SEMARAK ILMU
PUBLISHING
202103268166(003316878-P)

Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage: https://jaraset.com/
ISSN: 2462-1943

SEMARAK ILMU
Journal of
ADVANCED RESEARCH IN APPLIED SCIENCES AND ENGINEERING TECHNOLOGY
ISSN 2462 - 1943

# INTEGRATING BLOCKCHAIN TECHNOLOGY WITH CLOUD COMPUTING: DESIGN AND IMPLEMENTATION

**LAKSHMI CHANDRAKANTH KASIREDDY [1*], VINOD KUMAR UPPALAPU [2]**

[1] *Software Engineer, Department of R&D Engineering, Thoughtspot Inc*
[2] *Professor, Department of Computer Science and Engineering, GIET Engineering College, Andhra Pradesh, India*

**ARTICLE INFO**

***Article history:***
Received: 13-09-2024
Received in revised form: 16-10-2024
Accepted: 28-12-2024
Available online: 10-01-2025

***Keywords:***

*Blockchain, Security and the computational cost, blockchain enabled cloud, data security, Cloud Computing.*

**ABSTRACT**

Blockchain technology is an innovative economic development that is transforming corporate relationships. Distributed ledgers, safely shared and dispersed across network nodes, comprise its structure and hold detailed transaction records. As communication technologies progress at a rapid pace, the Internet of Things (IoT) is emerging from its early stages and into a fully developed state. Its rapid expansion is shown by the amount of data being processed and sent. A consensus method verifies every transaction that is logged in the network, guaranteeing that the data that is saved is unchangeable. Alongside the growth of the well-known digital currency Bitcoin, blockchain technology has gained popularity. Instead of depending on a single server or personal computer, cloud computing uses a network of distant servers housed on the internet to store, manage, and process data. In this regard, blockchain offers creative answers to problems with network security, data privacy, and decentralisation in cloud computing. Concurrently, Cloud of Things provides scalability and flexibility features to improve blockchain operations efficiency. A recently developed blockchain and cloud of things (BoCoT) combination is well known for being a powerful facilitator for a broad variety of application scenarios. This article provides readers with an in-depth examination of the most recent state-of-the-art blockchain integration, covering a range of topics such as history, driving forces, and integrated design. The goal is to provide a comprehensive overview of blockchain's capabilities and how it integrates into different fields.

## INTRODUCTION

The next wave of innovation in the industrial and economic service sectors is being enabled by the fast adoption of blockchain, a disruptive technology. Adoption of this technology has several advantages, such as lower maintenance and hardware costs, worldwide accessibility, automation, and smooth scaling. A distributed form of operation known as cloud computing reduces the user's total storage load while facilitating cooperation amongst several users [4]. Blockchain has seen a rise in attention recently for a variety of uses, from industries to cryptocurrency [1], [2]. Major companies that have adopted cloud-like services include Google, IBM, Amazon, and others [3]. Numerous businesses have adopted a paradigm similar to that of well-known cloud service providers like Google and Amazon [4]. Generally speaking, the blockchain system consists of several schemes that produce and transmit enormous volumes of data that are sensitive to privacy and safety. To improve operational efficiency, it provides a pay-per-use approach and flexible IT provisioning that is accessible from beginning to finish via the internet [14]. Despite the cloud's many benefits, businesses are wary because of privacy issues. Adoption of the cloud is hampered by security and privacy issues [14]. Blockchain technology must be used to improve data confidentiality and handle security issues in order to advance cloud computing.

Blockchain technology is the way of the future for sectors looking to improve privacy and security. A distributed ledger without a central authority, blockchain stores tamper-evident data in a chain. Nodes are participants or equipment in the blockchain technology. Blockchain offers a decentralised network in which every node actively contributes to data validation and verification. A thorough grasp of how blockchain affects various cloud components is necessary in order to take full advantage of this cloud-blockchain connection [5]. Cryptography will be used to encrypt data that is going to be kept on the blockchain. Every block in the chain is connected by an encrypted hash, timestamp, and hash of the block before it. This guarantees the tamper-evident nature of the data on the blockchain. Blockchain addresses concerns about data privacy by offering data security and requiring network authentication for participating users [7].

For consumers, the cloud functions as a utility model in the context of cloud computing. Cloud users may access, share, and trade data at any time and from any location, depending on their needs. This in no way suggests that users of the cloud have direct control over the resources that are uploaded to the cloud server. The cloud source provides services on an as-is and as-available basis, depending on the situation [1]. As we continue to explore the "data age," we find that the amount, speed, and diversity of data available on the internet have increased significantly. Numerous sources, including mobile devices, sensors, archives, and social networks, may provide data [6].

Delegation, accountability, and security are three particularly appealing aspects of blockchain technology that increase service effectiveness and save operating expenses. These characteristics have contributed to the rise in popularity of blockchain-based apps in recent years. With services that connect servers, networks, and data centres online, cloud computing has several benefits. The pay-per-use model governs how these services are used. The services improve teamwork by being accessible worldwide and at a substantial discount. Thus, it is the right moment to concentrate on this area of study [8].

Conversely, the data and communication revolution has opened up a world of possibilities for cutting edge technology, especially cloud computing and the Internet of Things (IoT). With its many new industrial, consumer, and corporate services and uses, IoT has completely changed and revolutionised our way of life [8], [9]. Smart cities, smart industries, and other pervasive industrial services are made possible by the Internet of Things (IoT), which is primarily composed of physical items that can be monitored, controlled, or interacted with by ubiquitous electronic devices. The Cloud of Things paradigm emerged as a result of IoT devices' limited capabilities, which often assign IoT application duties to cloud computing [10], [11]. It offers a stable, adaptable cloud computing environment for handling and processing Internet of Things

(IoT) services, with great potential to boost infrastructure performance and optimise service delivery [12]. Cloud computing has many important features. Users may rapidly deploy network storage capabilities using on-demand self-service. Wide network access provides services across the network that may be accessed using common methods to support different client systems. However, because of the following issues, conventional infrastructures are often inefficient.

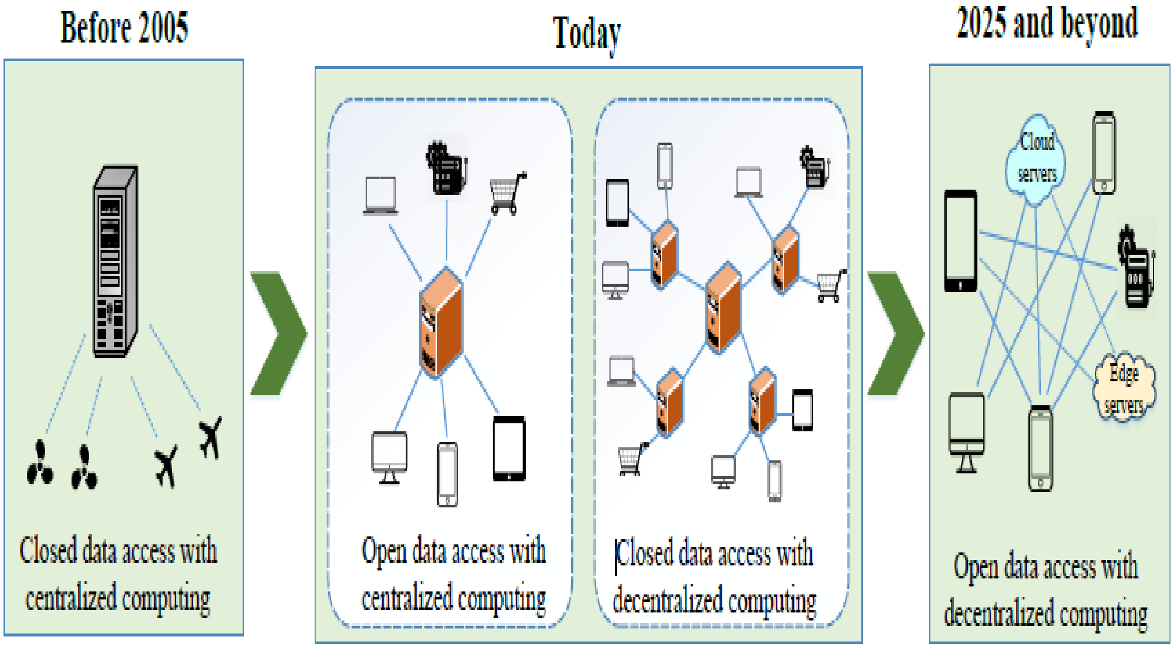
Before 2005
Today
2025 and beyond
Closed data access with centralized computing
Open data access with centralized computing
Closed data access with decentralized computing
Cloud servers
Edge servers
Open data access with decentralized computing

Figure 01: Timeline period Cloud of Things infrastructure.

a block is a crucial component of blockchain technology. In a chain including a timestamp, cryptographic communication, and the address of the preceding block, a block functions as a directory address. The block becomes invalid if there is a discrepancy, breaking the chain as a whole. The fundamental unit of communication that contributes to an entry in the hash algorithm is the nonce.

