Blockchain-Cloud Integration: Comprehensive Survey and Open Research Issues

Houaida Ghanmi (houaida.ghanmi22@gmail.com)
Manouba University
Nasreddine Hajlaoui
Qassim University
Haifa Touati
University of Gabès
Mohamed Hadded
Abu Dhabi University
Paul Muhlethaler
National Institute for Research in Digital Science and Technology (INRIA)

Research Article

Keywords: Cloud Security, Blockchain, Data Sharing, Access control, Privacy, Integrity

Posted Date: May 30th, 2023

DOI: https://doi.org/10.21203/rs.3.rs-2980314/v1

Additional Declarations: No competing interests reported.

Blockchain-Cloud Integration: Comprehensive Survey and Open Research Issues

Houaida Ghanmi[a,1,2], **Nasreddine Hajlaoui**[b,1,3] **Haifa Touati** [c,1] **Mohamed Hadded**[d,4] **and Paul Muhlethaler**[e,5]

[1]Hatem Bettaher IResCoMath Research Lab, University of Gabes, Gabes 6033, Tunisia
[2]National School of Computer Science (ENSI), University of Manouba, Manouba 2011, Tunisia
[3]Unit of Scientific Research, Applied College, Qassim University, Unayzah 56435, Saudi Arabia
[4]Abu Dhabi University, Abu Dhabi, United Arab Emirates
[5]National Institute for Research in Digital Science and Technology (INRIA), 78150 Paris, France

Received: date / Accepted: date

Abstract Cloud computing has attracted great interest in various scientific and technical fields recently as one of the widely adopted networking technologies. Despite their many benefits and applications, it still faces many security and trust challenges, including managing and controlling services, privacy, data integrity in distributed databases, data backup, and synchronization. Moreover, due to its centralized architecture, and lack of transparency and traceability, the results of the trust assessment cannot be fully recognized by all users. However, creating a trust-based transaction environment has become its key factor. Blockchain, with its nature of decentralization and security, can be leveraged to address these challenges and build a distributed and decentralized trust architecture, due to the underlying characteristics such as transparency, traceability, decentralization, security, immutability, and automation. This article makes a comprehensive study of how Blockchain is applied to deliver security services in the cloud computing model, focusing on up-to-date approaches, opportunities, and future directions. This survey also discusses the benefits of the technical fusion of Blockchain and cloud. It provides a classification of proposed systems based on privacy and key sharing, data sharing, authentication, and access control, as well as auditing and data integrity. Finally, the main conclusions of this study will be the challenges and future directions to stimulate further research in this promising field.

Keywords Cloud Security, Blockchain, Data Sharing, Access control, Privacy, Integrity

[a]e-mail: houaida.ghanmi22@gmail.com
[b]e-mail: nasreddine.hajlaoui@fsg.rnu.tn
[c]e-mail: haifa.touati@cristal.rnu.tn
[d]e-mail: haddedmohamed88@gmail.com
[e]e-mail: paul.muhlethaler@inria.fr

1 Introduction

With the unlimited expansion of resource sharing, cloud computing has become one of the hottest computing research issues in recent years and has attracted the attention of the scientific community and businesses. It is a well-defined technology that has emerged from large-scale distributed computing technology. There are many advantages such as flexibility with a highly automated process, worldwide availability, reduced hardware and maintenance costs, and resource pooling with rapid elasticity via the Internet from portable devices [1].

Although one of the greatest innovations in the field of computing is the storage and remote access to data in the cloud, there are many security, and trust issues concerning this technology [2]. One of the main problems with cloud storage is the lack of transparency, traceability, and control over the data stored. In other words, users do not know where their data is stored, how and when it is processed, or even if their data is lost or compromised. Another problem with such systems is a lack of trust. Since users and service providers typically do not sign formal contracts, there is no legal framework for users to claim compensation if their data is damaged, leaked, or sold to third-party companies. Additionally, the traditional cloud security trust model typically adopts a centralized architecture, resulting in significant management overhead, network congestion, and even a single point of failure.

Moreover, compromised cloud service providers can also pose huge security breach risks to users. For example, a for-profit CSP (Cloud Service Provider) may delete infrequently accessed outsourcing data without users' permission and may even alter some data to gain economic benefits [3]. Therefore, it is essential to design a schema to verify whether the data stored in the cloud is intact. To ensure the

integrity of remote data, many researchers have proposed the use of a private audit between the CSP and the DO (Data Owner), where the DO generates a challenge to the CSP and verifies the corresponding evidence of the CSP to verify data integrity. However, the limitation of this solution (private audit) is that the verification procedure is only performed by the DO, which means that the DOs will bear a large computational load due to the increase in data volume and audit requests. Due to the inherent nature of the cloud, its security gaps cannot be fully closed despite the development of improved security solutions over the past few years.

As an emerging decentralized framework and distributed computing paradigm, Blockchain is considered an adaptable alternative to establishing a trusted platform due to a few of its features, e.g. transparency, traceability, decentralization, security, immutability, and automation. It is a distributed ledger that stores tamper-proof data in the form of a string without going through trusted intermediaries (central authority). Blockchain was first proposed by Nakamoto [4], which provides a decentralized network, where all nodes are equal and no control center exists. It has been widely accepted that Blockchain can not only be used in financial services such as Bitcoin but also implemented in application-oriented scenarios [5]. In this context, smart contracts are software used to facilitate, verify and enforce the negotiation of a transaction on a Blockchain platform as it introduces the capability of automatic control [6]. Since its proposal in 2008, Blockchain technology has witnessed a growing integration across various domains, including but not limited to C-ITS (Cooperative Intelligent Transport Systems) [7, 8], IoT (Internet of Things), and recently extending into the realm of cloud computing. In fact, to facilitate the growth of cloud computing, we can overcome access control and data security issues by integrating Blockchain technology. Table 1 shows the comparison of our survey with other existing surveys. Unfortunately, a concise, service-oriented review of Blockchain-cloud integration is missing. For that, this survey focuses on the technical fusion of Blockchain and cloud computing and discusses current trends, classifications, and unresolved difficulties. This survey aims to indicate recent research on Blockchains that can be used to power cloud systems or these new mechanisms to empower Blockchain systems using cloud-based approaches. The 21 most representative articles have been selected in this article. These valuable methods are analyzed, classified, and compared.

1.1 Literature review of existing surveys

In recent years, the security of data stored in a cloud environment has attracted the attention of many researchers. According to our review of the existing literature, a Blockchain-based approach is currently the most reliable way to achieve distributed and decentralized storage. Several surveys have been published on similar topics in recent years. Table 1 reviews related literature surveys on trust approaches incorporating cloud computing and Blockchain technology. These surveys mainly concern the introduction and integration of Blockchain technology with cloud computing [18], [20], [16] and integrity audit for cloud data [19]. These surveys are chosen according to the following main criteria: we have selected recent surveys published between 2019 and 2022, which deal with topics in the field of cloud integration with Blockchain to strengthen the level of data security.

Gai, Keke, et al. [13] conducted a survey that provides recent Blockchain studies that can be used to power cloud systems or those new mechanisms that use cloud-based methods to empower Blockchain systems. In this study, the authors neglected to compare the diagrams presented nor to identify the limits of each solution.

Although the investigation in [20] presents an overview of the use of Blockchain for cloud exchange, they only provide brief introductions on this topic without in-depth investigation, unlike our article.

The survey [9] focuses on the application of Blockchain technology in cloud data security after analyzing the threats in the cloud environment. In this investigation, the authors did not cover the most recent Blockchain technology mechanisms, especially those based on decentralized storage techniques. Murthy, Bharathi, et al. [11] briefly introduced cloud computing, and Blockchain technology, and discussed the benefits of integrating the Blockchain network with a scalable cloud environment. This survey did not cover recent solutions and focused on the benefits that Blockchain brings to cloud computing.

Li, Wenjuan, et al. [15] conducted a review of Blockchain-based trust management approaches in cloud computing systems. Also, they presented a comparison of existing Blockchain-based trust approaches. Despite the good analysis, they did not take into consideration several evaluation criteria. In addition, the study did not consider cloud-stored data integrity audit mechanisms and briefly discussed access control mechanisms.

Although the survey [10] examines the main challenges that can be solved by integrating cloud computing with Blockchain technology, it is very short and deals with solutions that have not been updated.

Soumik Sarker et al. [12] presented a review on Blockchain-cloud integration services. In this survey, the authors studied the industrial approaches and research approaches of "Blockchain as a service" technology, but they did not mention the mechanisms and protocols necessary to show the effectiveness of this technology.

The authors in [14] focused on introducing Blockchain-based storage systems and how they work, a comparison of these systems with cloud-based storage networks, and their

Table 1: Related surveys

Ref [1]	Publication	NSS [2]	Period	Idea of paper	Research Challenges
[9]	2019	13	2016-2019	Summarizes the classification of current Blockchain technology to address cloud data security issues	Improving Blockchain encryption algorithms and consensus mechanisms
[10]	2020	8	2012-2019	Investigation of solving cloud computing problems using Blockchain	-
[11]	2020	20	2016-2019	Discuss the benefits of integrating Blockchain with a cloud to build trust and data security	Blockchain scalability and data privacy
[12]	2020	19	2017-2020	Provide a service-focused review of Blockchain-cloud integration	Blockchains scalability and privacy
[13]	2020	48	2016-2019	Learn how Blockchain technology into currently deployed cloud solutions	High performance in the fits field of Blockchain-cloud
[14]	2020	17	2017-2019	A study on Blockchain-based storage systems and how they work	Scalability issues, lack of legal constraints and Access control
[15]	2021	33	2017-2020	Study Blockchain-based trust approaches in cloud computing systems.	Adaptability of Blockchain trust management, data privacy, and risk control.
[16]	2021	26	2016-2020	Investigate how Blockchain is applied to provide security services for the cloud computing.	Mixed Blockchain-cloud and challenges faced by cloud computing itself.
[17]	2022	28	2016-2019	Reviews the challenges of trust in cloud computing and analyzes how Blockchain addresses these challenges.	Energy efficiency Solutions, integrating, learning and Blockchain edge computing.
[18]	2022	18	2017-2021	Examine release patterns in areas of Blockchain technology associated with cloud computing, healthcare, and finance.	Challenges of scalability, power consumption and infrastructure requirements.
[19]	2022	13	2015-2020	Give a comprehensive evaluation and benchmarking of Blockchain-based cloud data integrity audit systems.	Data recovery, reputation evaluation, and attack detection and defense.
Our survey	2023	29	2019-2022	Study how to apply Blockchain to provide access control, data sharing, auditing, and data privacy for cloud computing.	Design a CSP reputation assessment mechanism, need for decentralized user identity management, and solve the scalability scalability problem.

[1] References
[2] Number of solutions studied

advantages. Thus, the different techniques of consensus protocols in each group are also explored. However, this survey did not cover recent solutions. Moreover, the authors focus on the theoretical explanation of each mechanism without making an effective comparison.

Jinglin Zou, et al. [16] presented an in-depth study of how Blockchain is applied to provide security services in the cloud computing model, classifying and discussing them. They lightly discussed proposed solutions to address security challenges in the cloud. Moreover, the study did not take into account the comparison of the methods proposed in the literature or identify their limits.

1.2 Motivation and main contributions

Motivated by the above observations, we provide a comprehensive survey of Blockchain for storing data in an untrusted environment, services fundamental knowledge, up-to-date approaches, opportunities, research challenges, issues, and future directions. The main objective of this survey is to give an in-depth analysis of the latest research on Blockchain technology and its applications in powering cloud systems. The study's most important contributions can be summarized as follows:

- We identify the most important security policies and requirements associated with using an untrusted cloud service provider and the security issues associated with their use.
- We define a new classification of Blockchain applications in cloud systems. We identify four categories based on their security services: Privacy and Key Sharing, Data Sharing, Authentication and Access Control, Audit, and Data Integrity. A summary is given at the end of each category in order to specify the usefulness of the Blockchain

