on the blockchain network, which presents privacy issues. As a result, it will take time and effort to incorporate privacy-preserving methods like anonymization or mixing with blockchain-based AC for cloud systems.

What cloud resources are restricted? Due to their limited storage and processing power, cloud devices face a significant problem during the mining process. On the other side, off-chain can improve performance and decrease latency by offloading data from the blockchain. Future research will focus on low latency and low computation consensus systems that could be employed in the cloud due to worries about security and privacy. There is no resource classification enforcement because of the cloud's dispersed topology. The techniques are compared with regard to scalability, dissemination, user-centricity, privacy protection, self-enforcing rules, and security. Any AC mechanism for the cloud, on the other hand, must have the following characteristics: scalability, dynamicity, and user participation. Because Cloud devices are constrained and cannot support large computational activities, any Cloud resource classification technique must include a lightweight characteristic. As a result, utilizing blockchain technology to classify resources can make it difficult to find a balance between auditability and privacy. Therefore, future blockchain-based resource classification initiatives should pay more attention to security, user privacy, self-enforcing norms, and cloud-friendly resource classification.

4. SCALABILITY AND PRIVACY FOR SMART CONTRACT

In this chapter, we demonstrate how HSMs and ZoKrates can improve the privacy features of blockchain-based healthcare applications. We discuss a blockchain-based approach that helps a community's internal healthcare system maintain privacy and trust through zero-knowledge verified off-chain computations. In addition to safeguarding patient privacy, this technology increases the scalability of the system. In a broader sense, we demonstrate how a group of distrusting individuals can execute algorithms using ZoKrates off-chain computations together with on-chain commitments. This chapter is based on our paper [5] and includes it.

4.1 INTRODUCTION

For administration and sponsorship that depends on a centralized authority. The conventional administration of healthcare systems would collapse owing to the increased demand for healthcare services by people as a result of the fast rise of the global population. Furthermore, since these systems rely solely on points of control, they are subject to failure [55]. Careful and long-term management of these services is necessary to address the imbalance between the demand for healthcare services and the availability of resources. Decentralized blockchain technology holds the most promise for governing and maintaining healthcare delivery systems while also boosting security and privacy, which are both important considerations for patients [78]. For a blockchain-based system to be effective in decentralization, smart contracts, which are a collection of automated or modified scenarios based on blockchain platforms, have been developed [56]. Smart contracts were created to allow decentralized systems by automating or transforming a number of situations on a blockchain. In healthcare, smart contracts guarantee that the systems' individual parts are interoperable (e.g. hospitals, ambulances, and emergency response systems). Smart healthcare systems can administer treatment, especially in remote healthcare systems, because doctors can aid in real-time decision-making. Through the use of smart contracts built on the blockchain, health data will be preserved safely and permanently. It also allows patients to have easy and flexible access to their data [57]. blockchain is a collection of cryptographically connected data. It is distributed ledgers that depict peer-to-peer links that are validated by third parties. Bitcoin and Ethereum are essential ideas that represent crucial stages in the development of blockchain technology. Satoshi Nakamoto offered it first [43]. Bitcoin is a blockchain-based form of electronic money. The usage of Bitcoins, which handle value transfers through peer-to-peer communication without the need for a reliable middleman, enables decentralized networks. In the Bitcoin network, a consensus algorithm and

asymmetric cryptography-encrypted transactions are combined to form a voting system. Independent peers can validate Bitcoin transactions without the use of reputable intermediaries. [58]. Bitcoin uses a consensus method called Proof of Work (PoW). In order to prevent network overload and in accordance with link rights of computational power, the PoW protocol links newly added transactions and computing efforts with a peer. The PoW eliminates the communication complexity while traditional consensus algorithms like Paxos and Raft are not scalable enough to ensure Sybil-resistance. Due to the cost of direct approval of the transaction sequence, the data structure of chain-linked is made up of blocks that are accumulated by several transactions, then organized and connected by a prior hash to identify the predecessor block. [59]. Ethereum uses complicated protocols to allow users to send and receive currency. Peers on Ethereum employ independent validation to ensure that they agree on a result [60]. Smart contracts, one of Ethereum's newest features, are complicated user-defined programs that can be installed and run on the blockchain network. Various objectives can be achieved, such as reducing fraud losses, enforcement costs, and other transaction costs. Also, economic objectives can be achieved (such as payment periods, liens, secrecy, etc.) [21][61]. With the help of smart contracts, which are Ethereum apps, it is possible to run a system's transition function on the network in a secure and trustworthy manner. Smart contracts are self-executing contracts that are carried out by an independent agent in accordance with contract requirements. According to Ethereum's gas idea, two things must be stated: a price for gas used during each execution and an initial endowment for a smart contract function. Bound-upper is employed in this case to restrict the cost of block validation for network peers, hence reducing the number of processes that can be computed and the size of the data that can be stored. The gas also specifies the highest level of complexity for blockchain operations [84]. Two key concepts need to be explained: sidechain and off-chain computing. A reliable third party is not initially required when using the sidechain to move assets between distributed ledgers [85]. a source blockchain ledger that includes data from the source blockchain The source blockchain's in-network activities are participated in by light clients, while the destination blockchain verifies the block headers that commit consensus rules. Rules.A regular order is also applied to the hash-block chain's headers [86]. The proof-of-work (PoW) of blockchains verifies submitted block hashes and ensures direct invariance based on the current difficulty. The XCLAIM method generates a chain for transferring assets on a cryptocurrency-backed host ledger [62]. In addition, Jacob Eberhardt [63] proposed an off-chain approach for doing verified computing. By allowing computations to take place from outside blockchain resources and ensuring implementation integrity using zero-knowledge testing, this solution takes advantage of the

growing scalability and processing limitations of privacy in blockchains [64]. When putting this strategy into practice, you'll need a verifiable calculation scheme as well as an efficient and safe solution. The ZoKrates provides an on-chain verifiable high-level programming language and a set of tools for off-chain computations[65]. Initialization and computing off-chain are two essential operations for ZoKrates, as shown in Figure 4.1.[59]. Initialization is a three-step procedure that takes performed before off-chain computations:

a) The ZoKrates program generates a key pair for a purpose specific to that program, as point (1) in figure 4.1.

b) In the first step, the key pair must be proved and validated. This can be done by one-party trusted computations or by multi-party computations (MPC) on both sides, as point (2) in figure 4.1.

c) A smart contract is constructed and then published on a blockchain in order to validate the verification key, as point (3) in figure 4.1.

The off-chain computations were executed and confirmed during initialization by: An execution trace known as a witness is produced as a result of the created program processing the input set.

a) When given a set of inputs, it also produces proof that a program is being executed correctly, as point (a) in figure 4.1.

b) In this stage, the witness and the proof key that were both obtained during the starting process are combined, as point (b) in figure 4.1.

c) The off-chain method checks the validity of computations by evaluating the proof submitted to the blockchain, as point (c) in figure 4.1.

