Integrated Blockchain and Cloud Computing Systems: A Systematic Survey, Solutions, and Challenges

JINGLIN ZOU and DEBIAO HE, School of Cyber Science and Engineering, Wuhan University and Shanghai Key Laboratory of Privacy-Preserving Computation, MatrixElements Technologies, China
SHERALI ZEADALLY, College of Communication and Information, University of Kentucky, USA
NEERAJ KUMAR, Department of Computer Science and Engineering, Thapar University, India
HUAQUN WANG, College of Computer, Nanjing University of Posts and Telecommunications, China
KIM-KWANG RAYMOND CHOO, Department of Information Systems and Cyber Security, University of Texas at San Antonio, USA

Cloud computing is a network model of on-demand access for sharing configurable computing resource pools. Compared with conventional service architectures, cloud computing introduces new security challenges in secure service management and control, privacy protection, data integrity protection in distributed databases, data backup, and synchronization. Blockchain can be leveraged to address these challenges, partly due to the underlying characteristics such as transparency, traceability, decentralization, security, immutability, and automation. We present a comprehensive survey of how blockchain is applied to provide security services in the cloud computing model and we analyze the research trends of blockchain-related techniques in current cloud computing models. During the reviewing, we also briefly investigate how cloud computing can affect blockchain, especially about the performance improvements that cloud computing can provide for the blockchain. Our contributions include the following: (i) summarizing the possible architectures and models of the integration of blockchain and cloud computing and the roles of cloud computing in blockchain; (ii) classifying and discussing recent, relevant works based on different blockchain-based security services in the cloud computing model; (iii) simply investigating what improvements cloud computing can provide for the blockchain; (iv) introducing the current development status of the industry/major cloud providers in the direction of combining cloud and blockchain; (v) analyzing the main barriers and challenges of

The work was supported by the National Key Research and Development Program of China (No. 2019QY0800), the Blockchain Core Technology Strategic Research Program of Ministry of Education of China (No. 2020KJ010301), the Shandong Provincial Key Research and Development Program (No. 2020CXGC010107), the National Natural Science Foundation of China (Nos. 61972294, 61932016, 61872192), the Special Project on Science and Technology Program of Hubei Provience (No. 2020AEA013), the Natural Science Foundation of Hubei Province (No. 2020CFA052), and the Wuhan Municipal Science and Technology Project (No. 2020010601012187). The work of K.-K. R. Choo was supported only by National Science Foundation CREST under Grant HRD-1736209, and the Cloud Technology Endowed Professorship.

Authors' addresses: J. Zou and D. He (corresponding author), School of Cyber Science and Engineering, Wuhan University, Wuhan, China, 430072 and Shanghai Key Laboratory of Privacy-Preserving Computation, MatrixElements Technologies, Shanghai, China, 201204; emails: cielozou@foxmail.com, hedebiao@163.com; S. Zeadally, College of Communication and Information, University of Kentucky, Lexington, KY, 40506-0224; email: szeadally@uky.edu; N. Kumar, Department of Computer Science and Engineering, Thapar University, Patiala, India, 147004; email: neeraj.kumar@thapar.edu; H. Wang, College of Computer, Nanjing University of Posts and Telecommunications, Nanjing, China, 210003; email: wanghuaqun@aliyun.com; K.-K. R. Choo, Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX 78249; email: raymond.choo@fulbrightmail.org.

0360-0300/2021/10-ART160 $15.00
https://doi.org/10.1145/3456628

integrated blockchain and cloud computing systems; and (vi) providing recommendations for future research and improvement on the integration of blockchain and cloud systems.

CCS Concepts: • **General and reference** → **Surveys and overviews**; • **Networks** → **Cloud computing**; *Network properties*; • **Computer systems organization** → **Cloud computing;**

Additional Key Words and Phrases: Blockchain, cloud computing, security service

ACM Reference format:
Jinglin Zou, Debiao He, Sherali Zeadally, Neeraj Kumar, Huaqun Wang, and Kim-Kwang Raymond Choo. 2021. Integrated Blockchain and Cloud Computing Systems: A Systematic Survey, Solutions, and Challenges. *ACM Comput. Surv.* 54, 8, Article 160 (October 2021), 36 pages.
https://doi.org/10.1145/3456628

1 INTRODUCTION

Over the past few years, we have witnessed a surge in interests in how blockchain can be applied to provide security services in the cloud computing model along with recently proposed blockchain-related techniques in current cloud computing models. Traditional security requirements include privacy protection, data protection, communication protection, and access control. The highly centralized and flexible architecture of the cloud computing model enables centralized processing for security requirements listed above, with guaranteed security benefits, but the model also introduces many unique security challenges [79, 171], which include damage to the data integrity, data leakage, unauthorized access, and so on. When multiple cloud users access the IT resources provided by the same **Cloud Service Provider (CSP)**, their trust boundaries overlap, which also brings about some new privacy and access control issues.

In the cloud computing model, users can access its resource pool and its services over the network, and in this environment, trust issues are critical [90]. If a system is trusted, then it means that users of the system are convinced that the system is correct and secure [84]. Some cases of dishonesty may occur in the cloud environment. For example, the data that should be deleted are not successfully deleted, and the CSP provides inaccurate services during the cloud service transaction and the **Service Level Agreements (SLAs)** of the cloud are not guaranteed. Therefore, the data operation security issues, audit issues, log security issues, and data source security issues in the cloud need to be taken seriously. This requires cloud providers to provide security services such as secure authentication, secure auditing, identity management [125], secure access control, and data encryption [18].

Blockchain is a distributed shared ledger maintained by multiple parties, featuring transparency, decentralization, traceability, security, immutability, and automation. The characteristics of blockchain allow it improve the security services in the cloud computing model.

The main advantages of the combination of blockchain and cloud computing are as follows: (1) Blockchain can replace trusted third parties in cloud; (2) stability (data backup is not easy to lose) [7]; (3) accessibility (blockchain can provide a more reliable access control methods); (4) Blockchain can help fight against corruption in CSPs [57]; (5) blockchain can automate various services in cloud, further reducing management costs and service errors; (6) blockchain can improve security issues and privacy issues in cloud computing [57, 89] and provide reliable auditing, certification, and services management and monitoring; (7) blockchain can establish a reliable reputation system in cloud computing [140]; and (8) cloud computing can meet the computing and storage requirements of the blockchain.

Gai et al. [33] discussed security and privacy issues in cloud computing and proposed three development type of Blockchain-Cloud Fusion model, namely, **Cloud over Blockchain (CoB)**,

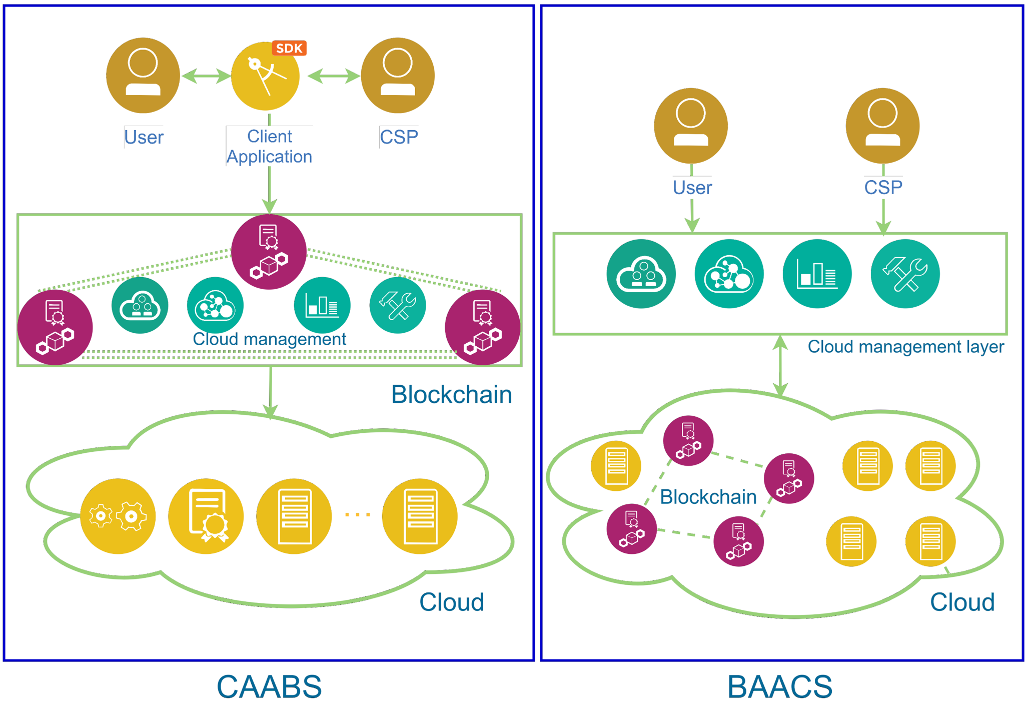

Fig. 1. BAACS and CAABS.

Blockchain over Cloud (BoC), and **Mixed Blockchain-Cloud (MBC)**. The CoB model is the model that deploys blockchain on the cloud as a functional tool such as to protect the data in cloud. BoC generally refers to the use of resources in cloud computing to undertake part of the workload of the blockchain. MBC commonly uses blockchain to record data usage in cloud systems and authenticate identities. In the MBC model, blockchain and cloud computing are two independent networks.

Based on Gai's work, we rename and further modify and clarify the integration models of blockchain and cloud. There are three types of integration model between blockchain and cloud: (1) **Cloud as a Blockchain Service (CAABS)**, use blockchain to manage cloud computing; (2) **Blockchain as a Cloud Service (BAACS)**, provide blockchain services in cloud computing platforms; (3) MBC, blockchain and cloud computing are two independent networks and the data of single or multiple layers in a cloud computing model is recorded, witnessed or verified by blockchain. The verb "witness" here means to record the hash values of certain data by blockchain as trusted evidence because of the immutability and security of the blockchain. The third combination is more complex.

The architectures of the BAACS and CAABS are shown in Figure 1, and the architecture of the MBC model is shown in Figure 2.

From the perspective of the overall architecture shown in Figure 2, the third combination of cloud and blockchain for security services has the following types:

(1) At the user layer, users can participate in the trading of cloud resources with smart contracts. The user's identity information can be managed and verified by blockchain. At the same time, when uploading, sharing, modifying, deleting and downloading data, users' operations can be supervised, verified and recorded by blockchain. For example, the operation of users can be supervised by event

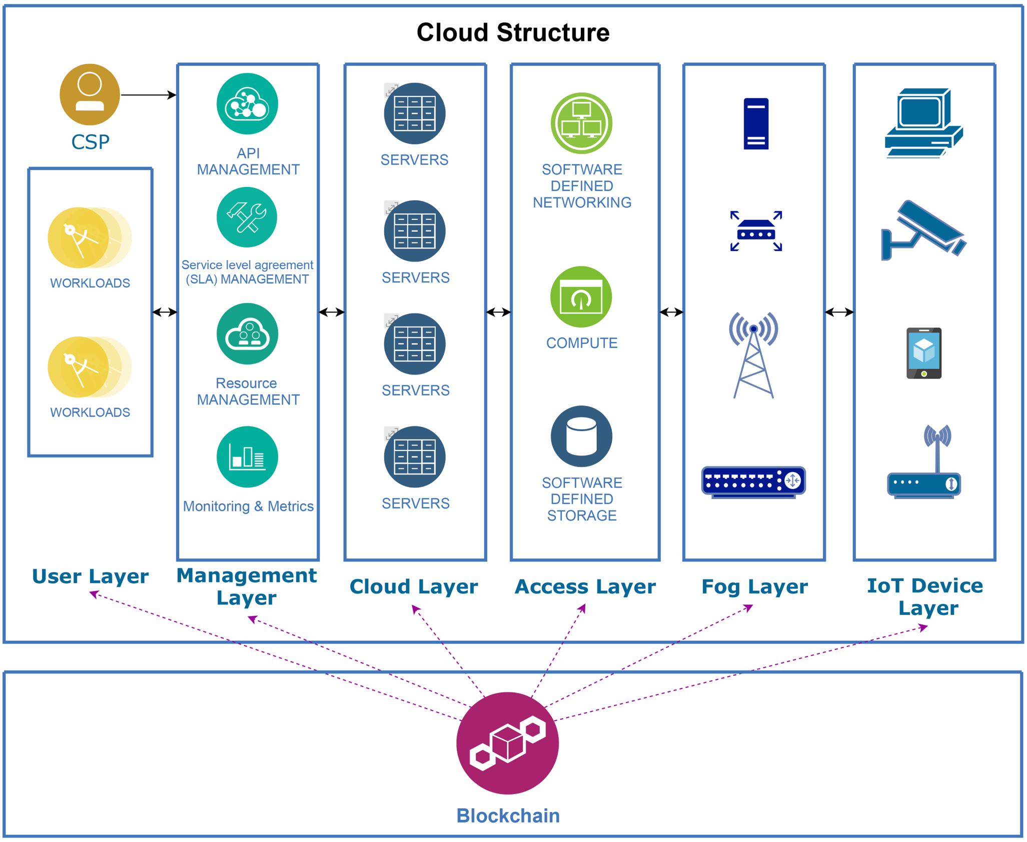

Fig. 2. Mixed blockchain-cloud.

listeners or smart contracts (users manipulate data through smart contracts). If the user is a visitor to the blockchain service instead of a member of the blockchain network, then the user layer does not need to be combined with the blockchain network.

(2) The management layer can be considered as a CSP management center. If multiple CSPs provide resources for the same cloud, then a blockchain-based platform can be designed for decentralized cloud resource management, price settlement, and data sharing between the CSPs. Similarly to the user layer, CSPs' operations can be supervised, verified, and recorded by blockchain. Users interact with cloud resources through this layer. Thus, designers can deploy access control, identity authentication, and logging functions at this layer in conjunction with blockchain.

(3) At the cloud layer, blockchain can be used to monitor and record, schedule resources, and migrate data.

(4) At the access layer, the blockchain can be used for device access management, authentication, and logging. Traffic from the fog layer and IoT devices can be directed to the access layer in conjunction with **Software Defined Networking (SDN)** technology.

(5) At the fog layer, the combination of the blockchain and the fog nodes enables the decisions of the fog nodes to be consistent. The blockchain can also be deployed at this level to prevent Byzantine nodes from doing evil and automatically supervising IoT devices.

(6) At the IoT layer, the blockchain is generally used to assist in device authentication and device management or to process information sent by IoT devices.

Based the above discussions, we summarize the roles of cloud in blockchain as follows:

(1) Client. As the client of blockchain network, cloud computing uses blockchain to store, authenticate, or witness data.

