# Blockchain Technology Innovative Exploring the Synergy and Potential Seamlessly Integrated with Cloud Computing

**M. Lova kumari**[1], Research scholar of Koneru Lakshmaiah Education Foundation Guntur, Asst. Professor(c), Department of Computer Science and Engineering, University College of Engineering, JNTUK, Kakinada, Andhra Pradesh, India,

**Dr. G.Bindu**[2], Associate Professor, Department of Computer Science and Engineering Koneru Lakshmaiah Education Foundation Guntur, Andhra Pradesh, India,

**Abstract:**

This paper presents innovative research that explores the integration of blockchain technology with cloud computing, aiming to enhance security, scalability, and efficiency within the realms of distributed ledger technology and cloud computing environments. As the digital landscape evolves, the demand for secure and efficient data management solutions intensifies. The convergence of blockchain and cloud computing holds promise as it addresses critical challenges associated with data security, scalability, and resource optimization. In this study, we investigate the synergies and potential benefits of combining these two technologies, emphasizing the advantages they bring to various industry sectors. The research findings shed light on novel approaches to fortifying data integrity, reducing latency, and optimizing resource allocation, contributing to the ongoing discourse on the fusion of blockchain and cloud technologies.

**Keywords:** blockchain; cloud computing; decentralization; Blockchain-as-a-Service

## 1. Introduction

The intersection of blockchain technology and cloud computing represents a compelling frontier in the domain of distributed ledger technology and cloud-based services. In today's data-driven world, where digital transactions and information exchange have become ubiquitous, the need for robust, secure, and efficient data management solutions is more pressing than ever before. Blockchain, heralded for its immutable ledger and cryptographic security features, has emerged as a potent tool for securing data and enabling trust in a decentralized manner. Meanwhile, cloud computing has revolutionized how organizations manage and scale their computing resources, offering flexibility, accessibility, and cost-efficiency. However, both technologies come with their own sets of challenges. While blockchain ensures data integrity and trust, it struggles with scalability and performance issues, often hampering its widespread adoption. On the other hand, cloud computing, while providing scalable resources, raises concerns about data security, privacy, and centralization. Recognizing these limitations, researchers and practitioners have begun exploring ways to synergize blockchain and cloud computing to harness their respective strengths while mitigating weaknesses.

This paper embarks on a journey to investigate the potential benefits and challenges associated with integrating blockchain technology into cloud computing environments. Our aim is to delve into the intricate interplay between these technologies and shed light on how their convergence can enhance security, scalability, and efficiency in diverse application domains. By bridging the worlds of decentralized ledger systems and cloud-based infrastructure, we endeavor to contribute to the ongoing discourse surrounding the fusion of blockchain and cloud technologies, ultimately offering insights that can pave the way for innovative solutions in data management and secure computing.[1].

Blockchain technology is advancing rapidly, initially gaining prominence through its association with Bitcoin and subsequently diversifying into various types to cater to specific organizational needs and advantages. One significant breakthrough in blockchain innovation is its capability to enable participants to transfer assets over the Internet without relying on a centralized intermediary. Initially conceived as the foundational technology for the cryptocurrency Bitcoin, blockchain has now undergone extensive testing across numerous sectors, including asset management and procurement services, resulting in a multitude of practical applications.

In contrast to the complex and often opaque processes seen in contemporary supply chains, characterized by numerous intermediaries and extensive documentation requirements, a decentralized blockchain system offers a solution. Such a system can link the diverse interests of supply chain participants to a public ledger, mitigating issues related to transparency and accountability. The inherent flexibility of blockchain technology has already instigated profound changes in business models, potentially surpassing the profitability of existing paradigms [2].

Blockchain technology represents a groundbreaking innovation that enables secure, reliable, and non-transient transactions among multiple parties. It functions as an authoritative trail for verifying the origin of products within the food supply chain, effectively reducing the likelihood of legal disputes. On a global scale, blockchain can be a valuable asset to international supply chains, provided that all nations adopt and effectively enforce a comprehensive set of universally applicable laws. Below, we outline some of the notable contributions of our research:

1. Conducting a comprehensive examination of Blockchain technology concerning its integration with Cloud Computing.
2. Demonstrating notable research endeavors that delve into the practical applications of Blockchain-Cloud integration.
3. Offering an in-depth bibliometric analysis across five real-world application domains where Blockchain-Cloud integration is prominent, accompanied by a reference architecture.
4. Investigating the three primary facets of Cloud computing that have experienced the most significant impact from Blockchain integration, followed by a bibliometric assessment.
5. Identifying the top three complementary technologies that enhance Blockchain-Cloud integration for the development of cutting-edge solutions, along with a bibliometric analysis of their relevance.
6. Presenting a structured overview and elucidating publication trends for Blockchain-as-a-Service (BaaS) and the leading Cloud Service Providers offering integrated Blockchain services.

The remainder of this paper is structured as follows. Section 2 provides an overview of Cloud computing and its various deployment models. Section 3 explores the advantages of integrating Blockchain with Cloud technology, while Section 4 delves into the specific areas of Cloud computing where Blockchain can yield substantial benefits. Notable research and developments related to Blockchain-Cloud integration are discussed in Section 5, while Section 6 addresses the challenges associated with adopting this integration. In Section 7, we identify and examine emerging technologies that complement Blockchain-Cloud integration, offering innovative solutions across diverse research domains. Our research methodology and a comprehensive bibliometric analysis based on existing academic literature are detailed in Section 8. Section 9 focuses on prominent Cloud Service Providers offering services that involve the fusion of Blockchain and Cloud computing. Finally, Section 10 provides a summary of our findings and concludes this study.

## 2. Cloud Computing and Deployment Models

Cloud computing represents a highly versatile model that allows both individuals and organizations to procure services tailored to their specific requirements. This model encompasses a wide range of services, including storage, provisioning, and convenient access to web-based functionalities. However, a common challenge in the cloud computing landscape is the efficient management of application performance while balancing Quality of Service (QoS) metrics and adhering to service level agreements (SLAs).

Cloud computing stands as an innovative, organization-centric framework adept at handling diverse requests originating from the cloud, delivering rapid support to users. It is a computational and processing paradigm widely embraced across the globe. This technology can be leveraged to streamline the pricing process through robust computational capabilities, providing on-demand access to extensive computing resources such as CPU, memory, network, server, storage, and software applications. Notably, these resources are frequently allocated to users at the most cost-effective rates [3].

Cloud Computing has emerged as a prominent trend in the field of information technology, capturing the attention of researchers worldwide. This technology offers users an accessible, flexible, and scalable computing environment accessible via the internet. It empowers individuals and organizations to utilize computing resources remotely through internet connections, resulting in substantial cost savings compared to the traditional establishment and maintenance of on-premises computing infrastructure.

In today's fast-paced world, vast amounts of data are continuously generated and refined every second to deliver high-quality services. Various companies have user bases that contribute their data and activities to enhance the services provided. This collaborative data sharing and processing play a pivotal role in service improvement.
As we progress, the evolving landscape poses a significant threat to user data privacy. While retrieving data from local machines was sufficient in the past, modern users now have the capability to synchronize their data with the cloud, enabling remote access from anywhere worldwide. However, this expanded accessibility also creates an additional avenue for potential breaches of user data. Consequently, it is imperative for organizations to implement a robust user access control and management system.

This paper delves into various algorithms and methodologies aimed at enhancing security and accuracy in the realm of cloud service access, addressing these emerging challenges.

The categorization of cloud deployment models is conducted with careful consideration of where the model is hosted and who has control over the network. Each model comes with specific requirements, making the selection of an appropriate model a crucial decision for both clients and organizations. Among the primary decisions to be made is choosing the most suitable model based on your specific requirements.

Every cloud deployment model offers a distinct set of features and services, each with its own range of cost options. Therefore, making an informed choice is vital when selecting the right model for your organization. In the past decade, Cloud computing has become increasingly essential for organizations seeking enhanced efficiency, flexibility, and accelerated time-to-market for their products. However, determining the ideal cloud model for an organization hinges on its unique demands and objectives as part of its strategy.

Selecting the right model is integral in helping organizations achieve their long-term digital goals. It ensures that your business receives the necessary elements of protection, security, flexibility, compliance, and cost-effectiveness. Below, we provide an overview of various types of cloud deployment models.

### 2.1. Private Cloud

The concept of a private cloud revolves around its exclusive ownership, operation, and management by an organization. Typically, the entire infrastructure is situated within a datacenter controlled or overseen by the said organization. Consequently, this organization assumes responsibility for procurement, maintenance, and support services. Within the private cloud environment, all resources remain confined solely to the organization that owns it. Essentially, a private cloud serves as a dedicated space catering to a single client. It does not involve the sharing of infrastructure with other clients.

Private clouds are the preferred choice when data security is paramount, and access needs to be restricted to specific user groups. They find utility in scenarios where organizations establish cloud environments exclusively for their employees' use, ensuring that only authorized personnel within that organization can access it. This exclusive access ensures that data stored in the private cloud remains accessible only to select individuals, offering enhanced security, quality, and privacy features. Typically, all the hardware resources within a private cloud belong to the organization itself.

Examples of private cloud providers include IBM Bluemix, Rackspace, Red Hat OpenStack, VMware, and Microsoft Azure Stack. Private clouds are particularly advantageous for safeguarding corporate data, allowing access solely to authorized personnel and emphasizing data privacy. Additionally, private clouds excel in providing heightened security measures and controlled access, as all resources are contained within the same organization. This makes them well-suited for supporting legacy systems [4].

### 2.2. Public Cloud

The public cloud is accessible to everyone, allowing individuals, including the general public, to utilize and store their data. Typically, individual users make use of this type of cloud service. Cloud service providers catering to mid-sized organizations offer their resources and services to anyone based on their specific requirements. Public cloud infrastructure is hosted on the service provider's premises and is not inherently designed to guarantee comprehensive security. Consequently, it is well-suited for organizations where security is not a primary concern when handling their data. Examples of public cloud providers include Google App Engine and Salesforce Heroku.