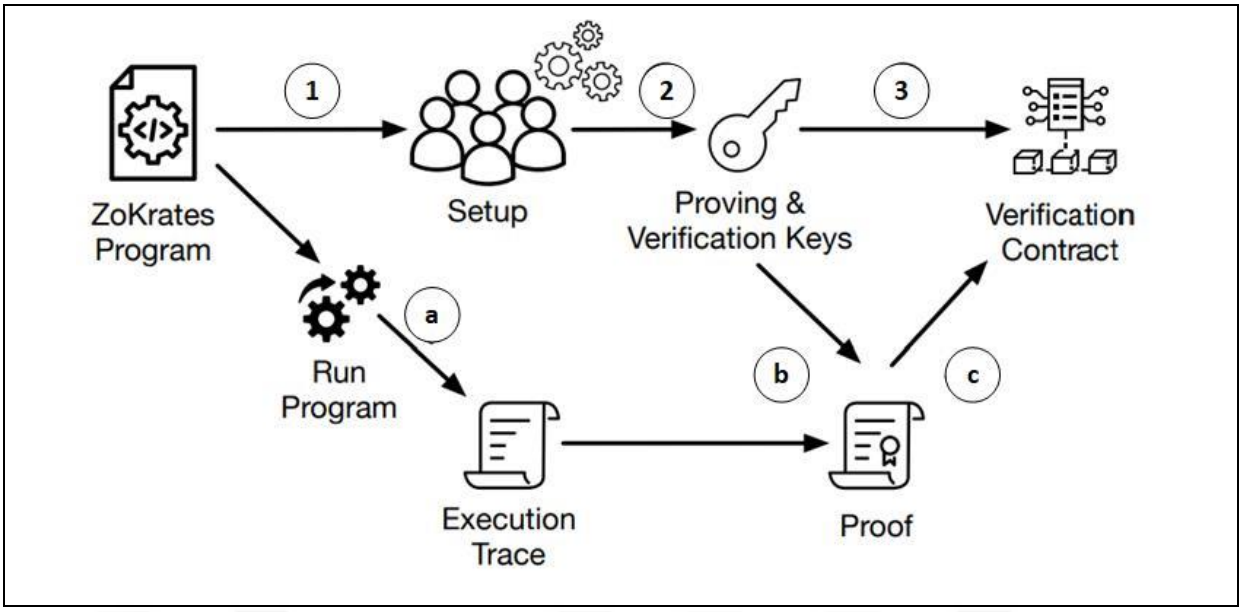

Figure 4.1: Shows Two Essential ZoKrates processes: off-chain initialization and calculation.

As a continuation of this chapter, here is what follows. A quick overview of Blockchain deployment in healthcare is illustrated in section 4.2. As shown in Section 4.3, we talk about related work. In Section 4.4, we talk about our system's design architecture. Experiments concentrating on Blockchain are addressed, contrasting on-chain and off-chain situations. At the end, Section 4.5 contains chapter's conclusion.

4.2 RELATED WORK

Researchers demonstrated usable technologies using diverse methods in a range of healthcare tests, indicating that smart contracts and blockchain technology offer workable solutions. With their research, Griggs et al. provided significant results for healthcare systems that were based on precise information and enormous amounts of data collected by sensors [80]. Health information security can be enhanced, remote monitoring can be carried out, and alerts can be generated automatically when using blockchain to its maximum potential. Although transactions cannot be connected when anonymizers are used, this level of privacy protection falls short for patients. Mettler et al. [91] claim that their system focuses on preventing the manipulation of medications, safely accessing data, and efficiently managing healthcare. The system's adaptability and scalability are constrained, though. [92] Yue et al. established Healthcare Data Gateway (HDG), an electronic medical records system that complies with legal and regulatory requirements. Data held by the HOG is secure and unalterable. This fabric's foundation is Hyperledger.

A pervasive social network (PSN) is used by Zhang et al. [93] to establish connections for exchanging health-related data. However, the PSN would not offer tamper-proof data auditing or secure data access. [94] Wang et al. present a framework for the exchange of data, facilitation of forecasting, and provision of illness treatment recommendations. The difficulties of data integrity and scalability are still not addressed in their method of data management. [94] In their system design, Ismail et al. make use of demographic clusters to ensure that partners are present in the subnetworks that are connected by servers. Therefore, reducing computational overhead reduces system efficiency. System forking is also prevented as a result of this. Therefore, performance evaluation and architecture shouldn't present any issues while implementing them. In their work [95], J. Wang et al. provided details of an eHealthcare system that utilized WBANs and the IEEE 802.15.6 standard. Data security, performance stability, and the usage of inexpensive technology were all demonstrated by an eHealthcare system. EHealthcare is not suited for a medical system with many participants because the system cannot be supported by more than 51 members.

Omar et al. [96] created a cloud platform for healthcare based on hospital clusters, with the ledger for each cluster being hosted on its own node. It receives queries from other nodes in the same cluster. Outstanding issues with the platform include entity interoperability and key theft or loss techniques. Furthermore, neither security nor privacy nor performance were subjected to thorough evaluations. The Internet of Medical Things (IoMT) paradigm was introduced by Nguyen et al. in [97], which is monitored by smart healthcare systems using smartphones. IoMT is a data sharing and exchange mechanism that fuses mobile applications with blockchain network applications. Additionally, the IoMT model was capable of securely transferring data between mobile cloud users and smartphone users. The benefits of integrating blockchain and the Internet of Things have been proved by Simic et al[98] .'s technology (IoT). The method provided scalability in the event of enormous data even though BlockchainDB had been tested. Regarding data gathering and storage on public/private blockchains, it was not adequately tested. The Federated Hospital IoT Clouds (FHCs) solution was proposed by Celesti et al. [99], and it specified a telemedical laboratory service and developed a healthcare workflow based on a blockchain and Ethereum hybrid network environment. But it made no recommendations for enhancing the scalability and performance of the blockchain. A three-tier system has been created and developed by Shukla et al. [100] using advanced signature-based encryption (ASE), fog computing, and the blockchain. The framework finds verified IoT healthcare devices that securely communicate patient health data (PHD). The ASE method

reduces packet-to-packet errors in PHD transmissions between IoT devices and end-users. The ASE method enhances both the accuracy and the reliability of malicious node identification. PHD transmission between healthcare IoT and end users is also improved with the ASE technique. As a result of using the ASE technique, malicious nodes can be detected more accurately. A decentralized blockchain approach is used to secure healthcare data. However, when coupled with healthcare IoT and fog computing, the framework was unable to overcome blockchain's scaling limitations. The methodology identifies trusted IoT medical devices that safely convey patient health information (PHD). In PHD transfers between IoT devices and end users, the ASE approach lowers packet-to-packet errors. The ASE approach improves the reliability and accuracy of malicious node identification. The ASE approach further enhances PHD transfer between end users and healthcare IoT. By employing the ASE method, malicious nodes can be identified more precisely. Healthcare data is secured via a decentralized blockchain strategy. The platform, however, was unable to get beyond the scaling issues with blockchain when combined with healthcare IoT and fog computing.

4.3 MOTIVATION

Healthcare on the online is still developing. Technology plays a crucial part in the health profession; it has offered a plethora of benefits to physicians as they continue to look for innovative methods to treat patients. Patients may now have access to medical treatments and information that might not otherwise be available because to technological breakthroughs. These remote gadgets regularly collect data and send it to different health authorities for review. A nurse might visit the patient's home, set up all the necessary tools, do the relevant tests, and then send the results to the doctor. Healthcare is essential for doctors and patients seeking medical treatment when it comes to therapy and diagnostics [101]. For instance, a patient with cancer might utilize the system to interact with other patients and obtain specialized expertise. Peer conversations offer helpful information and, most importantly, support. This enables doctors and other healthcare professionals to access knowledge without leaving their employment, in addition to periodically brushing up on their skills. Most patients should be able to easily meet health insurance company requirements while using medical remote services. To determine if blockchain and IoT may be used to remotely improve healthcare results. The addition of smart contracts to the blockchain has opened up a number of new possibilities for trustless decentralization. The blockchain's decentralized and self-reliant personality makes it an excellent choice for interfacing with IoT networks. Additionally,

by integrating the two systems, problems that arise can be resolved. highlighted in [66], the blockchain saves data from IoT devices as transactions, much to the decentralized peer-to-peer architecture of that technology. Each transaction is confirmed by all blockchain peers before being included in a block of data. For blockchain-based IoT applications, in-depth familiarity with the logical and architectural underpinnings of complex scenarios is necessary. Several challenges in this integration process still need to be resolved. [30]. Given that IoT has been implemented across numerous industrial sectors and has proven to significantly lower operating and maintenance costs, it is crucial to establish the best implementation strategy possible, especially in light of security concerns. Blockchain technology must be used to protect patient data because it is exposed to several risks as a result of being moved from biomedical sensors to cloud servers. It could be done in the way that follows:

The ledger can store encrypted keys, allowing for safe communication. The sender will then request its node for the target device's public key before encrypting the message [67].

a) Individual authentication: Individual authentication is the procedure through which the network ascertains whether or not the user entering the network is authorized [68].

b) IoT devices that are authorized to connect to the network must be prevented by a rule or other framework. In order to obtain credentials from the network's root server, it may be done by setting up an enrolment process for new nodes. The remote access server must verify the IoT devices' authenticity before presenting the node list that is available in the network [69].

c) Scalability: Many blockchain systems have a low throughput. Blockchain-based solutions, in particular IoT [106], might not be the best choice for applications with a high volume of transactions.