It is often accepted that blockchain technology will play a significant role in helping future organisations become fully decentralised. In particular, the incorporation of blockchain results in the creation of a novel paradigm known as BCoT. The combination of these cutting-edge technology benefits both domains greatly and is attracting a lot of attention from the academic and business communities [13]. In fact, there are some complementing linkages between blockchain technology and cloud computing for real-world applications. Blockchain has been acknowledged as a service within the cloud computing setting, known as Blockchain as a Service (BaaS). Blockchain may open up whole new cloud storage possibilities that are very resistant to data manipulation by offering a decentralised storage architecture via virtual storage nodes. Blockchain joins computer nodes, both external and cloud-based virtual machines, to create a completely decentralised storage system that does not need a central authority, in contrast to typical cloud data centres. In addition, blockchain serves as a network management tool for apps that use smart contracts. By using a variety of security measures, the majority of cloud providers guarantee data protection. Nonetheless, there have been instances of data leaks [13]. There is an issue with iCloud data leaks, when a large amount of public data about celebrities was exposed. It is preferred to store data online in the cloud and allow users to access it without their awareness. The primary issue that prevents businesses from using the cloud and its services is security. Within these situations, end users, IoT devices, and cloud servers communicate with one other using blockchain technology.

By doing away with the need for a reliable third party in the network, blockchain's decentralised structure offers a viable solution to bottleneck and single-point failure problems [15]. Service Level Agreements will govern the provision of cloud services, allowing the duplication of numerous instances of a same application on different servers as needed, contingent upon priority. Should the application be deemed less important, the cloud could terminate or restrict its use. The primary obstacle faced by cloud consumers is assessing the Service Level Agreements that have been reached with cloud providers. Moreover, every network user has equal access to validate the accuracy of IoT data and guarantee immutability thanks to blockchain's distributed design.

By leveraging blockchain-enabled smart contracts [16–17], which allow for the automatic validation of all actions taken by cloud providers and IoT devices, averting potential threats to cloud resources, and improving fine-grained control over IoT data, the BCoT system can achieve dependable access control in the context of security and privacy. Additionally, blockchain gives customers the ability to track their network transactions in order to preserve device and data ownership, which enhances data security.

With no need for mutual trust, the Blockchain Consortium model establishes a new kind of cooperative environment where many groups may share infinite amounts of data. The third party's removal creates an atmosphere of open circumstances where cloud providers and IoT users with an interest in the system may work together to accomplish shared objectives inside the BCoT ecosystem [18].

In recent years, a broad variety of technological topics have been covered in several research on blockchain and associated challenges. Numerous attempts have been undertaken to provide survey papers in different scopes on this field of study. In contrasting Blockchain with Bitcoin, we may say that several cryptocurrencies, including Bitcoin, use blockchain technology to facilitate safe and anonymous transactions [19]. But Bitcoin offers privacy, whereas blockchain is a visible technology. While blockchain transmits data, rights, etc., Bitcoin is utilised for online transactions. As a result, Blockchain may be used for many purposes, while Bitcoin can only be used for cryptocurrency exchanges [10]. "Transparent distributed records of digitally signed transactions grouped into blocks" is how one defines a blockchain. Each block holds the transaction data, a timestamp, and a hash value produced by cryptography that connects the blocks. Design changes cannot be made to blockchain data [20]. It is a distributed public ledger that effectively and permanently records all of the parties' transactions.

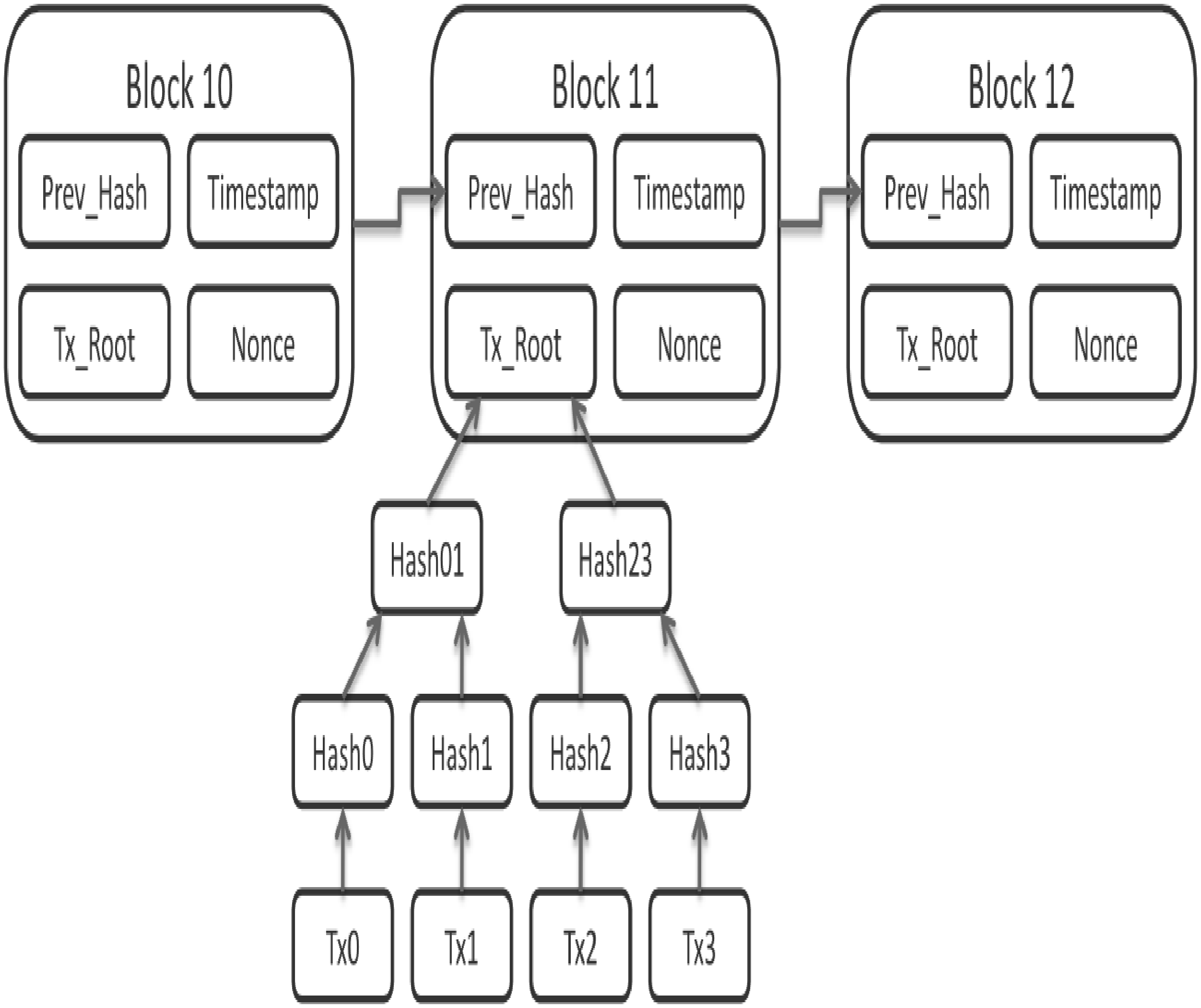

Figure 02: Blocks in Chain.