Public cloud models are particularly suitable for organizations with fluctuating and growing demands, as they enable you to pay the cloud service provider for infrastructure, computing power, and networking services on a flexible basis. Additionally, the public cloud is advantageous in situations where upfront investment is minimal, as there are no significant initial costs. It is an excellent choice for organizations that require immediate access to resources and where the entire infrastructure is hosted by the cloud provider. This model eliminates the need for infrastructure management.

### 2.3. Hybrid Cloud

A hybrid cloud combines elements of both public and private clouds, offering clients the flexibility to leverage the advantages of both environments. In cases where specific data must remain confidential and not accessible to the public, it can be stored in the private segment of the hybrid cloud. Conversely, for non-sensitive, publicly available resources and data, the public segment of the cloud can be utilized. This approach provides infrastructure at a cost that falls between that of the public and private clouds, making it a cost-effective choice.

However, hybrid cloud adoption is contingent upon an organization's ability to segregate its data into private and public components. Many organizations possess their own resources and seek to augment their infrastructure by borrowing resources from cloud vendors. In such scenarios, the hybrid cloud model becomes instrumental and is a preferred option. It stands as the second-most popular cloud deployment model, enabling organizations to utilize some of their existing on-premises infrastructure while leveraging additional resources from the public cloud. This approach is a judicious and valuable choice, particularly for organizations where security and data protection are paramount concerns.

It's important to note that this model, while advantageous, comes with associated costs. Implementing and maintaining a hybrid cloud can be relatively expensive due to its complexity and the need for robust security measures. Nevertheless, for organizations prioritizing security alongside the benefits of public cloud resources, the hybrid cloud remains a compelling solution.

### 2.4. Community Cloud

The community cloud is tailored for a collective of individuals with shared interests, often referred to as a community. When two or more organizations share similar requirements, they turn to a community cloud that offers services common to their needs. This deployment model proves highly advantageous for organizations collaborating on joint projects or initiatives. In this type of deployment, bandwidth and storage limitations are predefined. The community cloud is exclusively dedicated to a select group of organizations from the same communities. Neither fully public nor entirely private, it remains inaccessible to the general public and is not controlled by a single organization or vendor; instead, it is governed collectively by a group of organizations. This shared cloud infrastructure serves the purpose of assisting these organizations in achieving their common goals. Community clouds are particularly suited for situations where the initial investment is modest, and the setup benefits are substantial.

### 2.5. Multi-Cloud Deployment Model

Within the Multi-Cloud deployment model, various cloud providers are sequentially employed, combining both private and public clouds, bearing similarities to the Hybrid cloud approach. This model involves the utilization of multiple cloud types to enhance service accessibility. One compelling reason for adopting a Multi-Cloud strategy is when an organization seeks specific infrastructure or services from one public cloud provider while requiring specialized support from another. The Multi-Cloud model offers diverse options for organizations to enhance service reliability.

## 3. Advantages of Integrating Blockchain with Cloud Computing

Blockchain technology is a transformative innovation with significant appeal across industries, offering the potential to enhance various services. It stands as a revolutionary technology capable of revolutionizing existing market trading platforms. The advent of Industry 4.0 integrates cutting-edge technologies such as blockchain, AI, cloud computing, and IoT to optimize system functionality and efficiency [5–8]. Emphasizing the benefits of integrating blockchain and cloud computing, we delve into the prominent advantages of this integration.

### 3.1. Decentralization

In traditional cloud computing, data resides within centralized servers, posing significant security concerns. This challenge can be effectively addressed through the integration of blockchain technology into cloud computing. Within the realms of IoT and cloud computing, a notable issue arises from the dependency on centralized servers for data management and decision-making processes. Blockchain offers a solution by establishing a decentralized framework where identical data copies are stored across multiple nodes, thereby eliminating the risk of system-wide failures. Furthermore, data loss ceases to be a concern, as numerous data duplicates exist across various nodes. The fusion of blockchain and cloud computing presents a promising solution for achieving decentralization and ensuring complete user privacy.

### 3.2. Data Security

Blockchain systems inherently incorporate robust data security features. Given the extensive data transactions and storage in cloud computing, data security is a paramount concern. Blockchain-cloud integration serves as a solution to address this concern across various sectors. Even within the Internet of Things (IoT) domain, securely storing data in the cloud presents a significant challenge. IoT devices store various data types, including personal information of homeowners such as voice recordings, video footage, household items, property details, and personal habits. Any compromise of this data can lead to severe breaches of individual privacy, including potential attacks, theft, and illicit sale of personal data for financial gain. Such scenarios pose a significant threat to both IoT and cloud infrastructure. The remedy to this issue lies in the adoption of blockchain technology within cloud computing, as it holds the potential to enhance security throughout the entire architecture.

### 3.3. Flexibility

In the realm of blockchain applications, the volume of transactions within blockchain networks can be substantial. Blockchain technology boasts robust data processing capabilities, allowing for the handling of large-scale transactions to support flexible blockchain services. Consequently, cloud computing can offer on-demand resources for blockchain operations due to its scalability. The fusion of blockchain and cloud computing results in a highly adaptable integrated system.

### 3.4. Enhanced Supply Chain Management Efficiency

Blockchain stands as a pivotal technology in the quest to develop cost-effective and more efficient methods for supply chain management. It empowers improved end-to-end tracking of goods and services and can be seamlessly integrated with cloud computing to yield superior outcomes in the supply chain industry. One of the significant challenges faced by supply chain management is the continuous monitoring of all vehicles within an organization, including their current locations and the duration they remain stationary. Similarly, the tracking of various services such as products and parcels faces issues due to centralized design approaches. Blockchain holds significant potential for the traceability of these goods and services.

### 3.5. Fault Tolerance and Error Resilience

Blockchain necessitates data replication across diverse servers within a network, a task effectively facilitated by cloud computing. This approach minimizes the risk associated with a single point of failure, particularly in the event of a disruption in any cloud hub. Consequently, blockchain can deliver uninterrupted services, ensuring robust fault tolerance and error resilience.

## 4. Impact of Blockchain on Cloud Computing Domains

Cloud computing plays a pivotal role as a supporting technology for the establishment and operation of blockchain systems. We have already examined the significant advantages of integrating blockchain with cloud services in the preceding section. In this section, we delve into the specific domains of cloud computing that have experienced notable transformations due to the fusion with blockchain technology. Notably, areas such as "Security," "Privacy," and "Storage" within cloud computing have witnessed substantial advancements as a consequence of blockchain integration.

Section 6 of this paper further delves into a bibliometric analysis of these three domains, shedding light on research interests and publication trends among scholars. Additionally, it becomes evident that overcoming the hurdles of data security and privacy is crucial for fostering the growth of cloud computing, and blockchain emerges as an ideal solution to address these challenges effectively. To provide a comprehensive overview, Table 1 summarizes key works in these areas.

**Table 1.** Blockchain impact areas in Cloud Computing.

| | Theme | Publications |
|---|---|---|
| Cloud Impact Areas | Security | [9–12] |
| | Privacy | [13–17] |
| | Storage | [18–24] |

Ensuring data security and safeguarding user privacy stands as pivotal concerns when considering Cloud adoption. The integration of Blockchain technology into Cloud environments holds the promise of addressing these security and privacy challenges [10]. Leveraging the Blockchain-Cloud synergy enables the efficient distribution of vast data volumes, enhancing accuracy while minimizing costs [22]. Additionally, Blockchain integration offers an avenue to implement enhanced access control mechanisms within Cloud setups. Unlike the prevalent centralized access control approach adopted by most Cloud organizations, blockchain integration introduces decentralization, effectively thwarting any attempts at data tampering or leaks through internal cloud management channels [15].

Blockchain-powered Cloud solutions are poised to establish a robust framework for identity access control, bolstering privacy protection [25–28]. Privacy is also paramount in the domain of Cloud auditing, where comprehensive tracking and logging of all operations and associated data are essential. The integration of Blockchain into Cloud environments guarantees the preservation of data provenance, safeguarding it from breaches within the Cloud ecosystem. The decentralized nature of blockchain technology lends itself to securing the origin of data and maintaining information on data owners, effectively resolving a significant concern in cloud storage applications.

**Enhancing Cloud Data Security Through Blockchain-Based Mechanisms**

In recent years, cloud computing has seen significant advancements; however, the challenges of ensuring data security and trusted computing persist in various cloud applications. Despite extensive research efforts and the proposal of various models, such as data integrity testing and multiparity calculations, these approaches continue to grapple with issues like computational complexity and scalability limitations.

Blockchain technology has emerged as a transformative computing paradigm, introducing a cryptographic algorithm-driven generation of data blocks within databases. The inherent features of blockchain, including decentralization, anonymity, auditability and data persistence, have unlocked its potential for diverse applications. This paper explores the integration of blockchain technology into cloud computing to enhance security mechanisms and improve both secure storage and computing performance.

The discussion within this paper delves into the utilization of blockchain technology to bolster security in cloud computing. Specifically, it examines how blockchain can address the requirements for secure cloud storage data. Additionally, the paper explores cryptographic text access control techniques and integrity verification technologies to provide a comprehensive understanding of the potential improvements blockchain can offer in the realm of cloud data security.

In reference to source [29], the study delves into the implementation of a distributed virtual machine agent model within the cloud environment, employing mobile agent technology. In this setup, multiple tenants collaborate to ensure the trustworthiness of data through the virtual machine agent. This virtual machine agent assumes responsibility for critical monitoring and verification tasks, essential for the establishment of a blockchain-based integrity protection mechanism. This innovative integrity protection system, founded on blockchain principles, is constructed by leveraging the virtual machine proxy model in conjunction with the distinctive hash values generated by the Merkel hash tree. Its primary purpose lies in the continuous monitoring of data alterations, utilizing smart contracts within the blockchain database and the real-time data utilization.