(2) Tradable resources. As a resource in the blockchain network, the cloud services are traded, delivered, and managed by blockchain.

(3) Management platform. Cloud can be used as a management platform of blockchain, and clients can obtain a deployed blockchain through the cloud trading platform. The nodes in the blockchain are composed of virtual machines in cloud.

(4) Computing resources. Cloud can be used as the computing resource of blockchain network. When some operations have heavy computation works, cloud can take the mission of them.

(5) Storage resources. Cloud can be used as a storage resource of blockchain to store data.

(6) Peers. Cloud can be acted as a peer node in the blockchain network. This blockchain network can be composed of CPSs for data sharing and mutual supervision or can be a complex blockchain network with multiple peers in which the server in the cloud acts as a common peer node member in the blockchain network.

Contributions of this work. This article focuses on the classification of security services' challenges that blockchain technology can solve in the cloud computing model. We summarize the main contributions of this work as follows: (i) We present recently proposed architectures and models that integrate blockchain with cloud computing, and the roles of cloud computing in blockchain in Section 1; (ii) we classify and discuss recent relevant works based on different blockchain-based security services in the cloud computing model; (iii) we investigate the performance improvements cloud computing can provide for blockchain; (iv) we present the current development status of the industry and major cloud providers in the areas of combining cloud and blockchain in the fourth section of the supplementary materials; (v) we analyze the main barriers and challenges when blockchain and cloud computing systems are integrated; and (vi) we provide recommendations for future research and improvements on the integration of blockchain and cloud systems.

1.1 Notations

We summarize and list acronyms that appear frequently in this article with standard definitions, as shown in Table 1.

1.2 Organization

The rest of the article is organized as follows. Section 2 is the core of this article, describing the literature on the integration of cloud and blockchain focusing on security services, applications, and methods. Section 3 concludes the use of cloud computing in blockchain environments. In Section 4, we analyze the current issues and challenges, discuss recently proposed integration solutions of cloud and blockchain, and the security attacks/threats blockchain-based security solutions can or cannot protect against in a cloud computing system and provide some recommendations for future research. Finally, Section 5 summarizes our work.

In the supplementary materials, we present related reviews on cloud computing and blockchain integration, describe the methodology we used in our survey, present some basic concepts of cloud computing and blockchain and summarize the current efforts and research results of industry/major CSPs. In addition, we have added two discussions in the supplementary materials. One is to classify the literature studied in this article according to the four solutions in Section 4.2.1, further subdivide the approaches used in the literature, and describe the advantages and disadvantages of these approaches. The other is to discuss how blockchain logs can help improve the compliance of cloud services specifically considering EU GDPR and its offshoots.

Table 1. List of Acronyms with Standard Definitions

Standard definition	Acronym	Standard definition	Acronym
Denial of Service	DOS	Distributed Denial of Service	DDOS
Cloud Service Provider	CSP	Service Level Agreement	SLA
Quality of Service	QoS	Research Question	RQ
Elliptic Curve Digital Signature Algorithm	ECDSA	Proof of Work	PoW
Proof of Stake	PoS	Practical Byzantine Fault Tolerant	PBFT
Inter Planetary File System	IPFS	Electronic Health Record	EHR
Public Key Infrastructure	PKI	Virtual Machine	VM
Third-Party Auditor	TPA	Ciphertext-Policy Attribute-Based Encryption	CP-ABE
Edge Computing Service Provider	ESP	Cloud as a Blockchain Service	CAABS
Blockchain as a Cloud Service	BAACS	Mixed Blockchain-Cloud	MBC
Blockchain as a Service	BaaS	European Union General Data Protection Regulation	EU GDPR

2 BLOCKCHAIN IN CLOUD ENVIRONMENTS

Blockchain can achieve consensus on a mutual untrustworthy scenario. For the cloud computing model, the application of blockchain technology enables users to trust CSPs. For example, blockchain can be used to implement identity management and access control systems. When managing users through smart contracts, without third-party participation, all records can be traced and records are difficult to modify. The goal of this article is to explore how blockchain and cloud can be combined and propose blockchain-based security solutions that can address security, privacy, and trust issues in the cloud computing model.

In this section, we classify the reviewed papers into five sub-categories based on their security services: data integrity, data sharing, data provenance and auditing, monitor and management, authentication, and access control. We analyze and describe the issues covered by the five categories of articles and the solutions they propose. Under each category, we further classify papers according to application scenarios. The second table in the supplementary materials classifies the collected papers based on the five categories and further sorts the papers by their application scenarios.

2.1 Data Integrity

Cloud computing is considered to be a good solution to the problem of growing data storage costs [60]. An increasing number of businesses and individual users choose to store and process their data with cloud computing services to save costs. Users can access the data kept by cloud through the network. This means that the integrity of the data may be compromised when it is stored in the cloud. In other words, the likelihood of whether the data have not been tampered with or destroyed while being stored in the cloud is not guaranteed.

2.1.1 Data Integrity in Database. In terms of data integrity protection in the database infrastructure in the cloud computing architecture, Ren et al. [103] discussed the threats of electronic record management in the cloud computing architecture and proposed to store the electronic record with blockchain in cloud. Du et al. [23] also store the data directly in the blockchain. To solve the query efficiency problem of the Merkle tree, they propose to use the Skip List structure instead of the Merkle tree. However, the method of using blockchain to store all data is not suitable, because the blockchain stores data with high overhead and peers having a copy of the blockchain locally would be able to see the contents of a file. Hence the blockchain is not suitable for applications that need to store large amounts of data.

Storing the data themselves in the cloud and storing the metadata of the data in the blockchain is a better solution. For example, in Deng's work [104], only the hash value of the electronic record is stored in the blockchain and the electronic records thenselves are stored in the cloud when solving the problem of integrity, authenticity, and reliability of electronic records. In Zhu's work [168], a blockchain-based decentralized cloud resource scheduling architecture, the hash of the data (the original data are in the cloud database), commands, and scheduling data are recorded by blockchain.

To weaken the CSPs, a searchable encryption scheme for multiple cloud storage using double-layer blockchain [30] no longer uses the cloud to store encrypted data. They use **Inter Planetary File System (IPFS)** [13] to store encrypted data, a consortium chain composed of CSPs to store indexes in IPFS and keywords in searchable encryption scheme, and a public blockchain to witness the consortuim chain.

Other researchers have proposed data integrity protection schemes from the perspective of database operations. For example, Gaetani et al. [32] described the importance of data integrity and some of the current issues data faces. They further analyze the threat of data integrity in the cloud environment. They identified three integrity threats of the database in cloud environments: (i) the attacker directly tampers with or destroys the database to destroy the integrity of the data, (ii) a member updates the database secretly, and (iii) multiple members collude to maliciously alter the database. They design a two-layer blockchain to record the cloud members' operations on the database. The first-layer blockchain logs the operations in the database. The second-layer **Proof of Work– (PoW)** based blockchain witnesses the first blockchain by the anchoring technique, which means that the hash of the first-layer blockchain will be kept by the second-layer blockchain to prove the integrity of the first layer. Considering the performance of PoW, the first blockchain layer uses the method of rotating master node that is called the mining rotation consensus mechanism instead of the PoW consensus mechanism. The consensus algorithm reduces the difficulty of tampering with the blockchain data to some extent, so they introduce a second blockchain layer to witness the data in the first blockchain layer, for further ensuring the security and reliability of the data recorded in the first blockchain layer.

2.1.2 *Protection of Key Data.*

In addition to using blockchain to record the hash value or metadata of the data, blockchain can also be used to record important information related to the integrity of the data. ChainFS [126] stores files with the cloud computing services and transfers minimal and necessary functions such as key distribution and logging of file operations to the blockchain. Angelo et al. [21] also proposed a similar approach for the protection of flight data.

Deng et al. [22] proposed a blockchain-based trusted electronic records preservation scheme. They store the owner of the record and generate the Submittal Information Package, Archive Information Package, and Dissemination Information Package and the corresponding metadata in the blockchain where these data are obtained from from the Open Archival Information System model [62]. They use this model to store the original electronic records in the cloud architecture. Additionally, they use the traditional Provable Data Possession or Proofs of Retrievability [46] to check the integrity of the original records regularly and use erasure code technology to recover any missing records.

2.1.3 Protection of Files. It is common to use blockchain to store files or store metadata of files [23, 126]. There are also some researchers who use smart contracts instead of transaction fields to record data such as metadata of files, which has the advantage of being able to track operations on files using smart contracts. Wang et al. [137] upload the encrypted file to the cloud and generate a smart contract with the file address, encryption key, and other information in the blockchain. A cloud blockchain-based public key infrastructure [51] is designed to protect the integrity of certificates. They embed the certificate data and status into smart contracts instead of the transaction data field of a block to reduce the size of block to be mined and save 87% cost per certificate.

Some researchers have taken full advantage of the characteristics of the Merkle tree. Xie et al. [141] uses the characteristics of the Merkle tree to store the hash digests of all root nodes of the Merkle tree in the master node and protect the leaf node's file on the Merkle tree by continuously examining the consistency of the hash value of the root node. Yue et al. [152] made further improvements over Xie's work [141] by using the characteristics of the Merkle tree. In their proposal, the data of the client are sliced into several parts that are constructed into a hash Merkle tree. Then, the client uploads his/her data and the hash Merkle trees to the **Cloud Storage Servers (CSS)** and uploads the root of the hash tree to blockchain. When the client needs to verify the integrity of one slice of data, he/she sends a challenge to the cloud. 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 data integrity.

2.1.4 Data Integrity Protection in Specific Application Scenarios. In terms of protecting the **Electronic Health Records (EHRs)**, Nagasubramanian [85] and Omar [3] store the personal EHR [35] in the blockchain directly. Nagasubramanian et al. [85] put e-health records in a blockchain that is deployed in the cloud. In addition to using attribute-based encryption schemes to protect user privacy data, they also use Keyless Signature Infrastructure to allow users to prove the registered time of health data. The system proposed by Omar et al. [3] is relatively simple. They use the blockchain as a database for storing healthcare data and use public key technology (for example, Elliptic Curve Cryptography [45, 54]) to encrypt private data.

Similarly to the previous description, in addition to storing data directly using blockchain, there are other ways to protect the integrity of EHRs with blockchain. Wang et al. [135] encrypted the data by using attribute-based encryption and uploaded it to the cloud for storage. The blockchain is used to record the message of the encrypted data and the address information. To prevent a malicious doctor from colluding with the CSPs to modify EHRs, Cao et al. [16] proposed a system that records EHRs into cloud servers after integrating EHRs into a transaction (metadata including the hash value of EHRs and warrants) on the blockchain while every operation was recorded in the blockchain. CSSs authenticated the doctor(s) by examining the validity of the patient's delegation.

To better monitor and record the operations on EHRs, some researchers use smart contracts instead of transaction fields to record data. Qi et al. [139] monitor data operations on the database facilities and controlled the access rights with a smart contract. Qi et al. developed a blockchain-based data-sharing mechanism for EHRs to ensure data security and data source security while allowing data sharing among untrusted parties through blockchain technology and digital signature technology on existing database facilities. After the user's request is translated by the Data Query layer, the validity of the request is verified in the Data Structuring and Provenance layer. Then, the data are acquired after the request is successfully verified. After processing the sensitive data and generating a tracking smart contract, the request and the operation data are recorded in the blockchain. Similarly, Liu et al. [73] store the key data of EHRs in the blockchain and use smart contract to audit and manage the access and permissions. To further protect user privacy information in the wireless network environment, Liu et al. [73] designed a scheme that is used when storing data in the blockchain and cloud: a heterogeneous signcryption scheme based on **Public Key Infrastructure (PKI)** and Certificateless Cryptosystem.

To store the **Virtual Machine (VM)** measurement data in the IaaS cloud in the blockchain for protection and to optimize the performance of the blockchain, Zhao et al. [162] designed a two-layer blockchain. After the first layer verifies the packet, a semi-finished block is constructed on a candidate block. The semi-finished block is then broadcasted to all nodes. In the second layer, a PoW task needs to be performed on the semi-finished product block. The metadata generated in this way is tamper-resistant.

Under the premise of providing storage resources in P2P form, Li et al. [64] considered all the free storage space of all users as a storage pool and provide cloud storage services to other users. The blockchain is used to record the URL of file blocks, file hashes, and transactions.

2.2 Data Sharing

Data encryption can improve the security and privacy of data stored in the cloud so that the CSP can provide an encryption scheme and schedule data backups [50]. In addition to storing and transmitting data reliably, it is also important to share data securely among users. Data Sharing involves the questions of when and where the data are encrypted, when and where it is decrypted, and the methods used to share the key. This section introduces the works of researchers who are using blockchain to handle data sharing in the cloud computing architecture.

2.2.1 Data Sharing. To enable the data owner to control the anonymization process, Yang et al. [149] use blockchain smart contracts and differential privacy technology [25] to store, verify, and adaptively allocate privacy budget consumption according to the data owner's requirements. The privacy budget is the amount of noise produced in the obfuscation process of privacy. Once the privacy budget is exhausted, data sharing ends.

To avoid obtaining incorrect data in the cloud caused by a malicious database, Hu et al. [37] suggested not to use a centralized server but to outsource search queries to a smart contract and propose a decentralized privacy-preserving search schema. They combine the search service and the transaction so that the decrypted data can be obtained only with a certain fee. Li et al. [67, 68] used a similar approach wherein they complete the transaction and payment by using a smart contract for data-sharing purposes.

2.2.2 File Sharing. Figueira et al. [28] discussed various blockchain technologies in detail and introduced the technical analysis and the decision processes of implementing their data-sharing scheme. They designed three smart contracts for data sharing. The functions of the three smart contracts include: file management and tracking, share agreements management, and access request submission. There are some schemes [26, 138] uses the proxy re-encryption method to re-encrypt data to better protect the confidentiality of the data. When a user requests to download an encrypted data, the cloud will re-encrypt the data encrypted by the data owner before sending it to the user. Blockchain is used to record the ciritical data such as the index and location of a data during the sharing process.

To resolve operational conflicts of the shared file, Huang et al. [38] considered using the blockchain "fork" [112] conflict resolution method. They introduced a group manager to record previous changes. When a signature conflict occurs, each signature of the file in the blockchain is recorded in chronological order, and only one person can sign. With reference to the processing method of the consensus algorithm, when multiple members update the same file, and other members must update according to the latest version in the data-sharing group, the group's administrator accepts the earliest update.