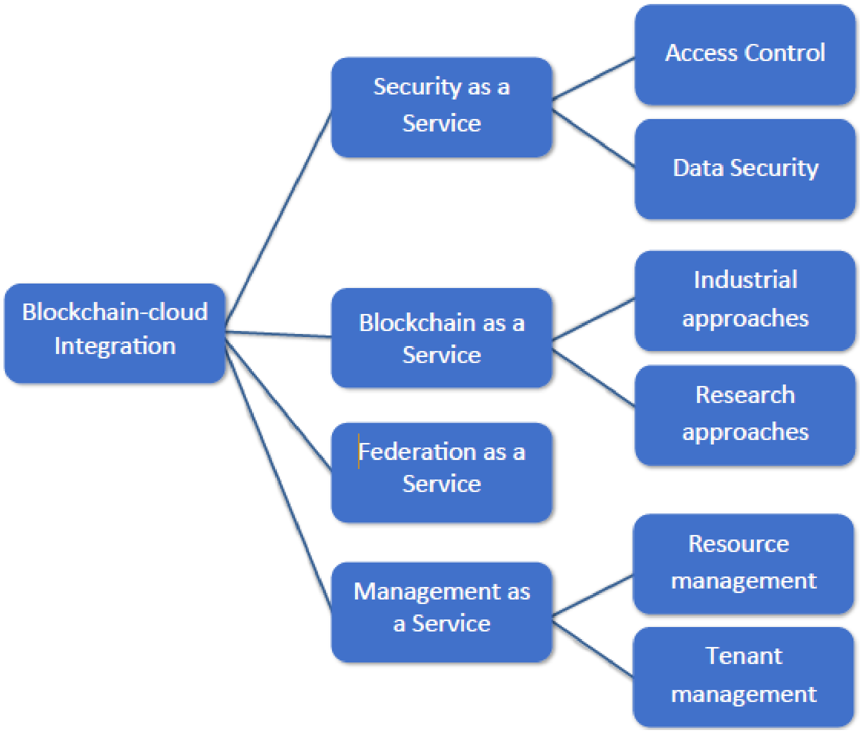

Figure 03: Integration of blockchain-cloud

Bitcoin and Ethereum are well-known blockchain platforms that leverage hybrid mechanisms and the power of labour to prepare for the future. However, they make a sacrifice on the combined POW and POS capabilities. Another technique that the systems use is Proof of Bandwidth, and its other options include Proof of elapsed time, Proof of authority, Delegated Proof of Stake, and Practical Byzantine Fault Tolerance [14] [15] [16].

## BLOCKCHAIN and CoT

### Blockchain and Cloud of Things

**Blockchain:** When it was first released in 2008, the technology was widely used in applications like Bitcoin and other cryptocurrencies. Blockchain prototypes include supply networks, business models, commercial applications, and a number of other initiatives. The blockchain community's decentralised application programmers have created several popular apps, such as the Web 3 standard.

This emerging technology has also recently been a contentious topic for experts to discuss, with some arguing that it will propel blockchain-based applications beyond Bitcoin. Decentralisation, which means blockchain is transmitted via a network of hubs, is the central idea of the blockchain network. Each hub has the opportunity to monitor the actions of various substances inside the company, as well as create, validate, and authorise new exchanges that are going to be added to the blockchain. The benefits of this decentralised architecture include no single-point disappointment flaws and robust and secure blockchain operations. Blockchain may be broadly classified into two categories: permissioned (private) and public (also known as consent-less) blockchain [21].

An open organisation, such as the Bitcoin stage, indicates that anybody may join, conduct transactions, and participate in the agreement cycle on a public blockchain. For the time being, a private blockchain is a welcoming organisation managed by a central component, and any interest in submitting or creating exchanges on the blockchain has to have authorization from an approval tool. Key components of a blockchain network include an information block, an appropriated record, an agreement, and keen agreements. To be honest, every square has different exchanges and is linked to the block that came before it instantly by a hash identifier. As a result, every square in the chain can be traced back to its predecessor, and it is impossible for a modification or rotation to impede information [9]. A kind of data collection that is exchanged and replicated across the components of a distributed organisation is called a dispersed record. Furthermore, blockchain consensus is a process by which disparate unstable hubs come to an agreement on a single block of data in order to ensure network security. Last but not least, clever agreements are programmed programmes that detect an abrupt increase in demand for a blockchain network based on predetermined authoritative circumstances, such as payment terms, liens, privacy, and even prerequisites [3].

Blockchain can provide its implemented scenarios exceptional security characteristics. The primary element is decentralisation, meaning that blockchain is not dependent on a crucial control problem to manage transactions. This exceptional feature offers many exciting benefits, such as eliminating the risk of a single point of disappointment due to focal position disruption, reducing operational costs, and improving reliability. Furthermore, over time, blockchain may maintain persistent information sharing. This makes the chain absolutely unchangeable since the hash value of the previous block is continuously included in the metadata of another square's hashing mechanism. In light of this, once information on the square is authorised and added to the blockchain, it becomes difficult to amend, remove, or modify it. Transparency is another important element, which stems from the fact that every exchange's data on the blockchain is accessible to all participants in the organisation. For the sake of public confidence, comparable blockchain record duplications are dispersed across a large organisation [22]. As a result, every blockchain client has equal access to, ability to verify, and ability to monitor trade activities across the organisation.

**Internet of things:** The client-server model that underpins the internet of things ensures that system communication via the network is unaffected by distance. However, when manufacturers use disparate communication methods that need disparate platform requirements, machine-to-machine communication becomes challenging. The strategy works well for small businesses, but it may cause problems with device expansion when used to big networks. In addition, the model's high cost is a result of the centralised cloud and massive data rubbing expenses [4]. While the aforementioned problems may be resolved by a decentralised system with peer-to-peer connections, which can also reduce system failures linked to centralised systems and boost communication rates. As a result, IOT has faced challenges with managing massive data and security [23].

## THE ARCHITECTURE OF INTEGRATION BLOCKCHAIN AND COT

In this section, we thoroughly examine the material that is directed towards the integrated blockchain and CoT models (BCoT). At that point, we provide a calculated BCoT engineering that incorporates the main concept and essential ideas of the joining and is applicable to many scenarios. Numerous new integrated BCoT stages and frameworks have been offered in writing studies to provide security arrangements and applications in light of the current growing income in the blockchain and CoT [3, 4, 5, 9, 7]. A cloud-based Internet of Things system with blockchain and astute agreements to ensure safe information provenance was suggested by the review [5]. Distributed computing and blockchain work together to create a vast security network where real information is stored in distributed storage and IoT metadata (such as cryptographic hashes) is stored in blockchain. This makes blockchain very flexible for dense IoT deployments.

The blockchain network architecture consists of many blockchains operating in the cloud and distributed side chains transmitted at mist hubs. This would speed up access checks and provide flexible storage for adaptable IoT enterprises. Additionally, a quantifiable assessment mechanism using decentralised blockchain is suggested in order to guarantee BCoT in security-basic applications [1]. The advantages of the BCoT combination were followed by [6], [16], which provided secure character to the executive arrangements that allow cloud specialist co-ops to autonomously regulate and verify client personality in BCoT. Blockchain technology is combined with virtual mists to provide identity verification in a way that eliminates the need for prior trust requirements between cloud providers and customers. Conversely, data governance is also essential in networked CoT, where a vast amount of IoT data is generated, necessitating careful management for data security locations. Motivated by this, the study [6] presented a blockchain-based information assurance system that may prevent the generation of sufficiently unsightly IoT data due to harmful changes that occur during the migration of Virtual Machines (VMs) on distributed computing.