In this context, users have the capability to report instances of data tampering, and a blockchain-based cloud data integrity verification system is established using a "block-and-response" approach (Reference [30]). Additionally, Reference [31] delves into the implementation of a decentralized virtual machine specialist model within the cloud environment, leveraging mobile agent technology. This model facilitates collaborative interactions among multiple tenants, ensuring data trust verification through the virtual machine specialist. The virtual machine specialist plays a pivotal role in monitoring and verifying tasks, a crucial component of

the blockchain-based integrity protection mechanism. In parallel, users within the system can signal incidents of data tampering, leading to the development of a blockchain-based cloud data verification system (Reference [32]). Furthermore, Reference [33] presents a technology application scheme for blockchain-based cloud computing by harnessing the strengths of both blockchain and cloud computing. This scheme offers data protection and integrity verification. Notably, it introduces a multi-parity scheme based on blockchain technology, along with an exploration of security mechanisms, algorithms in blockchain, and general scalable multiparity computing schemes.

**Diverse Applications of Integrating Blockchain with Cloud Technology**

Cloud computing has become a predominant computing model over the last decade, with a recent surge in organizations transitioning their operations to the Cloud. This shift can be attributed to several factors, including the widespread availability of resources, appealing pricing structures, customizable solutions, and a multitude of market players. In recent times, the term "Cloud" has evolved into a catch-all phrase representing computing and storage capabilities accessible via the internet. The Cloud has transcended its initial definition to become a versatile computing paradigm that complements and supports various cutting-edge technologies. Leading Cloud Service Providers (CSPs) now offer an array of services, including containerization, artificial intelligence (AI), the Internet of Things (IoT), and Big Data analytics, which seamlessly integrate with their existing offerings.

**Application Domains of Blockchain-Cloud Integration: A Comprehensive Review**

The integration of Cloud technology with other cutting-edge technologies has long been acknowledged as a means to foster the development of more resilient, scalable, and secure applications. Among the latest additions to this integration landscape is Blockchain technology, which has ignited significant interest among researchers and industry experts in recent years. Blockchain, as a distributed ledger technology, offers a secure and automated framework for conducting transactions. Illustrated in Figure 1, our study presents a reference architecture for Blockchain-Cloud integration.

This research section delves into the synergy between Blockchain technology and Cloud computing.
We conducted an extensive literature review, resulting in the identification of five primary application domains for Blockchain-Cloud

integration, namely: (1) Healthcare, (2) Supply Chain, (3) Finance, (4) Smart Cities, and (5) Agriculture. Table 2 offers a concise summary of noteworthy works within each of these application areas.

**Table 2.** Blockchain–Cloud Application Areas

| | Theme | Publications |
|---|---|---|
| Blockchain and Cloud | Healthcare | [34–41] |
| | Supply Chain | [42–47] |
| | Finance | [48–51] |
| | Smart Cities | [52–59] |
| | Agriculture | [60–65] |

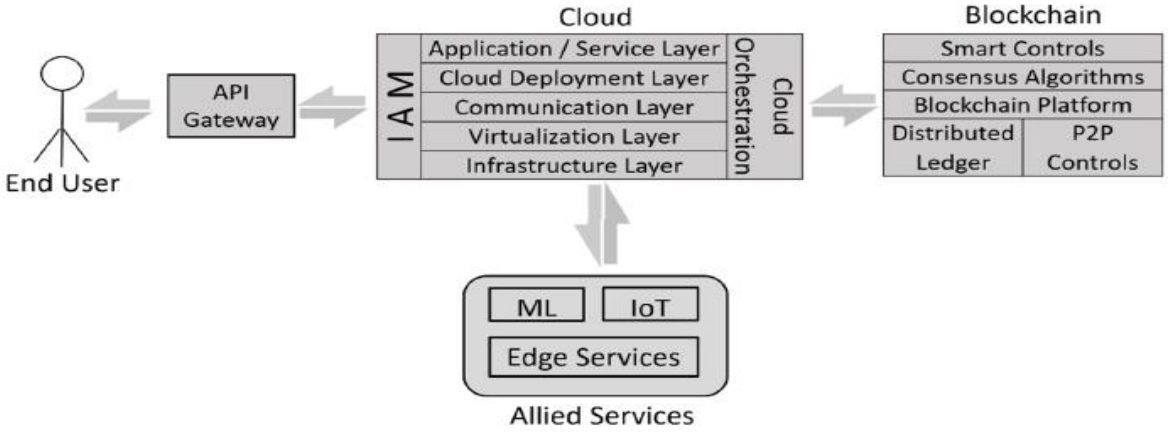



**Figure 1: Blockchain Cloud Reference Architecture**

In recent times, the concept of "smart cities" has garnered significant attention within the global research community. The proliferation of Cloud computing and the Internet of Things (IoT) has provided a robust technological foundation for the development of smart cities. Blockchain technology, a relatively new addition to the ever-expanding arsenal of technologies, aspires to facilitate the creation of citizen-centric

applications within the context of smart urban environments. By harnessing the power of blockchain in conjunction with IoT, Artificial Intelligence (AI), and Cloud computing, it becomes possible to operate an entire smart city in an autonomous manner. Notably, blockchain-enabled IoT solutions have been gaining momentum among industry stakeholders due to their support for pervasive sensing capabilities and sophisticated information exchange and processing. Blockchain, through the use of smart contracts and consensus algorithms, enables secure and transparent information exchange among IoT devices. This integration finds applications in diverse areas such as energy trading and distribution platforms, traffic management systems, smart homes, and various IoT applications. Furthermore, blockchain holds the potential to elevate the scope of e-governance, thereby enhancing citizen engagement and the formulation of government initiatives within the context of a smart city.

### 5.2. The Impact of Blockchain on Healthcare

Blockchain technology has ushered in a transformative era within the healthcare sector, introducing novel applications for the management of health records, streamlining medical insurance claims processing, and optimizing pharmaceutical supply chain operations. This innovation empowers healthcare professionals to securely manage patient data without the need for third-party intermediaries. Additionally, it equips government authorities with the tools to design and implement more effective healthcare programs based on comprehensive citizen health records.

One notable advantage of blockchain technology is its ability to expedite the dissemination of diagnostic reports to medical practitioners and insurance providers, facilitating faster and more efficient claim settlements. The inherent immutability of blockchain technology further enhances trust and accountability within the healthcare ecosystem, fostering the development of patient-centric healthcare solutions.

When integrated with complementary technologies such as Artificial Intelligence (AI), Cloud computing, and the Internet of Things (IoT), blockchain achieves even greater success in modernizing healthcare systems. This convergence of technologies has given rise to innovative applications, including the Internet of Medical Things (IoMT), Edge-based healthcare systems, and AI-enhanced medical imaging platforms. Notably, in the post-pandemic landscape, extensive research and discussions have emerged surrounding the practical implementation of blockchain, IoT, and AI in contact tracing efforts and the distribution and validation of vaccination certificates. These advancements signify a promising future for the intersection of cutting-edge technologies in healthcare.

### 5.3. Integration of Blockchain Technology in Supply Chain Management

Recent research in the field of blockchain technology has demonstrated its growing significance beyond the domain of cryptocurrencies. Among the various domains exploring the potential of blockchain, Supply Chain Management (SCM) has emerged as a prominent area of interest. Several previous studies have shed light on the application of blockchain technology in the management of supply chains across industries such as food, agriculture, retail, hospitality, and pharmaceuticals.

SCM has long presented a formidable challenge for organizations, and the complexity of this task has only intensified, especially in the post-pandemic era. The efficient functioning of SCM is pivotal to a nation's economic activities, and any disruptions in this domain can result in significant fiscal deficits and job losses. To remain competitive and relevant in this rapidly changing landscape, companies are compelled to modernize their SCM practices. Herein, the integration of blockchain technology with SCM emerges as a valuable solution, offering effective asset tracking mechanisms while safeguarding security and data integrity.At every stage of the supply chain, data is generated and recorded as transactions. Blockchain-based systems are inherently transparent and capable of real-time data collection, providing an unbroken trail of a product's journey throughout the entire supply chain. Blockchain technology can effectively manage the entire product lifecycle, ensuring rigorous quality control. Moreover, it holds the potential to enhance various aspects of SCM, encompassing physical and digital asset tracking, order and payment tracking, and the management of invoices, licenses, and copyrights.

The decentralized nature of blockchain technology fosters a continuous flow of information, facilitating seamless sharing among suppliers, vendors, manufacturers, and end-user customers across the entire supply chain. With no central authority, the presence of a distributed ledger, and a trust-based ecosystem, blockchain intricately weaves a network of interconnected assembly lines.

In summary, blockchain technology's integration into Supply Chain Management represents a promising avenue for addressing the evolving complexities of SCM. It offers transparency, security, and efficiency, making it a valuable tool for organizations seeking to adapt and thrive in today's dynamic business environment.

### 5.4 Revolutionizing Agriculture Through Blockchain Technology

Blockchain technology plays a pivotal role in transforming the agricultural sector by eliminating intermediaries and facilitating direct communication between farmers and end-users. This article highlights the significant advantages that blockchain technology offers to agriculture, including the establishment of smart-contract-enabled trading platforms that empower farmers to sell their produce directly to consumers at favorable rates. Furthermore, blockchain advocates for information-intensive farming practices, involving the assimilation of agricultural data and intelligent decision-making processes. The adoption of smart agriculture, driven by cutting-edge technologies, is imperative for rural development and the revitalization of the agricultural economy. A blockchain-powered token-based economy can further enhance security and efficiency in crop produce trading, providing invaluable support to farmers in their quest for sustainable growth and prosperity.

## 6. Blockchain-Cloud Integration Hurdles

### 6.1. Interoperability Constraints

Within the realm of enterprise-grade blockchain platforms, numerous options are available, each capable of handling complex business transactions. However, a major stumbling block to their widespread adoption lies in the absence of standardized protocols that facilitate seamless communication among these platforms. To achieve the seamless collaboration of businesses operating on diverse blockchain infrastructures, a proven cross-platform system is imperative. Presently, no such system is in place, leaving companies using, for instance, Hyperledger Fabric to encounter compatibility issues when interfacing with their partners relying on Corda services. Addressing this critical challenge has seen the emergence of Blockchain Platform Services. Notably, industry leaders such as Hyperledger and the Enterprise Ethereum Alliance, representing two of the most prominent enterprise blockchain platforms, have embarked on collaborative efforts to define and establish interoperability standards. Nevertheless, substantial work remains to be done before this concern can be adequately addressed, paving the way for the widespread adoption of enterprise blockchain solutions.