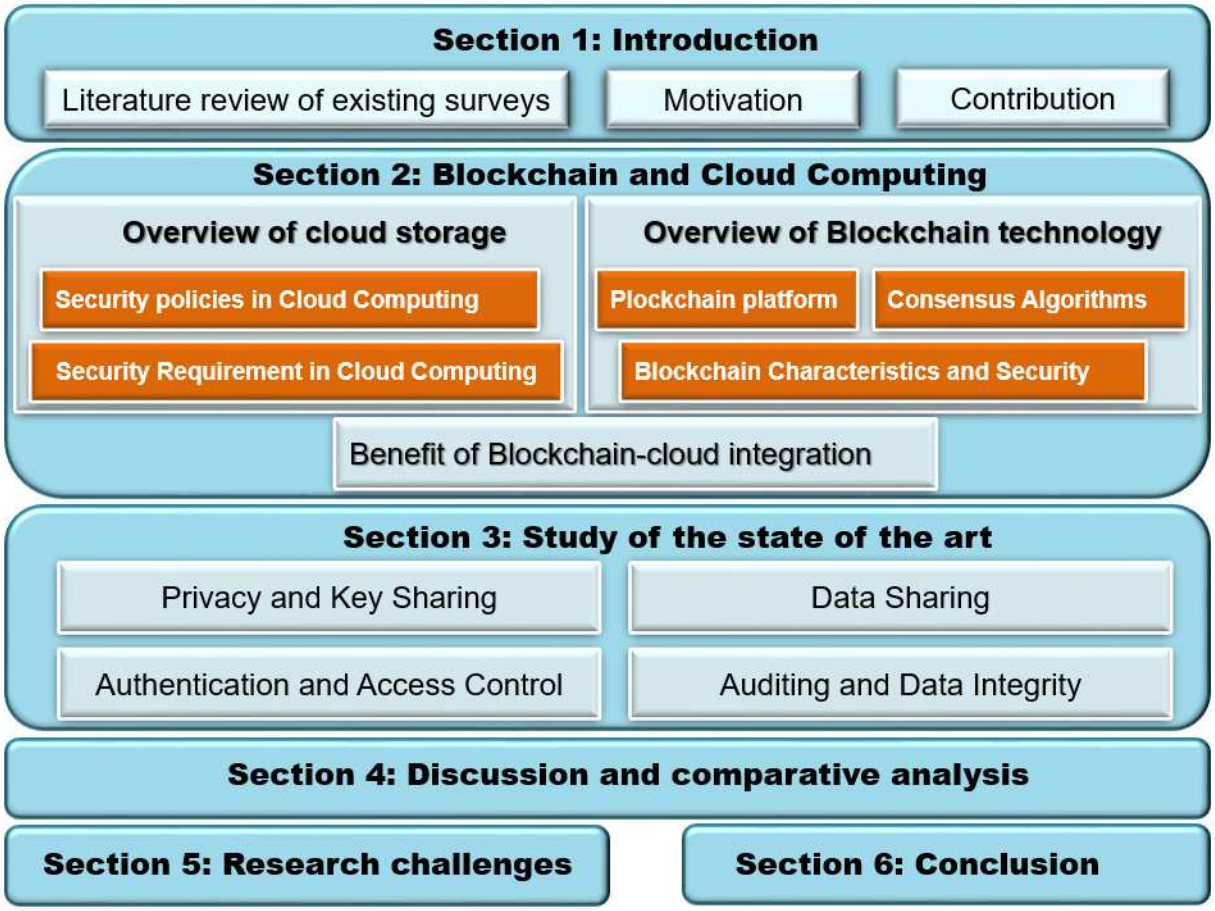

Fig. 1: Survey outline.

for each of them. Our classification could help academics and industry improve their understanding of this emerging research area.
- We provide an in-depth comparison of the solutions discussed in order to identify the strengths and weaknesses of each proposal and to identify the main issues of each architecture that proposes to integrate Blockchain technology into cloud computing environments.
- Finally, we discuss a number of research challenges, including cloud data access control challenges, cloud user authentication challenges, latency challenges,. . . , to guide scientists and practitioners, and show them where they should focus their future research.

1.3 The organization of the survey

The organizational structure of this survey is shown in Fig. 1. In Section 2, we provide an overview of cloud and Blockchain technology as well as the motivations behind using Blockchain for the cloud. The benefits of using Blockchain in several applications and its great potential to improve the security of data stored in the cloud are discussed in the same section. Then, Section 3 describes a comparative analysis of relevant recent works based on different Blockchain-based security services in the cloud computing model. Additionally, we synthesize the work on methods for integrating the cloud with Blockchain. Section 4 highlights and summarizes current research challenges and solutions. Finally, the investigation is concluded in section 5. The acronyms used in this paper are listed in Table 2.

2 Blockchain and cloud computing

Before delving deeper into the state of the art on Blockchains in cloud computing, it is necessary to introduce several basic concepts on Blockchain technology and cloud systems. Hence, in this section, we will provide a brief background on cloud storage and Blockchain operations, followed by highlighting the key advantages that emerge from the integration of Blockchain and cloud computing.

Table 2: Abbreviations

CSP	Cloud Services Providers	DO	Data Owner
NSS	Number of Solutions Studied	TPA	Third Party Auditor
MHT	Merkle Hash Tree	MT	Merkle Tree
PoW	Proof of Work	PoS	Proof of Stake
DSL	Domain Specific Languages	DGA	Directed Acyclic Graph
P2P	Peer-to-Peer	DPoS	Delegated Proof of Stake
PBFT	Practical Byzantine Fault Tolerance	UNL	Unique Node Liste
PoA	Proof of Authority	ABE	Attribute-Based Encryption
AES	Advanced Encryption Standard	IBE	Identity Based Encryption
IBS	Identity Based Signatures	IoT	Internet of Things
IPFS	Interplanetary File System	EMRs	Electronic Medical Records
ECC	Elliptic curve cryptography	CP-ABE	Ciphertext Policy Attribute Based Encryption
SHA	Secure Hash Algorithm	RSA	Rivest Shamir Adleman
DSN	Decentralized Storage Networks	C-ITS	Cooperative Intelligent Transport Systems
IoT	Internet of Things		

2.1 Overview of cloud storage

Cloud computing is the use of a network of remote servers to store, manage and process data on demand from any corner of the world. Cloud computing applications and services such as data storage are delivered to organizational devices via the Internet [21]. Cloud computing offers many advantages through services (based on pay-as-you-go regulation) combining data centers, resources, and servers on the Internet. The services are available all over the world and with a much cheaper payment, which reduces the cost of investing in new local resources and thus improves collaboration between companies. Automatic updating of software present in the cloud makes the cloud easily manageable. It also has some limitations due to its rapid growth, which also increases security concerns for cloud developers [22]. As user data is stored in a cloud environment and controlled by centralized third parties like in[23, 24], this introduces new security challenges in managing and controlling secure services, privacy, data confidentiality, protection of data integrity in distributed databases, data backup, synchronization and the procedures necessary for their processing. Therefore, the lack of security in the cloud can lead to a loss of user confidence.

A) Security policies in Cloud Computing
The use of cloud computing has offered several advantages and has simplified certain tasks, but it has also raised new security issues. There are likely a large number of distinct vulnerabilities that can be exploited by malicious actors, due to various types of data being scattered across the network and stored in a variety of cloud services. Technologies such as data storage outsourcing, virtualization, multi-tenancy, and big data make users fear the risk of privacy leakage, as shown in Fig. 2 below.

- **Security of confidential data:** Security risks such as leaks of confidential data in the cloud, confidential disclosure, management of access rights, and difficulties in data destruction are particularly important, due to the outsourcing model of services.
- **Cloud data storage:** Data security in cloud centers is the responsibility of service providers rather than the user. The information is physically stored on a large number of servers, and the user management of these records is controlled by legal contracts. Concerns about storage, availability, privacy; and other types of security have arisen as a direct result of data management issues. Moreover, the service provider has a monopoly on the formulation of the terms and conditions while the users have no role in the creation of the contract. Additionally, there is a growing need for distributed computing systems to store data in a manner that is both secure and accessible [25].
- **Identity and access management:** Identity and access management, which is a policy-based framework for controlling digital identity within an organization, is one of the major requirements of cloud security. Access management systems to identity are required to take all necessary measures to ensure the security of user credentials during storage and registration, as well as to prevent any possibility of predicting the encryption key with brute force attacks or by cryptanalysis [26].
- **Authentication:** A fundamental authentication method that does not allow access to data from a variety of cloud service providers. Ensuring that only legiti-

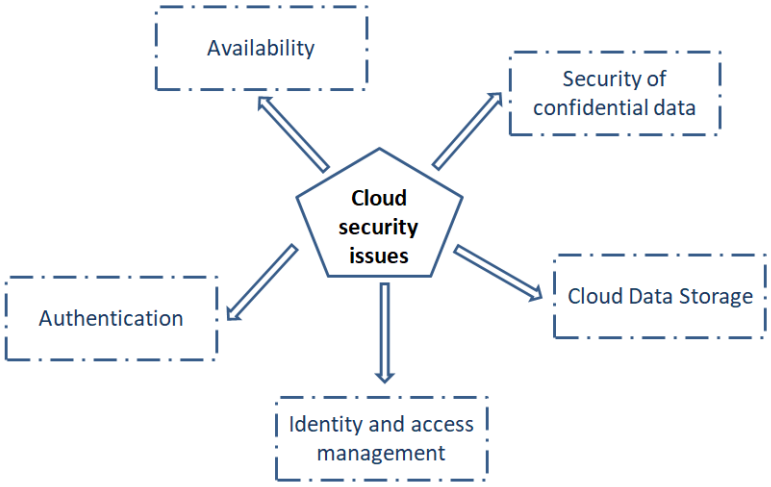

Fig. 2: Taxonomy of Cloud security issues.

mate users have access to data is a challenge for cloud service providers when users need to be able to access their applications from anywhere and from any device such as mobile phones, tablets, laptops, smart TVs, etc. In addition, it should be noted that there are various authentication threats and attacks in the cloud environment, such as password discovery attacks, cookie response attacks, man-in-the-middle attacks, medium, and many others.

- **Availability:** The centralization of cloud systems can lead to several issues such as single point of failure vulnerability and falsification of data information. Meanwhile, malicious users who have hacked into the system can modify the data as they wish. Additionally, rogue cloud providers may display harassing advertisements when users search for appropriate resources. This highlights the need for a decentralized system.

B) Security requirement in Cloud Computing

- **Data sharing**
  With the opening of the cloud and the sharing of virtualized resources by the multi-tenant, the data of the owners of the data can be accessed by other unauthorized users [27]. However, data encryption can improve the security and privacy of data stored in the cloud so that the CSP can schedule data backups. In addition to storing and sharing data reliably, it is also important to transmit data securely between users. Data sharing involves the questions of when and where data is encrypted, when and where it is decrypted, and the methods used to share the encryption key.
- **Data integrity**
  Cloud computing has been seen as a good solution to the problem of growing data storage costs [28]. A growing number of businesses and individual users are choosing to store and process their data with cloud computing services. Users can access data held by the cloud anytime via the Internet. This means that data integrity may be compromised when stored in the cloud (the likelihood that the data has not been altered or destroyed is not guaranteed). Therefore, one of the critical customer concerns to address is ensuring the integrity and accuracy of their data in the cloud.
- **Data auditing**
  For many enterprises and users, the remaining barriers to adopting cloud computing services are related to security. One such significant security issue is the lack of audibility for various aspects of security [29]. However, the user must regularly check the integrity of the data, and frequent interaction with the CSP and auditing operations can lead to significant consumption of computer resources. Thus, the user can verify the integrity of outsourced data via a remote public data audit solution. However, the auditing procedure has a large computational load, which employs a third-party auditor (TPA) to perform the auditing task on behalf of the users and the users only need to know the audit results of the TPA. While in most existing public auditing systems, TPA is a centralized party and was considered completely trustworthy, which also raises security risks. For example, if an irresponsible TPA only tells the user that the audit results are correct in every audit without performing an actual audit, the user's data will be at great risk.
- **Authentication and access control**

  Identity authentication and access control ensure that participants in cloud marketplaces, including service providers and users, are authenticated legitimate nodes [30]. It is undeniable that the identification and authentication mechanisms of systems must deal with vulnerabilities to avoid exposing sensitive information. Moreover, an unreliable access control method can also affect other functions, such as authentication, authorization, and data auditing. A common weakness of traditional access control mechanisms is that they generally require a third-party management center, which can lead to security risks and generally lacks transparency, traceability, inviolability, and governance.

2.2 Overview of Blockchain technology

The term Blockchain was first introduced by Satoshi Nakamoto in [4]. Blockchain technology is informally defined as a distributed database (peer-to-peer network) that records all transactions that occur in the network in which smart contracts operate in a decentralized, secure, and reliable manner. Smart contracts [31] are one of the best applications of Blockchain technologies and are also crucial in facilitating the negotiation of a transaction (traceable and irreversible) without third parties in a Blockchain. The history of all transactions is stored in the Blockchain, which makes it immutable and very difficult to tamper with. Nowadays, the use of Blockchain in cloud computing is one of the most common innovations that can solve the challenges of security, anonymity, and data integrity without any third party in a cloud environment because of its underlying characteristics such as transparency, traceability, decentralization, security, immutability, and automation. There are three types of Blockchains as shown in Fig. 3:
As depicted in Fig. 3, three main types of Blockchains exist within the realm of Blockchain technology, namely public, private, and consortium:

(1) The public Blockchain: A public Blockchain is an open and decentralized register in which anyone can connect to the network via a consensus mechanism [32]. Network participants can send, receive and verify transactions by participating in the consensus process. Economic incentives are offered to those involved in the consensus mechanism.

(2) Private Blockchain is a type of centralized Blockchain controlled by a central authority for accessibility (invitation-only Blockchain and managed by an administrator) [33]. Permission to read data is selectively open to the public (only those who get admin permissions can read or write).

(3) Consortium Blockchain: A consortium Blockchain is a partially decentralized chain (a semi-private system) with a group of persons usually belonging to an organization [34]. Its write permissions (permissions can be public or restricted) are limited so that only a pre-selected entity can participate in registry maintenance.

Merkle trees: Data is encrypted with hashing algorithms when a transaction occurs for efficient storage and verification of large sets of data, then it is transmitted to each node. The Merkle tree function was used by the Blockchain to produce a final hash value and Merkle tree root because it could contain thousands of transaction records in each node's block. The root of the tree (Merkle root) contains the hash of all transactions in a block while the leaf nodes contain the hash of the Blockchain transaction. Merkle trees can be used to effectively validate data integrity and its tree takes up very little disk space compared to other data structures. Thus, they can be broken down into small data elements for verification purposes. Several researchers have taken full advantage of the characteristics of the Merkle tree. For example, Yue et al. [35] propose an architecture where the customer data is split into several parts which are built in a Merkle hash tree. Then the client uploads the root of the hash tree to the Blockchain and uploads its data and the Merkle hash trees to the cloud storage servers. When the client needs to verify the integrity of a slice of data, a smart contract calculates the hash value of the data in the Blockchain and compares it with the hash calculated by the cloud to verify the integrity of the data. Fig. 4 gives the representation of the Merkle tree as follows:
Smart contracts: Smart contracts are self-executing contracts launched in 1994 by Nick Szabo, which consist of a group of codes defining the rules governing transactions and are built on an underlying cryptocurrency platform. Users can create their smart contracts in digital form as a series of commitments by writing the logic in a few lines of code to transfer their digital assets without third parties according to predefined arbitrary rules [36]. The data present in the block will be executed within the Blockchain, which offers reliability, uniqueness, traceability, and irreversibility. As smart contract data is present in the Blockchain, the relationship between the parties is built by rules that establish trust between the parties who do not know each other. Some research offers the results that Ethereum is the best example of building smart contracts [37]. Fig. 5 gives the representation of the Smart Contract.