Organising vapour nodes and numerous Blockchain occupancy in the cloud is made easier with the elevation block chains that blockchain uses. It facilitates storage scalability in IoT networks and raises access confirmation. Predicting the usage of decentralised blockchain and maintaining BCOT as a crucial security function are presented in a forensic research framework [1].

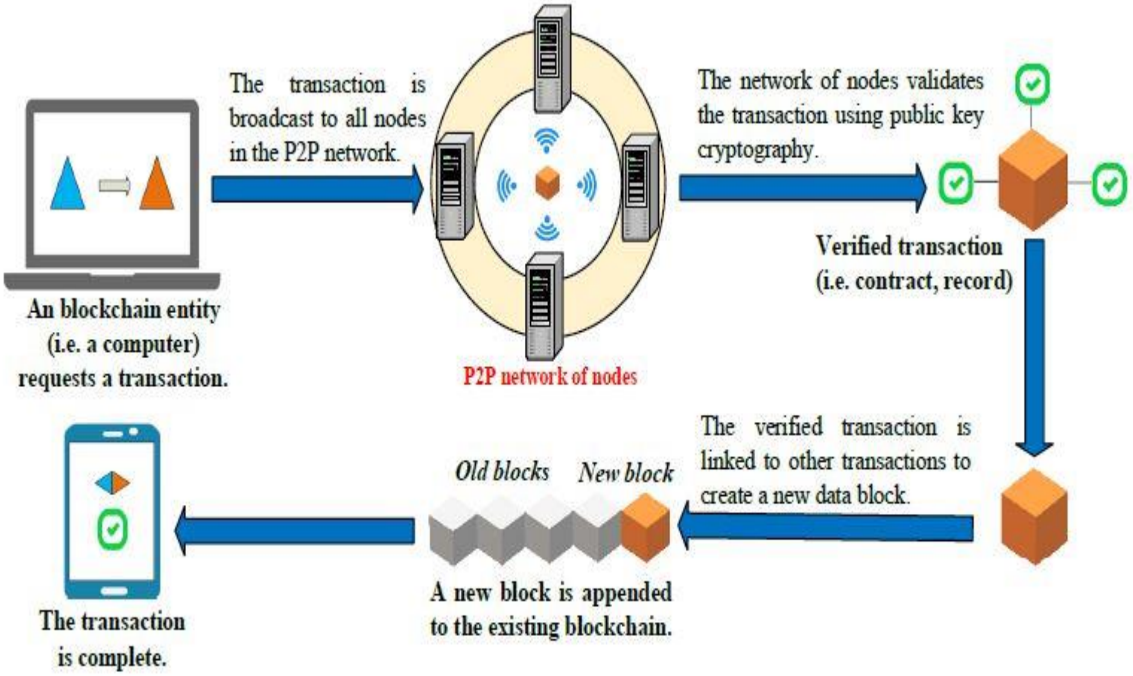
The transaction is broadcast to all nodes in the P2P network.
The network of nodes validates the transaction using public key cryptography.
An blockchain entity (i.e. a computer) requests a transaction.
P2P network of nodes
Verified transaction (i.e. contract, record)
The verified transaction is linked to other transactions to create a new data block.
Old blocks
New block
A new block is appended to the existing blockchain.
The transaction is complete.

Figure 04: The concept of blockchain operation.

Furthermore, the work in [7] is also seen as an integrated blockchain-CoT engineering, with the focus being on resolving the mining problem by shifting mining tasks from IoT devices to cloud hubs. Subsequently, a combined problem of cloud asset assignment and client access affiliation arises, which is subsequently handled by deep support learning (DRL). In a similar vein, the authors of [19], [20] also considered the offloading problem in BCoT organisations, in order to increase the cost of IoT devices. The emphasis in [21] was on the BCoT frameworks' cloud management quality. In this case, a major role of the blockchain is to provide reliability and confidence to excellent cloud management arrangements. The combination of blockchain technology and distributed computing was also considered in [22]. The computing power of the distant cloud is distributed here at the edge of the organisation to provide low-dormancy and continuous registration services for IoT devices. In the meanwhile, the focus of the asset board in BCoT frameworks was on [24], where blockchain technology may preserve data security while trading assets between cloud providers and Internet of Things customers. Most of the aforementioned BCoT phases rely on a single cloud and may be enough for certain applications. However, a combination of cloud-based edge-to-edge technology and edge computing would be more advantageous and useful in sophisticated IoT frameworks that need massive amounts of network resources to cater to different IoT clients [18]. As a result, multicloud models have been contacted about BCoT designs for intricate synergistic scenarios [3], [4].

For example, a distributed edge network securely links many mists in a combined cloud coordinated effort climate where a BCoT structure was presented [5]. Additionally, the single cloud may use blockchain to provide real-time services for IoT users, reducing the risk of malicious attacks [7]. Additionally, [4] presented a cloud alliance concept that enables distributed asset arrangements using a single cloud managed by a blockchain network. Additionally, [17] used blockchain enabled disseminated documents to present a BCoT model with tiny mists.

The BCoT Architecture Conceptualized Driven by a comprehensive literature review, we suggest a methodical BCoT architecture including three essential tiers: the Internet of Things (IoT) layer, cloud blockchain layer, and application layer. As an accompaniment, subtleties of each layer and the general concept will be discussed.

**IoT Layer:** IoT devices are in charge of gathering data from local circumstances and transmitting it remotely to entry points such as base stations, switches, or distant passageways. An Internet of Things device has a blockchain account, similar to a Bitcoin wallet that enables it to connect to the blockchain network and carry out conversations and transactions (such information offloading) with cloud services. Exceptionally, any asset-restricted IoT device (such as a wearable sensor) may function as a small hub that can participate in an exchange's approval cycle via its agent passing. It makes sense in scenarios involving blockchain-based sensor networks, such as those in [10], [20], and [14], where tiny sensors—like a mobile phone or haze hub are connected to the blockchain via its door. The entrance handles all sensor relationships with blockchain, including exchanges, information unloading, and mining tasks [8].

In the meanwhile, IoT devices with reasonably large resources, such as PCs or amazing smart phones, possess sufficient capabilities to support more lightweight IoT sensors and maintain consistency with the whole blockchain. In order to achieve corporative communication (such as gadget-to-gadget (D2D) correspondence in cooperative organisations), IoT devices may also communicate to one another via IoT doors. For IoT customers, a specifically mixed correspondence notion provides highly adaptive services in a secure and efficient manner.

Blockchain Cloud Layer: In the BCoT design, this functions as a mediator between the mechanical applications and the IoT organisation. We concentrate on a blockchain stage with several mists for a traditional architecture, but it also represents highly specialised components of a single cloud BCoT engineering. This concept demonstrates two advantages: 1) using blockchain technology to provide very secure organisation leadership; and 2) providing trustworthy on-demand processing services for a wide range of Internet of Things applications. Distributed computing services and blockchain services make up the coordinated cloud blockchain layer.

Blockchain managers: Giving secure organisations the board is the main motivation for the suggested engineering's use of blockchain. Blockchain as a Service (BaaS) is a cloud-based platform that transmits and facilitates the blockchain network. In particular, BaaS may provide a range of blockchain-powered services to support Internet of Things applications.

Shared record: It refers to the database that is distributed and exchanged across BCoT participants (such as IoT clients, cloud hubs, and blockchain materials). Exchanges such as data transfers or information partitioning between IoT devices and the cloud are documented in the common record. It enables contemporary businesses by enabling cloud customers to manage and verify their own communications with blockchain clouds.