4.4 SYSTEM PROTOTYPE

The proposed system, which is based on the Kristen model [80] and Eberhardt [84], consists of individuals, monitors, digital phones, blockchain based, blockchain, insurance companies, and healthcare professionals. A healthcare professional connects sensor-equipped nodes to the patient in order to monitor them remotely. There are further medical gadgets accessible for use (e.g. insulin pumps). Smart devices receive unprocessed data from sensor nodes (such as smartphones, tablets, and personal assistants). The data is then compiled and formatted with

the aid of smart devices. The data is then reviewed and processed in a smart contract that is applicable to the data from a smart device. In effect, the Ethereum protocol sends data to pertinent smart contracts, which are connected to the smart device immediately. Data analysis, alarms, and automatic therapeutic directions are provided to the patient and the smart contract. In accordance with the contract the healthcare provider. Additionally, smart contracts give authorized healthcare practitioners easy access to patient data by providing the necessary tools and standards. Which points will be covered and which won't depend on what the insurance providers decide. It will be decided whether or not to get the insurance based on these requirements. Based on the requirements of the patient, hospitals, clinics, blood banks, physicians, pharmacists, and other healthcare providers provide a range of services. On the blockchain, smart contracts are created, which restricts access to data by allowing only vetted people to read blocks, operate specific nodes, and validate brand-new blocks. Additionally, smart contract awards may be customized to meet the unique needs and circumstances of every patient. Every device that calls the initial is divided up into subcontracts in a smart contract, and each subcontract calls the proper subcontract and delivers input data to it, including the device used by the patient and thresholds.

Data is examined, and depending on the threshold values in each contract, notifications or treatment orders will be sent out if necessary. A smart contract cannot be modified after it has been released. It will instead be "finished" prior to the publication of a new contract. As a result, a contract can be swiftly changed using a modular structure without affecting other contracts. A healthcare smart contract is a smart contract that exchanges data with a smart device. Healthcare providers also need to make sure insurance companies are covered by processing data from insurance documents that include components from healthcare providers. It is considered valid if the transaction's sum is less than or equal to the cost of the gas delivered. We build end-to-end apps based on the analysis of the problem and its requirements, using key technologies that have been developed to support decentralized applications (Dapp). Figure 4.2 displays the tools and stages of the development environment. The process of development entails:

a) To produce the UML contract diagrams.

b) To design and test smart contracts, utilize the Remix IDE.

c) Truffle IDE facilitates the development of the contract's Dapp module.

d) Use the Ganache test chain to deploy the smart contract.

e) The decentralized apps module was built using Web3.js.

f) Create the system's web User Interface (UI) and web component.

g) Utilizing the MetaMask browser plugin to link the web user interface with contracts issued on the blockchain.