2.2.3 EHRs Sharing. To protect EHRs during sharing, a blockchain-based personal health data-sharing system [164] using cloud storage is proposed. A transaction is generated when encrypted data has been uploaded to a cloud by a user or when a customer wants to purchase data. The key to decrypt the data is divided into different shares that are kept by different key keepers. When a data-sharing transaction is verified, a notification requesting that the corresponding key share be released to the client of the transaction is sent to the key keepers. After confirmation, transactions are included into the blockchain. Besides, they also developed a quality inspection module that uses machine learning techniques to detect the quality of user data and record the results in transactions generated when the data are uploaded. This is a basic and effective data-sharing scheme that combines blockchain and cloud technologies.

There is another sharing scheme [139] proposed by Qi et al. for medical data sharing in a non-trusted environment. First, the requester uses the requester's private key to create, sign, and send a request to the data owner who uses the requester's public key to verify the signature to confirm the request. After successful confirmation, the entire package (the final processed data to be delivered to the requester) is encrypted by the authenticator's contract key, and the package is shared with the requester who then decrypts the packet.

Nguyen et al. [88] use smart contracts and blockchain to upload and share data securely. The medical records are stored in the IPFS nodes after being encrypted. Smart contracts are used to identify, validate the request and grant access permissions. They introduce an EHRs manager to verify requests with a strict control policy, decrypt EHRs and return these requested EHRs to the requestor. They also introduce a gateway to encrypt data with the public key of the EHR's manager and upload it to the IPFS.

2.2.4 IoT Data Sharing. The distributed nature of the blockchain coincides with the distributed nature of the IoT, so the blockchain is very suitable for data sharing in the IoT. Fu et al. [31] designed a blockchain-based mobile edge cloud resourses allocation system. In this system, blockchain is deployed at the network function virtualization management and orchestration systems to share messages and make sure everyone accept the same message. They improved PBFT based on the characteristics of their own network environment.

Intelligent and decentralized edge nodes of the IoT face the problem of difficulty in reaching consensus on learning results. To solve this problem, a blockchain-assisted collective Q-Learning approach [100] is proposed. In their approach, after local training of **deep neural networks (DNNs)**, each edge node of the IoT network shares the learning results through the blockchain and reaches a consensus. Here, the summary of the training parameters and other necessary records in DNNs are encapsulated into a transaction. They designed a new consensus mechanism, **Proof of Learning (PoL)**, in which the IoT node with the minimum reduced percentage of learning loss function gets the right to generate the current block. After the block is generated, other IoT edge nodes verify the hash result of the last block, the learning conditions of the transactions and whether the reduction percentage of the learning loss function is the smallest. Then the IoT edge nodes update the parameters of their local DNN.

2.3 Data Provenance and Auditing

Data provenance [116] describes where a piece of data has originated from and how it has arrived into a database. Data provenance and auditing have positive implications for accountability, auditability, and identification attacks. After summarizing the current technologies in cloud forensics storage, Ricci et al. [106] took STORJ as an example and discussed the issues and challenges of a blockchain-based distributed cloud storage system for digital forensics.

2.3.1 Data Integrity of Cloud Logs. Some blockchain-based cloud systems introduce a third-party auditor. In the field of cloud forensics, after the auditors have collected the forensics data and have signed using a group signature, Zhang et al. [159] anchored the data (i.e., recording the hash and signature of the relevant forensics data into the blockchain) to the blockchain network. Wang et al. [136] record the logs in the form of a Merkle tree structure. The third-party auditor can verify the integrity of the cloud logs with the corresponding records on the blockchain.

To keep auditors from procrastinating and doing evil and address the certificate management problem, Zhang et al. [160] proposed a Certificateless Public Verification scheme against Procrastinating Auditors. The original data are kept by the cloud. The **Third-Party Auditor (TPA)** sends the challenge message to the cloud server. If the corresponding proof from cloud server is valid, then the data integrity is not destroyed. If the checking fails, then TPA will inform the user. The TPA stores the proof in a log file and establishes a transaction in which a zero deposit will be transferred to the user's account (Ethereum). The user checks the logs in the blockchain. The TPA checks the data integrity according to the user-defined verification period and checks the validity of proof with the regenerated challenge message.

Rane et al. [101] designed BlockSLaaS to ensure the integrity and confidentiality of the logs from a virtual environment and record the encrypted logs with blockchain. The Cloud Forensic Investigator can only access logs via BlockSLaaS.

Reddy et al. [75] use the blockchain to record log information for auditing to ensure data integrity in cloud forensics. For saving computational overhead, some CSPs do not participate in the consensus. Similarly, blockchain is used to record alarms and logs in the **Intrusion Detection System (IDS)** system of cloud computing environment [6, 59]. Miao et al. [80] use zero-knowledge proof to prevent users' information from leaking to a TPA.

2.3.2 Automatic Auditing. Most systems do not consider third-party auditors. Li et al. [63] developed a blockchain-based behavior audit framework that records user's operations on files and stores the metadata of files with blockchain. The client automatically records all operations of the user on the file.

For the privacy issue of data provenance, Zhang et al. [158] proposed an efficient and secure data provenance scheme. The original data of all provenance record forms a record chain and each record is integrated into a transaction. To retain the revision history of **Building Information Modeling (BIM)**, Zheng et al. [163] proposed a BIM data organization method based on blockchain in which the BIMs and the modified message are stored in blocks of blockchain.

ProvChain [69] and Tosh et al. [130] use hooks and listeners (special classes of event listeners) to monitor the provenance data generated by a user and store the data in a blockchain. BlockCloud [114, 131] also uses hooks and listeners to generate provenance data. BlockCloud records the hash of the data and the hash of the user ID into the blockchain. The auditors cannot identify specific users and data operations, but they can verify audit data by retrieving transactions.

However, using hooks and listeners or manual operations still provide an opportunity for hackers to hack. Qi et al. [139], Reddy et al. [75], Renner et al. [105], and Wang et al. [137] use smart contracts for data auditing and data source recording. Qi et al. [139] designed MeDShare to verify the request sent by all users. After the verification is passed, the request is recorded in the blockchain and executed, tracked, and monitored by a smart contract. All the operations to data are recorded in the side chain. MeDShare's data source is obtained from smart contracts. Renner et al. [105] proposed Endolith based on Ethereum technology [15]. Endolith uses blockchain to store the selected metadata for files and uses smart contracts to provide auditing functions for file verification and history tracking. Wang et al. [137] generate a smart contract for each encrypted file that the data owner uploads into the cloud, using this smart contract to record all the actions that occurred on the file for auditing. The proposal of Ali et al. [4] on data provenance and auditing uses smart contract monitoring equipment, and stores the original data in the cloud while important information such as the hash of the original data is recorded by blockchain.

2.4 Monitor and Management

Traditional CSP is subject to external auditing, security verification and the service level agreements are regularly reviewed [19]. If the CSP does not follow the rules and protocols, then it results in a significant drop in the trust of customer. Ogiela et al. [91] introduced some new ideas for blockchain in data manipulation, data management, and services management. These protocols include a secure data distribution protocol between hierarchies and layers, a common data sharing and distribution protocol without any constraints for data fusion and relationships between layers, and an authentication protocol based on knowledge verification, in which only users who answer specific questions correctly can get access to data or computer systems. This section summarizes the researches on how to use blockchain technology to solve monitoring and management problems such as secure data deletion, secure data migration, data management, service management and device management in a cloud computing environment.

2.4.1 Secure Data Deletion. Yang et al. [147] addressed the problem when the data deletion service in the cloud could not be verified and presented a blockchain-based data deletion scheme. The user encrypts the data and uploads it to CSP and submits the deletion request when the data need to be deleted. After the CSP overwrites the deleted data, it generates a proof and submits it to the blockchain network. After the timestamp server receives the root hash of the proof tree, it verifies all the proofs and stamps it with a timestamp. With the signature and timestamp of the timestamp server, the cloud server can generate a block, and the user can find the corresponding proof from the blockchain and verify it. Li et al. [65] also focused on data deletion using smart contracts to manipulate the data and using blockchain to record data labels.

2.4.2 Secure Data Migration. When the network is congested, the migration of VMs between data centers may incur high overheads. Xu et al. [145] attempted to improve energy efficiency to task scheduling in blockchain-based cloud computing architectures through a cost minimization algorithm. The cost minimization algorithm is a smart contract that would migrate requests and VMs between data centers based on the energy cost of historical migration decisions. Meanwhile, the resource allocations are recorded by transactions.

A blockchain-based secure VM migration control mechanism [133] is proposed to address the problem of unaware and improper transfer of data during VM migration in the cloud computing environment. When requesting migration, the protection scheme gathers the <Country> attribute and the <Organization blockchain target host> attribute together and then stores them in the <Regulation> attribute and checks if the two attributes are legal. The proposed mechanism saves the modification history of the <Country> attribute and the <Organization blockchain target host> attribute, and checks whether tampered data exists in the blockchain.

2.4.3 Data Management. In the field of data monitoring, Kirkman et al. [53] pointed out the issue of SLAs that whether the SLA system is run and stored by the cloud itself or managed by a third party, it is not secure. Because when the SLA model is managed by the cloud itself, there is a conflict of interest; when the SLA model is managed by a third party, there are also trust issues. Therefore, Kirkman uses smart contracts to record the consumer's address and the cloud service strategy he/she uses. Zhou et al. [166, 167] extended the work of Kirkman et al. [53]. To address the challenge of proving the credibility of possible interventions in the SLA before recording them with blockchain, they proposed the use of smart contract monitoring, inspecting and processing the violations in cloud services. They introduce "witness" using game theory and smart contract technology to discover and report service violations and to guarantee the trustworthiness of the witness. Anyone can become a witness, but only if he or she is selected by an unbiased sortition algorithm to become a witness to a service and receive a certain amount of compensation. He/she is rewarded if he/she detects violations and reports them successfully. The specific violation reports and reward mechanisms are all executed through smart contracts.

Neidhardt et al. [87] proposed a blockchain-based cloud billing service solution, because the verification of the billing process and the provider's adherence to SLAs can be difficult to track for the customer. They introduce custom Service-Coins, which can be traded between Ethereum wallets, to track the services provided by service providers. They designed a SLA-monitoring smart contract to monitor whether the provided service was available, and if the service is not available, the smart contract sends SLA coins to a list of customers. Hwang et al. [39] adopted a similar method. When the smart contract detects a proof of violation, the user will receive digital currency compensation.

Sukhodolskiy et al. [122] have designed smart contracts that are related to access policy for users to access files. In Zhu's mechanism [169], the changes on files will be voted by users to decide whether users approve the change while the changed document will be stored in the cloud. Shu [115] designed a high-performance online auction system where blockchain was used to record the winner's data during the auction process.

2.4.4 Service Management. In the field of service management, the information obtained by users comes from CSPs. Therefore, these transactions on the cloud need to be truthful, transparent, and credible. BPay [157], a blockchain-based cloud outsourcing service payment framework, addressed data security and online payment threats. They propose an all-or-nothing checking-proof protocol wherein the outsourcing service provider either gets the services or loses everything. Blockchain is used to record the execution of services and the outsourcing service transaction is implemented based on the bitcoin-based timed commitment scheme [8]. If the service provider provides a valid service implementation proof in accordance with the commitments of the transaction, then the service fee can be obtained. If not, then the service provider will be compensated.

CloudChain [124], a blockchain-based cloud federation framework is designed to trade computing resources in cloud. CloudChain has three types of smart contracts, namely CloudChain Registry for mapping identification values to their Ethereum address identities or mapping identities to a **CloudChain Contract (CCC)** address, CloudChain Profile for recording the engagements of users and providing notifications, and the CCC for trading. Additionally, they designed and solved a differential game to optimize their transaction cost, time, and reputation value. Similarly, Pittl et al. [96] proposed a multi-round bilateral negotiation approach of cloud services' transactions by using a smart contract.

Yin et al. [150] developed a distributed cloud service evaluation method. The cloud service is measured by a unified description specification of cloud services based on different levels of indicators when multiple vehicular clouds collaborate. Oktian et al. [92] use smart contracts to enable clients to use fixed or pay-as-you-go subscription methods for cloud services. After a transaction, the client can obtain the access token from the CSP and the client needs to request an access token with a signature signed by the same public key used in the previous stage to pay for the subscription fee. Hence the provider can check the eligibility of the client with the signature and the information of corresponding smart contract.

Similarly to cloud service transactions, other transactions that use cloud computing services also need to be regulated.

2.4.5 Device Management. Cloud manufacturing [127] has brought about a new service-oriented and real-time manufacturing model, and users can access the services provided by cloud manufacturing on-demand via the network [127]. A manufacturing knowledge sharing system [66, 67] uses cloud storage Injection Mould Redesign data, keyword extraction methods to build a unified data structure, and smart contracts to complete knowledge transactions. They describe the architecture, which includes five main layers. The data collected by an IoT device are changed into a hash in the **Manufacturing Service Provider Layer (MSPL)** and the blockchain client is also located at the MSPL. The blockchain client is in charge of connecting to the network and monitoring the block and note. Note saves all hash data and transactions on the cloud database. Each note will create a new block after winning the consensus contest. Moreover, users can request services through blockchain and trade manufacturing services with the service providers using smart contract.

Celiz et al. [17] proposed a cloud model to manage drug procurement based on IoT and blockchain. The IoT layer sends the information (such as location, humidity, and temperature) about the product, to the blockchain layer deployed at the cloud. If the order conditions are met, then a corresponding smart contract is created. Barenji et al. [9] use two blockchain services in their systems, and the public chain is used at the service provider level. The public chain consists of service providers and users. They complete communications and transactions on the public chain; the private chain is used at the machine level and it is connected to the machine level for data reception and collection.

In a service composition architecture [151] in cloud manufacturing, the smart contract records the **Quality of Service (QoS)** attributes of the service provider. If a manufacturing proposal is agreed by users, then a corresponding smart contract is created and the manufacturing is initiated.

Ali et al. [4] use smart contract monitoring equipment and the hash of the original data is stored in the blockchain. Nadeem et al. [83], Sharma et al. [113], and Qiao et al. [98] also use blockchain to establish a trust relationship between SDN controllers. Because the computing power of the fog node may not be high, Sharma [113] proposed a new consensus mechanism, Proof of Service, which determines who gets the right to generate blocks by the contributions of nodes. Actions outside the blockchain are contributions, such as sharing a file or find some data. The architecture enables every IoT device to access computing capabilities with low end-to-end latency. In this proposal, users choose a CSP. In addition, all the SDN controllers in the fog nodes are connected in a distributed way using blockchain.