2.2.1 Blockchain platform

In this section, we present the most popular Blockchain platforms available, i.e. whose code is open source: Bitcoin, Ethereum, Hyperledger, and IOTA, as illustrated in Table 3. Note that many different cryptocurrencies exist today [38], comparing cryptocurrency frameworks is beyond the scope of this article, although it is an interesting topic.

- **Bitcoin**
  Bitcoin is the first and most popular distributed and widely used Blockchain platform that introduced Blockchain technology and platform to the world [4]. It offers a reliable, fast, and cheap mechanism to conduct digital financial transactions without the need for a central bank or central authority. Bitcoin enables the implementation of smart contacts using a scripting language to create and send transactions to the Blockchain network. Bitcoin uses the PoW consensus protocol to verify transactions and therefore consumes a lot of energy. Many other alternative cryptocurrencies and consensus protocols have been proposed and developed due to the suc-

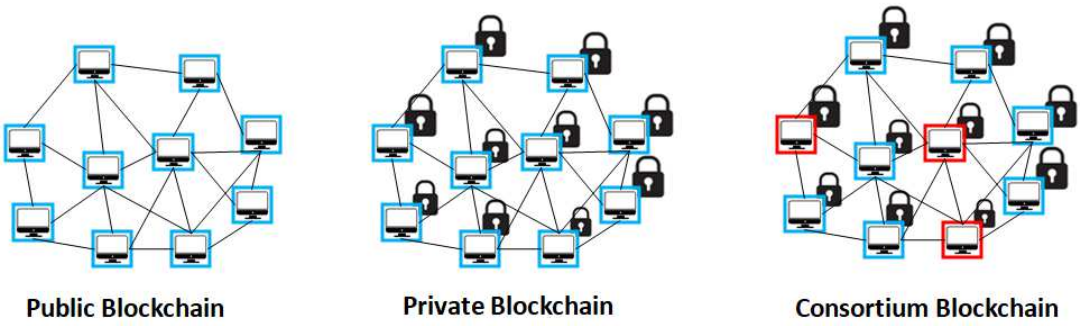

Fig. 3: Blockchain type.

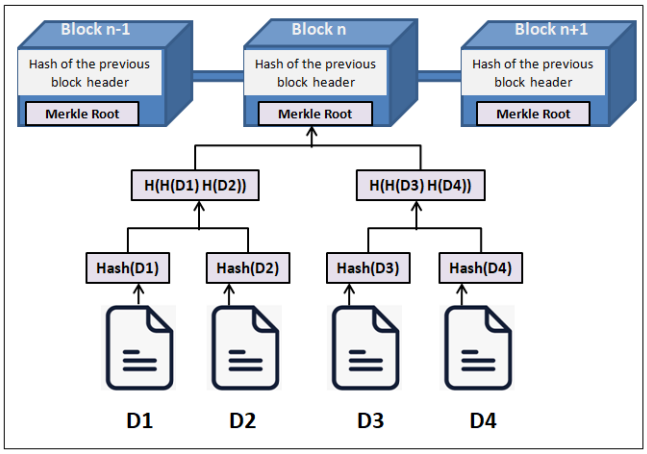

Fig. 4: Structure of Merkle Tree.

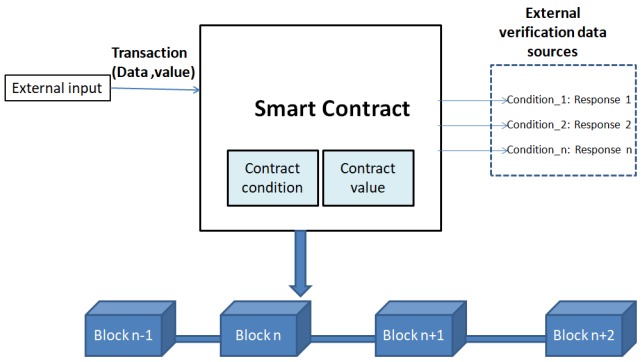

Fig. 5: Structure of Smart Contract.

cess of Bitcoin, including the other platforms reviewed in this study.

– **Ethereum**
Ethereum has proven to be the most well-known platform for creating and using decentralized applications based on smart contracts using an integrated scripting language, named Solidity, which runs on Blockchain technology [39]. In recent years, Ethereum has had a profound effect on the evolution of Blockchain technology. Ethereum makes it possible to apply Blockchain technology not only to cryptocurrencies but also to different fields of application due to the simplicity of creating smart contracts. This has made Ethereum the most popular solution for developing reliable, secure, and decentralized Blockchain applications. It adapts the Proof of Stake consensus protocol. Ethereum is also cryptocurrency-based like Bitcoin, i.e. it manages budgets (measured in gas and paid for by transaction originators) used to pay for transaction fees and services in the network Ethereum.

– **Hyperledger Fabric**
Hyperledger Fabric platform is an open-source Blockchain infrastructure designed for use in private Blockchain systems, it does not have the concept of miners. It is a platform developed under the Linux foundation for use in the enterprise context [40]. As the use of Blockchain should meet different needs, Hyperledger Fabric facilitates the creation of smart contracts using general-purpose scripting languages such as Go, Java, and Node.js rather than domain-specific languages (DSL) limited. Thus, it supported pluggable consensus protocols, allowing the platform to be customized for industry-specific use cases. It should also be noted that Hyperledger has global collaborations with several companies.

– **IOTA**
Similar to Bitcoin and Ethereum, IOTA is a public (permissionless) Blockchain system designed to support IoT applications, and its cryptocurrency is known as MIOTA. The main difference is IOTA organizes transactions in bundles instead of blocks; a single transaction in a bundle cannot be understood or trained independently of other transactions in the bundle. IOTA achieves higher throughput than Bitcoin and Ethereum by organizing bundles in a directed acyclic graph (DAG) rather than blocks in a chain. Typically, a bundle contains related input and output transactions, as well as other types of transac-

tions. The main purpose of aggregating transactions into a block in Bitcoin, Ethereum, and Hyperledger Fabric is to increase the throughput of the consensus protocol used to update the ledger, on the contrary bundles cannot be used at this end because they cannot combine unrelated transactions.

2.2.2 *Blockchain characteristics and security*

- **Traceability**
  In a Blockchain network, blocks are encrypted using hashing algorithms. Each block in the network will have a hash key where a block represents all of the different transactions. It contains the timestamp of the transaction as well as the details of the participants involved in the transaction and the hash key of the previous blocks and is linked through them [45]. Therefore, tracing the block through the hash key is comfortable in the Blockchain network and it provides a full audit trail where we can find the various steps an asset has passed through as it travels through the supply chain.
- **Immutability**
  Immutability simply refers to the permanence of data (i.e. the data in the blocks cannot be tampered with because the data in the blocks is linked via the hash key, and changing the data would invalidate subsequent blocks). Instead of relying on centralized authorities, Blockchain technology works through a collection of nodes and each node in the network has a copy of the digital ledger. When a transaction is initiated, each node checks the validity of the transaction and if the majority of nodes think it is valid, then it is added to the network. This means that without the approval of a majority of nodes, any committed record is irreversible and cannot be changed and no one can just go back and change it [41].
- **Decentralization**
  The Blockchain network adopts a P2P network which has no governing authority that will be responsible for all decisions. This approach eliminates the communication delay problem in traditional systems where nodes must be validated through a centralized trusted server. Each node realizes self-verification, information transmission, and management through distributed storage, and the newly added node can choose to download all or part of the block data from the old nodes to query or verify the block data. This decentralized approach allows participants to not rely on any third-party management institution or hardware facility that could provide complete privacy to users.
- **Consensus**
  The operation of Blockchain frameworks is based on associated consensus algorithms, which are responsible for helping the network make quick and unbiased decisions. This makes the validation process of a transaction faster and similar to a voting system where the majority wins and the minority must support it [42].
- **Data security**
  The decentralized and immutable nature of Blockchain and the use of encryption provide another high level of security to the system. The use of cryptography involves the implementation of complex algorithms that help prevent unauthorized attacks. Every piece of information on the Blockchain is hashed, which means that all blocks contain their unique hash and the hash of the previous block. Any attempt to modify the data means modifying all the hash ids, which is quite impossible, and due to this hash property, the blocks are cryptographically linked to each other.

2.2.3 *Consensus algorithms*

When a block needs to be added to the Blockchain, that block must be verified as valid by all nodes in the network distributed together. Otherwise, some nodes may be maliciously attacked. Consensus algorithms are a kind of protocol that determines which blocks are inserted (added) to the BC and the current state to reach transaction order decisions and filter out invalid transactions. To solve the decision problem, various methods are designed and developed as consensus algorithms. However, in this section, we make a detailed description of the principles of these most important consensus algorithms that are widely used in Blockchain networks. Table 4 details a comparison of various consensus models.

- Proof of Work (PoW):
  POW is the first and oldest Blockchain consensus algorithm introduced by Nakomoto (Nakamoto, 2019) and is used in Bitcoin [4]. The main purpose of consensus models is to perform many calculations to solve a mathematical puzzle. The miners (i.e. the computer trying to solve the mathematical puzzle) will calculate the value which is equal to or less than the consensus value such that this value has a predefined condition. When a miner hits the target value, they broadcast the block to the entire network and all other nodes must mutually confirm the correctness of the hash value. The advantage of the Proof of Work algorithm is its decentralization, high levels of security, and acceptable levels of scalability. On the other hand, although the complexity of the hash function may be scalable, due to the complexity of solving the hash function, solving this puzzle must use a lot of computing power. Therefore, this algorithm is unsuitable for large, fast-growing networks that require many transactions (This process wastes too much of its resources,

Table 3: Comparison of the most popular Blockchain platforms

Features	Bitcoin	Ethereum	Hyperledger Fabric	IOTA
Blockchain type	Public	Public	Private	Public
Smart contract	Yes	Yes	Yes	No support yet
Objectif	Cryptocurrency, store transaction data	Execute smart contracts, store cryptocurrency transactions	Create a Blockchain for industries, store chain code and smart contracts	-
Access Mechanism	Anyone. Decentralized	Anyone. Decentralized	Selected users. Partially decentralized	-
Execution Time	High	High	Low	-
Latency	High	High	Low	-
Throughput	Low	Low	High	-
Block-release timing	10 min	12 s	Configurable	-
Consensus	PoW, PoS. Energy-intensive	PoW, PoS. Energy-intensive	PBFT, Raft. Energy-efficient	-

has a high computational cost, and has large bandwidth requirements).

– Proof of Stake (PoS):
PoS offers a lightweight and power-efficient alternative to PoW without wasting resources. In PoS, the age of a coin is its value multiplied by the time period after its creation, i.e. the longer a node holds the coins, the more rights it can obtain on the network. Proof of Stake (POS) is considered less risky when it comes to the potential of an attack on the network, as the holders of the coins will receive a certain reward based on the age of the coin which makes an attack less advantageous. Moreover, the richest miner in the network would start dominating the others. With the concept of the coin age, the Blockchain no longer relies entirely on proof of work and many Blockchains plan to gradually transition from PoW to PoS [43]. PoS is well-suited for applications that operate in low-power environments.

– Delegated Proof of Stake (DPoS):
DPoS is an advancement of the core concepts of Proof Of Stake and minor node selection is based on delegation. In this process, stakeholders select representatives by vote to validate the blocks. Chosen parties create new blocks one by one as assigned and get rewards. Transactions are finalized faster due to fewer nodes and blocks. The adjunct nodes could reject dishonest stakeholders and the decision is made taking into account the block size and block intervals such that at least 50% of the voting actors believe that decentralization is sufficient. Despite the advantages of this mechanism (scalability, energy efficiency, and low-cost transactions), it is a semi-centralized mechanism and is best used in private Blockchains.

– Practical Byzantine Fault Tolerance (PBFT):
PBFT is like a consensus mechanism introduced in the late 90s by Barbara Liskov and Miguel Castro that can withstand Byzantine flaws. In distributed systems, Byzantine fault tolerance is to guard against system failures using collective decision-making that aims to reduce the influence of faulty nodes. In this method, all nodes must participate in the voting process to add the next block, and the consensus is reached when more than two-thirds of the nodes have a favorable opinion on the block. Otherwise, agreement and consensus cannot be reached. This way, consensus can be achieved faster and more cost-effectively compared to proof-of-work. Hyperledger Fabrics uses PBFT as its consensus algorithm since PBFT handles up to one-third of Byzantine replicas.

– RIPPLE:
In Ripple, we use trusted subnets that are collectively trusted in the existing network. It was developed to solve three main problems that the distributed payment system faces, namely accuracy, agreement, and usefulness. The nodes can be divided into two types in this network: one is a server that participates in the consensus activity and the other is the client which only transfers the funds. Each server will have a unique node list (UNL). The database will ask the nodes present in the UNL to determine whether to post transactions to the ledger and if it gets agreement from more than 80% of all servers, those transactions would be aggregated into the distributed ledger and successfully verified by enough servers.