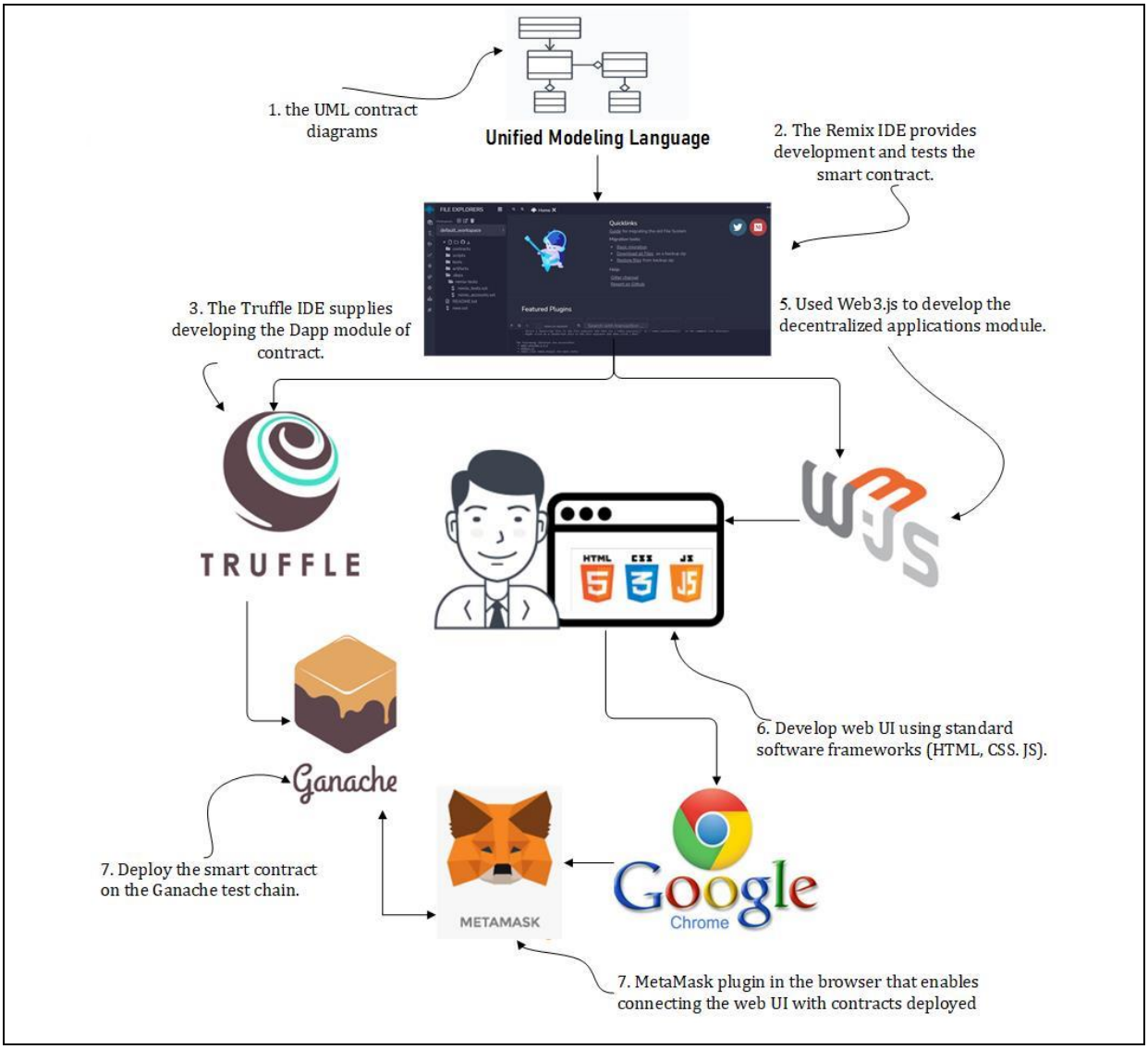

Figure 4.2: Tools, Processes, and environment for developing apps

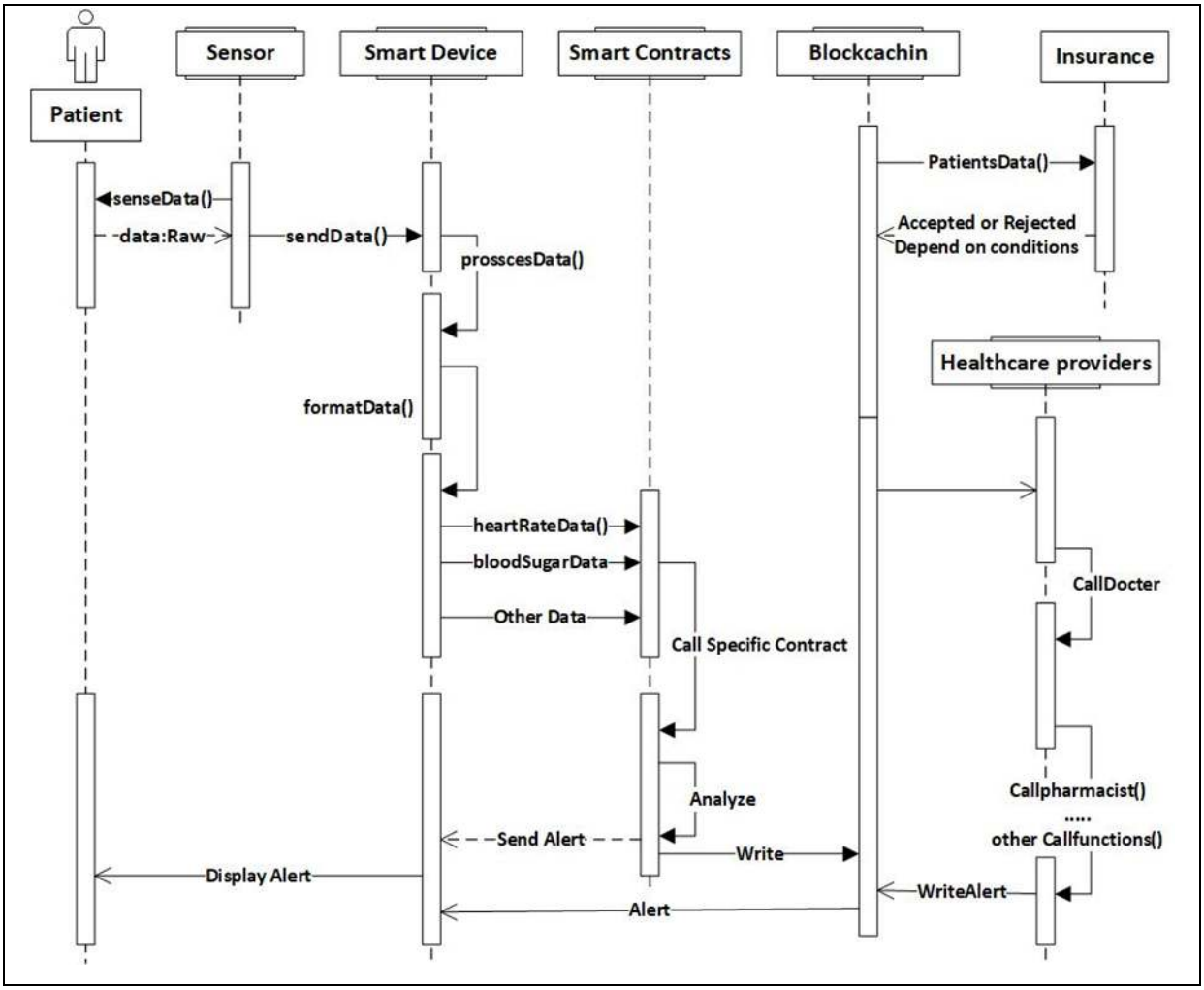

Figure 4.3: Shows The System's proposed sequence diagram.

Starting with a healthcare smart contract, data is sent to the smart contract via a smart device. Healthcare providers must also make sure insurance companies are covered by processing insurance documents that include characteristics of the suppliers of healthcare. A transaction is lawful if, as shown in Figure 4.3, its value is lower than or equal to the cost of the gas being given. A smart contract for healthcare is a three-stage Hierarchical State Machine contract:

a) Processing, Formatting, and Classification are all part of the data collection process.

b) Three contracts—Specific Contract, Analyze Contract, and Blockchain—that together make up Health Contract and Blockchain.

c) Healthcare provider, doctor, and insurance provider monitoring and surveillance.

We express the group of states smoothly using HSM characteristics, which are made up of a limited set of states linked by transitions. The guards of the transition have actions connected

with circumstances. Given that our system relies on a single node for input data and a second node for output data to each Figure 4.4, HSMs provide an adequate level of transitions between states. Despite the HSMs' intensive use of case testing and validation, we might also incorporate patterns into our system that might be suitable for off-chain processing. We deploy ZoKrates, a collection of on-chain verification and off-chain computation techniques, to allay these worries. In this paradigm, we address the difficulties associated with validating and verifying off-chain computations, with a focus on the proof verification for smart contract relay on the target blockchain and the verification of a single block header off-chain computation. We also broaden this technique to take into account batches of headers that are epoch-sized. In this scenario, incoming data is processed by specialized contracts, which then automatically carry out reaction activities. Contracts are deployed in different files on the blockchain and are linked by addresses to make contract change and maintenance easier.