Blockchains can also be used to monitor IoT devices [94]. Yang et al. [148] proposed a Blockchain-based Trusted Authentication architecture that was also associated with SDN controllers. They were concerned about the access problem of multiple IoT devices in the 5G environment. They used blockchain to submit requests to the SDN controller and record the reply and all committed access identification information. Then, they proposed a Blockchain-based Anonymous Access scheme by negotiating the key material and using the zero knowledge proof.

Liu et al. [72] implemented PoW by introducing data coins and energy coins and applying data contribution frequency and energy contribution to safeguard vehicle interactions in cloud computing and edge computing for electric vehicles. Vehicular records created during vehicle interactions are kept by a consortium blockchain. The blockchain strategy is also commonly used in access control and identity management in the IoT scenario [2, 128].

Singh et al. [118] proposed an IoT smart home architecture. Transactions stored in the local blockchain, which is also known as sidechain, manage all devices. A consortium blockchain is deployed to perform access control on requests that need to access the IoT data. The smart home can get more information and services from the cloud. A blockchain-based reputation system [102] is designed for incentivizing crowdsourcing [82] and identifying the malicious participants of Mobile Ad-hoc Cloud [78] who would present fake results for rewards. They maintain and update the credit and score of every device with blockchain. In their proposal, a non-trusted device will become a trusted device after its legitimate computational efforts have reached some threshold. Once a fake result submission is identified, the corresponding malicious device will be transferred to a blocked device group and will no longer be scheduled with work.

2.5 Authentication and Access Control

Access control refers to restricting the activities of legitimate users and authorization [111] is a function of granting access right to users. The decentralized, autonomous nature of blockchain allows it to control the access well.

2.5.1 *User Authentication.*

Saranyu [86] is designed to manage tenants and service accounts in cloud centers. Identity management and authentication are handled by the public and private keys of the blockchain account. Authorization and billing are handled through smart contract operations.

Ahmad et al. [2] integrated face recognition and blockchain technology to improve IDentity Management. Specifically, they combined the faceID with the blockchain account and used the blockchain to verify the information identified by the cloudlet and performed other operations based on the smart contract.

Bendiab et al. [12] proposed a cloud identity management trust model with blockchain. In their proposal, the blockchain network consists of some CSPs and all authentication transactions are kept in the blockchain. Access tokens are created and stored by transactions. An access token is about the identity and privileges of the specific user. If a user uses multiple cloud platforms at the same time, then Fiore [29] tried to aggregate their accounts from different clouds by recording and managing metadata about users, clouds, files, and permission with blockchain.

A human-centric, intelligent, and secure authentication management scheme [52] is proposed with using blockchain to store trusted personal resource information in a mobile cloud computing environment. If a client mobile device node wants to connect with a master mobile device node, then it needs to create a block and send the block and its information to the master node. The master node creates a block after receiving the client's information and the block is compared with the block created by the client node. If there is no difference, then the client block is connected to the master block. If there is already a client node connected to the master node, then the block created by the new client and its information need to be sent to all linked client nodes.

2.5.2 *Device Authentication.*

Yang et al. [148] access the SDN controller through the blockchain to solve the problem of trusted access network. In Tapas's work [128], an IoT-Cloud authorization and delegation mechanism with blockchain, and smart contracts is used to authorize roles, validate user access, and log the request to avoid the possible threat from malicious administrators and/or unfair internal policies.

Barger et al. [10] proposed combining the **Cloud Object Store (COS)** with the blockchain and using the blockchain for COS's access control.

2.5.3 *Access Control.*

In terms of access control, Du et al. [23] stored the data in the blockchain and included an Identity layer above the blockchain. The Hierarchical Identity-Based Broadcast Encryption scheme is used for identity management and access management. Sukhodolskiy et al. [**?**] record the events (such as key generation and access policy assignment) related to access control by blockchain. Blockchain can also be used to store access control lists such as BACC [120], a decentralized blockchain-Based access control model, and Liu's work [73]. In BACC, after data are encrypted and uploaded to the cloud, the decryption key is divided into n decryption key pieces according to Shamir secret sharing scheme. After the user is checked for access permission through the smart contract, he obtains the addresses of t nodes with decryption key pieces through another smart contract. Qi et al. [139] use blockchain to authenticate user requests and share data.

Osei-Bryson et al. [93] proposed a blockchain-based security-oriented framework for cloud federation to permit secure access controls and QoS constraints. The secure communications between access control systems and the federation members are guaranteed by the asymmetric encryption algorithm of blockchain. They introduce a new layer called the infrastructure tenant to record access logs and deploy tasks to the corresponding service. The access logs created are preserved by the mining rotation-based blockchain layer while the mining rotation-based blockchain is witnessed by another PoW-based blockchain, which means the hash values of the mining rotation-based blockchain are kept by the PoW-based blockchain to further guarantees the security of the data stored in the mining rotation-based blockchain layer. The PoW-based blockchain is more secure, but the performance is worse. Therefore, the PoW-based blockchain is only suitable for storing a small amount of critical data. The PoW-based blockchain can verify whether the first layer of blockchain has errors.

In a healthcare application, the patient can change the nursing team, so Kurdi et al. [61] proposed HealthyBroker to establish trust and transparency among the care-team members by auditing service transactions and the care team's feedback on exchanged services with blockchain. HealthyBroker can identify care-team members and grant them access to patients' data on a "need-to-know" basis.

There are also some problems with the blockchain itself such as the risk of a majority (or 51%) attack, and some researchers believe that the regulation of the blockchain is insufficient. Therefore, a presented a blockchain-based data management scheme [169] is proposed to mitigate some of the limitations of blockchain. The operations on documents are voted by users to decide whether users approve the change after which the changed document will be stored in the cloud. Blockchain system counts the votes and record the operations. They introduced a **Trust Authority (TA)** that could reject invalid operations regardless of other users' opinions to prevent malicious voting. As Public-key Encryption with Keyword Search is vulnerable to **Keyword Guessing Attacks (KGA)**, Zhang et al. [161] integrate keyword request from users into a transaction to protect key servers from KGA. When the number of transactions created by a user reaches a certain limit, the key servers will stop responding to the user.

Sukhodolskiy et al. [122] proposed new cryptographic protocols 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. Through smart contract, the location of files in the cloud, access policies, and additional owner information are recorded in the blockchain. In addition, interactions with files are performed through smart contracts.

Guo et al. [34] proposed a similar access control solution and employed the Shamir secret sharing scheme for key management of cloud users. The data owner first registers legitimate user identities and access control policies. The blockchain network verifies if the visitor has the permission to a file based on the record in blockchain and all the logs are kept by the blockchain.

Liu et al. [74] applied **Ciphertext-Policy Attribute-Based Encryption (CP-ABE)** on an efficient data access control scheme for cloud storage where the key parameters of the encryption algorithm are recorded in the blockchain. The sensitive file is encrypted using symmetric encryption algorithms. The encrypted file is then stored into the cloud storing center and the metadata of the file, the encryption key, and the public key of the data owner are recorded in the blockchain. Similarly, Wang et al. [137] proposed a secure cloud storage framework and proposed a valid access period to eliminate the operation of revoking permissions in their proposed access control scheme.

They use a smart contract to store information about encrypted file for better tracking of the file. Their framework can be used in conjunction with most CP-ABE algorithms and they use access tree [156] in their access control policy. A several multi-authority CP-ABE blockchain-based access control scheme [99] manages attributes and shares key ciphertexts and attribute tokens with blockchain.

3 CLOUD COMPUTING IN BLOCKCHAIN ENVIRONMENTS

The blockchain can solve the cloud trust problem and can guarantee the security of the cloud to a certain extent. Cloud computing can also solve the scalability problem and consumption problem of the blockchain to a certain extent. The main drawback of blockchain including majority attack (51% Attacks) [70], fork problems [70], integrated cost problem [70] and scalability problem [165]. However, the combination of the two is still facing many challenges, including (1) the security problems and vulnerability of blockchain and smart contract, (2) the balance between system performance optimization and decentralization, (3) the solutions of scalability problem, (4) resource utilization optimization and cost reduction, (5) improvements of QoS, and (6) cloud management and user management.

Researchers have proposed corresponding solutions to some of the problems listed above. We will introduce some of the researchers' solutions in this section.

3.1 Trust Optimization

Zhu et al. [169] introduced a TA, because they believed that an authoritative trust center is needed to check operations to avoid 51% attacks.

3.2 Computation and Storage Optimization

To reduce the storage pressure of blockchain peers, Xu et al. [146] suggested to store parts of blockchain in the cloud. They turned the storage optimization problem into a problem of selecting some blocks to store in the cloud, which is a multiobjective optimization problem. They proposed a nondominated sorting genetic algorithm with clustering to solve the multiobjective optimization problem.

To resolve the performance issues, Gaetani et al. [32], Zhao et al. [162], and Osei-Bryson et al. [93] chose to use double-layer blockchain structure to process data. The first blockchain layer that is directly used to store data is designed with a simple consensus mechanism for electing the primary node with low energy consumption, and the second blockchain layer used for witnessing the first layer uses PoW. More people choose to use blockchain technology cautiously, such as only recording the key data or combining cloud storage with the blockchain, that is, to store the hash and address information of the data into the blockchain.

To balance the load between the blockchain and the cloud computing model, Xiong et al. [143] investigated an optimal price-based computing resource management schemes in which the lightweight miners could transfer the PoW computing tasks to the cloud/fog providers. Jiao et al. [42] also held the same view. Considering the competition among miners, they proposed an auction mechanism to maximize the social welfare of miners of the blockchain network.

3.3 Maximization of the Profits

To maximize the profits of each service provider and miners, a mobile blockchain mining game [40] is proposed based on hierarchical edge-cloud computing. This game is a multi-leader multi-follower Stackelberg game. In their case, Miner can transfer its PoW computing tasks to a nearby **edge computing service provider (ESP)** or a remote CSP or both of them. There is a similar pricing scheme [144] with a multi-leader multi-follower Stackelberg game. Because IoT should provide an solution for the condition constrained devices to be participated in consensus, Kumar et al. [58] proposed an efficient statistical method to improve PoW by using the expectation maximization algorithm and polynomial matrix factorization to reduce energy and memory consumption.

Zhang et al. [155] designed a two-stage Stackelberg game by using game theory. The two phases of the game are the cloud/mist provider setting price and the number of services the miner decides to purchase accordingly.

3.4 Innovation in Consensus Mechanism

Some researchers have modified the PoW mechanism based on specific application to reduce the computing cost and optimize the designed system. For example, Liu et al. [72] applied data contribution frequency and energy contribution amount to implement PoW for securing vehicular interactions. To adapt to the high dynamics of mobile networks, a new **Stability-Aware PoW consensus Protocol (SEAP)** [43] is proposed. The movement of nodes has a relatively large impact on the stability and performance of the system, because the network needs to re-establish routing. SEAP integrates mobility into the PoW miner election process. In the process of mining, nodes not only need to submit answers to the hash puzzle but also need to prove their stability. To avoid forging their own stability information, nodes need to periodically exchange location information with neighboring nodes. Qiu et al. [100] cleverly used the computing power in the computing power proof (PoW) for useful machine learning, that is, changed PoW to PoL. The node that has trained the best model wins the right to generate the block currently. Proof-of-Service [**?**] consensus is related to the service provided by CSP and it is designed combining the mechanisms of PoS and PoW [24]. Proof-of-Service determines who gets the right to generate blocks by the contributions of nodes. Actions outside the blockchain are contributions, such as sharing a file or find some data.

Pohl et al. [97] proposed a preliminary idea of a consensus mechanism used in a cloud computing environment, Proof of Provision. The system packs blocks periodically, and a randomly selected CSP selects a client in order who is responsible for verifying the block. After the verification passes, the system synchronizes the blocks.

Because current PoS protocols designed in cryptocurrency domains are not well suited for cloud computing environments, Tosh et al. [130] tried to design an improved PoS mechanism, CloudPoS, where the keys are the definitions of the stake component of participants and the appropriate role of the CSP’s resource manager and blockchain consensus verifier. The stake component of participants consists of (1) CPU performance, (2) amount of memory and temporary buffer, and (3) network capability. The CPU performance is provided by CSP. Bendiab et al. [12] also designed an improved PoS protocol for cloud identity management. A CSP’s eligibility to become a leader is determined by systemwide target, stake, trust value, and the elapsed time of the last block generated from a particular CSP.

Malomo et al. [77] presented a federal cloud computing framework that supports blockchain, which uses the Demster-Shafer theory to reduce data breaches and breach detection gap. Clients need to join the network through smart contract. The consensus mechanism is Federal Proof of Stake, which is based on a threshold of the number of validators and the number of signatures required to adopt a block.

The Byzantine fault-tolerant algorithm commonly used in the consortium blockchains also has room for improvement. For example, Fu et al. [31] modified PBFT to a consensus mechanism suitable for edge networks; Tong et al. [129] uses a peer trust model and selected part nodes with high credibility to attend the PBFT consensus process. The communication load and complexity of the consensus are reduced, so that the network can accommodate more nodes. To improve the efficiency and reliability of PBFT, Zhu et al. [170] modified the first phase of the PBFT consensus.

Their Synchronous Byzantine Fault Tolerance detects faulty nodes in the network that cannot send or receive messages in the first phase.

4 CHALLENGES, DISCUSSION, AND FUTURE WORK

4.1 Challenges

We summarized the challenges faced by the integration of blockchain and cloud computing from the three models of integrating blockchain and cloud summarized in the introduction section.

BAACS: (1) security of tools that encapsulate blockchain, (2) privacy, (3) the protection of private keys of nodes, (4) security challenges faced by cloud computing itself, (5) smart contract code security audit, (6) cross-chain, and (7) in the case that a blockchain network is deployed by one user, how do different organizations or members of the blockchain access the nodes in the cloud service platform?

CAABS: (1) reward and punishment strategy for the nodes participating in the blockchain; (2) service supervision, settlement (SLA and QoS), and upgrade; (3) standardization and benchmarking; (4) the security and performance problems faced by the blockchain itself; (5) the pricing strategy and trading strategy of the service; and (6) how to expand and add other procedures, such as cloud computing firewalls and IDS?

MBC: (1) authentication and access control, (2) the blockchain programs deployed on fog nodes and IoT devices need to be lightweight, (3) equipments and devices dynamic management, (4) security challenges faced by cloud computing itself, and (5) the security and performance problems faced by the blockchain itself.

Besides, there are already some solutions to the problem (6) under the BCCAS model, the cross-chain problem. If the CSP adopts a cross-chain solution, then it will bring new challenges in addition to the challenges mentioned above. We also discuss these challenges in this section. They include the following: (1) the notary scheme solutions rely on trusted third parties, (2) atomicity and consistency, (3) interoperability between permissionless ledger and permissioned ledger, (4) cost, and (5) privacy.