### 6.2. Regulatory Challenges

The adoption of enterprise blockchain technology is still in its nascent stages, characterized by a limited number of pilot projects having been successfully executed. Consequently, the development of comprehensive regulatory frameworks for the governance of enterprise blockchain networks remains a challenging endeavor. The inherent nature of these networks, which often span multiple geographical jurisdictions, adds layers of complexity to the task of legislating their operation. This global dispersion of blockchain networks presents a formidable obstacle for governments seeking to establish rules pertaining to data storage and sharing within them.

The intricate structure of blockchain networks further complicates matters. In cases of illicit transactions, the intricacies involved may pose significant challenges for authorities in their efforts to trace and identify the legal responsibilities of the parties involved. This multifaceted landscape necessitates careful consideration as lawmakers work towards crafting effective regulatory solutions.

### 6.3. Lack of Regulatory Framework

One of the predominant challenges confronting the blockchain industry pertains to the absence of regulatory oversight across various organizations. Within the realm of IT, a growing number of entities are embracing blockchain technology as a means to facilitate transactions, and in some cases, entire product ecosystems hinge on this innovative technology. However, the absence of clear-cut regulations has introduced a perplexing conundrum, as there is no standardized set of rules governing the blockchain market. Consequently, the absence of a regulatory framework hinders effective management and standardization. In order to foster the successful integration of blockchain into real-world applications and address the inherent challenges, it becomes imperative for governmental and regulatory bodies to establish comprehensive rules, protocols, and guidelines specifically tailored for the blockchain domain.

### 6.4. Tensions regarding Criminal Activities and Cyber security

The prevailing narrative surrounding blockchain technology often spotlights its association with criminal activities and cyber security threats, thus casting a shadow over its merits. According to data from Chainalysis, a blockchain analysis company, a mere 0.34% of all cryptocurrency transactions in 2020 were deemed illegal, while ransomware incidents experienced an alarming 311% surge. These statistics, though relatively low in the broader context, fuel apprehensions among enterprises considering blockchain adoption. Notably, blockchain technology inherently boasts security features, yet businesses exhibit reluctance to integrate it into their operations. While phishing scams predominantly affect cryptocurrency transactions, enterprise blockchains remain resilient to such threats. Nevertheless, ransomware attacks continue to pose a potential risk to enterprise blockchains, albeit mitigatable through robust multi-factor authentication measures.

### 6.5. Ambiguity Surrounding Return on Investment (ROI)

One of the pivotal concerns confronting companies embarking on the adoption of blockchain technology is the uncertain return on investment (ROI). As previously elucidated, integrating blockchain comes with substantial costs, underscoring the criticality of ROI assessment. According to research conducted by IBM, organizations anticipate a mere 20% ROI on their blockchain investments within the next 4 to 5 years, with a more promising 50% ROI expected within a decade. However, forecasting the ROI for a blockchain project remains a multifaceted challenge, devoid of a proven, standardized formula. This formidable obstacle acts as a significant deterrent to organizations contemplating the adoption of blockchain technology.

### 6.6. Bridging the Gap: Integrating Blockchain-Cloud with Legacy Systems

The contemporary challenge facing industries is the seamless integration of blockchain with legacy systems. Achieving full integration necessitates a comprehensive overhaul of the entire system, entailing the amalgamation of diverse technologies. During this process, several issues emerge, such as a scarcity of skilled labor—specifically, a dearth of developers equipped with the requisite blockchain expertise. Consequently, organizations may find themselves compelled to rely on third-party entities, further complicating the integration. Consequently, organizations must commit substantial time and resources to complete this transition. Many companies are now actively endorsing the shift towards blockchain integration due to escalating concerns regarding data loss. The reluctance to modify existing databases poses a substantial risk, as data loss and data corruption are major liabilities for IT firms. With the adoption of blockchain technology, these companies stand to benefit. In response to growing market demands, new enterprises are investing in and devising novel methodologies for integrating blockchain with legacy systems. One such product

exemplifying this approach is the Modex Blockchain database, designed to accommodate users with limited blockchain knowledge, thereby mitigating the risk of sensitive data loss.

### 6.7. Scalability Challenges

One significant hurdle encountered in the implementation of blockchain technology is scalability. While blockchain functions smoothly when the user base is relatively small, issues arise when attempting to accommodate a large influx of users. Notably, popular blockchain networks like Ethereum and Bitcoin, despite their extensive user counts, struggle to efficiently manage and accommodate their growing user bases. As the number of users on a blockchain network increases, the transaction process becomes more time-consuming, resulting in elevated transition costs. Consequently, this discourages the growth of the technology, making it less economically viable. Some alternative blockchain technologies initially demonstrate faster processing speeds but tend to slow down as user numbers rise. Managing this scalability challenge is imperative to prevent the stagnation of blockchain technology.

### 6.8. High Energy Consumption

Energy consumption is another formidable challenge associated with blockchain technology. A majority of blockchain systems adhere to the Proof of Work consensus algorithm, which demands substantial computational power to maintain the network's integrity. The process of mining, involving the solution of complex equations through computing power, leads to an exponential increase in electricity consumption. Presently, miners consume approximately 0.2% of the world's total electricity, raising concerns about sustainability if this trend continues. To address this challenge, blockchain technology can transition to consensus algorithms that are significantly more energy-efficient. Embracing such energy-efficient consensus methods is vital to ensure that blockchain technology remains a boon rather than a burden on global energy resources.

## 7. Allied Technologies

The fusion of advanced technologies, such as Cloud Computing, Blockchain, and IoT, has demonstrated significant potential in the advancement of IoT solutions. Although distinct technologies in their own right, IoT and Blockchain can synergize to develop innovative solutions. Blockchain, in particular, presents a compelling solution to address privacy and security concerns within the IoT domain [66–68]. The integration of technology with cloud computing holds great promise for diverse IoT applications, including identity management, data storage, and autonomous processing. Various sectors, including Supply Chain Management, Smart Cities, and Intelligent Healthcare Systems, have recently recognized the advantages of incorporating Blockchain with Cloud technology [69 and 70].

Smart contracts have demonstrated their significant value in the effective management and operation of supply chains and smart cities. The synergy between the Internet of Vehicles (IoV) and Device-to-Device communication relies heavily on the integration of Blockchain and Cloud technologies. Blockchain ensures the secure exchange of data among devices, establishing trust and traceability among diverse users, while the Cloud ensures data availability, interoperability, and standardization. In the realm of intelligent healthcare systems, data gathered from a multitude of sensors is seamlessly exchanged, stored, and processed through Blockchain-Cloud integration. This fusion of technologies empowers healthcare professionals to monitor their patients' health in real-time with optimal efficiency and privacy safeguards in place.

The exponential growth in the proliferation of IoT devices has resulted in a significant upsurge in data transmission to the Cloud endpoint, leading to a substantial strain on network bandwidth resources. To address the challenges posed by centralized failures and the escalating bandwidth demands, an innovative approach known as edge computing has been introduced. In this paradigm, data from diverse IoT devices are strategically stored across various edge servers to facilitate swift processing and seamless real-time accessibility [71–73]. However, managing the storage and processing of sensitive data on these edge servers remains a formidable task, necessitating integration with blockchain technology. Blockchain serves as a foundational framework for establishing a secure and decentralized system that offers robust safeguards for privacy preservation, encrypted data storage and retrieval, secure access control, intrusion detection, and robust authentication mechanisms. The consensus mechanisms inherent in blockchain play a pivotal role in effectively managing distributed databases spanning multiple edge servers. The seamless integration of blockchain with Cloud computing within the context of edge computing creates a distributed edge-computing ecosystem that empowers the tracking of assets and ensures the integrity of transactions among IoT devices [74].

The decentralized architecture of this system serves as a robust safeguard against potential internal threats, while simultaneously upholding data transparency. The integration of Blockchain and Cloud technologies enhances collaboration among IoT devices and edge servers. This synergy between Blockchain, Cloud, and edge computing is mutually advantageous, with edge servers contributing to efficient mining management and blockchain scalability. Notably, the fusion of Blockchain with 6G-enabled edge services and autonomous vehicles driven by edge computing represents a pivotal focus in the research landscape. Additionally, Artificial Intelligence (AI) emerges as the third pivotal component in the realm of Blockchain-Cloud integration. The proliferation of data from IoT devices, web applications, and social media platforms has spawned a multitude of AI and deep learning applications [75–78]. Given the intricate nature of machine learning models and the sheer diversity and volume of data they handle, Cloud hosting becomes imperative. Nonetheless, it is essential to address concerns tied to the centralized nature of AI, which could potentially give rise to data breaches and data authenticity issues [79].

The fusion of blockchain and artificial intelligence (AI) has given birth to an innovative concept known as Decentralized AI. This concept revolves around the secure storage and sharing of data through the utilization of digital signatures and decentralized encryption techniques. It establishes a foundation for trustworthy decision-making and robust data governance mechanisms, particularly when combining Blockchain-CloIntegrating AI into the mix enhances the potential of smart contracts, which play a pivotal role in the development of autonomous systems. These smart contracts empower intelligent machines to make decisions that can be scrutinized and validated by miner nodes within the blockchain network, ensuring transparency and reliability.

Furthermore, the integration of blockchain with AI extends its support to the notion of decentralized learning. This approach facilitates the secure and dependable distribution of decision outcomes, hyperparameter values, and neural network weights [80–83]. Decentralized learning represents the convergence of autonomous intelligent machines, collectively contributing to more precise decision-making processes.