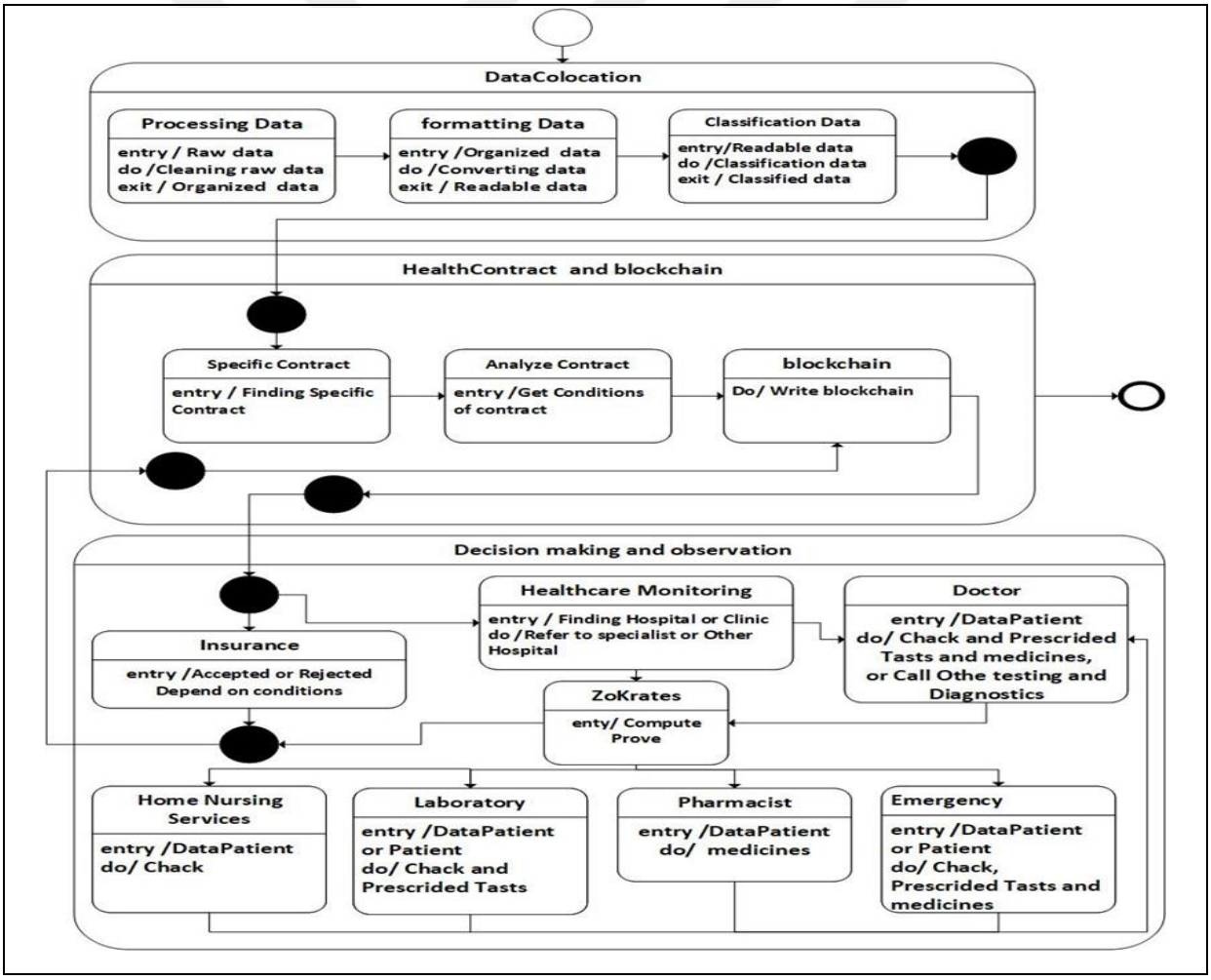

Figure 4.4: Demonstrates proposed HSMs for the healthcare system's smart contract

4.5 THE EXPERIMENTS

One of the most significant cryptocurrencies now based on blockchain technology is Ethereum. Each transaction on Ethereum necessitates payment. On the Ethereum blockchain, gas is the cost of completing a transaction. Miners set gas prices depending on the availability and demand for network processing power required to conduct smart contracts and other transactions. Gwei is a tiny ether fraction used to predict gas costs. This chapter's Ethereum experiment aims to determine whether the proposed off-chain method can be optimized for both scalability and use Gas in a blockchain healthcare system that provides services remotely. . In only a few months, a little deposit in Ether might secure meaningful quantities (USD, EUR, etc.). The analysis of our system's gas usage, which contrasts the costs of off-chain and on-chain operations as well as memory use The goal of the system evaluation was to ascertain how long it would take for a healthcare workflow to complete varying numbers of transactions. Simulation of a system with the following server configuration: (hardware, software): Intel(R) Core(TM) i7-6700HQ CPU @ 2.60GHz, 4 core CPU, 8 GB RAM running Ubuntu Server 20.04.

Table 4.1 summarizes the results of the experiments. The off-chain method relies on generating validation algorithms with batch sizes determined by epoch length L and computing L mod N = 0 [70]. Because resource consumption grows with batch size when performed off-chain, as shown in Figure 4.5, memory consumption grows quasi-linearly with batch size. While the on-chain processing expenses remain unchanged. When every validation for batch is processed off-chain, ZoKrates gets and verifies evidence, and it stores the final header for batch on blockchain. Comparison of the two Ethereum approaches' prices is shown in Figure 4.6. (ETH). Total transactions are represented on the X-axis, and transaction costs are represented on the Y-axis. We decided on a single transaction cost as the standard fee (For example, a simple transaction signifying the learning or change of brand-new therapy). The outcome of our experiment was the average cost of a single transaction. The off-chain technique is used to write around 0.00064 ETH.

Table 4.1: A List of the outcomes of the trials.

Parameter	Value
Tested number of transactions	[1:1000]
Test executed for each run	30
Price of Gas (Gwei)	2
Average cost per transaction (ETH)	0.00084

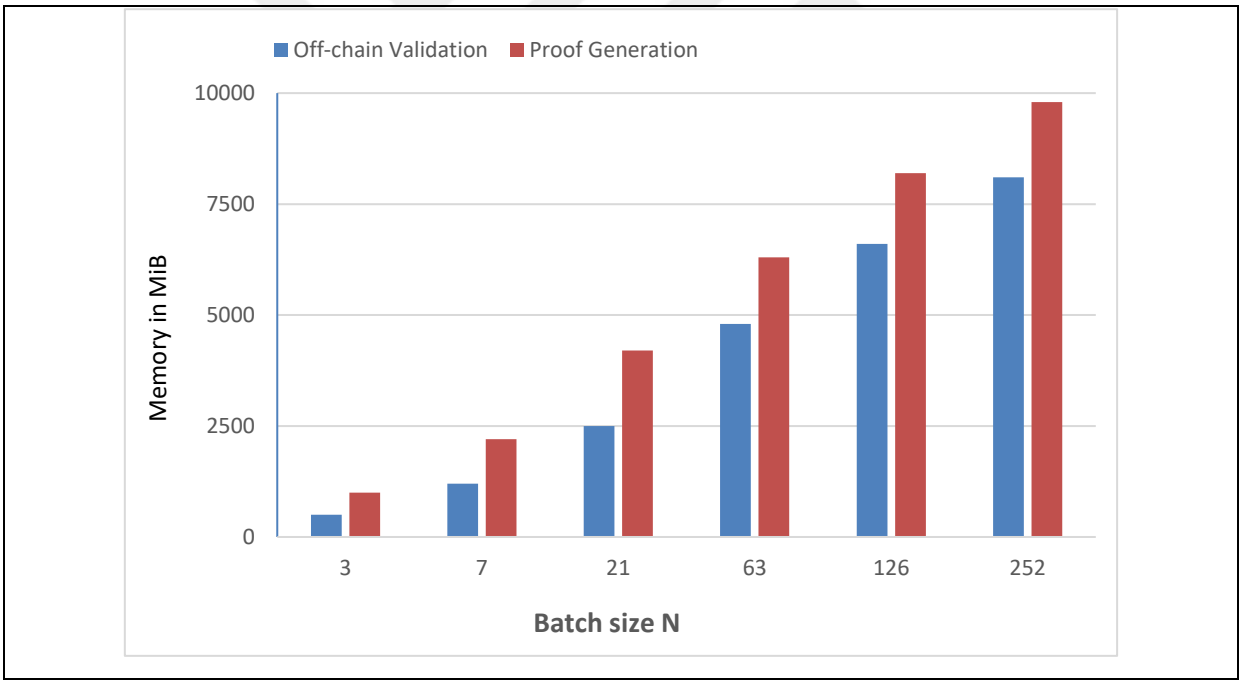

Figure 4.5: Memory use for off-chain processing of validation and proof generation.