4.1.1 Blockchain as a Cloud Service. The BAACS model is rarely discussed by researchers, but it is very common in the industry. As described in the Section 4 of the supplementary materials, many companies have released the BAACS platform. However, these platforms have some shortcomings in privacy protection, system supervision, scalability, and so on. The challenges that BAACS faces are as follows:

(1) Security of tools that encapsulate blockchain. CSPs use container management tools to simplify the process of blockchain deployment. In this process, the certificate, key, and chaincode information of the blockchain nodes will be exposed to CSPs. This brings great security risks. Even if CSPs need to maintain their reputation, their own cloud security issues plus this security risk will also provide a convenient way for malicious attackers to attack.

Compared with virtual machines, containers are lightweight, fast, easier to deploy, high resource utilization, and easier version control. Therefore, CSPs use containers to deliver blockchain services. Container security is a relatively complex and huge topic. The existing container security solutions are considered from both the hardware and software perspectives. Hardware solutions are generally related to trusted computing, such as Trusted Platform Modules. Software solutions are generally related to Linux security mechanisms, such as Linux Security Function and Linux Security Module. For detailed latest scientific research results, please refer to Reference [123].

(2) Privacy. As a service, the blockchain is managed by the cloud computing platform, and the data and node information in it may be transparent to CSPs.

We need to consider the security, integrity, and non-repudiation of the entire lifecycle of data (application data, identity data, network data) from generation, use to destruction. Some newer cryptography schemes such as secure multi-party computation, searchable encryption, group signature, ring signature, homomorphic cryptosystem and zero-knowledge proof are adapted to solve the privacy problems [18, 27].

(3) The protection of private keys of nodes. Like the two issues described above, the cloud computing management platform manages most of the deployment process of the blockchain, and the security of the private keys of the blockchain nodes needs to be guaranteed.

Key security of nodes in blockchain involves container security and privacy issues, and no solution to this problem is currently seen.

(4) Security challenges faced by cloud computing itself. In the BAACS model, an attacker can successfully attack the blockchain application by successfully attacking the cloud computing platform. Therefore, the security issues of cloud computing itself will bring security risks to blockchain applications under the BAACS model.

The security issues of cloud computing involve a wide range of aspects, including virtualization security, Internet security (web security, network protocol security), service availability security, access control, software security, trust management issues, physical security, and so on. [117]. The latest existing solutions include but are not limited to firewalls and IDSs based on Machine Learning, secure runtime environment, secure network protocol, load balancer, port monitoring, some encryption and decryption schemes or authentication schemes with higher security and stronger functionality, and blockchain-based management solusions, and so on [117].

(5) Smart contract code security audit. Errors in smart contracts will bring great security risks to blockchain applications. CSP should consider the review of smart contract code when integrating blockchain services to assist users in deploying smart contracts.

In the security audit of smart contracts, it is more common to audit codes through experience and code analysis to help ensure code correctness. Code auditing tools, a reliable compiler and formal verification techniques are needed [172]. There are also researchers who use machine learning to find loopholes in smart contracts [142].

(6) Cross-chain. CSP encapsulates most of the deployment process of blockchain, but it also affects the scalability and interoperability of the blockchain itself. CSPs should consider multi-cloud blockchain deployment and cross-chain issues.

There are five types of cross-chain solutions [14]: notary scheme solutions, sidechain/relay solutions, smart contract solutions, bridging solutions, and blockchain router solutions. The notary scheme uses a trusted third party who is responsible for the management and execution of cross-chain services. This third party can also be a blockchain. The sidechain/relay solution refers to a scheme that uses a two-way peg to connect the sidechain to the main chain. The smart contract solution achieves atomic cross-chain transactions using hash-lock and time-locks. The bridging solution uses smart contracts or other modules instead of using any main chain. The blockchain router solution provides the blockchain nodes router functions, so that they can perform the communications between blockchain platforms [134].

(7) In the case that a blockchain network is deployed by one user, how do different organizations or members of the blockchain access the nodes in the cloud service platform? Although most of the blockchain services provided by CSPs are consortium blockchains for enterprises, consortium blockchains also involve the participation of different organizations or individuals. However, the services provided by the current CSPs are for a user to deploy a blockchain network with one click, which does not conform to the blockchain design concept and the demands of multiple alliances.

There is currently no solution to this problem.

4.1.2 *Cloud as a Blockchain Service.*

In the CAABS model, the members that make up the blockchain network are generally CSPs. CPSs can share resources, supervise each other, legally compete under standardized trading rules, and automatically settle service fees through blockchain. We can see many researches related to the CAABS model but rarely see the application of CAABS in the industry. This may be because CSPs are unwilling, do not need, and cannot form a trust domain. Users do not care about the benefits of standardization and transaction transparency brought by the CAABS model, so CSPs are unwilling and do not need to rebuild their own service platform from the architecture and because each CSP has different standards, such as pricing strategy and SLA Regulatory strategies, and so on, so it is almost impossible to develop a standard for all CSPs without changing many original services. The challenges that CAABS faces are as follows:

(1) Reward and punishment strategy for the nodes participating in the blockchain. Blockchain nodes that maintain CAABS need to be motivated, and mechanisms are needed to prevent them from doing evil. Therefore, CAABS needs an appropriate reward and punishment mechanism that is related to management of blockchain and reputation system for blockchain nodes or something.

Researchers often use game theory to analyze and construct appropriate reward and punishment mechanisms [40, 58, 144, 155].

(2) Service supervision, settlement (SLA and QoS) and upgrade. Once CAABS is deployed, it is difficult to update the smart contract of the blockchain, because the update may involve the adjustment of the cloud computing services it manages. Therefore, before applying CAABS, it is necessary to design a reasonable supervision strategy, service settlement, and transaction strategy (SLA and QoS). To solve the problem of difficulty in upgrading, CAABS designers should also consider the modularization of various components of CAABS when designing the architecture to facilitate the update.

The supervision and settlement proposals under the CAABS model are not much different from the ways the blockchain is used under the BAACS model and the MBC model [39, 53, 87, 151, 166, 167]. But researchers need to consider the flexibility and scalability of the scheme under the BAACS model. At present, we have not seen the research results on the upgrade plan of supervision and settlement under the BAACS model. The existing problems and solutions of SLA can be referred to Reference [48].

(3) Standardization and benchmarking. CAABS is a relatively rare architecture. It involves managing the cloud computing resources of multiple CSPs and trading them. To facilitate the management of cloud computing resources of different CSPs and provide users with the same usage methods and interfaces, CAABS requires standards and benchmarks.

No one has proposed relevant standards and benchmarks.

(4) The security and performance problems faced by the blockchain itself. Just as in the BAACS model, the security issues of cloud computing pose a major threat to the blockchain applications deployed on it. In the CAABS model, the security issues of the blockchain pose a major threat to the cloud services it manages. Attackers can damage cloud services by attacking the blockchain.

Most of the security issues of the blockchain are resolved through a more secure cryptographic mechanism and a more reasonable consensus mechanism [71]. There are many researchers studying the performance issues of blockchain technology. Usually, researchers will discuss the storage, consensus mechanism and concurrency issues of the blockchain. Improvements in storage methods include not limited to sharding [20], side chains, changing the structure of blockchain to a **Directed Acyclic Graph (DAG)** structure [95] or tree structure, and so on. Improvements in consensus mechanism can refer to Reference [81] and Section 3.4 in this article. The improvement of concurrency problems is usually related to the consensus mechanism, the strategy of generating the blockchain and the structure of blockchain. The concurrency performance of the DAG structured blockchain is relatively high, because it can generate multiple blocks at the same time.

(5) The pricing strategy and trading strategy of the service. Pricing strategy and trading strategy are related to service supervision and standardization. When designing CAABS, it is also necessary to carefully consider the design of the strategy.

The pricing and trading strategies under the CAABS model must be realized by smart contracts. There are already some pricing and trading solutions based on smart contracts [39, 87, 92, 96, 124, 157]. Because the smart contract cannot be changed once deployed (Ethereum) [15], or it may be incompatible with the previous data after the change (Hyperledger Fabric), it is very important to design a reasonable and scalable strategy that facilitates the system's automatic settlement. Researchers can try to use game theory to analyze and construct appropriate pricing strategy and trading strategy.

(6) How to expand and add other procedures, such as cloud computing firewalls and IDS? Many security services adopted by cloud computing are difficult to be compatible with the CAABS model. How to use some of the original security services to protect cloud computing resources under the CAABS model is a problem. This is a scalability problem.

There is currently no discussion about this problem.

4.1.3 *Mixed Blockchain-Cloud.*

MBC model is very common in research and application. As two relatively independent networks, cloud computing and blockchain provide different services. All kinds of data in cloud computing can be recorded, witnessed, and verified by the blockchain. The complex calculations and huge storage load in the blockchain can be borne by cloud. In this way, the MBC model faces more problems in communication security and identity authentication. If we need to deploy a blockchain at the fog node layer and the IoT device layer, then we need to consider the issue of lightweight blockchain. The challenges that MBC faces are as follows:

(1) Authentication and access control. In the MBC model, blockchain and cloud computing are two independent network resources. In this case, when cloud computing needs to use blockchain, authentication and access control issues need to be considered, especially for IoT devices and fog nodes with a large number of low performance.

Authentication and access control can be solved with advanced cryptographic technologies, such as CP-ABE, identity-based encryption, aggregated identifier-based protocols, PKI-based protocols, and so on [74, 99, 108, 137].

(2) The blockchain programs deployed on fog nodes and IoT devices need to be lightweight. If we choose to deploy a blockchain at the fog node layer or the IoT device layer to achieve consistent decision-making or information sharing, then the deployed blockchain needs to be lightweight.

In addition to the new blockchain storage structure [95] and consensus mechanism [31, 43, 72, 77] that can solve the lightweight problem, some researchers use a multi-layer blockchain structure to allow a blockchain composed of low-performance devices to be responsible for less work.

(3) Equipments and devices dynamic management. In the MBC model, the devices at the fog node layer and the IoT layer may change dynamically, and the frequency of joining and exiting the blockchain network is relatively high. Therefore, if the blockchain is deployed at the fog node layer and the IoT layer, the efficiency and operability of the dynamic joining of devices and nodes need to be considered.

Device dynamic management is generally related to mobile devices, especially the authentication protocol of mobile devices. The existing authentication protocols for mobile devices are generally identity-based authentication methods and context-based authentication methods [5]. The consensus mechanism can also be modified to adapt to the dynamic of the network. For example, [43] takes stability as another factor that needs to be considered in the mining process.

(4) Security challenges faced by cloud computing itself. Blockchain and cloud computing are relatively independent, so they may be attacked separately. The security issues of cloud computing itself need to be considered.

Same as the (4) challenge of BAACS.

(5) The security and performance problems faced by the blockchain itself. Blockchain and cloud computing are relatively independent, so they may be attacked separately. The security and performance issues of the blockchain itself need to be considered.

Same as the (4) challenge of CAABS.

4.1.4 Cross-chain Challenges. As explained in question (6) under the BCCAS model, CSP aims to address the scalability and interoperability limitations of the blockchain under the BCCAS model and improve the performance of the blockchain at the same time. CSP can use the following cross-chain solutions [14]: notary scheme solutions, sidechain/relay solutions, smart contract solutions, bridging solutions, and blockchain router solutions. However, once the cross-chain solution is adopted, the blockchain has some new interfaces that expose data management operations. This will open up new challenges to security and data management in the cloud service environment. In this section, we discuss these challenges.

(1) The notary scheme solutions rely on trusted third parties. The third party in the notary scheme has certain control over the two ledgers that need to interact with each other. This increases the degree of centralization of the entire architecture, and has brought about several problems that a highly centralized system has, such as single point of failure and corruption. In addition to the ledger, data also exists in third parties.

The notary scheme sacrifices some decentralization to improve the efficiency and scalability of cross-chain transaction. If CSPs do not trust this mechanism, then they can choose other cross-chain solutions based on their specific needs.

(2) Atomicity and consistency. Cross-chain must ensure atomicity, that is, a cross-chain transaction has either successfully completed or failed. However, when any one or both of the two ledgers adopt a probabilistic consensus algorithm, there may be a situation where a newly generated block is replaced by another block [49]. This may destroy the atomicity and the consistency of the two ledgers [55].

Jin et al. [44] believe that some improvements can be made to the consensus process between blockchains, interpreting the consensus algorithm as a verification protocol, and checking whether the source chain has successfully submitted a transaction or the current transaction is still uncertain. An open permissionless network of witnesses [153] is designed to solve this conflict in Zakhary’s work. Game theory can also be considered to solve the problem of atomicity [11].

(3) Interoperability between permissionless ledger and permissioned ledger. Some anonymous users who use permissionless blockchain cannot use the services of real-name permissioned blockchains. This does not comply with the rules of industries (such as the finance sector and society sector) that use permissioned blockchains. Therefore, to achieve interoperability between these two types of blockchains, user identity and authentication issues need to be considered.

Kannengiesse et al. [49] pointed out that the existing interoperability solutions between permissionless ledger and permissioned ledger have some limitations, such as requiring participants to have accounts on both blockchain platforms, using a relayer to access the insensitive data in private chains, and so on. Different levels of privacy should be adopted [119].

(4) Cost. To achieve non-centralized consensus requires more communication and calculations. Cross-chain transactions increase the cost of communication and calculation to reach an agreement between two ledgers using different consensus strategies in addition to the cost of the blockchain. The cost of the notary scheme is lower, but in different application scenarios, it is necessary to make a tradeoff between the degree of centralization and the cost.

The cost of smart contracts has been considered high [119]. But we also need to pay attention to the performance, efficiency and energy consumption of cross-chain technology. Jin et al. [44] divided cross-chain technologies into active mode and passive mode. Active mode means that the initiator of a cross-chain transaction actively sends information. Passive mode means that the initiator of a cross-chain transaction passively receives information. Jin believes that polling in passive mode requires more consumption. The notary scheme has better efficiency, because it sacrifices some decentralization. We can also simplify calculations to reduce costs by optimizing the agreement [36].

(5) Privacy. The completion of the cross-chain function means that the blockchain can be read and written or controlled by other blockchains or a third party, which greatly increases the privacy threat of the data stored in the blockchain. It is necessary to consider access control and authentication schemes that adapt to cross-chain schemes.

Advanced encryption techniques can be used to solve the privacy problem [76]. Multi-signature may expose access control information. Therefore, the notary scheme using this technology should be improved by adding other signature schemes [47]. In other cross-chain solutions, privacy issues still need to be discussed [36, 55, 119].