Additionally, the synergy between blockchain, cloud integration, and AI holds promise in the storage and processing of tamper-proof data. This data is cryptographically signed before distribution and subsequently subjected to validation prior to further processing. One specific domain where these technologies find significant applicability is in the development of smart cities [84]. Through the harmonious utilization of these technologies, we can envision the creation of truly intelligent, self-sustaining, and sustainable smart cities. For a comprehensive overview of the research in this field, please refer to Table 3, which provides a comparative analysis of notable works related to Blockchain-Cloud integration in conjunction with allied technologies.

**Table 3. Blockchain–Cloud Integration with Allied Technologies.**

| Serial No | Allied Technology | Cloud Deployment Model | Cloud Impact Area | Blockchain Type | Blockchain Platform |
|---|---|---|---|---|---|
| [85] | IoT, AI | Private Cloud | Computation | Private | Ethereum |
| [86] | IoT | Public/Private Cloud | Storage | Private | - |
| 87] | IoT,Deep Learning | Public Cloud | Security, Privacy | Private | Ethereum |
| [88] | IoT | Private Cloud | Security | Consortium | Ethereum |
| [89] | IoT | Private Cloud | Security, Storage | Consortium | - |
| [90] | Edge Computing | Public Cloud | Computation | Consortium | - |
| [91] | Edge Computing | Public Cloud | Computation | - | - |
| [92] | Edge Computing | Private Cloud | Computation ,Security | Multichain | - |
| [93] | AI, Edge Computing | Private Cloud | Privacy | Public, Private | - |
| [94] | AI, IoT | Public Cloud | Computation, Storage | Public | Customized Blockchain |
| [95] | Edge Computing, AI | Public Cloud | Privacy | Private | Ethereum |
| [96] | AI, IoT | Private Cloud | Security, Computation | Public | - |
| [97] | IoT | Public/Private Cloud | Security, Privacy, Storage | Public | - |
| [98] | Edge Computing, Deep Learning | Public Cloud | Security, Computation | Private | Ethereum |
| [99] | IoT, Edge Computing | Private Cloud | Security, Privacy | Private | - |

## 8. Literature Review

### 8.1. Research Methodology

This study employs a comprehensive research approach to examine publication trends within the domains of Blockchain technology and Cloud computing. We conducted a systematic survey utilizing the Scopus database [100], with a focus on articles published between 2017 and 2021. To ensure consistency, we exclusively considered papers written in the English language.

Our research methodology encompassed several stages. Initially, we initiated the search by utilizing keywords such as "Blockchain AND Cloud," ensuring that these terms appeared either
in the paper's abstract or title. This initial search revealed three prominent sub-domains where

Blockchain and Cloud technologies intersect. Subsequently, we expanded our investigation by conducting searches using keywords like "Blockchain AND Fintech," "Blockchain AND Smart City," and "Blockchain AND Healthcare."

To enhance our understanding of the research landscape in Blockchain technology and Cloud computing, we analyzed our search results using three key dimensions. Finally, we dedicated a subsection of our study to publications centered on Blockchain-as-a-Service (BaaS). The keyword "BaaS" was employed to categorize works discussing the implementation or utilization of Blockchain-as-a-Service.

Below is the list of keywords utilized during our comprehensive survey:
1. Blockchain + Cloud Computing
2. Blockchain + Cloud + Smart Healthcare
3. Blockchain + Cloud + Finance/DeFi
4. Blockchain + Cloud + Agriculture
5. Blockchain + Cloud + Supply Chain
6. Blockchain + Cloud + Smart City

7. Blockchain + Cloud Security
8. Blockchain + Cloud Privacy
9. Blockchain + Cloud Storage

**8.2.Utilization of Blockchain-Cloud Technology in Various Sectors**

In Figure 2, we present a comparative analysis of significant application areas, considering the volume of research publications starting from the year 2017. Our comprehensive survey highlights five prominent subdomains that have garnered substantial attention in the context of the integration of Blockchain and Cloud technologies.

**Figure 3** offers insights into the distribution of publications based on different article classifications, such as conference papers, book chapters, articles, and conference review papers. It is noteworthy that, except for the healthcare sector, conference papers constitute the most significant segment in terms of research output across all other subdomains.

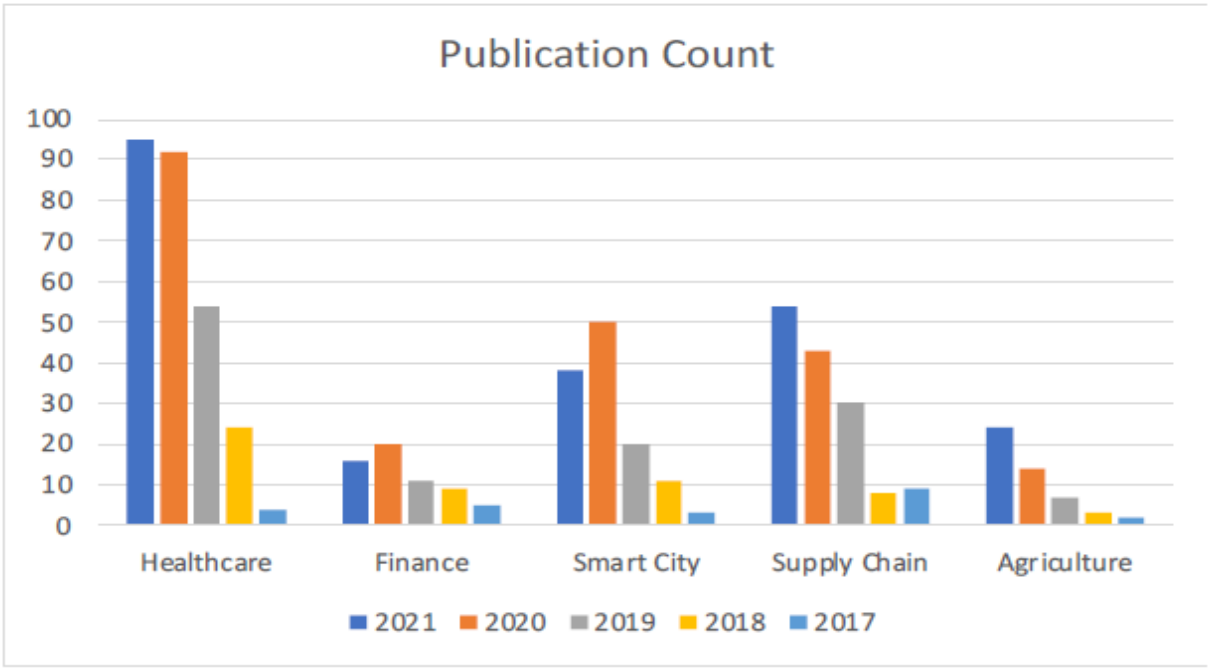
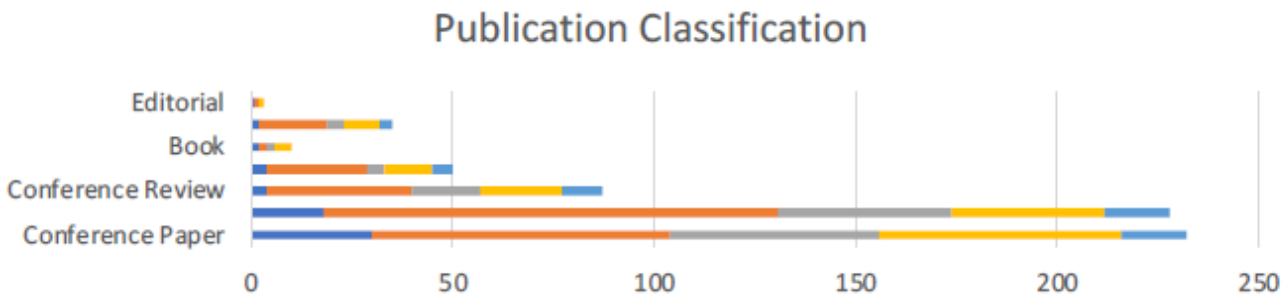



**Figure 2.** Publication count comparison among application areas.




| | Conference Paper | Article | Conference Review | Review | Book | Book Chapter | Editorial |
|---|---|---|---|---|---|---|---|
| Finance | 30 | 18 | 4 | 4 | 2 | 2 | 1 |
| Healthcare | 74 | 113 | 36 | 25 | 2 | 17 | 1 |
| Smart City | 52 | 43 | 17 | 4 | 2 | 4 | 0 |
| Supply Chain | 60 | 38 | 20 | 12 | 4 | 9 | 1 |
| Agriculture | 16 | 16 | 10 | 5 | 0 | 3 | 0 |

**Figure 3.** Publication classification comparison among application areas.

In Figure 4, we present a breakdown of publications by country in the field of Supply Chain Management, specifically focusing on the integration of Blockchain and Cloud technologies. India emerges as the frontrunner in this domain, with China and the United States following closely behind. India's dominant position in terms of publication output signifies its pivotal role in spearheading innovative supply chain

solutions, a crucial component of its overarching strategy to establish itself as a global manufacturing hub. This prominence underscores India's commitment to advancing the field of supply chain management through cutting-edge technologies.

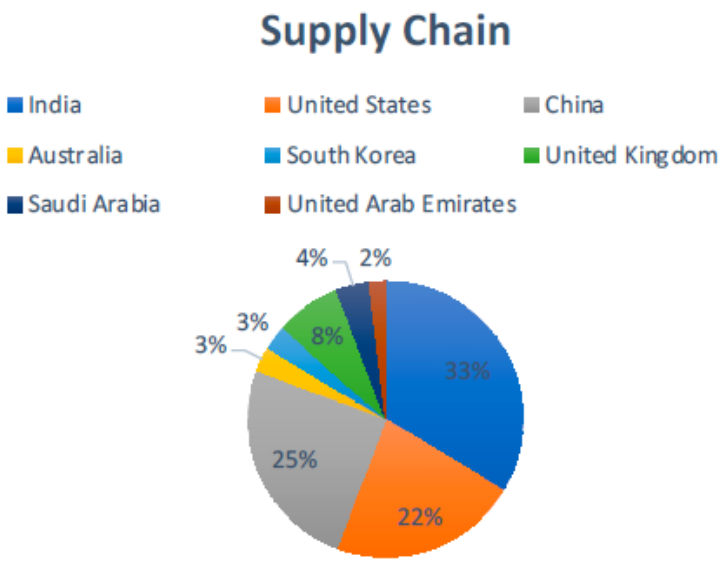



**Figure 4. Region-specific publication distribution for Blockchain–Cloud and Supply Chain.**

In Figure 5 illustrates the distribution of publications by country in the field of utilizing Blockchain and Cloud technology within the healthcare sector. India emerges as the foremost contributor, trailed by the United States and China. This chart reaffirms the observation that nations like India and China are actively engaged in pioneering innovative healthcare solutions that integrate various cutting-edge technologies.