– Proof of Authority (PoA):
This consensus algorithm aims to give a small, designated number of Blockchain actors the power to validate transactions or interactions with the network and update

its more or less distributed ledger [44]. There are many similarities between PoA and PoS, for example, they do not require mining to generate a new block and hence the rights to generate new blocks are granted to nodes that have proven their authority to do so. The disadvantage of this method is the low level of decentralization it has generated.

2.3 Benefit of Blockchain-cloud integration

Combining Blockchain with cloud computing can improve data security, privacy, and traceability. It can create an immutable and transparent transaction ledger, prevent data tampering, and enable secure data access control. Some of the benefits are below as follows:

Adaptability

Blockchain has amazing information processing techniques to have large-scale exchanges in organizations to enable adaptable Blockchain services. Due to the scalability capabilities of cloud computing, it can provide on-demand services for Blockchain businesses. In this way, an exceptionally versatile coordinated system can be provided with a mixture of Blockchain and cloud computing.

Blockchain for secure data sharing and storage

Blockchain, with its decentralized and immutable nature, is capable of supporting reliable data transmissions and data sharing, to solve the security and privacy issues that remain in traditional data transmission protocols. Users, especially organizations, are reluctant to store sensitive information on a system managed by a trusted third party because there are several issues regarding data application security, privacy leaks, and trust crisis, as well as the centralized data single point of failure. The cloud provider still faces some challenges in terms of security, although encrypting files before storing them in the cloud is one of the solutions. If shared, user data is used illegally and user privacy is compromised. Some mechanisms should be adopted to control access and ensure the confidentiality of data. Blockchain sets a unique hash value for the stored file to provide proof of authenticity for user verification. Decentralized Blockchain can provide the solution to such kind of security issues and helps to ensure safe file storage and avoid a single point of failure. However, the combination of the two (Blockchain and cloud computing) still faces many challenges, including solutions to the single point of failure problem, congestion and availability issues, the balance between optimizing system performance and decentralization, optimization of the use of resources and reduction of costs, and improvement of the quality of service[45].
Considering the existing security issues in storing data in a traditional cloud, researchers have proposed many distributed and Blockchain-based schemes.

Decentralization

Information stored in cloud computing is kept in a centralized server for data management and decision-making, which is one of the major issues from a security perspective; it is possible that this problem can be solved by accepting decentralized Blockchain in cloud computing. Blockchain can solve these problems because in the decentralized framework, the information is stored on many servers, which eliminates the risk of failure of the whole system and there is no more risk of the whole system going down. crash if only one server does it. Moreover, integrating Blockchain with cloud computing is a good possible solution for decentralization and could provide complete privacy to users. However, since there is a lot of duplicate information available on different nodes, a lack of information cannot be a problem.

Tolerance for errors

The Blockchain requires the replication of information on a network of computer servers firmly connected to each other by collaborative clouds. This will minimize the risk of single failure due to disruption of any cloud node so that the Blockchain can provide uninterrupted services and continuous operation.

Scalability

It is very important to have robust powerful data processing services to have high transaction execution, due to the huge number of transactions on large-scale Blockchain applications, to enable scalable Blockchain services. Thus, we can see that the combination of cloud computing and Blockchain can provide a highly scalable integrated system.

Audibility

The most critical threats of cloud storage are privacy leaks and data integrity. Additionally, an auditing scheme based on a trust architecture is becoming increasingly important in the cloud [46]. Users can verify the integrity of outsourced data via a remote data audit solution, however, the audit procedure has a heavy computational load, which employs a third-party auditor (TPA) to perform the task of the audit. But, TPA is not so reliable, it may collude with CSP or users for activating economic benefits, or some users may maliciously declare data loss for high compensation. Meanwhile, the emergence of Blockchain technology and its advantage of decentralization, trustless consensus, inviolability, and traceability, can provide a new research idea to solve the problem of mutual trust. With a decentralized public audit scheme for Blockchain-based cloud storage, the audit task was assigned to multiple CSPs, and Blockchain technology was used to record the audit process.

Table 4: Blockchain consensus algorithm

Protocol type	Block creating speed	Powerful hardware	Byzantine fault tolerance	Energy saving	Example	Scalability
PoW	high	Very important	50%	No	Bitcoin	High
PoS	Low	No need	50%	Patial	Ethereum	High
DPoS	Medium	No need	50%	Partial	Bitshares	High
PBFT	Fast	Important	33%	Yes	Hyperleger Fabric	Low
RIPPLE	Low	No need	-	Yes	Ripple	-
PoA	Low	No need	-	Yes	VeChain	-

3 Study of the state of the art

In this section, we categorize the reviewed articles into four subcategories based on their security services: Privacy and Key Sharing, Data Sharing, Authentication and Access Control, Auditing, and Data Integrity, as shown in Fig. 6. To select articles that have the same subject as our survey, we used the following keywords; Cloud storage based on Blockchain technology, Blockchain access control, and data audit,. . . , and we have selected recent articles published from 2018 to 2023. We analyze and describe the issues covered by the four categories of articles and the solutions they offer. In each category, we further categorize the items according to the application scenarios. The main Blockchain-based cloud computing solutions are summarized and compared in Table 5.

3.1 Privacy and key sharing

Privacy and secure key sharing are considered highly relevant to cloud data security, along with other security attributes that have positive or negative influences on privacy. Key management forms the basis of all data security since keys ensure the secure transmission of data over an Internet connection. Well-protected keys should only be accessible to users who need them, as the loss or compromise of any encryption key would invalidate the data security measures in place. However, to ensure that only authorized users can read or access data, good key management should ensure high levels of security around encrypted data.

In this context, the authors of [47] proposed a decentralized storage mechanism with the Ethereum Blockchain to develop a data storage and sharing scheme for decentralized cloud storage systems. Under the proposed framework, shared data is stored in the cloud, while metadata such as hash values or user address information can be kept securely on the Blockchain for sharing, to overcome the risks of centralized storage, i.e. leakage of sensitive data and a single point of failure. The data holder can encrypt the shared information by specifying the access policy and technique that has been used with fine-grained data access control, then forwarding the secret key to authorized users. The limitation of this work is that data owners were responsible for all required tasks, from generating secret keys to encrypting files to setting up a secure channel to communicate with another party (users allowed).

However, the paper [48] proposed an accurate Blockchain-based timestamp scheme for data outsourcing to solve the traditional timestamp problem that requires a credible third-party provider. This system could guarantee the accuracy, security, and scalability of cloud storage.

Feng et al. [49] proposed a Blockchain-based privacy protection scheme based on zero-knowledge proof combined with smart contracts for secure data sharing between data owners and cloud service providers. This scheme stores sensitive data encrypted in the cloud and maintains the hash and digital signature in the Blockchain. By combining zero-knowledge proof and smart contracts, they aim at the availability of data between the owner and the requester with the aim of protecting data privacy. Although in their use case, full data traceability is important, for a fully anonymous data-sharing system the data must be untraceable. Moreover, this model is still in the research phase and has not yet been implemented.

Sukhodolskiy et al. [50] provided the distributed ledger, based on the Blockchain to protect the privacy of cryptographic operations such as key generation and access policy assignment. Files are stored in the cloud after being encrypted by the attribute encryption scheme on the user device and the cloud file location, access policies, and additional owner information are recorded in the Blockchain, thanks to a smart contract. The system provides all security-significant immutable event logs, but these works only consider single-cloud aspects and do not concern themselves with the decentralized sharing of resources across multiple clouds.

Wang et al. [51] designed a cloud-assisted consortium Blockchain-based framework to store and share electronic health data and maintain privacy using searchable encryption and proxy

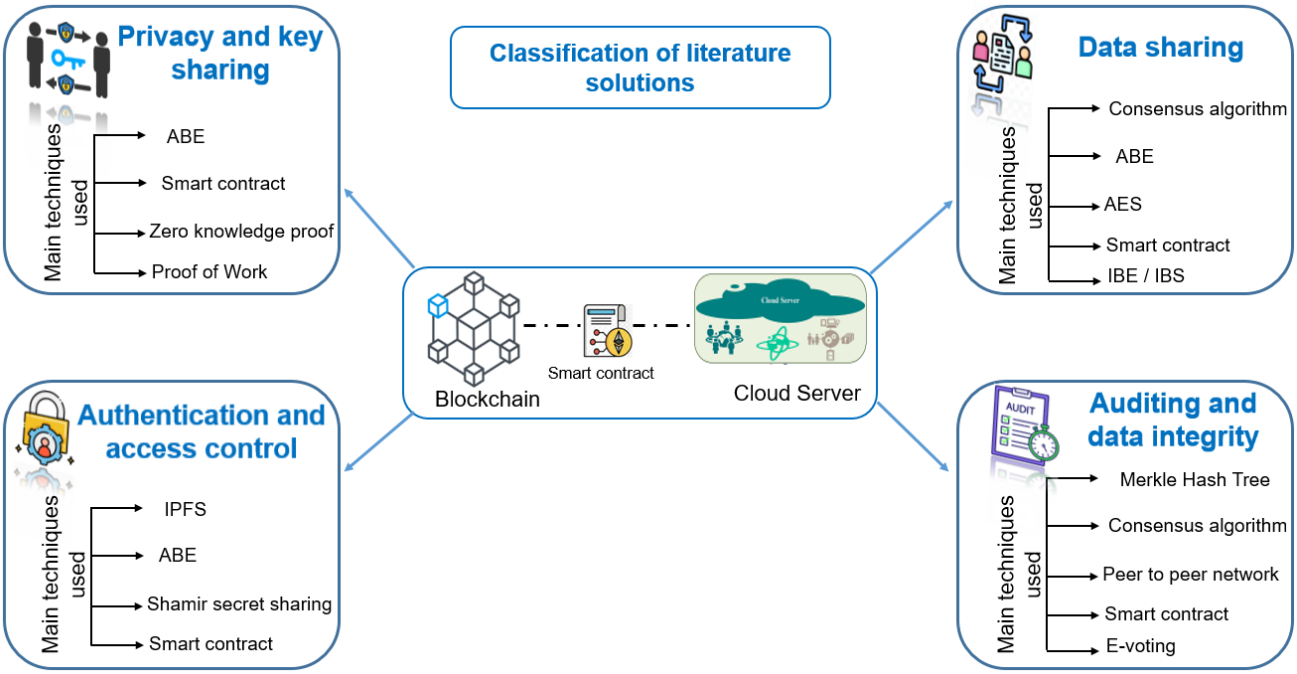

Fig. 6: Blockchain-based solutions and used techniques.

re-encryption. They defined block and transaction structure and implemented primitive cryptographic protocols to store data securely and used public-key encryption with keyword search to ensure data security. Public key encryption with joint keyword search allows data users to search a document containing multiple keywords on a public key encryption setting. Also, only the authorized DR can decrypt the target ciphertext using their private key with the correct file location and keyword. This scheme however cannot be fully efficient as it involves a semi-trusted part which affects the overall security of the architecture and it requires more processing time due to the involvement of proxy servers.

3.2 Data sharing

Shen, Meng, et al. [52] have proposed a new architecture to describe the Blockchain application in a multi-cloud environment, to improve the security and efficiency of data sharing, where data is shared via Blockchain and recorded by a smart contract. This architecture has four parts which are, data owners, data service agents, Blockchain network, and cloud users. All data management behaviors have been recorded in the Blockchain network. However, the main contribution of the paper includes building a dynamic and fair data sharing and incentive mechanism using Shapley's value. But, the problem with this model is that it is not a completely decentralized trust model, since the deployment of the model still relied on a credible third-party agency.

L. Zhu, et al. [53] established a data management system using a Blockchain-distributed consensus mechanism and a third-party trust center for cloud computing systems. The uniqueness of this work is that it uses both ordinary voting nodes and higher-level third-party trust agencies for transaction verification, which can be seen as a compromise between Blockchain and traditional centralized architecture. Although this model has improved the efficiency of consensus and network management, it is not a completely decentralized and scalable trust model.

Paper [54] proposed a model that can provide energy-efficient data collection and security for data sharing in a distributed environment. Each Merkle Tree (MT), provides extensive data collection and maximum range for sensing devices. MTs share data while an Ethereum Blockchain platform is used to ensure data reliability and security. Ethereum maintains a secure, shared distributed ledger with cooperating MTs without a trusted third party. This approach offers solutions for various attacks such as majority attacks, device failure, eclipse attacks, etc.