Agreement: Using agreement components like PoW and PoS, which are managed by a group of excavators, it provides confirmation services on client exchanges. In order to provide strong security for the framework and improve blockchain consistency, BCoT greatly needs this assistance. Intriguingly, IoT customers may use their virtual cloud computers to participate in the agreement conversation and get payments for their efforts (such as Bitcoin's crypto currency).

Shared agreement: BCoT also provides apps with astute agreement services. As the BCoT framework is self-executing and provides free provisions, clever agreements are very beneficial in building business case and trust in the framework. Additionally, as soon as the IoT peer hubs conduct exchanges, keen agreements provide security administrations on client access confirmation or information sharing check, which further helps to maintain security over the cloud blockchain.

Public key cryptography is responsible for obtaining all data and information capacity from IoT and cloud materials. Advanced markings further improve changelessness and security for client transactions by ensuring that any information stored in blockchain is legitimate and unhindered.

In addition to these services, BaaS provides cloud blockchain capability. The cloud stage may serve as the foundation for blockchain-dependent decentralised distributed storage. Blockchain-based capability manages IoT data using hash values and periodically performs checks to find any opportunities for data modification. One blockchain-based capacity framework that is now available on the cloud, for example, is the Inter Planetary File System (IPFS) [8], which enables secure storage across capacity hubs. Furthermore, it has been shown to effectively address information hoarding concerns arising from unified cloud architectures about information leakage and executive capacity.

Administrations of distributed computing: Distributed computing leverages all of its administrations in the BCoT architecture to support applications, such as Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and Software as a Service (SaaS). IoT door-collected data will be received by cloud workers and stored on the cloud blockchain. The cloud worker also provides intelligent services on decommissioned IoT data by using devices that are readily available, including AI or information mining. IoT data may be stored on-chain in a blockchain or off-chain in a cloud data collection. On the other hand, many mists may be combined to provide certain functions, such information exchange or community structure for executives. In this particular scenario, the blockchain layer plays a crucial role in managing and overseeing cloud partnerships in order to facilitate cloud management delivery to Internet of Things clients and prevent conflicts across fogs.

Layer of Application: Many mechanical applications, such as astute medical services, brilliant transportation, astute city, astute energy, and astute industry, may profit from the BCoT coordination in diverse IoT scenarios. In addition to providing beneficial forms of support to contemporary applications, including network the board and QoS enhancement, BCoT also guarantees security and protection attributes for applied areas. For example, in the field of intelligent medical services, BCoT can support information preparation services because to cloud computing power, which may assist medical service providers in analysing intelligently tolerant data for improved clinical judgement. Blockchain, which provides discernibility and confirmation administrations throughout the clinical information trade and information handling, ensures the network security of medical services in the meanwhile. In the next section, a thorough examination of the application of BCoT mix and its benefits to IoT use cases such as astute industry, brilliant energy, and astute transportation will be conducted.

Sometimes, industries with inadequate preparation are unaware of the untested vulnerability of blockchain. The scatter ledger architecture, although potentially useful as an alternative, has never been fully realised.

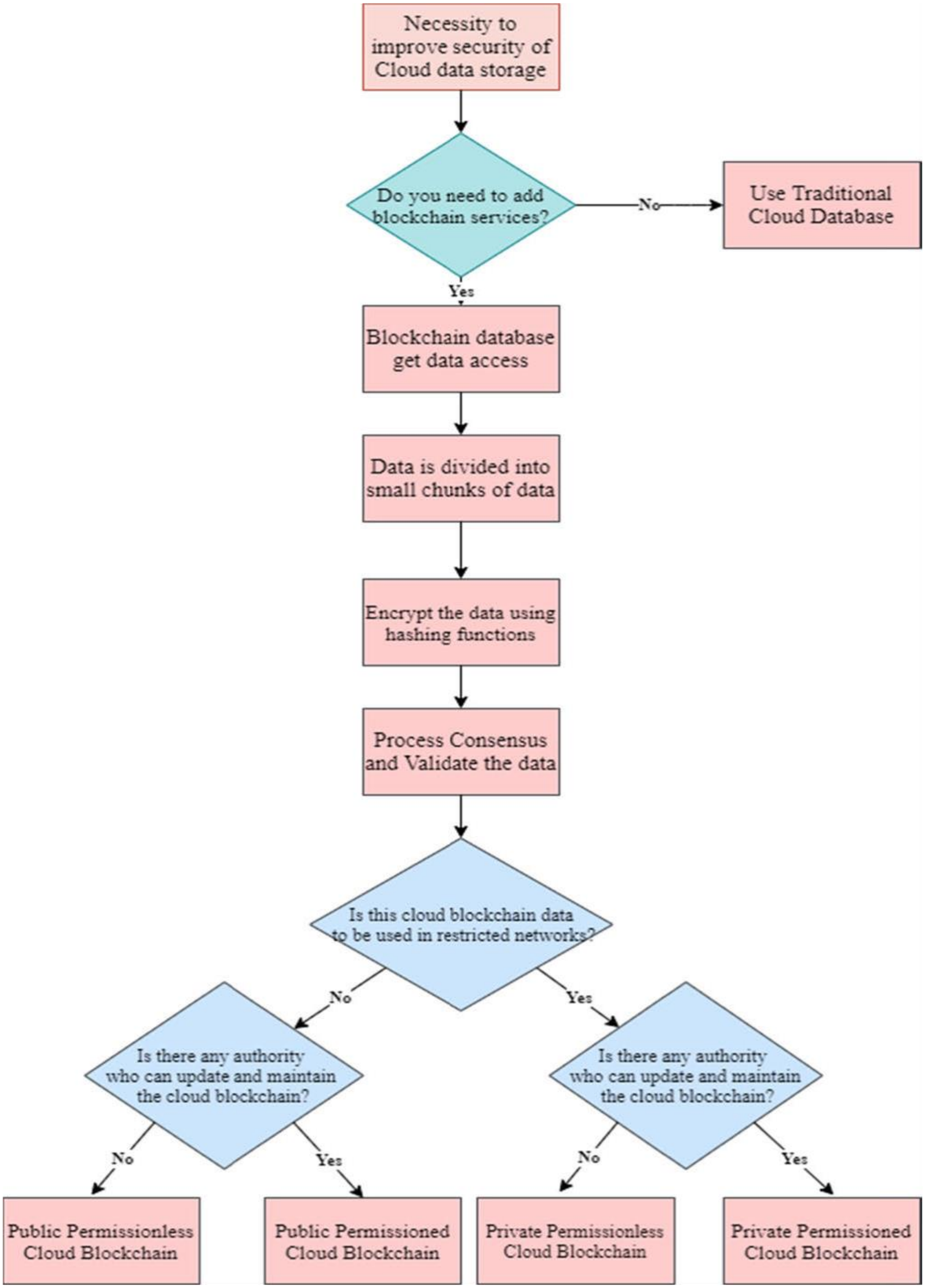
Necessity to improve security of Cloud data storage
Do you need to add blockchain services?
No
Use Traditional Cloud Database
Yes
Blockchain database get data access
Data is divided into small chunks of data
Encrypt the data using hashing functions
Process Consensus and Validate the data
Is this cloud blockchain data to be used in restricted networks?
No
Yes
Is there any authority who can update and maintain the cloud blockchain?
Is there any authority who can update and maintain the cloud blockchain?
No
Yes
No
Yes
Public Permissionless Cloud Blockchain
Public Permissioned Cloud Blockchain
Private Permissionless Cloud Blockchain
Private Permissioned Cloud Blockchain

Figure 05: Flowchart process of blockchain with cloud data.