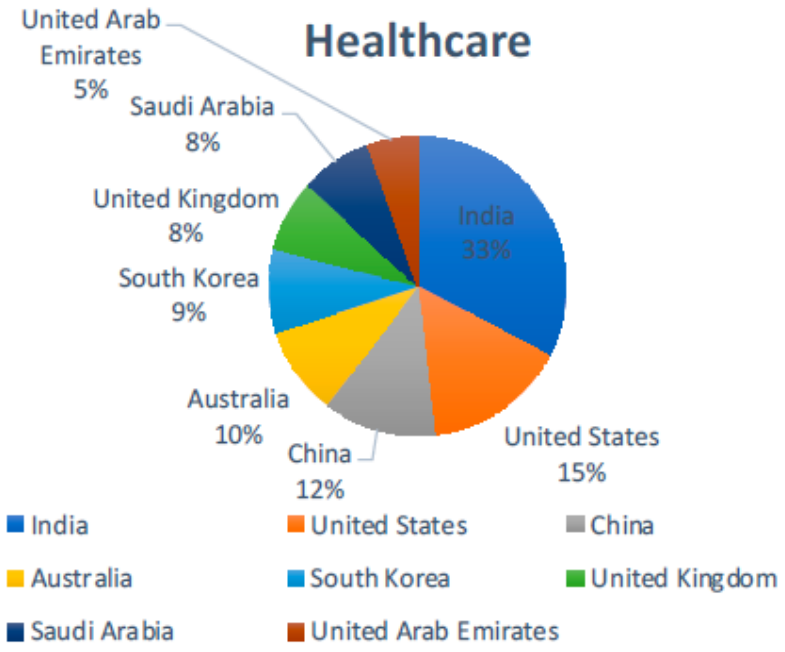



**Figure 5.** Region-specific publication distribution for Blockchain–Cloud and Healthcare.

In Figure 6: The analysis reveals that among the 68 studies examined, 14 of them delve into the intricacies of trust management and its potential solutions. Privacy management is a topic of focus in 13 out of the 68 studies, while general security concerns are addressed in 16 of the selected works. This underscores the enduring significance of security in blockchain-based Vehicular Ad-Hoc Networks (VANETs). Additionally, three of the selected studies delve into the issues related to proposed blockchain frameworks and provide validation for their approaches.

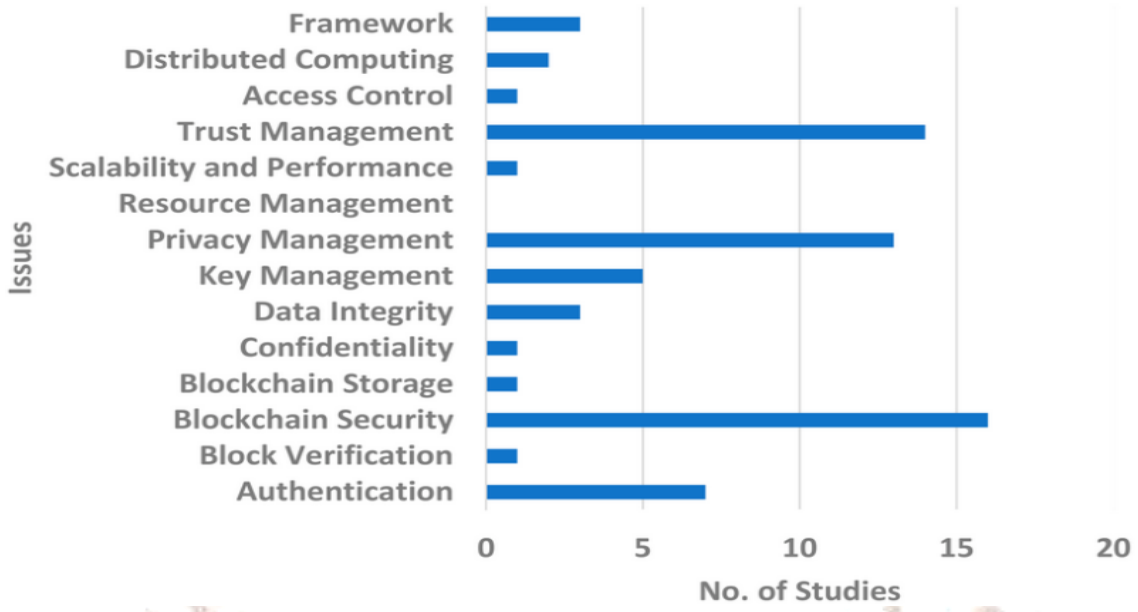



**Figure 6.** General Blockchain issues and number of studies.

**References**


1. Benil, T.; Jasper, J. Cloud based security on outsourcing using blockchain in E-health systems. Comput. Netw. 2020, 178, 107344
2. Huang, H.; Zhu, P.; Xiao, F.; Sun, X.; Huang, Q. A blockchain-based scheme for privacy-preserving and secure sharing of medical data. Comput. Secur. 2020, 99, 102010.
3. Negi, D.; Sah, A.; Rawat, S.; Choudhury, T.; Khanna, A. Block Chain Platforms and Smart Contracts. In Blockchain Applications inIoT Ecosystem; Choudhury, T., Khanna, A., Toe, T.T., Khurana, M., Gia Nhu, N., Eds.; EAI/Springer Innovations in Communication and Computing; Springer: Cham, Switzerland, 2021.
4. Bommadevara, N.; Del Miglio, A.; Jansen, S. Cloud Adoption to Accelerate IT Modernization; McKinsey Digital: Atlanta, GA,USA, 2018.
5. Miyachi, K.; Mackey, T.K. hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design. Inf. Process. Manag. 2021, 58, 102535.
6. Teufel, B.; Sentic, A.; Barmet, M. Blockchain energy: Blockchain in future energy systems. J. Electron. Sci. Technol. 2019, 17, 100011.
7. Unal, D.; Hammoudeh, M.; Kiraz, M.S. Policy specification and verification for blockchain and smart contracts in 5G networks. ICT Express 2020, 6, 43–47.
8. Wang, K.; Kim, H.S. FastChain: Scaling Blockchain System with Informed Neighbor Selection. In Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 14–17 July 2019; pp. 376–383.
9. Pavithra, S.; Ramya, S.; Prathibha, S. A survey on cloud security issues and blockchain. In Proceedings of the 2019 3rd International Conference on Computing and Communications Technologies (ICCCT), Chennai, India, 21–22 February 2019; IEEE: Piscataway,NJ, USA, 2019; pp. 136–140.
10. Park, J.H.; Park, J.H. Blockchain security in cloud computing: Use cases, challenges, and solutions. Symmetry 2017, 9, 164.
11. Gai, K.; Choo, K.-K.R.; Zhu, L. Blockchain-Enabled Reengineering of Cloud Datacenters. IEEE Cloud Comput. 2018, 5, 21–25.
12. Yadav, D.; Shinde, A.; Nair, A.; Patil, Y.; Kanchan, S. Enhancing data security in cloud using blockchain. In Proceedings of the 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 13–15 May 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 753–757.
13. Esposito, C.; De Santis, A.; Tortora, G.; Chang, H.; Choo, K.-K.R. Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? IEEE Cloud Comput. 2018, 5, 31–37.
14. Liang, X.; Shetty, S.; Tosh, D.; Kamhoua, C.; Kwiat, K.; Njilla, L. Provchain: A blockchain-based data prove-nance architecture in cloud environment with enhanced privacy and availability. In Proceedings of the 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), Madrid, Spain, 14–17 May 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 468–477.
15. Yang, C.; Tan, L.; Shi, N.; Xu, B.; Cao, Y.; Yu, K. AuthPrivacyChain: A Blockchain-Based Access Control Framework with Privacy Protection in Cloud. IEEE Access 2020, 8, 70604–70615.