Gousteris, Solonas, et al. [55] proposed a general secure cloud data storage system that supports confidentiality, integrity, and availability. In this work, the researchers used the Blockchain Ethereum and its Smart Contracts to guarantee data availability and integrity. The RSA encryption scheme has been used to provide confidentiality of sensitive data and source authentication through the storage of public keys in Ethereum smart contracts. However, this work has

some shortcomings such as; the encryption process with an asymmetric algorithm, which may lead to high communication costs, especially for users with limited hardware resources, moreover, this work does not provide specific details about each process.
Yue et al. [35] proposed a general framework for sharing and verifying data integrity in Blockchain-based decentralized Edge-Cloud storage that eliminates semi-honest TPA. In this work, the researchers also proposed sampling verification and formulated rational sampling strategies to make sampling verification more efficient. Thus, only the DO can generate the leaf node of MHT, which improves the preservation of confidentiality. Additionally, they designed two types of smart contracts for data integrity verification. However, this work has some shortcomings such as; traceability cannot be satisfied because relevant operation logs of data are not stored on the Blockchain, dynamic operations of data are not supported, and computational and communication costs cannot be assessed because this work does not provide specific details on each phase.
Nabeil Eltayieba et al. [56] has developed a mechanism that combines the concept of attribute-based encryption and Blockchain technology to provide secure data sharing accompanying the Blockchain concept with attribute-based sign encryption in the cloud environment. Additionally, smart contracts are used to secure data-sharing capabilities between different data owners and data users. They analyzed the communication cost of the attribute-based signature encryption scheme for the cloud environment, which includes signing key size, decryption key, and ciphertext. But, this work fails to minimize communication overhead.
The authors in [57] proposed an efficient approach to share continuous IoT data using Blockchain which also relies on cloud storage. A key feature of the proposed system is that they focus on continuous dynamic data, which represents most of the data generated by wearables and mobile devices, and integrate Blockchain and cloud storage technologies to collect and share data from dynamic personal health. Instead of storing original data in a Blockchain, only raw data metadata is kept in a Blockchain, which would overcome the size limitation of large data storage in a Blockchain. However, no mechanism to verify the accuracy and integrity of personal health records returned from cloud servers, especially when a user wishes to verify the accuracy and integrity of encrypted personal health records returned from the server cloud, it is necessary to interact frequently with the cloud server, which makes the scheme inefficient in practice.
Wang and Song [58] introduced a new attribute-based record-sharing scheme for medical data systems in addition to the signature concept. They used signature-based verification to verify encrypted data and provide access authorization. For the encryption of medical data, they combined attribute-based encryption (ABE) and identity-based encryption (IBE) with a signature algorithm. They further used Identity Based Signatures (IBS) to implement the digital signatures. However, the limitation of this work is that their scheme suffers from significant computational overhead on the user side.

3.3 Authentication and access control

Access control refers to the restriction of activities of legitimate users and authorization [30] is the key technology to protect users' personal and business data in the cloud. Access control management is the fundamental part of trust-based cloud computing. However, centralized access control policies usually require a third-party management center, which can lead to risks of privacy leakage or hacker attack, such as a single point of failure. Thanks to the decentralized ledger technology used by the Blockchain, all security-related operations are preserved without modification, which makes it possible to overcome security and trust problems and control access well.
As a result, Lin et al. [59] proposed a Blockchain-based system for secure mutual authentication to enforce granular access control policies, which provides privacy and security guarantees such as anonymous authentication, audibility, and privacy through using a smart contract. The data is signed with the attribute-based signature (ABS) algorithm to be authenticated anonymously. In addition, the entire application process is carried out through interaction with smart contracts.
Li, Xinlong. et al [60] propose a Blockchain-based verifiable user data access control policy for secure storage of big data in the cloud which was analyzed based on the design of a data exchange network between systems that use cloud computing. Although this model allows data to be controlled and detected securely without any risk to its confidentiality using smart contracts, there is no mechanism to identify nodes and the risk of a single point of failure.
Yang et al. [61] proposed a Blockchain-based multi-authority attribute-based encryption scheme that enables access control of medical data in a cloud environment. The scheme relies on policy masking technology to protect data privacy. They achieved distributed attribute management and computation of different authorities using Shamir secret sharing and smart contracts. Analysis of this scheme shows that it reduces the computational cost and eliminates the single-point bottleneck problem of traditional Ciphertext Policy Attribute-Based Encryption (CP-ABE) schemes.
Yang et al [62] used Blockchain smart contracts and differential privacy technology to store, verify, and adaptively allocate privacy budget consumption based on data owner requirements, to allow the data owner to control the anonymization process. The amount of noise produced in the obfuscation process represents the privacy budget. Data sharing

ends once the privacy budget is exhausted.
Han et al. [63] implemented a flexible and privacy-preserving framework for searchable encryption on Ethereum by orienting Blockchain and attribute-based encryption, which enables granular access control. This framework manipulated access control via smart contracts, significantly reducing communication costs. But, they used a centralized trusted third party for key management, which makes their solution semi-reliable.
In [51], the authors proposed a Blockchain-based electronic health data sharing system, while security and privacy were maintained by using proxy-based re-encryption and proof-of-trust consensus mechanism. authorization (PoAuth). In this scheme, the cloud server is used for data storage and applies the consortium Blockchain so that data integrity and scalability are guaranteed. However, the proposed approach does not deal with the process of mutual authentication and key agreement and cannot fully guarantee the owner's data ownership due to the data provider uploading the data to the cloud server instead of the owner.
In [47], Authors designed a decentralized storage system by combining Interplanetary File System (IPFS), Ethereum Blockchain, and Attribute-Based Encryption (ABE) technologies. In this method, the authors aim to overcome the risks of centralized storage, i.e. leakage of sensitive data and a single point of failure. In the proposed framework, before storing data in IPFS, a data owner distributes a secret key to users and encrypts their data according to a predefined access policy to achieve fine-grained access control over cloud data. Smart contracts were designed to implement keyword research in decentralized storage systems. Shared data can be stored in cloud storage, while metadata can be kept securely on the Blockchain for sharing. However, if this solution is applied in the Internet of Things (IoT) scenario, it will not work efficiently due to increased computational overhead.
For secure data sharing, Xuanmei Qin et al. [64] proposed a Blockchain-based multi-authority access control scheme, which leverages the consortium Blockchain to establish trust between multiple attribute authorities. To avoid a single point of failure, it introduces Shamir secret sharing scheme and Blockchain authority and realizes joint management of each attribute by multiple authorities. Moreover, it builds trust between multiple authorities by using smart contracts to calculate tokens for managed qualities across multiple management domains. The use of smart contracts thus reduces the communication and calculation costs on the side of the data users. However, Blockchain technology helped establish trust between multiple network entities and contributed to a secure and auditable record of the access control procedure.
Furthermore, C. YANG, et al. [65] proposed a Blockchain-based access control framework, named AuthPrivacyChain, to address the problem that sensitive data is easily tampered with or leaked by hackers or internal cloud managers due to a mechanism of centralized access control in the cloud. By using the decentralized nature of the Blockchain, all transaction-related permissions are posted by the user on the Blockchain, enhancing the privacy and security of data applications, which can effectively resist internal and external attacks. However, among the shortcomings of this work is that the experimental results show that only legal users can access the resources, but this paper performed only limited performance testing and compared to two benchmark models.
Chen et al. [66] proposed an integrated framework based on Blockchain and cloud storage, to manage and share patients' medical data, and to ensure the safe storage and sharing of data. In addition, they used Blockchain as a storage supply chain in which all operations are verified, immutable and accountable and introduced a service framework for sharing medical records, which protects medical data management applications without violating privacy policies.
The authors of [67] proposed a decentralized and secure Blockchain-based architecture to provide access control and user revocation methods in the cloud storage system using the CP-ABE algorithm. The proposed methodology uses the key generation scheme based on two authorities, to solve the single point of failure problem. Access policy details related to keys and users are generated by data owners and authorities in a distributed manner using the Blockchain framework (Smart Contract), while the data is stored in the cloud. However, this solution ensured the privacy of outsourced data by preventing users from accessing the data without the proper credentials.
Saini, A., Zhu, et al. [68] proposed an access control system based on a distributed ledger (Blockchain) that can effectively check user behavior. The designed system exploits the concept of smart contracts for electronic medical record management and uses elliptic curve cryptography to encrypt health data before storing it in the cloud. To eliminate network congestion, the cloud helps back up medical data while the smart contracts used ensure the privacy of EMRs using cryptographic and access control features. However, they suffer from many drawbacks, such as the need for more processing time due to the involvement of proxy servers and the involvement of a semi-trusted party which affects the overall security of the architectures.

3.4 Auditing and data integrity

Traditional data integrity auditing techniques used to store data in a cloud computing environment are centralized, which faces huge security risks and vulnerabilities of the central audit server due to the point of a single failure. Blockchain technology is becoming a potential solution due to its properties of immutability and irreversibility which offers a new

Table 5: Comparison of literature solutions

References	Issue addressed	Technique used	Performance test	Platform	Gaps
[69] 2018	Integrity Audit, cloud storage	Censensus algorithm, MHT	Upload/download time, broadcasting operation	Ethereum	Data privacy has not been considered.
[57] 2018	Data sharing, cloud storage	AES, consensus algorithm	Theoretical analysis	Ethereum	No evidence is provided on how the simulation is performed.
[58] 2018	Confidentiality, authentication, integrity, cloud storage	ABE,IBE, IBS	Theoretical analysis	-	The real prototype is not implemented
[70] 2018	Centralized data storage, trusted third party	Hash Merkel tree, P2P networks, ECC	Number of users and network latency, number of file replicas	Self-deployed	No evidence was provided on the key sharing process. No mention of the cryptography used.
[47] 2018	Data sharing, access control	Smart contract, IPFS, ABE	Smart contract operation costs	Ethereum	Issues on data confidentiality and access control latency are not discussed in detail.
[71] 2019	Key sharing, centralization, access control	CP-ABE, Smart contract, Deffi-Hellman	Calculation cost	Ethereum	Encryption key stored in networks. Increasing the number of users can increase key storage and the cost of operation.
[72] 2019	Trusted Party, verification against auditors	Consensus algorithm	Calculation cost	Ethereum	Data privacy issues are not discussed in detail
[51] 2019	Access control	Proof of work	Execution time	Ethereum	Complex key management
[66] 2019	Trusted third party,Single point of failure	Hybrid encryption (Sym/ Asym)	Theoretical analysis	-	No process for patients to share data between different entities. This system is only intended for a single institution, so it may have scalability issues.
[73] 2019	Access control, integrity, audit	Proxy re-encryption, signature, sha2, asymmetric -cryptography	Storing time, retrieving time	Hyperledger	The running cost is very high due to proxy data re-encryption. The secret key-sharing process is unclear
[65] 2020	Access control	Smart contarct	Calculation overhead	Self-deployed	No evidence has been provided on how the data is encrypted.
[35] 2020	Verification of integrity, confidentiality	Smart contract	Comparision of MHT	Ethereum	No mention of the cryptography used.
[74] 2020	Integrity check, audit	Blockchain network, MHT	Storage latency	Self-deployed	Does not support dynamic verification .
[56] 2020	Access control and data sharing	Smart contract, ABE	Encryption cost	Self-deployed	Using a trusted authority to manage Keys.
[75] 2020	Secure storage, privacy, integrity-audit	Auditor, PoW, MHT	Communication cost	Ethereum	-
[68] 2020	Access control, cloud storage	Asymetric-cryptography, smart contract	Latency, transaction Cost	Ethereum	No data provided on how an entity checks into hospitals. Heavy encryption(asymmetric)
[76] 2021	Audit, data integrity	Smart contract, zero-knowledge proof	Auditing time, storage time, gas cost	Ethereum	Raising serious concerns about data harvesting attacks from audit trails stored on a Blockchain.
[64] 2021	Access control, trusted party	shamir secret sharing, ABE, smart contract	Communication cost, calculation cost	Hyperledger	-
[61]2022	Access control	Smart contract, CP-ABE, Shamir secret sharing	Response latency, decryption time	Ethereum	-
[77] 2022	Integrity audit, cloud storage	Smart contract, e-voting	Processing time, time cost of proof	Self-deployed	-
[49] 2022	Data privacy, data sharing data sharing	Smart contract, Zero-Knowledge Proof	Theoretical analysis	-	No evidence is provided on how the simulation is performed.
[63] 2022	Access control, privacy	ABE, smart contract	Search time, gas cost	Ethereum	Use of a trusted third party for key management.

Table 5: Comparison of literature solutions

References	Issue addressed	Technique used	Performance test	Platform	Gaps
[60] 2022	Access control policy	smart contract	Theoretical analysis	-	There is no mechanism to identify nodes and the risk of a single point of failure.
[67]2022	Access control, privacy	CP-ABE, smart contract	Key generation time, encryption time	java-based Blockchain network	No data was provided on how integrity is ensured.
[55]2023	Data sharing, cloud storage, privacy	RSA, smart contract	Key creation, file Encrypting	Ethereum	Heavy encryption process
[78]2023	Audit, data integrity	Quad Merkle Tree, smart contract	Verification time, gas consumption	Ethereum	No evidence is provided on how the data is encrypted and shared.

approach to this problem. Many researchers have endeavored to use Blockchain to verify and audit data integrity.

To monitor semi-reliable TPAs, Zhang et al. [72] addressed the challenges of the integrity of user data kept on external cloud storage and asked them to publish their audit logs on the Blockchain, to help users monitor untrusted TPAs. Cloud service providers may cover incidents of data corruption to protect the agency's reputation or delete certain data. This data may not have been processed to reduce storage costs. Although these schemes solve the centralization problem of traditional approaches, they are only suitable for single-cloud enabling environments, i.e. they increase the additional overhead caused by data duplication. Periodic auditing systems are necessary to prevent possible data tampering.

Li et al. [69] has developed a Blockchain-based behavioral auditing framework that records user operations on files and stores file metadata with Blockchain and protects data integrity in the cloud through auditing. They also used a proxy node to efficiently search for specific blocks and speed up the querying of block data, since the cloud environment and devices do not fully trust each other. Additionally, to verify integrity, the data owner had to download the entire file and could not afford to require verification from time to time.

Du et al. [76] proposed a storage audit design in decentralized storage networks (DSNs) based on Blockchain and zero-knowledge proof to ensure the integrity of outsourced data. The data owner and storage provider reach a consensus on the performance of a storage contract, through a negotiation phase, and the data is audited against the negotiated outcomes specified by the agreed smart contract. After the data has been outsourced to the storage provider, the storage provider is required to calculate the audit proof for the challenge and submit the proof to the Blockchain on time. They used smart contracts to manage the negotiation between the customer and the service provider and to perform the auditing process.