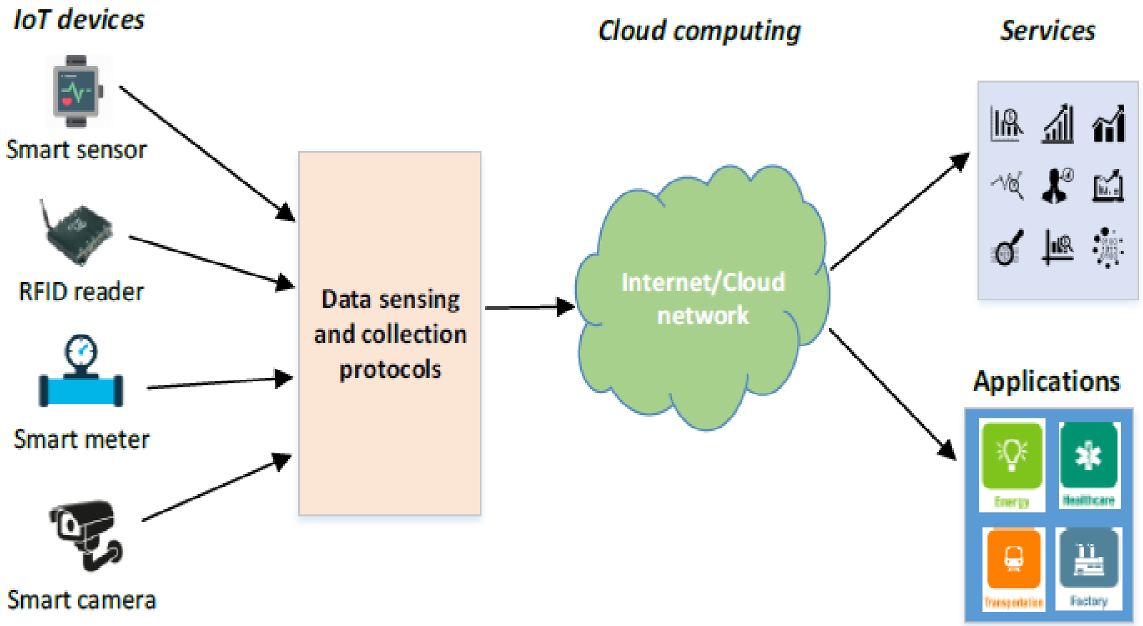

Figure 06: The general concept of CoT.

## RESEARCH AND TECHNOLOGY DEVELOPMENT OF BCOT

We have recognised BCoT technology and its contemporary improvements in the study. Results from recent studies examine how BCoT affects industry applications. Afterwards, we examine the platform development that is now underway in BCoT, together with its service initiatives and key findings.

In order to improve BCoT applications, the article will examine BCoT applications in the fields of industries, transportation, health care, and smart cities under the section headings. In conclusion, our study will look at potential reviews and findings of BCoT paradigms.

**Smart Healthcare:** BCoT investigates and offers effective smart services using data storage, analysis, and security technologies in the healthcare industry. Innovations abound in healthcare services when it comes to insurance and providing patients with the finest treatment possible. In addition to leading to an advanced zone of medical services, BCoT can provide fresh perspectives on how to address the fundamental problems with health care security and services [7], [8], [9], and [4].

**Smart City:** Thanks to recent technological advancements, cities have become more technologically adept and diverse. They are rich in IoT devices, networks, large amounts of storage in devices, and cloud computing. However, it is still a pipe dream to provide smart city services with fewer leftovers. Recent developments are opening up new possibilities for smart cities and holding out the possibility of smart gadgets offering services to their residents.

**Smart Industry:** As a decentralised P2P system, Blockchain is starting to take shape. It is investigating how it may push industries towards cutting-edge technology and make them more intelligent to boost production. With the aid of BCoT smart commerce, the developments in industrial regions will be finished with enhanced security and efficiency. We may investigate the delivery chain for chicks, intelligent construction, and the creation of intelligent energy further.

**Additional BCoT Applications:** The use of BCoT ideal models has been investigated in many scenarios, such as astute cloud management, astute executive resource allocation, and astute education.

### Smart cloud administrations

Distributed computing provides an alternative range of reclaiming services, including as the ability and computation to support individuals and projects. In general, web-based payment and security concerns are included in reevaluating services. However, the majority of traditional assistance programmes rely on a reliable outsider to approve the completion of payments. Therefore, for cloud-based apps, it is crucial to acknowledge the safe and fair payment of reconsidering services. Because blockchain is recognisable and permanent, it has emerged as a strong option to address security concerns with cloud advantages and enhance cloud management overall. A blockchain-based reasonable installment approach for rethinking distributed computing services is presented in the works [27], [18]. The suggested structure uses blockchain technology to assist the board convention and ensures adequate and virtuous capabilities. Fair payment may be made between customers and reassessing expert cooperatives on mists via exchanges that are stored and verified by blockchain without the involvement of third parties.

When a client wants the information on mists to be deleted during the most popular method of reclaiming it, he sends an erasure order to the cloud worker, instructing the worker to do so. However, the cloud worker is only partially trusted, and it may not really remove the specified data for financial reasons. In order to tackle this problem, the focus in [19] offers an additional freely verifiable information erasure scheme for distributed computing enabled by blockchain, which maintains public validation on erasure requests and eliminates the requirement for private information to be shared with outside parties. Blockchain provides decency confirmation services that enable all users to authorise requests for information deletion and regulate abusive activities on their cloud data with equal access rights. This blockchain-based solution reduces the need for cloud workers to handle customer data across the board and greatly simplifies the cancelling process.

To handle data security issues in a variety of cloud environments, the authors in [10] suggest a framework model for structured data visualisation termed bcBIM in the interim. In an exceptional instance, blockchain is used to record modifications of significant information sharing in conjunction with BIM information review. Coordinating blockchain in the BIM data set ensures the provenance and reliability of BIM information, and BIM cloud may facilitate the framework needed for executives. Designing machines and development robots are only two examples of the new applications that the cloud blockchain-based BIM model promises to foster. Blockchain is used by [13] and [12] to create decentralised distributed storage biological systems for security improvements in order to store information about executives on mists. Because it uses the plate space of a group of PCs and storage spaces to decentralise the data set, blockchain-based distributed stockpiling differs slightly from traditional distributed storage administrations. This ensures that any information owners can verify and check information respectability through the P2P network on blockchain. This high-level stockpiling concept also advances cloud computing dependability and information accessibility while preserving data over the long term.

## Smart asset the board

Growing interest is also being shown in the blockchain network's processing asset board for CoT. With the aid of an immutable blockchain and clever agreements for monitoring asset utilisation and information authenticity in distributed computing, numerous methodologies have been proposed to improve calculation resources and security administrations for BCoT applications in various types of undertakings like constant preparation, resource-intensive applications, and agreement measure. The study [13] offers an optimal asset allocation for edge-cloud-enabled IoT on the blockchain network that is contingent on a selling conspiracy. To establish asset exchange between asset vendors and buyers, a pure P2P processing asset exchange architecture on mists is being developed.