4.2 Discussion

In this section, we discuss possible solutions for integrating cloud and blockchain, and the security attacks/threats blockchain-based security solutions can and cannot protect against in a cloud computing system.

In addition, we have added two discussions in the supplementary materials. One is to classify the literature studied in this article according to the four solutions in Section 4.2.1, further subdivide the approaches used in the literature, and describe the advantages and disadvantages of these approaches. The other is to discuss how blockchain logs can help improve the compliance of cloud services specifically considering the EU GDPR and its offshoots.

4.2.1 Solutions of the Integration of Cloud and Blockchain. Based on previous surveys, we found that the integration of cloud and blockchain has the following main solutions:

(1) As a reliable distributed database, blockchain can be used to store all or important data generated by different applications with transactions, smart contracts or can store specific fields in a block to ensure the data integrity and it can also be used to store metadata of files to protect the integrity of the data. The guarantee of data security makes the blockchain able to endorse the reliability of user behavior.

(2) By using the characteristics of the smart contract "automatically execute under the qualified conditions," the blockchain can be used for resource scheduling, resource distribution, transaction, tracking, auditing, identity management, access control, authentication, and authorization in different application contexts.

(3) We could use the characteristics of the blockchain to design a suitable system for a specific application scenario. For example, the Merkle tree can be used to store files, the generation of a new block can be combined with the authentication of new devices, the public/private key pair of the blockchain can be used for authentication, the token can be used to measure the cloud service's value, and the solution of blockchain fork problem can solve access problems of critical resources.

(4) We can use the cloud to improve blockchain's efficiency and performance. For example, we can offload the PoW computing tasks to the cloud, modify the consensus mechanism according to specific requirements, use the cloud to store the original data while the blockchain to store the key information, and so on.

The characteristics of blockchain are transparency, traceability, decentralization, security, immutability, and automation. The traceability, security, and immutability of blockchain ensure the integrity of data in cloud computing models. By leveraging the aforementioned features and the auto-executing nature of smart contracts, the blockchain can achieve trusted data sharing without third parties. The transparent, traceable, and immutable nature of the blockchain addresses the reliability and integrity issues of auditing and data provenance data. With the blockchain, the management mechanism of cloud computing can be executed automatically, transparently, safely and reliably, which can greatly enhance the trust of users and reduce management costs. The characteristics of the blockchain and its own asymmetric encryption algorithm can help security services such as access control and identity authentication.

4.2.2 Security Attacks/threats and Blockchain-based Security Solutions. At the beginning of Section 1 we mentioned that traditional security requirements can be satisfied centrally under the cloud computing architecture, but there are also some new threats such as data integrity, data leakage, unauthorized access, and so on. In this article, we introduced blockchain-based security service solutions to provide security services for cloud computing. These security services solve some of the security threats faced by cloud computing, including some traditional attacks, but there are also some attacks that cannot be resolved. In this section, we have classified the security issues that can and cannot be solved by blockchain-based security services.

It should be noted that the blockchain is not a panacea [154]. The existing blockchain-based security service solutions not only take advantage of the characteristics of the blockchain, but more importantly, they have completed their designs and protocols to achieve a specific purpose.

The threats that can be mitigated by blockchain-based security service solutions include the following: (1) data confidentiality and integrity (Section 2.1); (2) data leakage and interception (Section 2.1, 2.2); (3) unauthorized access (Section 2.5.1, 2.5.3); (4) accountability (Section 2.3); (5) loss of governance (Section 2.4); (6) failure in isolation (Section 2.4); (7) compliance (Section 5.2 in the supplementary materials); (8) detecting insider attacks and corruption in CSPs (Section 2.3); (9) service errors and service availability (Section 2.4); (10) IP spoofing or IP address forgery (Section 2.5); (11) man-in-the-middle attack, impersonation, and replay attack (Section 2.5); (12) data interruption (deletion) (Section 2.4); and (13) session hijacking (Section 2.5).

The threats that cannot be mitigated by blockchain-based security service solutions include the following: (1) DoS and DDoS, although there are some solutions that use blockchain to mitigate DDoS attacks [1, 41, 107]. However, whether the blockchain itself can resist DoS and DDoS attacks well remains an open question [109, 110], especially permissioned blockchains [121]; (2) hardware failure, blockchain-based cloud computing services do not have to worry about the unavailability of services caused by single point of failure, but they cannot solve the failure of the device itself [56]; (3) connection flooding, adversaries can attack specific nodes in the permissioned blockchain that will affect the consensus of the blockchain and can even successfully halt the blockchain [121]; and (4) PKI key compromise [132], the identity management of the blockchain itself is highly dependent on the PKI system.

4.3 Future Work

Combined with the induction and analysis of the current papers of the security services of blockchain and cloud and the challenges we discussed in Section 4.1, we present the following trends in the future development:

4.3.1 Privacy Issues. Due to the transparency of the blockchain, privacy issues have always existed in blockchain-related applications. In cloud computing environment, privacy issues are also serious. CSPs and attackers can easily obtain unencrypted data stored in cloud. In the BAACS model, even the private information of the blockchain network itself may be exposed to CSPs because of container management tools that simplify deployment operations. Therefore, more suitable security protocols and encryption algorithms need to be designed. Security and privacy issues in the lifecycle of any data, including user identity information and network configuration information, need to be considered. The lifecycle of data includes generation, sharing, storage, use, and destruction.

There have been many solutions in terms of privacy protection. The commonly used solution is to use a symmetric encryption scheme to encrypt the original text of the data, combined with access control to use an asymmetric encryption scheme to share symmetric keys; use homomorphic encryption schemes or zero-knowledge proof when using data; and use a searchable encryption scheme when searching for data. However, there are few efficient and comprehensive privacy protection schemes specifically for the combination of cloud computing and blockchain, and most of them only consider a period of the data cycle or a type of data in the application scenario. A more suitable, efficient and comprehensive privacy protection scheme is worth looking forward to.

4.3.2 High Modularity and Strong Scalability. Blockchain cloud architecture should be designed with high modularity and strong scalability. We discussed in Section 4.1 that it is difficult to extend and apply other cloud computing security measures under the CAABS model. Higher modularity and scalability can bring more convenience to the combination of cloud computing and blockchain. Modularity can simplify the development, testing, and update of models and can provide customers with customized service combinations.

In fact, some existing blockchain projects have achieved modularity and flexibility, such as Hyperledger Fabric. But the framework that can be easily extended under the CAABS model still does not exist. As we mentioned in the challenges of the CAABS model, other existing applications are difficult to integrate into the CAABS model. Only when this problem is solved can a highly autonomous cloud service platform emerges.

4.3.3 Reasonable Supervision Strategy and Settlement Strategy. To ensure the quality of service and make CSPs comply with the SLA, supervision and settlement in cloud computing are indispensable. The smart contract of the blockchain can provide automatic supervision and automatic settlement functions. However, poor supervision and settlement strategies may be exploited by CSPs and malicious users. Therefore, appropriate supervision and settlement strategies are worthy of study.

As we discussed in the challenge of the CAABS model, there are already some smart contract-based supervision and settlement solutions, but their flexibility and scalability are relatively poor. Also, the security problems should be further considered. How to formulate a reasonable and appropriate supervision and settlement solution is still an important topic.

4.3.4 Lightweight Consensus Scheme and Lightweight Storage Scheme. In the MBC model, blockchain may be deployed at the fog node layer and the IoT layer. Devices at the fog node layer and IoT layer have the characteristics of low storage capacity and low computing capacity. To run the blockchain between low-performance devices, we need lightweight consensus mechanisms and storage strategies.

There are currently two mainstream ideas in the improvement of the consensus mechanism. One is to change the proof of work to the proof of other quantifiable data. The new consensus mechanism can make the election of the master node more random without consuming resources, the better. The other is to sacrifice a certain degree of decentralization, concentrate the rights on some people or introduce a trusted third party. There are also two mainstream ideas for storage improvement. One is to allow multiple nodes to store a copy of blockchain data, and each node is responsible for storing a small part of the blockchain. The other is to put most of the data in the cloud or database, and only part of the data or key data is stored on the nodes in blockchain. Obviously, how to find quantifiable data that replaces computing power, how to balance centralization and the establishment of trust relationships, and how to develop storage solutions are all issues worthy of discussion.

4.3.5 A Highly Autonomous Cloud. As a resource pool, the cloud can get the most trust only with blockchain when there is no supervision from an authoritative third party. In the cloud architecture, copyright protection of data and sensitive data processing should also be handled by smart contract rather than by human resources. Researchers and CSPs are now automating more and more functions on cloud computing model through smart contracts. CAABS is an ideal autonomous cloud computing service platform. A highly autonomous cloud computing service is one of the main research directions in the future.

4.3.6 Better System Performance and QoS Performance. The energy consumption problem and high cost of the blockchain itself have always been an obstacle to the development of it and its related systems. How to effectively use the blockchain in the cloud computing model and use the IT resources in the cloud to improve the performance of the blockchain system is obviously a topic worth exploring. Researchers should try to build appropriate solutions and architectures to address the performance issues and security issues of the blockchain itself.

We have discussed some new solutions to the problems of the blockchain under the new architecture combining cloud computing and blockchain in Section 3. In view of the powerful computing and storage capabilities of cloud computing, we believe that related solutions still have room for development.

4.3.7 Applying of Game Theory, and so on. Combine game theory, and so on, to build clever smart contract or architectures to solve specific problems or optimize blockchain architecture. In suitable scenarios, it is very interesting to use researches in other disciplines to try to provide solutions for blockchain and cloud computing applications. Game theory is a very classic example. The direction of game theory research is consistent with the multi-party profit-seeking situation of blockchain. Therefore, the game theory method is very suitable for designing and analyzing the incentive mechanism, consensus mechanism, and various service-related strategies in the blockchain.

For example, game theory can improve the security, collaboration, and availability of multiplayer collaboration systems. The combination of incentive mechanisms and game theory can largely avoid nodes doing evil. Similar ideas can be adopted for the improvement of the SLAs system. Using a trust mechanism established with game theory instead of the way how consensus mechanism elects the master node to choose the master node is also a way to improve system performance. Blockchain is a complex network structure, and the architecture combining cloud computing and blockchain is more complicated. There may also be some technologies and solutions that can play an excellent role under the new architecture of cloud computing and blockchain.

4.3.8 Applying of Big Data Analysis or Artificial Intelligence. Combine big data analysis or artificial intelligence, use cloud resources to analyze blockchain data transactions, and so on, and provide personalized services. The large amount of data kept by cloud need to be analyzed with big data technologies. At the same time, big data are also inseparable from cloud computing. The flexible and scalable infrastructure required by big data can be provided by cloud computing. In addition to providing personalized services, machine learning can also be used to detect intrusions.

The common researches are using machine learning to train some models to solve specific problems of blockchain and cloud computing applications, such as intrusion detection, smart contract code auditing; using blockchain to provide security services such as trusted auditing; using cloud computing to provide storage space and computing power for machine learning applications. We look forward to seeing the emergence of automatic data collection and training systems that combine blockchain computing, machine learning, and cloud computing.

5 CONCLUSION

As a highly centralized system architecture, the cloud computing model also faces the same security issues that centralized data centers are facing. However, compared with traditional data centers, the cloud also faces user management issues (including CSP management), device management issues (multiple CSPs), access control issues, privacy issues, and trust issues. The integration of cloud and blockchain can result in promising solutions for the security services of cloud computing model. The cloud platform makes the overall system more scalable and enables the system support for deep analysis. Blockchain can improve the security of the cloud computing model and solve some of its trust issues. The huge computing resources and storage resources of cloud computing can bear the workload of the blockchain.

In this article, we mainly discussed the following questions: (1) How blockchain is integrated with the cloud? (2) What role does cloud computing play in the blockchain network? (3) What solutions can blockchain provide to the security services of cloud computing? (4) What solutions can cloud computing provide for blockchain performance problems? (5) What are the current development status and research trends of the industry/major cloud providers in the direction of combining cloud and blockchain? (6) What are the current challenges with the integration of cloud computing and blockchain, and what are the future development directions? Researchers who are interested in these questions can find answers to related questions in this review. CSPs who want to use blockchain to solve the security problems of cloud computing and developers who want to know whether cloud computing can solve the performance problems of blockchain can find relevant introductions in this review.

In general, this article briefly introduces the basic concepts of blockchain and the cloud computing model. We reviewed recent works that have investigated the benefits and challenges when cloud computing is integrated with blockchain. We have systematically analyzed recent, relevant works in the literature based on different security services in cloud computing model. The systematic analysis includes the following: (i) introducing the overall background, summarizing the possible architectures and models of the integration of blockchain and cloud computing, and the roles of cloud computing in blockchain; (ii) classifying and discussing recent, relevant works based on different blockchain-based security services in the cloud computing model; (iii) simply investigating what improvements cloud computing can provide for the blockchain; (iv) introducing the existing development status of major cloud providers in the direction of combining cloud and blockchain in the fourth section of the supplementary materials; (v) analyzing the main barriers and challenges of integrated blockchain and cloud computing systems; and (vi) providing recommendations for future research and improvement on the integration of blockchain and cloud systems.

REFERENCES

[1] Zakaria Abou El Houda, Abdelhakim Senhaji Hafid, and Lyes Khoukhi. 2019. Cochain-SC: An intra-and inter-domain Ddos mitigation scheme based on blockchain using SDN and smart contract. *IEEE Access* 7 (2019), 98893–98907.

[2] Nazrul M. Ahmad, Siti Fatimah Abdul Razak, Subarmaniam Kannan, Ibrahim Yusof, and Anang Hudaya Muhamad Amin. 2018. Improving identity management of cloud-based IoT applications using blockchain. In *Proceedings of the International Conference on Intelligent and Advanced System (ICIAS'18).* IEEE, 1–6.

[3] Abdullah Al Omar, Md Zakirul Alam Bhuiyan, Anirban Basu, Shinsaku Kiyomoto, and Mohammad Shahriar Rahman. 2019. Privacy-friendly platform for healthcare data in cloud based on blockchain environment. *Fut. Gener. Comput. Syst.* 95 (2019), 511–521.

[4] Saqib Ali, Guojun Wang, Md Zakirul Alam Bhuiyan, and Hai Jiang. 2018. Secure data provenance in cloud-centric internet of things via blockchain smart contracts. In *Proceedings of the 2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People, and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI'18).* IEEE, 991–998.

[5] Mojtaba Alizadeh, Saeid Abolfazli, Mazdak Zamani, Sabariah Baharun, and Kouichi Sakurai. 2016. Authentication in mobile cloud computing: A survey. *J. Netw. Comput. Appl.* 61 (2016), 59–80.