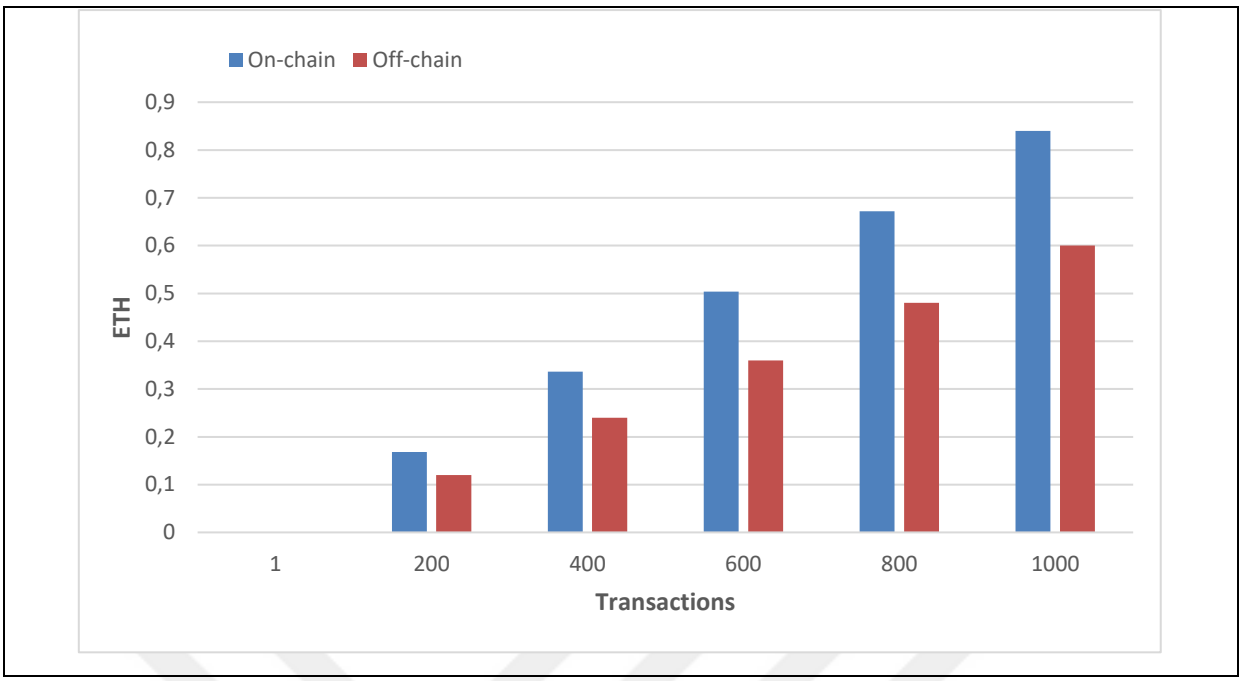

Figure 4.6: Ethereum network techniques' costs for on-chain and off-chain implementations are compared.

4.6 ANALYSIS AND DISCUSSION

The following part of the proposed system discusses significant blockchain-related characteristics and compares our results to Krishna al et al. in [66]. The identical to the table. 2 illustrate the outcomes overview.

Table 4.2: A Brief comparison of the simulation results in the suggested model with the model in [66].

Parameter	The Proposed Model	Model In [66]
Transaction Confirmation Time	1.15 seconds	1.7 seconds
The Block Time	10.68 seconds	11.21 seconds.
Migration And Deployment Time	9 seconds	9.14 seconds
Deployment Cost	0.00064171 ETH	0.00179117 ETH

The intended model has been effectively applied on an Ethereum-based blockchain network utilizing the off-chain technique. Essentially, this model resolves the two challenges of privacy

and scalability, notwithstanding the difficulties of connecting IoT devices with blockchain. The advantages of this integration technique for IoT solutions have been proposed further below.

A. Scalability

It is defined as a repository's ability to maintain a transition state in an information system. Blockchain scalability refers to the cost and capacity, networking, and throughput.

The cost and capacity: Blockchain implies that data is stored on the block, which actually starts with the genesis block and ends with the many transaction records. However, the resources and storage capacity of blockchain nodes are insufficient to accommodate such a large volume of data.

Networking: Once a block has been mined, it is once again published to all nodes of the blockchain, and transactions are sent to all blockchain nodes through broadcast. As a result, the operation might consume significant network resources while increasing propagation latency.

Throughput describes the size of a blockchain transaction block and the amount of time it takes to approve a single transaction. The size of blocks rises in proportion to the amount of transactions. As a reason, the blockchain network requires additional resources. The off-chain technique keeps data-related information in blockchain, whilst data is kept in a database outside of blockchain. This minimizes the quantity of transaction data while increasing number of transactions that may fit within a single block. That corollary, the system's overall throughput and scalability improve.

B. Privacy

The blockchain is only accessible to participants, and only authorized participants are able to access both on-chain and off-chain data, in accordance with the approved privacy technique. Our ZoKrates-based model illustrates how off-chain program execution verification may be employed in blockchain to improve secrecy and scalability. When at least one trustworthy participant is available, the setup phase among nodes is produced by the ZoKrates algorithm in a secure manner. In order to generate proof and verification keys, a lot more trust is now required.

4.7 CONCLUSION

This chapter adopts the HSMs strategy, which separates the problem into smaller challenges to facilitate off-chain processing, for smart contracts in the healthcare industry. The verified off-chain calculations can also be done with ZoKrates. By verifying a single block header off-chain calculation, we demonstrated how to address the challenges of validation and verifiable off-chain calculations as well as proof verification for smart contract-relay on the target blockchain. Furthermore, we extend this strategy to incorporate epoch-sized header chunks. Off-chain validation procedures executed on our relay system generate accuracy proofs for the headers chain. Proofs are validated in smart contracts, and corresponding block headers are approved. This approach reduces the complexity of calculations, lowering gas consumption and increasing the system's scalability, while simultaneously offering anonymity for off-chain procedures.

5. CONCLUSION AND FUTURE WORK

5.1 CONCLUSION

Despite the many advantages that cloud computing provides, it also creates categorization concerns based on the blockchain foundation, which slows down cloud computing adoption. Everyone who uses the cloud, whether an individual or a business, should be aware of the risks. Understanding blockchain-based classification and countermeasures will aid firms in calculating the cost of analytics and encourage them to migrate to the cloud. Cloud computing is feature-rich as well as categorized based on a unique blockchain architecture and employs numerous traditions as well as new technology. Different users (perhaps from different backgrounds) can use the same physical resources thanks to virtualization and numerous tenants.

The aforementioned categorization technologies result in a cloud-based blockchain architecture that needs the learning and management of new cloud display characteristics. Virtual networks, in addition to the challenges posed by traditional physical networks, raise classification considerations based on a unique blockchain foundation. Due to the lack of perfect isolation between virtual machines, unique development approaches that can define and illustrate physical separation are required. The global adoption of cloud computing has created a slew of legal issues affecting users' assets and local rules. Access control and identity management for the organization's digital resources Many sorts of cloud computing occur as a result of the organization's owner's lack of administrative control.

As a result of the sharing, virtualization, and general nature of cloud computing, this review highlights the classification challenges associated with the blockchain architecture. The resources then provide countermeasures. Table analysis provides ways of defining the scope of categorization services based on the blockchain architecture provided by the researched approaches. Table analysis greatly facilitates readers' comparing and analyzing the benefits and drawbacks of various research projects. MCC has been implemented as a result of the rising use of smartphones and mobile devices. We look at categorization concerns using the MCC blockchain technology. The tactics offered for publicizing some open subjects in order to motivate the research and academic community have resulted in a focus on the subject. Solutions are being developed using the data blockchain framework.

Encrypting data is the greatest approach to protect it. Whenever data is stored on a cloud server, it should be encrypted. Data owner can give a limited set of people access to the data so that they can easily read it. Data access is controlled through class heterogeneity, which is based on a data-driven blockchain framework. As part of the data security model, authentication, encryption, and integrity are combined with data recovery and protection in order to ensure data security. As a service, security as a service can provide privacy and data security. Data encryption makes data completely unusable, preventing it from being accessed by other users. Natural encryption can also make it more difficult to find information. Users should double-check that their data is stored on backup before uploading it.

The data will remain intact if the story composition is calculated before uploading to cloud servers. It is possible to achieve data integrity by calculating this combination, but it can be difficult to maintain.