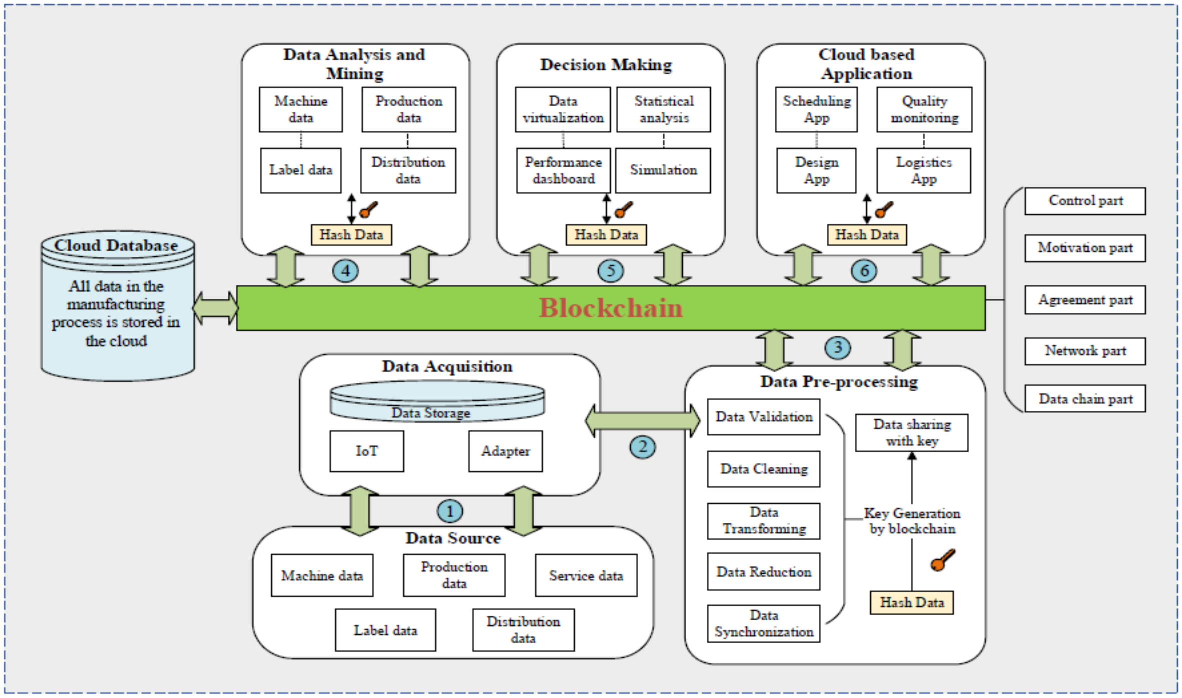

Figure 07: The blockchain cloud manufacturing system.

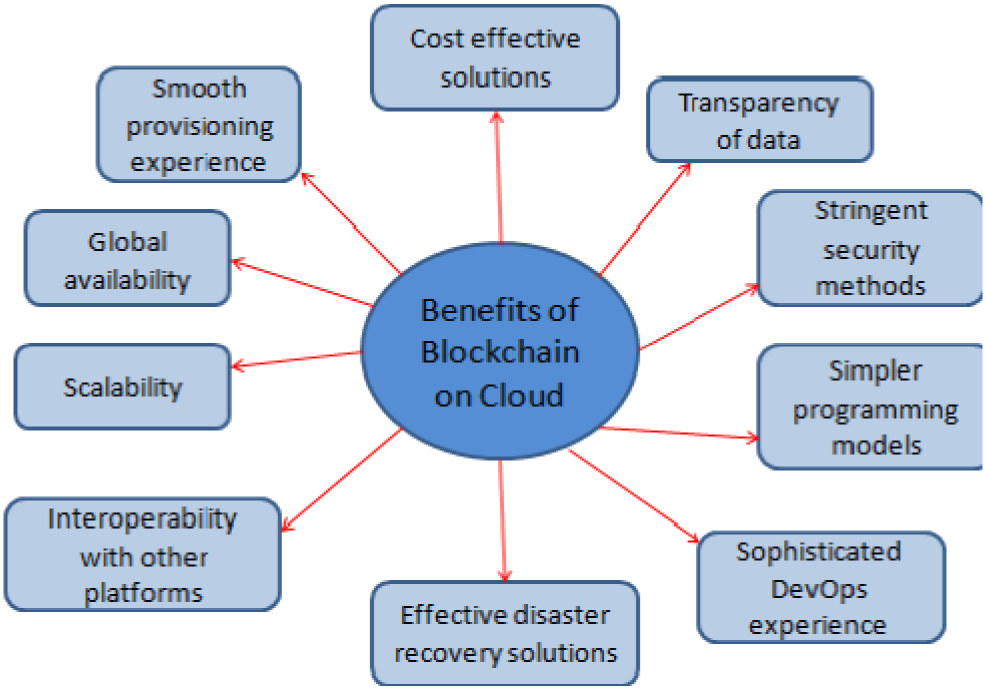
Cost effective solutions
Smooth provisioning experience
Transparency of data
Stringent security methods
Global availability
Benefits of Blockchain on Cloud
Scalability
Simpler programming models
Interoperability with other platforms
Effective disaster recovery solutions
Sophisticated DevOps experience

Figure 08: Blockchain benefit to cloud.

## RESEARCH CHALLENGES AND DISCUSSION

Based on the extensive audit of BCoT reconciliations, we have identified potential examination challenges and unresolved concerns in the field. We also discuss potential anticipated solutions to stimulate more research efforts in this exciting field.

**Research Challenges**

We highlight five key challenges in the field of BCoT research: asset the board, knowledge, protection spills, normalisation, and security weaknesses.

**Standardisation:** Since its inception, the blockchain technology has revolutionised business by presenting fresh, safe, decentralised organisational structures. This emerging invention has the ability to transform mechanical organisation models with state-of-the-art BCoT standards and alter the existing status of CoT exhibits. While combining blockchain technology with CoT may benefit Internet of Things applications in several ways, the BCoT invention has not been regulated and is only available to a small number of specialised companies. Crucially, unlike conventional plans that may be relevant to many use-case settings, each specialty co-op primarily develops and provides BCoT for defined uses. Because each supplier has their own set of rules, the lack of a framework standard may limit the ability of administrations suppliers to coordinate their efforts and make it difficult for customers to switch providers [21]. Furthermore, one fundamental problem still facing the BCoT market is the non-standard heterogeneous correspondence convention across different blockchain stages and CoT frameworks. For example, the three cloud blockchain projects that are examined in [22], Golem, SONM, and iExec, have different goals in terms of framework design, client objectives, and administrative setup. Three main factors contribute to this lack of standards: different organisational concepts, different functional theories, and different assistance definitions. As a result, they are unable to fulfil an administrative level policy, which is essential for their work improvements in the long term.

**Security Vulnerability:** Despite the fact that blockchain may improve CoT's security due to its distributed nature, changelessness, certainty, and encryption, security problems with BCoT persist due to flaws in both the CoT and blockchain frameworks. Because of the required assets of IoT devices, there has been an increase in the requirement for CoT to reacquire IoT data to mists for capacity and computation advantages. A series of new testing security problems, including as verification, framework respectability, character and access control, have emerged as a result of this special fuse [2]. Additionally, there are a number of fundamental security threats to CoT, such as prying eyes, malicious IoT attacks, shaky communication channels, and deterioration of association quality. Cloud services for BCoT are also vulnerable to real security threats, such as DoS attacks, malware infiltration, capacity and computation attacks, and virtual machine (VM) relocation attacks [15].

However, recent investigations have also shown intrinsic security flaws in blockchain applications, which are often associated with BCoT frameworks [16]. A true security bottleneck is a 51% attack, which means that a group of miners controls more than half of the company's processing power, or mining hash rate. This prevents new exchanges from receiving confirmations and halts payments between IoT customers and specialised co-ops. Attackers may really use this vulnerability to launch attacks; for example, they can manipulate exchange requests, interfere with regular mining operations, or launch a double spending attack, all of which have the potential to damage the blockchain network [10]. Similarly, the security component of brilliant agreement, which is thought of as core programming on blockchain, is also essential as even the smallest defect or attack may result in serious problems like security leaks or changes to the framework's logic [11], [12]. Basic security flaws include reentrancy attacks on cunning agreements in BCoT applications, timestamp dependency, and improper use of exemptions.

## Discussion

It is important for various BCoT service providers to come to a service agreement about the integration of CoT and blockchain. It is important to provide careful thought to technical elements such network configurations, blockchain implementation, IoT device integration, and service payment methods. To standardise BCoT technology, a federation of service providers may be required. To provide a generic functional architecture for blockchain platforms, several standardisation projects have been undertaken with the involvement of several organisations, including IEEE, ISTIC Europe, and ISO [15]. Furthermore, in order to serve the present BCoT-related businesses, it will be necessary for many service providers to concurrently build worldwide BCoT standards for cloud blockchain design, market formation, and customer service support [16]. Improvements in CoT and blockchain security may address BCoT security issues in the meantime. Security assessments and suitable solutions are critical from the perspective of the CoT.