16. Wang, Y.; Zhang, A.; Zhang, P.; Wang, H. Cloud-Assisted EHR Sharing with Security and Privacy Preservation via Consortium Blockchain. IEEE Access 2019, 7, 136704–136719.
17. Xu, J.; Xue, K.; Li, S.; Tian, H.; Hong, J.; Hong, P.; Yu, N. Healthchain: A Blockchain-Based Privacy Preserving Scheme for Large-Scale Health Data. IEEE Internet Things J. 2019, 6, 8770–8781.
18. Dwivedi, A.D.; Srivastava, G.; Dhar, S.; Singh, R. A Decentralized Privacy-Preserving Healthcare Blockchain for IoT. Sensors 2019,19, 326.
19. Sharma, P.; Jindal, R.; Borah, M.D. Blockchain technology for cloud storage: A systematic literature review. ACM Comput. Surv.(CSUR) 2020, 53, 1–32.
20. Li, J.; Wu, J.; Chen, L. Block-secure: Blockchain based scheme for secure P2P cloud storage. Inf. Sci. 2018, 465, 219–231.
21. Yang, C.; Chen, X.; Xiang, Y. Blockchain-based publicly verifiable data deletion scheme for cloud storage. J. Netw. Comput. Appl.2018, 103, 185–193.
22. Zhang, Y.; Xu, C.; Lin, X.; Shen, X.S. Blockchain-based public integrity verification for cloud storage against pro-crastinating auditors. IEEE Trans. Cloud Comput. 2019, 9, 923–937.
23. Zhu, Z.; Qi, G.; Zheng, M.; Sun, J.; Chai, Y. Blockchain based consensus checking in decentralized cloud storage. Simul. Model.Pract. Theory 2019, 102, 101987.
24. Tang, J.; Huang, C.; Liu, H.; Al-Nabhan, N. Cloud Storage Strategy of Blockchain Based on Genetic Prediction Dynamic Files.Electronics 2020, 9, 398.
25. Farouk, A.; Alahmadi, A.; Ghose, S.; Mashatan, A. Blockchain platform for industrial healthcare: Vision and future opportunities.Comput. Commun. 2020, 154, 223–235.
26. Ferrer-Gomila, J.-L.; Hinarejos, M.F.; Isern-Deyà, A.-P. A fair contract signing protocol with blockchain support. Electron. Commer. Res. Appl. 2019, 36, 100869.
27. Gul, M.J.; Subramanian, B.; Paul, A.; Kim, J. Blockchain for public health care in smart society. Microprocess. Microsystems 2021,80, 103524.
28. Liu, X.; Muhammad, K.; Lloret, J.; Chen, Y.-W.; Yuan, S.-M. Elastic and cost-effective data carrier architecture for smart contract in blockchain. Futur. Gener. Comput. Syst. 2019, 100, 590–599.
29. Wei, P.;Wang, D.; Zhao, Y.; Tyagi, S.K.S.; Kumar, N. Blockchain data-based cloud data integrity protection mechanism. Futur.Gener. Comput. Syst. 2019, 102, 902–911.
30. Xu, J.; Zhuang, Z.;Wang, K.; Liang,W. High-Accuracy Reliability Prediction Approach for Blockchain Services Under BaaS. In Blockchain and Trustworthy Systems; Springer: Cham, Switzerland, 2020; pp. 648–660.
31. Jo, Y.; Park, C. Codit: Collaborative auditing for baas. In Proceedings of the 3rdWorkshop on Scalable and Resilient Infrastructures for Distributed Ledgers, Davis, CA, USA, 9–13 December 2019; pp.11-12.
32. Onik, M.M.H.; Miraz, M.H. Performance analytical comparison of blockchain-as-a-service (baas) platforms. In Proceedings of the International Conference for Emerging Technologies in Computing, London, UK, 19–20 August 2019; Springer: Cham,Switzerland, 2019; pp. 3–18.
33. Zhu, L.; Wu, Y.; Gai, K.; Choo, K.-K.R. Controllable and trustworthy blockchain-based cloud data management. Futur. Gener.Comput. Syst. 2019, 91, 527–535.
34. Mamdouh, M.; Awad, A.I.; Khalaf, A.A.; Hamed, H.F. Authentication and Identity Management of IoHT Devices: Achievements,Challenges, and Future Directions. Comput. Secur. 2021, 111, 102491.
35. Shukla, S.; Thakur, S.; Hussain, S.; Breslin, J.G.; Jameel, S.M. Identification and Authentication in Healthcare In-ternet-of-Things Using Integrated Fog Computing Based Blockchain Model. Internet Things 2021, 15, 100422.
36. Purohit, S.; Calyam, P.; Alarcon, M.L.; Bhamidipati, N.R.; Mosa, A.; Salah, K. HonestChain: Consortium block-chain for protected data sharing in health information systems. Peer-Peer Netw. Appl. 2021, 14, 3012–3028.
37. Egala, B.S.; Pradhan, A.K.; Badarla, V.R.; Mohanty, S.P. Fortified-chain: A blockchain based framework for secu-rity and privacy assured internet of medical things with effective access control. IEEE Internet Things J. 2021, 8, 11717–11731.
38. Lakhan, A.; Mohammed, M.; Rashid, A.; Kadry, S.; Panityakul, T.; Abdulkareem, K.; Thinnukool, O. Smart-Contract Aware Ethereum and Client-Fog-Cloud Healthcare System. Sensors 2021, 21, 4093.
39. Ismail, L.; Materwala, H.; Hennebelle, A. A Scoping Review of Integrated Blockchain-Cloud (BcC) Architecture for Healthcare:Applications, Challenges and Solutions. Sensors 2021, 21, 3753. [CrossRef]
40. Mayer, A.H.; Rodrigues, V.F.; da Costa, C.A.; da Rosa Righi, R.; Roehrs, A.; Antunes, R.S. Fogchain: A fog com-puting architecture integrating blockchain and Internet of things for personal health records. IEEE Access 2021, 9, 122723–122737.
41. Jiang, C.; Duan, H. Research and implementation of Intelligent Service Platform for Flexible Employ-ment in Internet Sharing Economy. In Proceedings of the 2021 IEEE International Conference on

Computer Science, Electronic Information Engineering and Intelligent Control Technology (CEI), Fuzhou, China, 24–26 September 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 237–241.
42. Mehta, D.; Tanwar, S.; Bodkhe, U.; Shukla, A.; Kumar, N. Blockchain-based royalty contract transactions scheme for Industry 4.0 supply-chain management. Inf. Process. Manag. 2021, 58, 102586.
43. Niya, S.R.; Dordevic, D.; Stiller, B. ITrade: A Blockchain-based, Self-Sovereign, and Scalable Marketplace for IoT Data Streams. In Proceedings of the 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM), Bordeaux, France, 17–21 May 2021.
44. Bhagavan, S.; Rao, P.; Ngo, T. C3HSB: A Transparent Supply Chain for Multi-cloud and Hybrid Cloud Assets Powered by Blockchain. In Proceedings of the 2021 IEEE 37th International Conference on Data EngineeringWorkshops (ICDEW), Chania, Greece, 19–22 April 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 100–103.
45. Chinnaraj, G.; Antonidoss, A. A new methodology for secured inventory management by average fitness-based colliding bodies optimization integrated with block chain under cloud. Concurr. Comput. Pract. Exp. 2021, 34, e6540.
46. Subramanian, G.; Thampy, A.S. Implementation of Hybrid Blockchain in a Pre-Owned Electric Vehicle Supply Chain. IEEE Access 2021, 9, 82435–82454.
47. Lin, Y.-P.; Petway, J.R.; Anthony, J.; Mukhtar, H.; Liao, S.-W.; Chou, C.-F.; Ho, Y.-F. Blockchain: The Evolutionary Next Step for ICT E-Agriculture. Environments 2017, 4, 50.
48. Xiaoping, D.; Tao, L.; Xiaoyuan, D. Research on the intelligent settlement cloud platform of electric power materials based on the electronization of blockchain VAT special invoice. In Proceedings of the 2021 China International Conference on Electricity Distribution (CICED), Shanghai, China, 7–9 April 2021; pp. 948–952.
49. Zhang, H.; Zang, Z.; Muthu, B. Knowledge-based systems for blockchain-based cognitive cloud computing model for security purposes. Int. J. Model. Simul. Sci. Comput. 2021, 2241002.
50. Hassani, H.; Huang, X.; Silva, E.S. Fusing Big Data, blockchain, and cryptocurrency. In Fusing Big Data, Block-Chain and Cryptocurrency; Palgrave Pivot: Cham, Switzerland, 2019; pp. 99–117.
51. Mukhtar, A.; Romli, A.; Noor, N.M.; Abdullateef, M.; Al-Bashiri, H. Inventory Visibility Scenario to Reduce Safety Stock in Supply Chain Network Using Blockchain Hyperledger Composer. In Proceedings of the 2021 International Conference on Software Engineering & Computer Systems and 4th International Conference on Computational Science and Information Management (ICSECS-ICOCSIM), Online, 24–26 August 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 535–540.
52. Samuel, O.; Javaid, N.; Alghamdi, T.A.; Kumar, N. Towards sustainable smart cities: A secure and scalable trading system for residential homes using blockchain and artificial intelligence. Sustain. Cities Soc. 2022, 76, 103371.
53. Venkadeshan, R.; Jegatha, M. Blockchain-Based Fog Computing Model (BFCM) for IoT Smart Cities. In Convergence of Internet of Things and Blockchain Technologies; Springer: Cham, Switzerland, 2022; pp. 77–92.
54. Kumar, P.; Kumar, R.; Srivastava, G.; Gupta, G.P.; Tripathi, R.; Gadekallu, T.R.; Xiong, N. PPSF: A Priva-cy-Preserving and Secure Framework using Blockchain-based Machine-Learning for IoT-driven Smart Cities. IEEE Trans. Netw. Sci. Eng. 2021, 8, 2326–2341.
55. Aloqaily, M.; Bouachir, O.; Boukerche, A.; Al Ridhawi, I. Design guidelines for blockchain-assisted 5G-UAV net-works. IEEE Netw. 2021, 35, 64–71.
56. Aguilera, R.C.; Ortiz, M.P.; Banda, A.A. Internet of things expert system for smart cities using the blockchain technology. Fractals 2021, 29, 2150036.
57. Sharma, P.K.; Park, J.H. Blockchain based hybrid network architecture for the smart city. Futur. Gener. Comput. Syst. 2018, 86,650–655.
58. Treiblmaier, H.; Rejeb, A.; Strebinger, A. Blockchain as a Driver for Smart City Development: Application Fields and a Comprehensive Research Agenda. Smart Cities 2020, 3, 853–872.
59. Sharma, P.; Borah, M.D.; Namasudra, S. Improving security of medical big data by using Blockchain technology. Comput. Electr.Eng. 2021, 96, 107529.
60. Demestichas, K.; Peppes, N.; Alexakis, T.; Adamopoulou, E. Blockchain in Agriculture Traceability Systems: A Review. Appl. Sci.2020, 10, 4113.
61. Zhu, L.; Li, F. Agricultural data sharing and sustainable development of ecosystem based on block chain. J. Clean. Prod. 2021,315, 127869.
62. Hossain, S.; Rahman, H.; Rahman, S.; Hosen, A.S.M.S.; Seo, C.; Cho, G.H. Intellectual Property Theft Protection in IoT Based Precision Agriculture Using SDN. Electronics 2021, 10, 1987.
63. Vangala, A.; Sutrala, A.K.; Das, A.K.; Jo, M. Smart Contract-Based Blockchain-Envisioned Authentication Scheme for Smart Farming. IEEE Internet Things J. 2021, 8, 10792–10806.