[6] Osama Alkadi, Nour Moustafa, Benjamin Turnbull, and Kim-Kwang Raymond Choo. 2020. A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks. *IEEE Internet of Things Journal* 8, 12 (2020), 9463–9472. https://doi.org/10.1109/JIOT.2020.2996590

[7] Abhineet Anand and Achintya Jha. 2019. Application and usability of blockchain in cloud computing. *J. Cloud Comput.* 6, 2 (2019), 26.

[8] Marcin Andrychowicz, Stefan Dziembowski, Daniel Malinowski, and Lukasz Mazurek. 2014. Secure multiparty computations on bitcoin. In *Proceedings of the IEEE Symposium on Security and Privacy.* IEEE, 443–458.

[9] Ali Vatankhah Barenji, Zhi Li, and W. M. Wang. 2018. Blockchain cloud manufacturing: Shop floor and machine level. In *Proceedings of the European Conference on Smart Objects, Systems and Technologies (Smart SysTech'18).* VDE, 1–6.

[10] Artem Barger, Yacov Manevich, Vita Bortnikov, Yoav Tock, Michael Factor, and Michal Malka. 2018. Shared cloud object store, governed by permissioned blockchain. In *Proceedings of the 11th ACM International Systems and Storage Conference.* ACM, 114–114.

[11] Marianna Belotti, Stefano Moretti, Maria Potop-Butucaru, and Stefano Secci. 2020. Game theoretical analysis of atomic cross-chain swaps. In *Proceedings of the 40th IEEE International Conference on Distributed Computing Systems (ICDCS'20).*

[12] Keltoum Bendiab, Nicholas Kolokotronis, Stavros Shiaeles, and Samia Boucherkha. 2018. WiP: A novel blockchain-based trust model for cloud identity management. In *Proceedings of the IEEE 16th International Conference on Dependable, Autonomic and Secure Computing, the 16th International Conference on Pervasive Intelligence and Computing, and the 4th International Conference on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech'18).* IEEE, 724–729.

[13] Juan Benet. 2014. Ipfs-content addressed, versioned, p2p file system. CoRR abs/1407.3561 (2014). http://arxiv.org/abs/1407.3561.

[14] Monika Bishnoi. 2020. Interoperability solutions for blockchain. In *Proceedings of the 2020 International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE'20).* 381–385. https://doi.org/10.1109/ICSTCEE49637.2020.9277054

[15] Vitalik Buterin et al. 2014. *A Next-Generation Smart Contract and Decentralized Application Platform.* Technical Report. Ethereum. 1–35 pages.

[16] Sheng Cao, Gexiang Zhang, Pengfei Liu, Xiaosong Zhang, and Ferrante Neri. 2019. Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain. *Inf. Sci.* 485 (2019), 427–440.

[17] Rodrigo Cubas Celiz, Yasmin Escriba De La Cruz, and David Mauricio Sanchez. 2018. Cloud model for purchase management in health sector of peru based on IoT and blockchain. In *Proceedings of the IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON'18).* IEEE, 328–334.

[18] Deyan Chen and Hong Zhao. 2012. Data security and privacy protection issues in cloud computing. In *Proceedings of the International Conference on Computer Science and Electronics Engineering*, Vol. 1. IEEE, 647–651.

[19] Yuyu Chou and Jan Oetting. 2011. Risk assessment for cloud-based IT systems. *Int. J. Grid High Perf. Comput.* 3, 2 (2011), 1–13.

[20] Hung Dang, Tien Tuan Anh Dinh, Dumitrel Loghin, Ee-Chien Chang, Qian Lin, and Beng Chin Ooi. 2019. Towards scaling blockchain systems via sharding. In *Proceedings of the 2019 International Conference on Management of Data.* 123–140.

[21] Gabriele D'Angelo, Stefano Ferretti, and Moreno Marzolla. 2018. A blockchain-based flight data recorder for cloud accountability. In *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems.* ACM, 93–98.

[22] Z. L. Deng, Y. J. Ren, Y. P. Liu, Xiang Yin, Z. X. Shen, and Hye-Jin Kim. 2019. Blockchain-based trusted electronic records preservation in cloud storage. *Comput. Mater. Contin.* 58, 1 (2019), 135–151.

[23] Yiwen Du, Jianwei Liu, Zhenyu Guan, and Hanwen Feng. 2018. A medical information service platform based on distributed cloud and blockchain. In *Proceedings of the IEEE International Conference on Smart Cloud (SmartCloud'18).* IEEE, 34–39.

[24] Tuyet Duong, Lei Fan, and Hong-Sheng Zhou. 2016. 2-hop blockchain: Combining proof-of-work and proof-of-stake securely. In *Proceedings of the 25th European Symposium on Research in Computer Security Computer Security (ESORICS'20)*. Lecture Notes in Computer Science, Vol. 12309. Springer, 697–712.

[25] Cynthia Dwork. 2011. Differential privacy. In *Encyclopedia of Cryptography and Security*. 338–340.

[26] Nabeil Eltayieb, Liang Sun, Ke Wang, and Fagen Li. 2019. A certificateless proxy re-encryption scheme for cloud-based blockchain. In *Proceedings of the International Conference on Frontiers in Cyber Security*. Springer, 293–307.

[27] Qi Feng, Debiao He, Sherali Zeadally, Muhammad Khurram Khan, and Neeraj Kumar. 2018. A survey on privacy protection in blockchain system. *J. Netw. Comput. Appl.* 126 (2018), 45–58.

[28] André Figueira. 2018. *Secure Framework for Cloud Data Sharing Based on Blockchain*. Master's thesis. Universidade de Évora.

[29] Claudia Fiore. 2019. *Providing Trust to Multi-cloud Storage Platforms Through the Blockchain*. Ph.D. Dissertation. Politecnico di Torino.

[30] Shaojing Fu, Chao Zhang, and Weijun Ao. 2020. Searchable encryption scheme for multiple cloud storage using double-layer blockchain. *Concurr. Comput.: Pract. Exper.* (2020), 1–12. https://doi.org/10.1002/cpe.586

[31] Xiaoyuan Fu, F. Richard Yu, Jingyu Wang, Qi Qi, and Jianxin Liao. 2019. Resource allocation for blockchain-enabled distributed network function virtualization (NFV) with mobile edge cloud (MEC). In *Proceedings of the IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS'19)*. 1–6.

[32] Edoardo Gaetani, Leonardo Aniello, Roberto Baldoni, Federico Lombardi, Andrea Margheri, and Vladimiro Sassone. 2017. Blockchain-based database to ensure data integrity in cloud computing environments. 816 (2017), 146–155.

[33] Keke Gai, Kim-Kwang Raymond Choo, and Liehuang Zhu. 2018. Blockchain-enabled reengineering of cloud datacenters. *IEEE Cloud Comput.* 5, 6 (2018), 21–25.

[34] Jiale Guo, Wenzhuo Yang, Kwok-Yan Lam, and Xun Yi. 2018. Using blockchain to control access to cloud data. In *Proceedings of the International Conference on Information Security and Cryptology*. Springer, 274–288.

[35] Kristiina Häyrinen, Kaija Saranto, and Pirkko Nykänen. 2008. Definition, structure, content, use and impacts of electronic health records: A review of the research literature. *Int. J. Med. Inf.* 77, 5 (2008), 291–304.

[36] Maurice Herlihy. 2018. Atomic Cross-Chain Swaps. In *Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing, PODC 2018, Egham, United Kingdom, July 23-27, 2018*. 245–254. https://doi.org/10.1145/3212734.3212736

[37] Shengshan Hu, Chengjun Cai, Qian Wang, Cong Wang, Xiangyang Luo, and Kui Ren. 2018. Searching an encrypted cloud meets blockchain: A decentralized, reliable and fair realization. In *Proceedings of the IEEE Conference on Computer Communications*. IEEE, 792–800.

[38] Longxia Huang, Gongxuan Zhang, Shui Yu, Anmin Fu, and John Yearwood. 2017. SeShare: Secure cloud data sharing based on blockchain and public auditing. *Concurr. Comput.: Pract. Exp.* (2017), e4359.

[39] Gwanhwan Hwang, Peichun Tien, and Yihsiang Tang. 2020. Blockchain-based automatic indemnification mechanism based on proof of violation for cloud storage services. In *Proceedings of the 2nd International Conference on Blockchain Technology (ICBCT'20)*.

[40] Suhan iang, Xinyi Li, and Jie Wu. 2019. Hierarchical edge-cloud computing for mobile blockchain mining game. In *Proceedings of the IEEE 39th International Conference on Distributed Computing Systems (ICDCS'19)*. 1327–1336.

[41] Uzair Javaid, Ang Kiang Siang, Muhammad Naveed Aman, and Biplab Sikdar. 2018. Mitigating loT device based DDoS attacks using blockchain. In *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*. 71–76.

[42] Yutao Jiao, Ping Wang, Dusit Niyato, and Kongrath Suankaewmanee. 2019. Auction mechanisms in cloud/fog computing resource allocation for public blockchain networks. *IEEE Trans. Parallel Distrib. Syst.* (2019).

[43] Jiao,Zhenzhen, Baoxian Zhang, Li Zhang, Min Liu, Wei Gong, and Cheng Li. 2020. A blockchain-based computing architecture for mobile Ad Hoc cloud. *IEEE Netw.* 34, 4 (2020), 140–149.

[44] Hai Jin, Xiaohai Dai, and Jiang Xiao. 2018. Towards a novel architecture for enabling interoperability amongst multiple blockchains. In *Proceedings of the IEEE 38th International Conference on Distributed Computing Systems (ICDCS'18)*. IEEE, 1203–1211.

[45] Don Johnson, Alfred Menezes, and Scott Vanstone. 2001. The elliptic curve digital signature algorithm (ECDSA). *Int. J. Inf. Secur.* 1, 1 (2001), 36–63.

[46] Ari Juels and Burton S. Kaliski Jr. 2007. PORs: Proofs of retrievability for large files. In *Proceedings of the 14th ACM Conference on Computer and Communications Security*. ACM, 584–597.

[47] Harry Kalodner, Malte Möser, Kevin Lee, Steven Goldfeder, Martin Plattner, Alishah Chator, and Arvind Narayanan. 2020. BlockSci: Design and applications of a blockchain analysis platform. In *Proceedings of the 29th USENIX Security Symposium (USENIX Security'20)*. 2721–2738.

[48] Balachandra Reddy Kandukuri, V. R. Paturi, and Atanu Rakshit. 2009. Cloud security issues. In *Proceedings of the IEEE International Conference on Services Computing*. 517–520.

[49] Niclas Kannengießer, Michelle Pfister, Malte Greulich, Sebastian Lins, and Ali Sunyaev. 2020. Bridges between islands: Cross-chain technology for distributed ledger technology. In *Proceedings of the 53rd Hawaii International Conference on System Sciences*.

[50] Lori M. Kaufman. 2009. Data security in the world of cloud computing. *IEEE Secur. Priv.* 7, 4 (2009), 61–64.

[51] Brian Khieu and Melody Moh. 2019. CBPKI: Cloud blockchain-based public key infrastructure. In *Proceedings of the ACM Southeast Conference*. ACM, 58–63.

[52] Hyun-Woo Kim and Young-Sik Jeong. 2018. Secure authentication-management human-centric scheme for trusting personal resource information on mobile cloud computing with blockchain. *Human-centr. Comput. Inf. Sci.* 8, 1 (2018), 11.

[53] Stephen Kirkman and Richard Newman. 2018. A cloud data movement policy architecture based on smart contracts and the ethereum blockchain. In *Proceedings of the IEEE International Conference on Cloud Engineering (IC2E'18)*. IEEE, 371–377.

[54] Neal Koblitz. 1987. Elliptic curve cryptosystems. *Math. Comput.* 48, 177 (1987), 203–209.

[55] Tommy Koens and Erik Poll. 2019. Assessing interoperability solutions for distributed ledgers. *Perv. Mobile Comput.* 59 (2019), 101079.

[56] Nir Kshetri. 2017. Can blockchain strengthen the internet of things? *IT Prof.* 19, 4 (2017), 68–72.

[57] Raymond G. Kuebler. 2018. *Application of Blockchain for Authentication, Verification of Identity and Cloud Computing*. Ph.D. Dissertation. Utica College.

[58] Gulshan Kumar, Rahul Saha, Mritunjay Kumar Rai, Reji Thomas, and Tai-Hoon Kim. 2019. Proof-of-work consensus approach in blockchain technology for cloud and fog computing using maximization-factorization statistics. *IEEE IoT J.* (2019).

[59] Manish Kumar and Ashish Kumar Singh. 2020. Distributed intrusion detection system using blockchain and cloud computing infrastructure. In *Proceedings of the 4th International Conference on Trends in Electronics and Informatics (ICOEI'20)*.

[60] R. Sravan Kumar and Ashutosh Saxena. 2011. Data integrity proofs in cloud storage. In *Proceedings of the 3rd International Conference on Communication Systems and Networks (COMSNETS'11)*. IEEE, 1–4.

[61] Heba Kurdi, Shada Alsalamah, Asma Alatawi, Sara Alfaraj, Lina Altoaimy, and Syed Hassan Ahmed. 2019. HealthyBroker: A trustworthy blockchain-based multi-cloud broker for patient-centered ehealth services. *Electronics* 8, 6 (2019), 602.

[62] Christopher A. Lee. 2010. Open archival information system (OAIS) reference model. In *Encyclopedia of Library and Information Sciences*, 4020–4030.

[63] Chunhua Li, Jiaqi Hu, Ke Zhou, Yuanzhang Wang, and Hongyu Deng. 2018. Using blockchain for data auditing in cloud storage. In *Proceedings of the International Conference on Cloud Computing and Security*. Springer, 335–345.

[64] Jiaxing Li, Jigang Wu, and Long Chen. 2018. Block-secure: Blockchain based scheme for secure P2P cloud storage. *Inf. Sci.* 465 (2018), 219–231.

[65] Jingyi Li, Jigang Wu, Long Chen, and Jiaxing Li. 2018. Deduplication with blockchain for secure cloud storage. In *Proceedings of the CCF Conference on Big Data*. Springer, 558–570.

[66] Zhi Li, Ali Vatankhah Barenji, and George Q. Huang. 2018. Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform. *Robot. Comput.-Integr. Manufact.* 54 (2018), 133–144.

[67] Zhi Li, Layne Liu, Ali Vatankhah Barenji, and Waiming Wang. 2018. Cloud-based manufacturing blockchain: Secure knowledge sharing for injection mould redesign. *Proc. CIRP* 72, 1 (2018), 961–966.