Furthermore, a variety of cutting-edge techniques, including encryption, trustworthy cloud computing, effective user identification, access control, and intention concealment, have been explored to improve privacy for BCoT systems [17]. In order to enhance the privacy of Internet of Things data in cloud computing, access control architecture was recently presented in [13] with higher data dependability levels inherited by a consensus process. According to the blockchain perspective, anonymity is essential to provide BCoT users with strong privacy. This makes it possible to effectively conceal user information on blockchain, prevent attackers from figuring out the identity of transactions, and protect user privacy. For instance, a recent study in [14] suggests a novel approach that offers transaction privacy on the blockchain platform together with senders' anonymity and unlinking capability. Furthermore, the authors of [17] provide an anonymous reporting system that may protect blockchain system privacy while guaranteeing the accuracy of anonymous reporting data without disclosing IoT users' identities.

Using intelligent tools and expert systems from cloud computing might be a smart way to add intelligence to applications linked to BCoT. For instance, machine learning for smart health assessment systems is helpful to assist physicians in their medical procedures in BCoT-based smart healthcare [16], [19]. In the meanwhile, big data analytics software that can be found on the cloud is very beneficial in smart cities for resolving data-related problems including data gathering, processing, and visualisation for smart services from the city environment, residents, and different departments and agencies at the city scale [16]. In particular, a recent study [17] focused on the combination of blockchain technology with machine learning to allow decision-making services in a way that ensures security and dependability while enhancing the system's intelligence.

Recently, a few clever strategies have been put forward to improve BCoT's resource management effectiveness. For instance, a blockchain-based paradigm for energy-aware resource management in cloud data centres was given by the authors in [12]. Smart contracts include machine learning to optimise energy usage based on user demands.

Additionally, this method may result in considerable cost reductions when it comes to cloud blockchain request transfer and scheduling. In the meanwhile, the problem of resource management for blockchain mining in BCoT is examined in [18], wherein the least costs of service utilisation are achieved by optimising resources for computing in the blockchain consensus process. It also shows that under the suggested public cloud blockchain networks, cloud providers may earn more from the best resource management.

## FUTURE DIRECTIONS

Given the industry's and academia's keen interest in bit coins, it is envisaged that they will advance towards valuable via other technologies. The combination of this technology with Bitcoin has the potential to open up a wide range of opportunities for future services and applications. A thorough understanding of Bitcoin may aid in future research to incorporate BCoT so that we can combine the greatest features of both worlds.

A. Blockchain concert for expectations that are civilised Bitcoin

B. Bitcoin ML

C. Big Data BCoT

D. BCoT and the 5G network

## CONCLUSIONS

We were able to investigate many real-world BCoT model scenarios in the domains of smart health, cities, industries, and cloud services with the aid of the study. Additionally, it is conceivable to look at the possibilities of the BCoT platform in conjunction with Blockchain, which may draw in more industrialization by offering the sectors better service support, security, and privacy. A overview of the literature on BCoT systems, highlighting both current state improvements and potential latent possibilities, was produced by our investigation.

## REFERENCES

[1] J.-H. Lee and M. Pilkington, ″How the blockchain revolution will reshape the consumer electronics industry [future directions],” IEEE Consumer Electronics Magazine, vol. 6, no. 3, pp. 19–23, 2017.

[2] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, ″Blockchain for 5G and beyond networks: A state of the art survey,” Journal of Network and Computer Applications, vol. 166, 2020.

[3] P. Treleaven, R. G. Brown, and D. Yang, ″Blockchain technology in finance,” Computer, vol. 50, no. 9, pp. 14–17, 2017.

[4] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, P. Mc- Callum, and A. Peacock, ″Blockchain technology in the energy sector: A systematic review of challenges and opportunities,” Renewable and Sustainable Energy Reviews, vol. 100, pp. 143–174, 2019.

[5] A. Alketbi, Q. Nasir, and M. A. Talib, ″Blockchain for government servicesuse cases, security benefits and challenges,” in 2018 15th Learning and Technology Conference (L&T), 2018, pp. 112–119. [6] S. Nakamoto et al., ″Bitcoin: A peer-to-peer electronic cash system,”2008.

[7] F. Tschorsch and B. Scheuermann, ″Bitcoin and beyond: A technical survey on decentralized digital currencies,” IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2084–2123, 2016.

[8] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, ″A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications,” IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1125–1142, 2017.

[9] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, ″Internet of things: A survey on enabling technologies, protocols, and applications,” IEEE communications surveys & tutorials, vol. 17, no. 4, pp. 2347–2376, 2015.

[10] M. Aazam, I. Khan, A. A. Alsaffar, and E.-N. Huh, ″Cloud of things: Integrating internet of things and cloud computing and the issues involved,” in Proceedings of 2014 11th International Bhurban Conference on Applied Sciences & Technology (IBCAST) Islamabad, Pakistan, 14th-18th January, 2014, 2014, pp. 414–419.

[11] M. S. Karunarathne, S. A. Jones, S. W. Ekanayake, and P. N. Pathirana, "Remote monitoring system enabling cloud technology upon smart phones and inertial sensors for human kinematics," in 2014 IEEE Fourth International Conference on Big Data and Cloud Computing, 2014, pp. 137–142.

[12] B. Kantarci and H. T. Mouftah, "Sensing services in cloud-centric internet of things: A survey, taxonomy and challenges," in 2015 IEEE International Conference on Communication Workshop (ICCW), 2015, pp. 1865–1870.

[13] H. F. Atlam, A. Alenezi, A. Alharthi, R. J. Walters, and G. B. Wills, "Integration of cloud computing with internet of things: challenges and open issues," in 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2017, pp. 670–675.

[14] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and privacy for cloud-based IoT: Challenges," IEEE Communications Magazine, vol. 55, no. 1, pp. 26–33, 2017.

[15] K. Gai, K.-K. R. Choo, and L. Zhu, "Blockchain-enabled reengineering of cloud datacenters," IEEE Cloud Computing, vol. 5, no. 6, pp. 21–25, 2018.

[16] A. S. e. a. Yining Hu, "Blockchain-based smart contracts – applications and challenges," [Online]. Available: https://arxiv.org/abs/1810.04699.

[17] M. Ma, G. Shi, and F. Li, "Privacy-oriented blockchain-based distributed key management architecture for hierarchical access control in the IoT scenario," IEEE Access, vol. 7, pp. 34 045–34 059, 2019.

[18] Y. Li, L. Zhu, M. Shen, F. Gao, B. Zheng, X. Du, S. Liu, and S. Yin, "Cloudshare: Towards a cost-efficient and privacy-preserving alliance cloud using permissioned blockchains," in International Conference on Mobile Networks and Management. Springer, 2017, pp. 339–352.

[19] D. F.-C. JOANNA KOLODZIEJ, ANDRZEJ WILCZYNSKI and A. FERNNDEZ MONTES, "Blockchain secure cloud: a new generation integrated cloud and blockchain platforms general concepts and challenges," in https://www.awilczynski.me/wpcontent/uploads/2018/09/ECJvol4issue2.pdf.

[20] T. Hardjono and N. Smith, "Cloud-based commissioning of constrained devices using permissioned blockchains," in Proceedings of the 2nd ACM international workshop on IoT privacy, trust, and security. ACM, 2016, pp. 29–36.

[21] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, ″Blockchain technologies for the internet of things: Research issues and challenges," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2188–2204, 2018.

[22] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, ″Applications of blockchains in the internet of things: A comprehensive survey," IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1676–1717, 2018.

[23] T. M. Fern´andez-Caram´es and P. Fraga-Lamas, ″A review on the use of blockchain for the internet of things," IEEE Access, vol. 6, pp. 32 979– 33 001, 2018.

[24] H. Dai, Z. Zheng, and Y. Zhang, ″Blockchain for internet of things: A survey," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8076–8094, 2019.