Kun et al. [74] have implemented private Blockchain-based data validation to solve the security problem caused by using untrusted TPA. Unlike traditional Blockchain, which stores data such as financial transactions or smart contracts in the block body, in their approach, each block body stores records formed by a Merkle tree, while the en-block head retains the summary calculated by the previous block, but their solution does not support dynamic verification and requires building and deploying a private Blockchain, which is very difficult in practice.

Chen et al. [77] proposed a decentralized public audit system for Blockchain-based cloud storage. In their approach, the audit task was assigned to multiple CSPs, and Blockchain technology was used to record the audit process. However, they used the structure of the electronic voting system to realize the statistics of the audit results of multiple CSPs through a smart contract, and they assigned the same audit tasks to multiple CSPs and counted the audit results. independent. But, they used a centralized trusted third party for key management, which makes their solution semi-reliable.

Miao et al. [75] use zero-knowledge proof and PoW consensus mechanism during the auditing process to protect user privacy to solve the problem that the cloud server can guess the challenge messages in advance. This scheme could withstand auditor dithering and the risk that a malicious cloud server may guess the challenge messages before the audit time in which the challenge message is generated based on the latest successive block hashes. Therefore, a TPA does not know any additional information about the user's data.

Liu, Zhenpeng, et al. [78] have implemented a data integrity audit scheme that uses Blockchain instead of third-party auditors to ensure data audit reliability. Unlike the traditional binary hash tree, whose structure is linear and a large number of hash operations makes the processing speed unsatisfactory (which generates a large amount of storage overhead), they used a hash tree Quad Merkle that improves compute and storage efficiency. Additionally, to get a faster picture of data integrity, they have deployed smart contracts on the Blockchain that allows for automatic verification of

auditing activities. However, the client generates a quadruple Merkle hash tree using the data block signatures after encrypting the data, then it sends the root to the Blockchain for storage and sends the data encrypted with the Merkle hash tree to the cloud for storage.

4 Discussion and comparative analysis

In this section, we explain the main comparative results of the solutions described in the previous section. Table 6 shows us the characteristics used to evaluate the level of trust and security of the different solutions in the literature, namely confidentiality, integrity, authentication, access control, the process of sharing the key encryption, and auditing to trust the cloud service provider. Based on previous investigations, we have found that the integration of Blockchain and cloud has the following main advantages: Since Blockchain is a reliable distributed database, it can be used to store important data generated by different applications with transactions to ensure data integrity and it can also be used to store file metadata. However, using the characteristics of the smart contract, the cloud computing management mechanism can be run automatically, and the Blockchain can be used for resource planning, resource distribution, transactions, tracking, auditing, identity management, access control, and authentication. We can further use the cloud to improve the efficiency and performance of the Blockchain by using the cloud to store the original data while the Blockchain stores the key information etc. On the other hand, as shown in Figure 7, the research orientation of the selected studies shows that several solutions do not take into account some of these characteristics (i.e. there is no solution that satisfies all the evaluation criteria). However, cloud consumers' concerns about information security have caused them to rethink before using cloud services. For this, it is very important to ensure good key management, audit data integrity, and ensure data confidentiality and good access control management.

Figure 8 represents the percentage of satisfaction with the solutions in terms of confidentiality, integrity, auditing, authentication, data access control, and key sharing process regarding the use of Blockchain in cloud computing. As shown in the figure, 95% respond to integrity issues, 64% respond to access control issues, and 55%, 50%, and 45% respond to privacy, auditing, and key sharing issues, respectively. However, we observe that only 18% of the proposed solutions elaborate on authentication and identity verification issues.

5 Research challenges

Based on the review above, we realize that there is still a long way to go before Blockchain technology can be applied to cloud data storage. To meet the requirements needed to integrate Blockchain into cloud computing, it is important to address the challenges of authentication, scalability, network security, data integrity, verifiable computation, and low latency[79]. Fig. 9 illustrates the main challenges of this study.

- **Cloud data access control challenge** Using Blockchain to provide access control to data stored in the cloud can create a potential loophole (pseudo-anonymity), where the flow of transactions could be tracked to obtain the real identity of cloud users or other relevant [80] information due to the public nature of the Blockchain network. Thus, there are security vulnerabilities in the implementation of smart contracts to solve more serious crimes such as identity theft and data theft [81], which can compromise security in the architecture of cloud data storage based on smart contracts as in [71, 82]. For this, researchers are trying to increase the security and reduce the energy consumption of these algorithms because consensus algorithms are a major factor in determining the performance of the Blockchain [83]. Thus, it is very important to ensure secure access management to control participant access to data stored in the cloud.
- **Cloud storage consensus optimization challenge** Although Blockchain technology has great potential for handling access control requests in a cloud environment, it can also cause latency issues due to the use of consensus protocols. However, several issues still need to be addressed regarding the development of consensus protocols, as they consume a significant number of computational resources and energy in realistic transactions, resulting in poor system performance and long latency. The objective is to build consensus structures to improve the efficiency of the access management system and secure storage in the cloud in order to save time and money and manage competitors while ensuring scalability, execution, and a higher level of identity, confidentiality, and protection [84].
- **Scalability challenge** According to [85], scalability remains Blockchain's biggest challenge. Due to the growing number of cloud users, several transactions are increasing day by day in the Blockchain, which presents additional scalability issues in terms of improving overload capabilities. Rapid elasticity, one of the main characteristics of cloud computing, requires instantaneous scalability of resources, and therefore Blockchain is unlikely to work optimally with cloud computing. Many small transactions could be delayed as miners prefer trans-

Table 6: Strengths of works integrating Blockchain technology with cloud computing

References	Confidentiality	Integrity	Authentication	Access control	Auditing	key sharing process
[69]	✓	✓	-	✓	-	-
[57]	✓	✓	-	✓	-	✓
[58]	✓	✓	-	✓	-	✓
[70]	-	✓	-	-	✓	-
[47]	-	✓	✓	✓	-	✓
[71]	✓	✓	-	✓	-	✓
[72]	-	✓	✓	✓	✓	-
[51]	✓	✓	-	✓	-	✓
[66]	-	✓	-	-	✓	-
[73]	✓	✓	-	✓	-	-
[65]	-	✓	-	-	✓	-
[35]	✓	✓	-	✓	-	✓
[74]	-	✓	-	-	✓	-
[56]	-	✓	-	-	✓	-
[75]	✓	✓	-	✓	✓	✓
[68]	-	✓	-	-	✓	-
[64]	✓	✓	-	-	-	✓
[77]	✓	✓	-	✓	✓	-
[63]	-	✓	✓	✓	✓	✓
[78]	-	✓	-	-	✓	-
[67]	✓	-	✓	✓	-	✓
[49]	✓	✓	-	✓	-	-

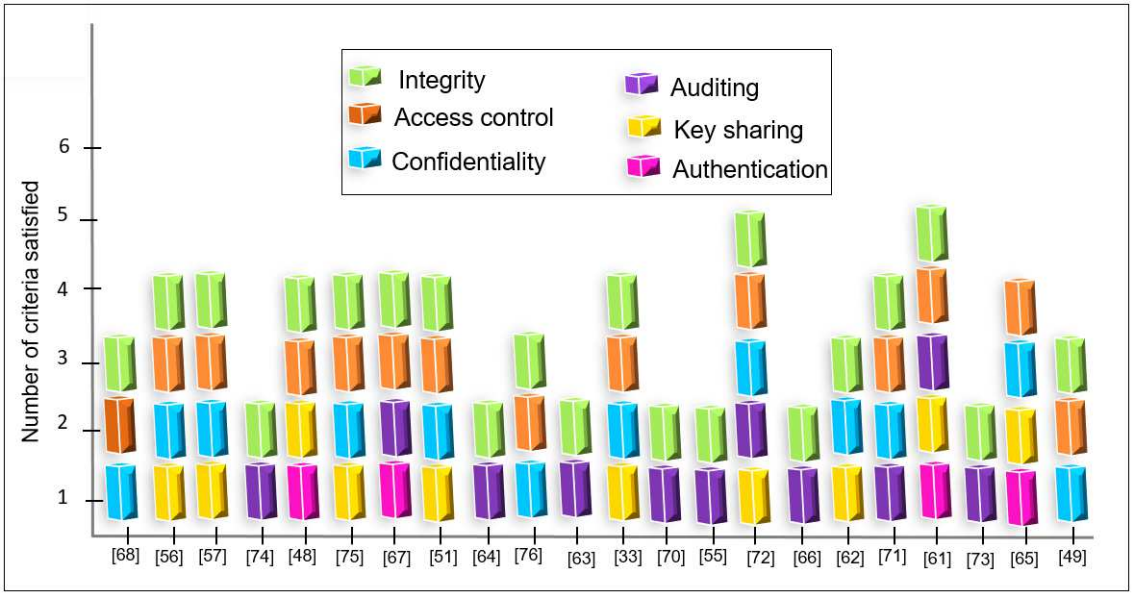

Fig. 7: Assessment of the level of trust and security for each solution.

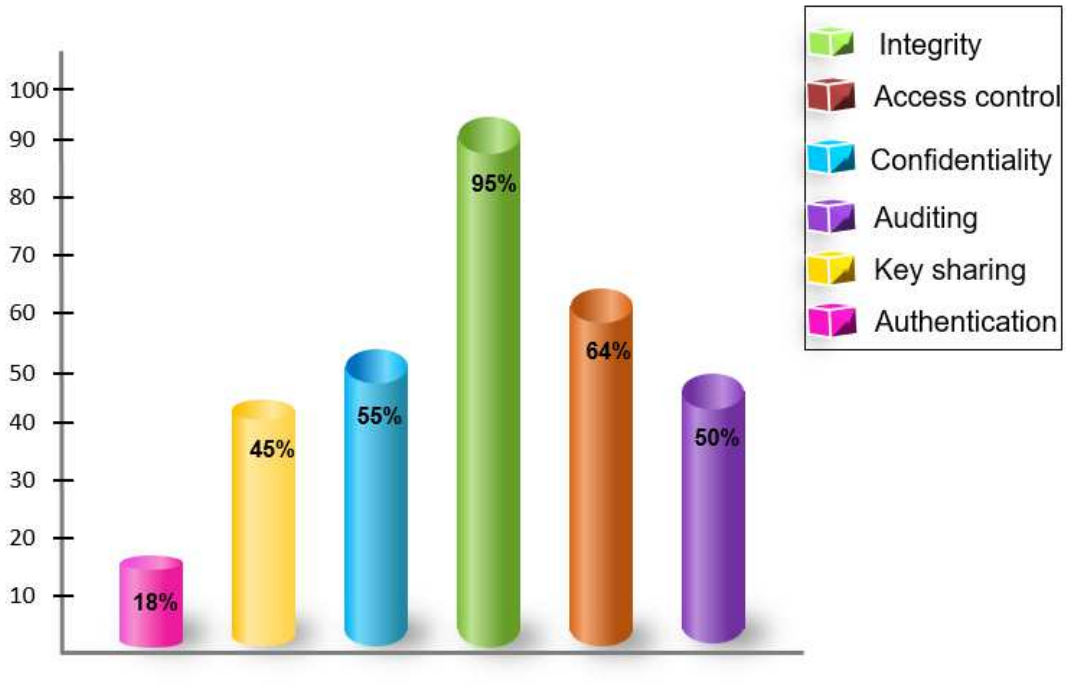

Fig. 8: Comparison of solutions meeting each security criteria.

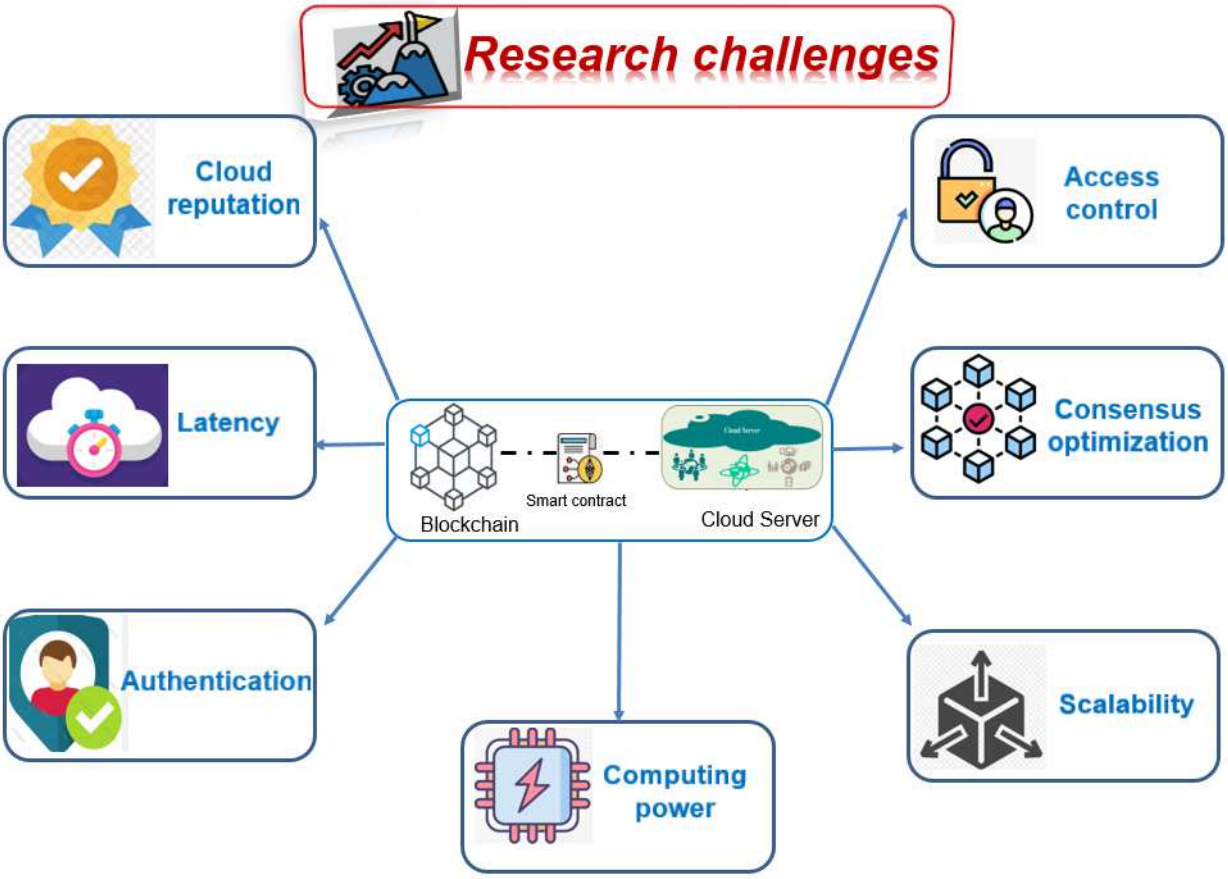

Fig. 9: Main challenges.

actions with higher transaction fees. However, this kind of difficulty could lead to increased computing requirements for the entire Blockchain system. So it is important to fix the scalability issue [81, 86].