64. Ren, W.; Wan, X.; Gan, P. A double-blockchain solution for agricultural sampled data security in Internet of Things network. Futur. Gener. Comput. Syst. 2021, 117, 453–461.
65. Khanna, A.; Sah, A.; Bolshev, V.; Jasinski, M.; Vinogradov, A.; Leonowicz, Z.; Jasi ´ nski, M. Blockchain: Future of e-Governance in Smart Cities. Sustainability 2021, 13, 11840.
66. Li, Z.; Kang, J.; Yu, R.; Ye, D.; Deng, Q.; Zhang, Y. Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things. IEEE Trans. Ind. Inform. 2017, 14, 3690–3700.
67. Liu, M.; Yu, F.R.; Teng, Y.; Leung, V.C.; Song, M. Performance optimization for blockchain-enabled industrial In-ternet of Things(IIoT) systems: A deep reinforcement learning approach. IEEE Trans. Ind. Inform. 2019, 15, 3559–3570.
68. Li,W.; Guo, H.; Nejad, M.; Shen, C.-C. Privacy-Preserving Traffic Management: A Blockchain and Zero-Knowledge Proof Inspired Approach. IEEE Access 2020, 8, 181733–181743.
69. Khanna, A.; Sah, A.; Choudhury, T.; Maheshwari, P. Blockchain Technology for Hospitality Industry. In Proceedings of the European, Mediterranean, and Middle Eastern Conference on Information Systems, Dubai, United Arab Emirates, 25–26 November 2020; Springer: Cham, Switzerland, 2020; pp. 99–112.
70. Choudhury, T.; Khanna, A.; Toe, T.T.; Khurana, M.; Nhu, N.G. Blockchain Applications in IoT Ecosystem; Springer: Cham,witzerland, 2021.
71. Sharma, A.; Awasthi, Y.; Kumar, S. The Role of Blockchain, AI and IoT for Smart Road Traffic Manage-ment System. In Proceedings of the 2020 IEEE India Council International Subsections Conference (INDISCON), Visakhapatnam, India, 3–4 October 2020;IEEE: Piscataway, NJ, USA, 2020; pp. 289–296.
72. Moniruzzaman; Khezr, S.; Yassine, A.; Benlamri, R. Blockchain for smart homes: Review of current trends and research challenges. Comput. Electr. Eng. 2020, 83, 106585.
73. Ren, Y.; Leng, Y.; Qi, J.; Sharma, P.K.; Wang, J.; Almakhadmeh, Z.; Tolba, A. Multiple cloud storage mechanism based on blockchain in smart homes. Futur. Gener. Comput. Syst. 2021, 115, 304–313.
74. Oliveira, T.A.; Oliver, M.; Ramalhinho, H. Challenges for Connecting Citizens and Smart Cities: ICT, E-Governance and Blockchain. Sustainability 2020, 12, 2926.
75. Nguyen, D.C.; Ding, M.; Pathirana, P.N.; Seneviratne, A. Blockchain and AI-based solutions to combat corona-virus (COVID-19)-like epidemics: A survey. IEEE Access 2021, 9, 95730–95753.
76. Kumari, A.; Gupta, R.; Tanwar, S.; Kumar, N. Blockchain and AI amalgamation for energy cloud management: Challenges,solutions, and future directions. J. Parallel Distrib. Comput. 2020, 143, 148–166.
77. Kumar, R.;Wang,W.; Kumar, J.; Yang, T.; Khan, A.; Ali,W.; Ali, I. An Integration of blockchain and AI for secure data sharing and detection of CT images for the hospitals. Comput. Med Imaging Graph. 2021, 87, 101812.
78. Mashamba-Thompson, T.P.; Crayton, E.D. Blockchain and Artificial Intelligence Technology for Novel Coronavirus Disease 2019 Self-Testing. Diagnostics 2020, 10, 198.
79. Deebak, B.D.; Fadi, A.T. A robust and distributed architecture for 5G-enabled networks in the smart blockchain era. Comput.Commun. 2021, 181, 293–308.
80. Sharma, A.; Podoplelova, E.; Shapovalov, G.; Tselykh, A.; Tselykh, A. Sustainable Smart Cities: Convergence of Artificial Intelligence and Blockchain. Sustainability 2021, 13, 13076.
81. Atlam, H.F.; Azad, M.A.; Alzahrani, A.G.; Wills, G. A Review of Blockchain in Internet of Things and AI. Big Data Cogn. Comput.2020, 4, 28.
82. Abid, A.; Cheikhrouhou, S.; Kallel, S.; Jmaiel, M. NovidChain: Blockchain-based privacy-preserving platform for COVID-19 test/vaccine certificates. Softw. Pract. Exp. 2021, 52, 841–867.
83. Xu, H.; Zhang, L.; Onireti, O.; Fang, Y.; Buchanan,W.J.; Imran, M.A. Beeptrace: Blockchain-enabled priva-cy-preserving contact tracing for COVID-19 pandemic and beyond. IEEE Internet Things J. 2020, 8, 3915–3929.
84. AlShamsi, M.; Salloum, S.A.; Alshurideh, M.; Abdallah, S. Artificial Intelligence and Blockchain for Transparency in Governance. In Artificial Intelligence for Sustainable Development: Theory, Practice and Future Applications; Springer: Cham, Switzerland, 2020;pp. 219–230.
85. Singh, S.K.; Rathore, S.; Park, J.H. BlockIoTIntelligence: A Blockchain-enabled Intelligent IoT Architecture with Artificial Intelligence. Futur. Gener. Comput. Syst. 2020, 110, 721–743.
86. Shafagh, H.; Burkhalter, L.; Hithnawi, A.; Duquennoy, S. Towards blockchain-based auditable storage and sharing of IoT data. In Proceedings of the 2017 on Cloud Computing Security Workshop, Dallas, TX, USA, 3 November 2017; pp. 45–50.
87. Alkadi, O.; Moustafa, N.; Turnbull, B.; Choo, K.-K.R. A deep blockchain framework-enabled collaborative intrusion de-tection for protecting IoT and cloud networks. IEEE Internet Things J. 2020, 8, 9463–9472. [CrossRef]
88. Sharma, P.K.; Chen, M.-Y.; Park, J.H. A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT.IEEE Access 2017, 6, 115–124.

89. Liu, S.; Yu, J.; Xiao, Y.; Wan, Z.; Wang, S.; Yan, B. BC-SABE: Blockchain-aided searchable attribute-based encryption for cloud-IoT.IEEE Internet Things J. 2020, 7, 7851–7867.
90. Zhang, L.; Zou, Y.; Wang, W.; Jin, Z.; Su, Y.; Chen, H. Resource allocation and trust computing for blockchain-enabled edge computing system. Comput. Secur. 2021, 105, 102249.
91. Fan, Y.;Wang, L.;Wu,W.; Du, D. Cloud/edge computing resource allocation and pricing for mobile blockchain: An itera-tive greedy and search approach. IEEE Trans. Comput. Soc. Syst. 2021, 8, 451–463.
92. Bai, F.; Shen, T.; Yu, Z.; Zeng, K.; Gong, B. Trustworthy blockchain-empowered collaborative edge compu-ting-as-a-service scheduling and data sharing in the IIoE. IEEE Internet Things J. 2021. [CrossRef]
93. Qu, G.; Cui, N.; Wu, H.; Li, R.; Ding, Y. ChainFL: A Simulation Platform for Joint Federated Learning and Blockchain in Edge/Cloud Computing Environments. IEEE Trans. Ind. Inform. 2021, 18, 3572–3581.
94. Alrubei, S.; Ball, E.; Rigelsford, J. The Use of Blockchain to Support Distributed AI Implementation in IoT Systems. IEEE Internet Things J. 2021.
95. Nawaz, A.; Gia, T.N.; Queralta, J.P.;Westerlund, T. Edge AI and blockchain for privacy-critical and da-ta-sensitive applications. In Proceedings of the 2019 Twelfth International Conference on Mobile Computing and Ubiquitous Network (ICMU), Kathmandu,Nepal, 4–6 November 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–2.
96. Das, A.K.; Bera, B.; Giri, D. Ai and blockchain-based cloud-assisted secure vaccine distribution and tracking in iomt-enabled COVID-19 environment. IEEE Internet Things Mag. 2021, 4, 26–32.
97. Gharbi, C.; Hsairi, L.; Zagrouba, E. A Secure Integrated Fog Cloud-IoT Architecture based on Multi-Agents Sys-tem and Blockchain. In Proceedings of the ICAART, Online, 4–6 February 2021; pp. 1184–1191.
98. Rathore, S.; Park, J.H. A Blockchain-Based Deep Learning Approach for Cyber Security in Next Generation Industrial Cyber-Physical Systems. IEEE Trans. Ind. Inform. 2020, 17, 5522–5532.
99. Medhane, D.V.; Sangaiah, A.K.; Hossain, M.S.; Muhammad, G.;Wang, J. Blockchain-Enabled Distributed Security Framework for Next-Generation IoT: An Edge Cloud and Software-Defined Network-Integrated Approach. IEEE Internet Things J. 2020, 7,6143–6149.
100. Scopus. Available online: https://www.scopus.com (accessed on 1 February 2022).
101. Rimba, P.; Tran, A.B.; Weber, I.; Staples, M.; Ponomarev, A.; Xu, X. Comparing blockchain and cloud services for business process execution. In Proceedings of the 2017 IEEE International Conference on Software Architecture (ICSA), Gothenburg, Sweden, 5–7 April 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 257–260.
102. Gai, K.; Guo, J.; Zhu, L.; Yu, S. Blockchain Meets Cloud Computing: A Survey. IEEE Commun. Surv. Tutor. 2020, 22, 2009–2030.
103. Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. Integration of blockchain and cloud of things: Archi-tecture, applications and challenges. IEEE Commun. Surv. Tutor. 2020, 22, 2521–2549.
104. Abhirup Khanna,Anushree Sah,Blockchain–Cloud Integration: A Survey,Sensors 2022, 22, 5238