Cryptographic identification and the RSA signature can be combined to offer an RSA based on data integrity. By clearly defining the physical and application layers, SAAS ensures a smooth user experience. A distribution control architecture is used in cloud computing to control access. It is advisable to make use of a service's capacity to inform a user on which parts of the data should be assessed. The user can compute compressed data without revealing the contents with a suitable control mechanism. For secure data processing and exchange among users, a data-driven framework could be used. A network-based intrusion prevention system identifies threats in real time with its storage security approach, it can handle RSA remote data security for large files of different sizes. Despite the fact which cloud computing is the product of the new technologies that have offered many benefits to clients, it faces certain classification challenges based on the blockchain framework. The categorization issue using the information blockchain framework is covered in this study, along with the strategies for reducing the risk associated with cloud computing. Cloud computing security will increase in the future. Modern encryption techniques can be used to store and retrieve data from the cloud securely. To distribute keys to cloud users and restrict data access to those who have been given permission, appropriate management mechanisms can be employed.

5.2 FUTURE WORK

The best job efficiency is what we're aiming for in this project, based on the justifications we've given and the suggested algorithms for various jobs. As a result, it is preferable to use additional layers for diagnostic work in order to make system identification easier. Existing layers will identify and degrade vulnerabilities that may have passed past the primary levels as a result of this action. Furthermore, using hub methods based on their intrinsic location attributes is recommended to make the findings more efficient for detecting infiltration in diverse systems. Much better outcomes can be obtained when the neural network pattern is used. Furthermore, this study could be been expanded to include various businesses, such as pharmaceutical enterprises, with all phases, starting with blockchain registration, medication development, patient clinical development, shipment, and other services.

REFERENCES

[1] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, “Blockchain,” Bus. \& Inf. Syst. Eng., vol. 59, no. 3, pp. 183–187, 2017.

[2] K. Gai, J. Guo, L. Zhu, and S. Yu, “Blockchain meets cloud computing: A survey,” IEEE Commun. Surv. \& Tutorials, vol. 22, no. 3, pp. 2009–2030, 2020.

[3] C. Dannen, Introducing Ethereum and solidity, vol. 1. Springer, 2017.

[4] R. Kher, S. Terjesen, and C. Liu, “Blockchain, Bitcoin, and ICOs: a review and research agenda,” Small Bus. Econ., vol. 56, no. 4, pp. 1699–1720, 2021.

[5] F. H. N. Al-mutar, O. N. Ucan, and A. A. Ibrahim, “Providing Scalability and Privacy for Smart Contract in the Healthcare System,” Optik (Stuttg)., p. 170077, 2022.

[6] A. Park and H. Li, “The effect of blockchain technology on supply chain sustainability performances,” Sustainability, vol. 13, no. 4, p. 1726, 2021.

[7] B. Esmaeilian, J. Sarkis, K. Lewis, and S. Behdad, “Blockchain for the future of sustainable supply chain management in Industry 4.0,” Resour. Conserv. Recycl., vol. 163, p. 105064, 2020.

[8] D. W. E. Allen, C. Berg, S. Davidson, M. Novak, and J. Potts, “International policy coordination for blockchain supply chains,” Asia \& Pacific Policy Stud., vol. 6, no. 3, pp. 367–380, 2019.

[9] T. Wang, H. Hua, Z. Wei, and J. Cao, “Challenges of blockchain in new generation energy systems and future outlooks,” Int. J. Electr. Power \& Energy Syst., vol. 135, p. 107499, 2022.

[10] K. Adel, A. Elhakeem, and M. Marzouk, “Decentralizing Construction AI Applications Using Blockchain Technology,” Expert Syst. Appl., p. 116548, 2022.

[11] S. Nayak, N. C. Narendra, A. Shukla, and J. Kempf, “Saranyu: Using smart contracts and blockchain for cloud tenant management,” in 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), 2018, pp. 857–861.

[12] K. R. Lakhani and M. Iansiti, “The truth about blockchain,” Harv. Bus. Rev., vol. 95, no. 1, pp. 119–127, 2017.

[13] C. F. Durach, T. Blesik, M. von Düring, and M. Bick, “Blockchain applications in supply chain transactions,” J. Bus. Logist., vol. 42, no. 1, pp. 7–24, 2021.

[14] K. S. Hald and A. Kinra, “How the blockchain enables and constrains supply chain performance,” Int. J. Phys. Distrib. \& Logist. Manag., 2019.

[15] M. K. Lim, Y. Li, C. Wang, and M.-L. Tseng, “A literature review of blockchain technology applications in supply chains: A comprehensive analysis of themes, methodologies and industries,” Comput. \& Ind. Eng., vol. 154, p. 107133, 2021.

[16] C. R. Carter, D. S. Rogers, and T. Y. Choi, “Toward the theory of the supply chain,” J. Supply Chain Manag., vol. 51, no. 2, pp. 89–97, 2015.

[17] H. Treiblmaier, “The impact of the blockchain on the supply chain: a theory-based research framework and a call for action,” Supply Chain Manag. an Int. J., 2018.

[18] C. G. Schmidt and S. M. Wagner, “Blockchain and supply chain relations: A transaction cost theory perspective,” J. Purch. Supply Manag., vol. 25, no. 4, p. 100552, 2019.

[19] I. Bashir, Mastering blockchain: Distributed ledger technology, decentralization, and smart contracts explained. Packt Publishing Ltd, 2018.

[20] V. Varriale, A. Cammarano, F. Michelino, and M. Caputo, “The unknown potential of blockchain for sustainable supply chains,” Sustainability, vol. 12, no. 22, p. 9400, 2020.

[21] I. Bashir, Mastering blockchain. Packt Publishing Ltd, 2017.

[22] D. Ongaro and J. Ousterhout, “The raft consensus algorithm,” 2015.

[23] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, “Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability,” in 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), 2017, pp. 468–477.

[24] V. K. Manupati, T. Schoenherr, M. Ramkumar, S. M. Wagner, S. K. Pabba, and R. Inder Raj Singh, “A blockchain-based approach for a multi-echelon sustainable supply chain,” Int. J. Prod. Res., vol. 58, no. 7, pp. 2222–2241, 2020.

[25] J. Yeung, S. Wong, A. Tam, and J. So, “Integrating machine learning technology to data analytics for e-commerce on cloud,” in 2019 Third World Conference on Smart Trends in Systems Security and Sustainablity (WorldS4), 2019, pp. 105–109.

[26] M. Koot, M. R. K. Mes, and M. E. Iacob, “A systematic literature review of supply chain decision making supported by the Internet of Things and Big Data Analytics,” Comput. \& Ind. Eng., vol. 154, p. 107076, 2021.

[27] G. Zhao et al., “Blockchain technology in agri-food value chain management: A synthesis of applications, challenges and future research directions,” Comput. Ind., vol. 109, pp. 83–99, 2019.

[28] Z. Liu and Z. Li, “A blockchain-based framework of cross-border e-commerce supply chain,” Int. J. Inf. Manage., vol. 52, p. 102059, 2020.

[29] M. Hölbl, M. Kompara, A. Kamišalić, and L. Nemec Zlatolas, “A systematic review of the use of blockchain in healthcare,” Symmetry (Basel)., vol. 10, no. 10, p. 470, 2018.

[30] R. C. Merkle, “A digital signature based on a conventional encryption function,” in Conference on the theory and application of cryptographic techniques, 1987, pp. 369–378.

[31] A. Hughes, A. Park, J. Kietzmann, and C. Archer-Brown, “Beyond Bitcoin: What blockchain and distributed ledger technologies mean for firms,” Bus. Horiz., vol. 62, no. 3, pp. 273–281, 2019.

[32] J. Feng, X. Zhao, K. Chen, F. Zhao, and G. Zhang, “Towards random-honest miners selection and multi-blocks creation: Proof-of-negotiation consensus mechanism in blockchain networks,” Futur. Gener. Comput. Syst., vol. 105, pp. 248–258, 2020.

[33] D. Tapscott and A. Tapscott, Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world. Penguin, 2016.