- **User resource computing power challenge** Blockchain data for cloud user devices is generally computationally constrained, which inhibits the adoption of cryptographic methods [87]. Among the performance and security issues is that a large portion of Blockchains deploys public critical cryptosystems based on asymmetric algorithms like ECC, which complicates the overall process of selecting appropriate cryptographic methods. However, it is worth researching energy-efficient quantum security techniques to maintain data security. Moreover, how to design an efficient data structure that supports dynamic data operations is an important research topic in Blockchain-based data storage schemes.
- **Cloud user authentication challenge** In traditional centralized cloud systems, user identity data is controlled by a third-party authority, therefore, user verification, authorization, and accountability are also implemented and guaranteed by a centralized authority. With a decentralized Blockchain network, identities collaborating and managing flexibly can also face significant challenges. In a Blockchain network, anyone can connect to the network and users can obtain an address without presenting their real identity and apply it for any identity authentication. Since users do not provide their true identity to interact with the cloud application and other users, this increases the potential for impersonation [88]. In some cloud applications, an actual identity-based user authentication mechanism is needed to control participant access and ensure transactions comply with regulatory requirements. Considering the need for decentralized identity management with accountability and privacy protection is a research gap and an important future research direction.
- **Latency challenge** Nowadays, medical systems are increasingly using cloud computing to store their data. If a patient wants to connect to the cloud, transaction latency represents the time it takes for a Blockchain to process a transaction with the cloud. Since all Blockchain systems require some time to establish confirmed transactions and consensus, this could aggravate the integration of Blockchains into healthcare applications, which must respond to actions and information received simultaneously. Addressing network latency [89] requires that researchers can ensure that proposed or tested designs improve their performance and efficiency to accommodate the increasing volume of transactions that can be projected with the additional implementation Blockchain systems [90].
- **Cloud reputation challenge** Credit ratings can be a good yardstick to assess the reputation of a communications service provider [91]. A CSP will receive a specified number of points if they provide legitimate cloud services; otherwise, his points will be deducted. This way, DOs can choose CSPs with high credit ratings to outsource their data for high security. Designing a CSP reputation evaluation mechanism in the cloud schema is a promising direction.

In summary, there is no easy approach to achieving the fusion of the concept of decentralization and the security methods of Blockchain technology. It's an environment that still has a lot of work to do.

6 Conclusion

The cloud computing model faces many of the security issues that centralized data centers face, due to its highly centralized architecture. However, the cloud also faces issues of data sharing, authentication, access control, privacy, data auditing, and trust. Blockchain is one of the most recent emerging technologies that has begun to see its applicability beyond the realm of cloud computing. Its features, such as traceability, immutability, and data security, in addition to its decentralized nature, have been the main reasons for its success. It is believed that the integration of the Cloud with Blockchain technology can mitigate these security issues and improve the development and deployment of decentralized applications with high security and efficient network management. This article presents a taxonomy and a review of the state of the art on the application of Blockchain in cloud computing systems. Specifically, this article has identified the extent of research that has been conducted regarding Blockchain-Cloud integration over the past few years. First, we briefly presented the basic concepts of cloud computing, namely their issues and their security requirements, and we gave an overview of the Blockchain. Next, we discuss the main opportunities offered by Blockchain to solve cloud computing problems and explain the motivation behind the integration of these two technologies. Moreover, for the existing Blockchain-based solutions to improve data storage in an untrusted cloud environment, we have compared them and categorized them into four main classes, namely data sharing, privacy and key sharing, authentication and access control, and auditing and data integrity. From the extensive review of the literature on cloud Blockchain services and applications, we suggest many possible future directions identified to stimulate research in this promising area. Therefore, it is apparent from the discussion that a robust Blockchain framework for the cloud encompasses many challenges to consider when integrating and deploying it. We believe that the main results of this survey will

offer theoretical support and practical advice to researchers and cloud users.

7 Declarations

Competing interests

The authors did not receive support from any organization for the submitted work.
The authors have no relevant financial or non-financial interests to disclose.
The authors have no competing interests to declare that are relevant to the content of this article.
All authors certify that they have no affiliations with or involvement in any organization or entity with any financial interest or non-financial interest in the subject matter or materials discussed in this manuscript.
The authors have no financial or proprietary interests in any material discussed in this article.

Research Data Policy and Data Availability Statements

All data generated or analyzed during this study are included in this published article.

Compliance with Ethical Standards

Conflict of interest
The authors declare that they have no competing interests.
Ethical approval
This article does not contain any studies with human participants or animals performed by any of the authors.
Informed consent
None.

References

1. Aaqib Rashid and Amit Chaturvedi. Cloud computing characteristics and services: a brief review. *International Journal of Computer Sciences and Engineering*, 7(2):421–426, 2019.
2. Hamed Tabrizchi and Marjan Kuchaki Rafsanjani. A survey on security challenges in cloud computing: issues, threats, and solutions. *The journal of supercomputing*, 76(12):9493–9532, 2020.
3. Diogo AB Fernandes, Liliana FB Soares, João V Gomes, Mário M Freire, and Pedro RM Inácio. Security issues in cloud environments: a survey. *International Journal of Information Security*, 13(2):113–170, 2014.
4. Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, page 21260, 2008.
5. Li Da Xu and Wattana Viriyasitavat. Application of blockchain in collaborative internet-of-things services. *IEEE Transactions on Computational Social Systems*, 6(6):1295–1305, 2019.
6. Ali Dorri, Marco Steger, Salil S Kanhere, and Raja Jurdak. Blockchain: A distributed solution to automotive security and privacy. *IEEE Communications Magazine*, 55(12):119–125, 2017.
7. Souad BelMannoubi, Haifa Touati, Mohamed Hadded, Khalifa Toumi, Oyunchimeg Shagdar, and Farouk Kamoun. A comprehensive survey on blockchain-based c-its applications: Classification, challenges, and open issues. *Vehicular Communications*, page 100607, 2023.
8. Souad BelMannoubi, Mohamed Hadded, Haifa Touati, and Farouk Kamoun. La technologie blockchain pour améliorer la sécurité des systèmes de transport intelligents. In *CSTI'20 – 1er Colloque Francophone des Systèmes de Transports Intelligents*, 2020.
9. Hang Xu, Jing Cao, Jian Zhang, Liangyi Gong, and Zhaojun Gu. A survey: cloud data security based on blockchain technology. In *2019 IEEE Fourth International Conference on Data Science in Cyberspace (DSC)*, pages 618–624. IEEE, 2019.
10. Ch VNU Bharathi Murthy and M Lawanya Shri. A survey on integrating cloud computing with blockchain. In *2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE)*, pages 1–6. IEEE, 2020.
11. Ch VNU Bharathi Murthy, M Lawanya Shri, Seifedine Kadry, and Sangsoon Lim. Blockchain based cloud computing: Architecture and research challenges. *IEEE Access*, 8:205190–205205, 2020.
12. Soumik Sarker, Arnob Kumar Saha, and Md Sadek Ferdous. A survey on blockchain & cloud integration. In *2020 23rd International Conference on Computer and Information Technology (ICCIT)*, pages 1–7. IEEE, 2020.
13. Keke Gai, Jinnan Guo, Liehuang Zhu, and Shui Yu. Blockchain meets cloud computing: a survey. *IEEE Communications Surveys & Tutorials*, 22(3):2009–2030, 2020.
14. Nazanin Zahed Benisi, Mehdi Aminian, and Bahman Javadi. Blockchain-based decentralized storage networks: A survey. *Journal of Network and Computer Applications*, 162:102656, 2020.
15. Wenjuan Li, Jiyi Wu, Jian Cao, Nan Chen, Qifei Zhang, and Rajkumar Buyya. Blockchain-based trust management in cloud computing systems: a taxonomy, review and future directions. *Journal of Cloud Computing*, 10(1):1–34, 2021.
16. Jinglin Zou, Debiao He, Sherali Zeadally, Neeraj Kumar, Huaqun Wang, and Kkwang Raymond Choo. Integrated blockchain and cloud computing systems: A sys-

tematic survey, solutions, and challenges. *ACM Computing Surveys (CSUR)*, 54(8):1–36, 2021.
17. Mohammad Khalid Imam Rahmani, Mohammed Shuaib, Shadab Alam, Shams Tabrez Siddiqui, Sadaf Ahmad, Surbhi Bhatia, and Arwa Mashat. Blockchain-based trust management framework for cloud computing-based internet of medical things (iomt): A systematic review. *Computational Intelligence and Neuroscience*, 2022.
18. Abhirup Khanna, Anushree Sah, Vadim Bolshev, Alessandro Burgio, Vladimir Panchenko, and Marek Jasiński. Blockchain–cloud integration: A survey. *Sensors*, 22(14):5238, 2022.
19. Haoxiang Han, Shufan Fei, Zheng Yan, and Xiaokang Zhou. A survey on blockchain-based integrity auditing for cloud data. *Digital Communications and Networks*, 2022.
20. Shaoan Xie, Zibin Zheng, Weili Chen, Jiajing Wu, Hong-Ning Dai, and Muhammad Imran. Blockchain for cloud exchange: A survey. *Computers & Electrical Engineering*, 81:106526, 2020.
21. Will Venters and Edgar A Whitley. A critical review of cloud computing: researching desires and realities. *Journal of Information Technology*, 27(3):179–197, 2012.
22. Shubhanjali Sharma, Garima Gupta, and PR Laxmi. A survey on cloud security issues and techniques. *arXiv preprint arXiv:1403.5627*, 2014.
23. Houaida Ghanmi, Nasreddine Hajlaoui, Haifa Touati, Mohamed Hadded, and Paul Muhlethaler. A secure data storage in multi-cloud architecture using blowfish encryption algorithm. In *Advanced Information Networking and Applications: Proceedings of the 36th International Conference on Advanced Information Networking and Applications (AINA-2022), Volume 2*, pages 398–408. Springer, 2022.
24. Tayssir Ismail, Haifa Touati, Nasreddine Hajlaoui, and Hassen Hamdi. Hybrid and secure e-health data sharing architecture in multi-clouds environment. In *The Impact of Digital Technologies on Public Health in Developed and Developing Countries: 18th International Conference, ICOST 2020, Hammamet, Tunisia, June 24–26, 2020, Proceedings 18*, pages 249–258. Springer, 2020.
25. Bahzad Taha Jijo, SR Zeebaree, Rizgar R Zebari, MA Sadeeq, Amira B Sallow, Sanaa Mohsin, and Zainab Salih Ageed. A comprehensive survey of 5g mm-wave technology design challenges. *Asian Journal of Research in Computer Science*, 8(1):1–20, 2021.
26. I Indu, PM Rubesh Anand, and Vidhyacharan Bhaskar. Identity and access management in cloud environment: Mechanisms and challenges. *Engineering science and technology, an international journal*, 21(4):574–588, 2018.
27. Deyan Chen and Hong Zhao. Data security and privacy protection issues in cloud computing. In *2012 international conference on computer science and electronics engineering*, volume 1, pages 647–651. IEEE, 2012.
28. R Sravan Kumar and Ashutosh Saxena. Data integrity proofs in cloud storage. In *2011 Third International Conference on Communication Systems and Networks (COMSNETS 2011)*, pages 1–4. IEEE, 2011.
29. Rakesh Kumar and Rinkaj Goyal. On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. *Computer Science Review*, 33:1–48, 2019.
30. Ravi S Sandhu and Pierangela Samarati. Access control: principle and practice. *IEEE communications magazine*, 32(9):40–48, 1994.
31. Nick Szabo. Formalizing and securing relationships on public networks. *First monday*, 1997.
32. Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Xiangping Chen, and Huaimin Wang. Blockchain challenges and opportunities: A survey. *International journal of web and grid services*, 14(4):352–375, 2018.
33. Sunny Pahlajani, Avinash Kshirsagar, and Vinod Pachghare. Survey on private blockchain consensus algorithms. In *2019 1st International Conference on Innovations in Information and Communication Technology (ICIICT)*, pages 1–6. IEEE, 2019.
34. Zhetao Li, Jiawen Kang, Rong Yu, Dongdong Ye, Qingyong Deng, and Yan Zhang. Consortium blockchain for secure energy trading in industrial internet of things. *IEEE transactions on industrial informatics*, 14(8):3690–3700, 2017.
35. Dongdong Yue, Ruixuan Li, Yan Zhang, Wenlong Tian, and Yongfeng Huang. Blockchain-based verification framework for data integrity in edge-cloud storage. *Journal of Parallel and Distributed Computing*, 146:1–14, 2020.
36. Lin William Cong and Zhiguo He. Blockchain disruption and smart contracts. *The Review of Financial Studies*, 32(5):1754–1797, 2019.
37. Samudaya Nanayakkara, Srinath Perera, and Sepani Senaratne. Stakeholders' perspective on blockchain and smart contracts solutions for construction supply chains. In *CIB World Building Congress*, pages 17–21. Hong Kong SAR China, 2019.
38. Florian Tschorsch and Björn Scheuermann. Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys & Tutorials*, 18(3):2084–2123, 2016.
39. Vitalik Buterin. Ethereum: platform review. *Opportunities and challenges for private and consortium blockchains*, 45, 2016.
40. Elli Androulaki, Artem Barger, Vita Bortnikov, Christian Cachin, Konstantinos Christidis, Angelo De Caro,

David Enyeart, Christopher Ferris, Gennady Laventman, Yacov Manevich, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains. In *Proceedings of the thirteenth EuroSys conference*, pages 1–15. EuroSys, 2018.
41. Huawei Huang, Wei Kong, Sicong Zhou, Zibin Zheng, and Song Guo. A survey of state-of-the-art on blockchains: Theories, modelings, and tools. *ACM Computing Surveys (CSUR)*, 54(2):1–42, 2021.
42. Stefanos Leonardos, Daniel Reijsbergen, and Georgios Piliouras. Presto: A systematic framework for blockchain consensus protocols. *IEEE Transactions on Engineering Management*, 67(4):1028–1044, 2020.
43. Deepak K Tosh, Sachin Shetty, Xueping Liang, Charles Kamhoua, and Laurent Njilla. Consensus protocols for blockchain-based data provenance: Challenges and opportunities. In *2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)*, pages 469–474. IEEE, 2017.
44. Stefano De Angelis, Leonardo Aniello, Roberto Baldoni, Federico Lombardi, Andrea Margheri, and Vladimiro Sassone. Pbft vs proof-of-authority: Applying the cap theorem to permissioned blockchain. In *talian Conference on Cyber Security, Milan, Italy*, 2018.
45. Jin Sun, Xiaomin Yao, Shangping Wang, and Ying Wu. Blockchain-based secure storage and access scheme for electronic medical records in ipfs. *IEEE Access*, 8:59389–59401, 2020.
46. Changyu Dong, Yilei Wang, Amjad Aldweesh, Patrick McCorry, and Aad van Moorsel. Betrayal, distrust, and rationality: Smart counter-collusion contracts for verifiable cloud computing. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 211–227. ACM SIGSAC, 2017.
47. Shangping Wang, Yinglong Zhang, and Yaling Zhang. A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. *Ieee Access*, 6:38437–38450, 2018.
48. Yuan Zhang, Chunxiang Xu, Nan Cheng, Hongwei Li, Haomiao Yang, and Xuemin Shen. Chronos : An accurate blockchain-based time-stamping scheme for cloud storage. *IEEE Transactions on Services Computing*, 13(2):216–229, 2019.
49. Tao Feng, Pu Yang, Chunyan Liu, Junli Fang, and Rong Ma. Blockchain data privacy protection and sharing scheme based on zero-knowledge proof. *Wireless Communications and Mobile Computing*, 2022:1–11, 2022.
50. Ilya Sukhodolskiy and Sergey Zapechnikov. A blockchain-based access control system for cloud storage. In *2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, pages 1575–1578. IEEE, 2018.
51. Yong Wang, Aiqing Zhang, Peiyun Zhang, and Huaqun Wang. Cloud-assisted ehr sharing with security and privacy preservation via consortium blockchain. *Ieee Access*, 7:136704–136719, 2019.
52. Meng Shen, Junxian Duan, Liehuang Zhu, Jie Zhang, Xiaojiang Du, and Mohsen Guizani. Blockchain-based incentives for secure and collaborative data sharing in multiple clouds. *IEEE Journal on Selected Areas in Communications*, 38(6):1229–1241, 2020.
53. Liehuang Zhu, Yulu Wu, Keke Gai, and Kim-Kwang Raymond Choo. Controllable and trustworthy blockchain-based cloud data management. *Future Generation Computer Systems*, 91:527–535, 2019.
54. Chi Harold Liu, Qiuxia Lin, and Shilin Wen. Blockchain-enabled data collection and sharing for industrial iot with deep reinforcement learning. *IEEE Transactions on Industrial Informatics*, 15(6):3516–3526, 2018.
55. Solonas Gousteris, Yoannis C Stamatiou, Constantinos Halkiopoulos, Hera Antonopoulou, and Nikos Kostopoulos. Secure distributed cloud storage based on the blockchain technology and smart contracts. *Emerging Science Journal*, 7(2):469–479, 2023.
56. Nabeil Eltayieb, Rashad Elhabob, Alzubair Hassan, and Fagen Li. A blockchain-based attribute-based signcryption scheme to secure data sharing in the cloud. *Journal of Systems Architecture*, 102:101653, 2020.
57. Xiaochen Zheng, Raghava Rao Mukkamala, Ravi Vatrapu, and Joaqun Ordieres-Mere. Blockchain-based personal health data sharing system using cloud storage. In *2018 IEEE 20th international conference on e-health networking, applications and services (Healthcom)*, pages 1–6. IEEE, 2018.
58. Hao Wang and Yujiao Song. Secure cloud-based ehr system using attribute-based cryptosystem and blockchain. *Journal of medical systems*, 42(8):1–9, 2018.
59. Chao Lin, Debiao He, Xinyi Huang, Kim-Kwang Raymond Choo, and Athanasios V Vasilakos. Bsein: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0. *Journal of network and computer applications*, 116:42–52, 2018.
60. Xinlong Li. A blockchain-based verifiable user data access control policy for secured cloud data storage. *Computational Intelligence and Neuroscience*, 2022, 2022.
61. Xiaohui Yang and Chenshuo Zhang. Blockchain-based multiple authorities attribute-based encryption for ehr access control scheme. *Applied Sciences*, 12(21):10812, 2022.
62. Mu Yang, Andrea Margheri, Runshan Hu, and Vladimiro Sassone. Differentially private data sharing in a cloud federation with blockchain. *IEEE Cloud*

Computing, 5(6):69–79, 2018.

63. Jiujiang Han, Ziyuan Li, Jian Liu, Huimei Wang, Ming Xian, Yuxiang Zhang, and Yu Chen. Attribute-based access control meets blockchain-enabled searchable encryption: A flexible and privacy-preserving framework for multi-user search. *Electronics*, 11(16):2536, 2022.
64. Xuanmei Qin, Yongfeng Huang, Zhen Yang, and Xing Li. A blockchain-based access control scheme with multiple attribute authorities for secure cloud data sharing. *Journal of Systems Architecture*, 112:101854, 2021.
65. Caixia Yang, Liang Tan, Na Shi, Bolei Xu, Yang Cao, and Keping Yu. Authprivacychain: A blockchain-based access control framework with privacy protection in cloud. *IEEE Access*, 8:70604–70615, 2020.
66. Yi Chen, Shuai Ding, Zheng Xu, Handong Zheng, and Shanlin Yang. Blockchain-based medical records secure storage and medical service framework. *Journal of medical systems*, 43(1):1–9, 2019.
67. Pratima Sharma, Rajni Jindal, and Malaya Dutta Borah. Blockchain-based cloud storage system with cp-abe-based access control and revocation process. *The Journal of Supercomputing*, pages 1–29, 2022.
68. Akanksha Saini, Qingyi Zhu, Navneet Singh, Yong Xiang, Longxiang Gao, and Yushu Zhang. A smart-contract-based access control framework for cloud smart healthcare system. *IEEE Internet of Things Journal*, 8(7):5914–5925, 2020.
69. Chunhua Li, Jiaqi Hu, Ke Zhou, Yuanzhang Wang, and Hongyu Deng. Using blockchain for data auditing in cloud storage. In *International Conference on Cloud Computing and Security*, pages 335–345. Springer, 2018.
70. Jiaxing Li, Jigang Wu, and Long Chen. Block-secure: Blockchain based scheme for secure p2p cloud storage. *Information Sciences*, 465:219–231, 2018.
71. Shangping Wang, Xu Wang, and Yaling Zhang. A secure cloud storage framework with access control based on blockchain. *IEEE access*, 7:112713–112725, 2019.
72. Yuan Zhang, Chunxiang Xu, Xiaodong Lin, and Xuemin Shen. Blockchain-based public integrity verification for cloud storage against procrastinating auditors. *IEEE Transactions on Cloud Computing*, 9(3):923–937, 2019.
73. Thein Than Thwin and Sangsuree Vasupongayya. Blockchain-based access control model to preserve privacy for personal health record systems. *Security and Communication Networks*, 2019, 2019.
74. Kun Hao, Junchang Xin, Zhiqiong Wang, and Guoren Wang. Outsourced data integrity verification based on blockchain in untrusted environment. *World Wide Web*, 23(4):2215–2238, 2020.
75. Ying Miao, Qiong Huang, Meiyan Xiao, and Hongbo Li. Decentralized and privacy-preserving public auditing for cloud storage based on blockchain. *IEEE Access*, 8:139813–139826, 2020.
76. Yuefeng Du, Huayi Duan, Anxin Zhou, Cong Wang, Man Ho Au, and Qian Wang. Enabling secure and efficient decentralized storage auditing with blockchain. *IEEE Transactions on Dependable and Secure Computing*, 19(5):3038–3054, 2021.
77. Jiannan Chen, Ying Wang, Zhaohui Huang, Conghao Ruan, Chunqiang Hu, et al. A decentralized public auditing scheme for secure cloud storage based on blockchain. *Wireless Communications and Mobile Computing*, 2022, 2022.
78. Zhenpeng Liu, Lele Ren, Yongjiang Feng, Shuo Wang, and Jianhang Wei. Data integrity audit scheme based on quad merkle tree and blockchain. *IEEE Access*, 2023.
79. Ruizhe Yang, F Richard Yu, Pengbo Si, Zhaoxin Yang, and Yanhua Zhang. Integrated blockchain and edge computing systems: A survey, some research issues and challenges. *IEEE Communications Surveys & Tutorials*, 21(2):1508–1532, 2019.
80. Qi Feng, Debiao He, Sherali Zeadally, Muhammad Khurram Khan, and Neeraj Kumar. A survey on privacy protection in blockchain system. *Journal of Network and Computer Applications*, 126:45–58, 2019.
81. Thomas McGhin, Kim-Kwang Raymond Choo, Charles Zhechao Liu, and Debiao He. Blockchain in healthcare applications: Research challenges and opportunities. *Journal of Network and Computer Applications*, 135:62–75, 2019.
82. Hao Wang, Hong Qin, Minghao Zhao, Xiaochao Wei, Hua Shen, and Willy Susilo. Blockchain-based fair payment smart contract for public cloud storage auditing. *Information Sciences*, 519:348–362, 2020.
83. Marko Vukolić. The quest for scalable blockchain fabric: Proof-of-work vs. bft replication. In *Open Problems in Network Security: IFIP WG 11.4 International Workshop, iNetSec 2015, Zurich, Switzerland, October 29, 2015, Revised Selected Papers*, pages 112–125. Springer, 2016.
84. Yang Lu. The blockchain: State-of-the-art and research challenges. *Journal of Industrial Information Integration*, 15:80–90, 2019.
85. Alex Kaplunovich, Karuna P Joshi, and Yelena Yesha. Scalability analysis of blockchain on a serverless cloud. In *2019 IEEE International Conference on Big Data (Big Data)*, pages 4214–4222. IEEE, 2019.
86. Ana Reyna, Cristian Martín, Jaime Chen, Enrique Soler, and Manuel Díaz. On blockchain and its integration with iot. challenges and opportunities. *Future generation computer systems*, 88:173–190, 2018.

87. Raad Mohammed, Raaid Alubady, and Ali Sherbaz. Utilizing blockchain technology for iot-based healthcare systems. In *Journal of Physics: Conference Series*, volume 1818, page 012111. IOP Publishing, 2021.
88. Yang Liu, Debiao He, Mohammad S Obaidat, Neeraj Kumar, Muhammad Khurram Khan, and Kim-Kwang Raymond Choo. Blockchain-based identity management systems: A review. *Journal of network and computer applications*, 166:102731, 2020.
89. Yingwen Chen, Linghang Meng, Huan Zhou, and Guangtao Xue. A blockchain-based medical data sharing mechanism with attribute-based access control and privacy protection. *Wireless Communications and Mobile Computing*, 2021:1–12, 2021.
90. Gábor Magyar. Blockchain: Solving the privacy and research availability tradeoff for ehr data: A new disruptive technology in health data management. In *2017 IEEE 30th Neumann Colloquium (NC)*, pages 000135–000140. IEEE, 2017.
91. Pei Huang, Kai Fan, Hanzhe Yang, Kuan Zhang, Hui Li, and Yintang Yang. A collaborative auditing blockchain for trustworthy data integrity in cloud storage system. *IEEE Access*, 8:94780–94794, 2020.