[34] R. L. Rana, P. Giungato, A. Tarabella, and C. Tricase, “Blockchain applications and sustainability issues,” Amfiteatru Econ., vol. 21, no. 13, pp. 861–870, 2019.

[35] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, “Blockchain challenges and opportunities: A survey,” Int. J. Web Grid Serv., vol. 14, no. 4, pp. 352–375, 2018.

[36] B. Bhushan, A. Khamparia, K. M. Sagayam, S. K. Sharma, M. A. Ahad, and N. C. Debnath, “Blockchain for smart cities: A review of architectures, integration trends and future research directions,” Sustain. Cities Soc., vol. 61, p. 102360, 2020.

[37] J. Wu and N. K. Tran, “Application of blockchain technology in sustainable energy systems: An overview,” Sustainability, vol. 10, no. 9, p. 3067, 2018.

[38] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, “A survey of distributed consensus protocols for blockchain networks,” IEEE Commun. Surv. \& Tutorials, vol. 22, no. 2, pp. 1432–1465, 2020.

[39] Y. Wang, X. Tao, J. Ni, and Y. Yu, “Data integrity checking with reliable data transfer for secure cloud storage,” Int. J. Web Grid Serv., vol. 14, no. 1, pp. 106–121, 2018.

[40] F. D. Davis, “Perceived usefulness, perceived ease of use, and user acceptance of information technology,” MIS Q., pp. 319–340, 1989.

[41] F. H. N. Al-mutar, A. A. Ibrahim, and O. N. Ucan, “Provide a new framework for blockchain-based integrated and resource classification for the cloud,” Appl. Nanosci., pp. 1–14, 2022.

[42] S. Seebacher and R. Schüritz, “Blockchain technology as an enabler of service systems: A structured literature review,” in International conference on exploring services science, 2017, pp. 12–23.

[43] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” Decentralized Bus. Rev., p. 21260, 2008.

[44] Y. Gupta, R. Shorey, D. Kulkarni, and J. Tew, “The applicability of blockchain in the Internet of Things,” in 2018 10th International Conference on Communication Systems \& Networks (COMSNETS), 2018, pp. 561–564.

[45] A. H. Lone and R. Naaz, “Applicability of Blockchain smart contracts in securing Internet and IoT: a systematic literature review,” Comput. Sci. Rev., vol. 39, p. 100360, 2021.

[46] “News | Healthcare IT News.” [Online]. Available: https://www.healthcareitnews.com/news/providence-st-joseph-health-acquires-lumedic blockchain-tech. [Accessed: 05-Mar-2022].

[47] N. Kawaguchi, “Application of blockchain to supply chain: flexible blockchain technology,” Procedia Comput. Sci., vol. 164, pp. 143–148, 2019.

[48] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, “FHIRChain: applying blockchain to securely and scalably share clinical data,” Comput. Struct. Biotechnol. J., vol. 16, pp. 267–278, 2018.

[49] N. Shah and M. Farik, “Static load balancing algorithms in cloud computing: Challenges and solutions,” Int. J. Sci. \& Technol. Res., vol. 4, no. 10, pp. 365–367, 2015.

[50] J. K. W. Yeung, S. C. W. Wong, and G. H. H. Chan, “Cloud infrastructure for public health blockchain,” in The Routledge Handbook of Public Health and the Community, Routledge, 2021, pp. 254–263.

[51] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, “Blockchain technology and its relationships to sustainable supply chain management,” Int. J. Prod. Res., vol. 57, no. 7, pp. 2117–2135, 2019.

[52] G. T. S. Ho, Y. M. Tang, K. Y. Tsang, V. Tang, and K. Y. Chau, “A blockchain-based system to enhance aircraft parts traceability and trackability for inventory management,” Expert Syst. Appl., vol. 179, p. 115101, 2021.

[53] L. Dong, Y. Qiu, and F. Xu, “Blockchain-enabled deep-tier supply chain finance,” Available SSRN, 2021.

[54] S. A. G. Naidu, R. A. Clemens, P. Pressman, M. Zaigham, K. J. A. Davies, and A. S. Naidu, “COVID-19 during Pregnancy and Postpartum: II) Antiviral spectrum of maternal lactoferrin in fetal and neonatal defense,” J. Diet. Suppl., vol. 19, no. 1, pp. 78–114, 2022.

[55] R. Chaudhary, A. Jindal, G. S. Aujla, N. Kumar, A. K. Das, and N. Saxena, “Lscsh: Lattice-based secure cryptosystem for smart healthcare in smart cities environment,” IEEE Commun. Mag., vol. 56, no. 4, pp. 24–32, 2018.

[56] C. Liu, P. Bodorik, and D. Jutla, “A Tool for Moving Blockchain Computations Off-Chain,” in Proceedings of the 3rd ACM International Symposium on Blockchain and Secure Critical Infrastructure, 2021, pp. 103–109.

[57] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, “Healthcare blockchain system using smart contracts for secure automated remote patient monitoring,” J. Med. Syst., vol. 42, no. 7, pp. 1–7, 2018.

[58] D. G. Baur and L. T. Hoang, “A crypto safe haven against Bitcoin,” Financ. Res. Lett., vol. 38, p. 101431, 2021.

[59] M. Westerkamp and J. Eberhardt, “zkrelay: Facilitating sidechains using zksnark-based chain-relays,” in 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS\&PW), 2020, pp. 378–386.

[60] Z. Wang, H. Jin, W. Dai, K.-K. R. Choo, and D. Zou, “Ethereum smart contract security research: survey and future research opportunities,” Front. Comput. Sci., vol. 15, no. 2, pp. 1–18, 2021.

[61] J. Eberhardt, “Scalable and privacy-preserving off-chain computations,” The Technical University of Berlin, 2021.

[62] A. Zamyatin, D. Harz, J. Lind, P. Panayiotou, A. Gervais, and W. Knottenbelt, “Xclaim: Trustless, interoperable, cryptocurrency-backed assets,” in 2019 IEEE Symposium on Security and Privacy (SP), 2019, pp. 193–210.

[63] J. Eberhardt and S. Tai, “On or off the blockchain Insights on off-chaining computation and data,” in European Conference on Service-Oriented and Cloud Computing, 2017, pp. 3–15.

[64] M. Rahnamaei, S. T. Saeidi, S. Khorsandi, and M. Shajari, “A Fair Model of Identity Information Exchange Leveraging Zero-Knowledge,” arXiv Prepr. arXiv2106.14180, 2021.

[65] J. Park, H. Kim, G. Kim, and J. Ryou, “Smart Contract Data Feed Framework for Privacy-Preserving Oracle System on Blockchain,” Computers, vol. 10, no. 1, p. 7, 2021.

[66] K. P. Satamraju and others, “Proof of concept of scalable integration of internet of things and blockchain in healthcare,” Sensors, vol. 20, no. 5, p. 1389, 2020.

[67] D. Job and V. Paul, “Challenges, Security Mechanisms, and Research Areas in IoT and IioT,” in Internet of Things and Its Applications, Springer, 2022, pp. 523–538.

[68] L. Da Xu, Y. Lu, and L. Li, “Embedding blockchain technology into IoT for security: A survey,” IEEE Internet Things J., vol. 8, no. 13, pp. 10452–10473, 2021.

[69] P. Kumar, P. Yadav, R. Agrawal, and K. K. Singh, “Amalgamation of IoT, ML, and Blockchain in the Healthcare Regime,” Mach. Learn. Approaches Converg. IoT Blockchain, pp. 93–108, 2021.

[70] Y. Tang et al., “ChainFS: Blockchain-secured cloud storage,” in 2018 IEEE 11th international conference on cloud computing (CLOUD), 2018, pp. 987–990.