[68] Zhi Li, Xinlai Liu, W. M. Wang, Ali Vatankhah Barenji, and George Q. Huang. 2019. CKshare: Secured cloud-based knowledge-sharing blockchain for injection mold redesign. *Enterpr. Inf. Syst.* 13, 1 (2019), 1–33.

[69] Xueping Liang, Sachin Shetty, Deepak Tosh, Charles Kamhoua, Kevin Kwiat, and Laurent Njilla. 2017. Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. In *Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*. IEEE Press, 468–477.

[70] Iuon-Chang Lin and Tzu-Chun Liao. 2017. A survey of blockchain security issues and challenges. *IJ Netw. Secur.* 19, 5 (2017), 653–659.

[71] Iuon Chang Lin and Tzu Chun Liao. 2017. A survey of blockchain security issues and challenges. *Int. J. Netw. Secur.* 19 (2017).

[72] Hong Liu, Yan Zhang, and Tao Yang. 2018. Blockchain-enabled security in electric vehicles cloud and edge computing. *IEEE Netw.* 32, 3 (2018), 78–83.

[73] Jingwei Liu, Gaojian Zhang, Rong Sun, Xiaojiang Du, and Mohsen Guizani. 2020. A blockchain-based conditional privacy-preserving traffic data sharing in cloud. In *Proceedings of the IEEE International Conference on Communications (ICC'20)*. IEEE, 1–6.

[74] Yuke Liu, Junwei Zhang, and Qi Gao. 2018. A blockchain-based secure cloud files sharing scheme with fine-grained access control. In *Proceedings of the 2018 International Conference on Networking and Network Applications (NaNA'18)*. IEEE, 277–283.

[75] Chintha Madhumohan Reddy and G. Raghavendra. 2018. Blockchain-based database to ensure data integrity in cloud forensics. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology* 3, 4 (2018), 186–193.

[76] Giulio Malavolta, Pedro Moreno-Sanchez, Clara Schneidewind, Aniket Kate, and Matteo Maffei. 2019. Anonymous multi-hop locks for blockchain scalability and interoperability. In *Proceedings of the Network and Distributed System Security Symposium (NDSS'19)*.

[77] Olumide O. Malomo, Danda B. Rawat, and Moses Garuba. 2018. Next-generation cybersecurity through a blockchain-enabled federated cloud framework. *J. Supercomput.* 74, 10 (2018), 5099–5126.

[78] Yuyi Mao, Changsheng You, Jun Zhang, Kaibin Huang, and Khaled B. Letaief. 2017. Mobile edge computing: Survey and research outlook. arXiv:1701.01090. Retrieved from https://arxiv.org/abs/1701.01090.

[79] Tim Mather, Subra Kumaraswamy, and Shahed Latif. 2009. *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*. O'Reilly Media, Inc.

[80] Ying Miao, Qiong Huang, Meiyan Xiao, and Hongbo Li. 2020. Decentralized and privacy-preserving public auditing for cloud storage based on blockchain. *IEEE Access* 8 (2020), 139813–139826. https://doi.org/10.1109/ACCESS.2020.3013153

[81] Du Mingxiao, Ma Xiaofeng, Zhang Zhe, Wang Xiangwei, and Chen Qijun. 2017. A review on consensus algorithm of blockchain. In *Proceedings of the 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC'17)*. IEEE, 2567–2572.

[82] Derek G. Murray, Eiko Yoneki, Jon Crowcroft, and Steven Hand. 2010. The case for crowd computing. In *Proceedings of the 2nd ACM SIGCOMM Workshop on Networking, Systems, and Applications on Mobile Handhelds*. ACM, 39–44.

[83] Sara Nadeem, Muhammad Rizwan, Fahad Ahmad, and Jaweria Manzoor. 2019. Securing cognitive radio vehicular ad hoc network with fog node based distributed blockchain cloud architecture. *Int. J Adv. Comput. Sci. Appl.* 10, 1 (2019), 288–295.

[84] Aarthi Nagarajan and Vijay Varadharajan. 2011. Dynamic trust enhanced security model for trusted platform based services. *Fut. Gener. Comput. Syst.* 27, 5 (2011), 564–573.

[85] Gayathri Nagasubramanian, Rakesh Kumar Sakthivel, Rizwan Patan, Amir H. Gandomi, Muthuramalingam Sankayya, and Balamurugan Balusamy. 2020. Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. *Neural Comput. Appl.* 32, 3 (2020), 639–647.

[86] Sambit Nayak, Nanjangud C. Narendra, Anshu Shukla, and James Kempf. 2018. Saranyu: Using smart contracts and blockchain for cloud tenant management. In *Proceedings of the IEEE 11th International Conference on Cloud Computing (CLOUD'18)*. IEEE, 857–861.

[87] Nils Neidhardt, Carsten Köhler, and Markus Nüttgens. 2018. Cloud service billing and service level agreement monitoring based on blockchain. In *Proceedings of the International Workshop on Enterprise Modeling and Information Systems Architectures (EMISA'18)*. 65–69.

[88] Dinh C. Nguyen, Pubudu N. Pathirana, Ming Ding, and Aruna Seneviratne. 2019. Blockchain for secure EHRs sharing of mobile cloud based e-health systems. *IEEE Access* 7 (2019), 66792–66806. https://doi.org/10.1109/ACCESS.2019.2917555

[89] Dinh C. Nguyen, Pubudu N. Pathirana, Ming Ding, and Aruna Seneviratne. 2019. Integration of blockchain and cloud of things: Architecture, applications and challenges. arXiv:1908.09058. Retrieved from https://arxiv.org/abs/1908.09058.

[90] Talal Noor, Quan Sheng, Sherali Zeadally, and Jian Yu. 2013. Trust management of services in cloud environments: Obstacles and solutions. *ACM Comput. Surv.* 46, 10 (2013). https://doi.org/10.1145/2522968.2522980

[91] Marek R. Ogiela and Lidia Ogiela. 2017. Secure data and services management in distributed structures and in the cloud with application of blockchain technologies. In *Proceedings of the International Symposium on Mobile Internet Security*. Springer, 110–119.

[92] Yustus Eko Oktian, Elizabeth Nathania Witanto, Sandra Kumi, and Sang-Gon Lee. 2019. BlockSubPay-a blockchain framework for subscription-based payment in cloud service. In *Proceedings of the 21st International Conference on Advanced Communication Technology (ICACT'19)*. IEEE, 153–158.

[93] Kweku Muata, A. Osei-Bryson, et al. 2018. A blockchain-based security-oriented framework for cloud federation. In *KSU proceeding on Cybersecurity Education, Research and Practice*. 1–18.

[94] Alfonso Panarello, Nachiket Tapas, Giovanni Merlino, Francesco Longo, and Antonio Puliafito. 2018. Blockchain and IoT integration: A systematic survey. *Sensors* 18, 8 (2018), 2575.

[95] Huma Pervez, Muhammad Muneeb, Muhammad Usama Irfan, and Irfan Ul Haq. 2018. A comparative analysis of DAG-based blockchain architectures. In *Proceedings of the 12th International Conference on Open Source Systems and Technologies (ICOSST'18)*. IEEE, 27–34.

[96] Benedikt Pittl, Werner Mach, and Erich Schikuta. 2018. Bazaar-blockchain: A blockchain for bazaar-based cloud markets. In *Proceedings of the 2018 IEEE International Conference on Services Computing (SCC'18)*. IEEE, 89–96.

[97] Matthias Pohl, Abdulrahman Nahhas, Sascha Bosse, and Klaus Turowski. 2019. Proof of provision: Improving blockchain technology by cloud computing. In *Proceedings of the International Conference on Cloud Computing and Services Science (CLOSER'19)*. 523–527.

[98] Qin Qiao, Xinghua Li, Yunwei Wang, Bin Luo, Yanbing Ren, and Jianfeng Ma. 2019. Credible routing scheme of SDN-based cloud using blockchain. In *Proceedings of the International Conference of Pioneering Computer Scientists, Engineers and Educators*. Springer, 189–206.

[99] Xuanmei Qin, Yongfeng Huang, Zhen Yang, and Xing Li. 2020. A blockchain-based access control scheme with multiple attribute authorities for secure cloud data sharing. *J. Syst. Arch.* (2020), 101854.

[100] Chao Qiu, Xiaofei Wang, Haipeng Yao, Jianbo Du, F. Richard Yu, and Song Guo. 2020. Networking integrated cloud-edge-end in IoT: A blockchain-assisted collective q-learning approach. *IEEE IoT J.* (2020), 1–1.

[101] Sagar Rane and Arati Dixit. 2019. BlockSLaaS: Blockchain assisted secure logging-as-a-service for cloud forensics. In *Proceedings of the International Conference on Security & Privacy*. Springer, 77–88.

[102] Saqib Rasool, Muddesar Iqbal, Tasos Dagiuklas, Zia Ql-Qayyum, and Shancang Li. 2018. Reliable data analysis through blockchain based crowdsourcing in mobile ad-hoc cloud. *Mobile Netw. Appl.* 25, 1 (2018), 153–163. https://doi.org/10.1007/s11036-019-01221-x

[103] Yongjun Ren, Linhui Kong, Yepeng Liu, and Jin Wang. 2018. Consistency guarantee method of electronic record based on blockchain in cloud storage. In *Proceedings of the International Conference on Cloud Computing and Security*. Springer, 633–642.

[104] Yongjun Ren, YePeng Liu, Xiang Yin, Zixuan Shen, and Hye-Jin Kim. 2019. Blockchain-based trusted electronic records preservation in cloud storage. *Comput. Mater. Contin.* 58, 1 (2019), 135–151.

[105] Thomas Renner, Johannes Müller, and Odej Kao. 2018. Endolith: A blockchain-based framework to enhance data retention in cloud storages. In *Proceedings of the 26th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP'18)*. IEEE, 627–634.

[106] Joseph Ricci, Ibrahim Baggili, and Frank Breitinger. 2019. Blockchain-based distributed cloud storage digital forensics: Where's the beef? *IEEE Secur. Priv.* 17, 1 (2019), 34–42.

[107] Bruno Rodrigues, Thomas Bocek, and Burkhard Stiller. 2017. Enabling a cooperative, multi-domain DDoS defense by a blockchain signaling system (BloSS). In *42nd IEEE Conference on Local Computer Networks 2017 (LCN'17)*. 1–3.

[108] Sara Rouhani and Ralph Deters. 2019. Blockchain based access control systems: State of the art and challenges. In *Proceedings of the IEEE/WIC/ACM International Conference on Web Intelligence (WI'19)*. ACM, 423–428. https://doi.org/10.1145/3350546.3352561

[109] Muhammad Saad, Laurent Njilla, Charles Kamhoua, Joongheon Kim, DaeHun Nyang, and Aziz Mohaisen. 2019. Mempool optimization for defending against DDoS attacks in PoW-based blockchain systems. In *Proceedings of the IEEE International Conference on Blockchain and Cryptocurrency (ICBC'19)*. IEEE, 285–292.

[110] Muhammad Saad, My T. Thai, and Aziz Mohaisen. 2018. POSTER: Deterring ddos attacks on blockchain-based cryptocurrencies through mempool optimization. In *Proceedings of the Asia Conference on Computer and Communications Security*. 809–811.

[111] Ravi S. Sandhu and Pierangela Samarati. 1994. Access control: Principle and practice. *IEEE Commun. Mag.* 32, 9 (1994), 40–48.

[112] Eli Ben Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. 2014. Zerocash: Decentralized anonymous payments from bitcoin. In *Proceedings of the IEEE Symposium on Security and Privacy*. IEEE, 459–474.

[113] Pradip Kumar Sharma, Mu Yen Chen, and Jong Hyuk Park. 2018. A software defined fog node based distributed blockchain cloud architecture for IoT. *IEEE Access* 6 (2018), 115–124.

[114] Sachin Shetty, Val Red, Charles Kamhoua, Kevin Kwiat, and Laurent Njilla. 2017. Data provenance assurance in the cloud using blockchain. In *Disruptive Technologies in Sensors and Sensor Systems*, Vol. 10206. International Society for Optics and Photonics, 1–11. https://doi.org/10.1117/12.2266994

[115] Yun Shu, Jian Yu, and Wei Qi Yan. 2019. Blockchain for security of cloud-based online auction. In *Exploring Security in Software Architecture and Design*. IGI Global, 189–210.

[116] Yogesh L. Simmhan, Beth Plale, and Dennis Gannon. 2005. A survey of data provenance in e-science. *ACM Sigmod Rec.* 34, 3 (2005), 31–36.

[117] Ashish Singh and Kakali Chatterjee. 2017. Cloud security issues and challenges: A survey. *J. Netw. Comput. Appl.* 79 (2017), 88–115.

[118] Saurabh Singh, In-Ho Ra, Weizhi Meng, Maninder Kaur, and Gi Hwan Cho. 2019. SH-BlockCC: A secure and efficient Internet of things smart home architecture based on cloud computing and blockchain technology. *Int. J. Distrib. Sens. Netw.* 15, 4 (2019), 1550147719844159.

[119] Vasilios A. Siris, Pekka Nikander, Spyros Voulgaris, Nikos Fotiou, and George C. Polyzos. 2019. Interledger approaches. *IEEE Access* 7, 99 (2019), 89948–89966.

[120] Nasrin Sohrabi, Xun Yi, Zahir Tari, and Ibrahim Khalil. 2020. BACC: Blockchain-based access control for cloud data. In *Proceedings of the Australasian Computer Science Week Multiconference*. ACM, 1–10. https://doi.org/10.1145/3373017.3373027

[121] Mathis Steichen, Stefan Hommes, and Radu State. 2017. ChainGuarda firewall for blockchain applications using SDN with OpenFlow. In *Proceedings of the 2017 Principles, Systems and Applications of IP Telecommunications (IPTComm'17)*. IEEE, 1–8.

[122] Ilya Sukhodolskiy and Sergey Zapechnikov. 2018. A blockchain-based access control system for cloud storage. In *Proceedings of the 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus'18)*. IEEE, 1575–1578.

[123] Sari Sultan, Imtiaz Ahmad, and Tassos Dimitriou. 2019. Container security: Issues, challenges, and the road ahead. *IEEE Access* 7 (2019), 52976–52996.

[124] Mona Taghavi, Jamal Bentahar, Hadi Otrok, and Kaveh Bakhtiyari. 2018. Cloudchain: A blockchain-based coopetition differential game model for cloud computing. In *Proceedings of the International Conference on Service-Oriented Computing*. Springer, 146–161.

[125] Hassan Takabi, James B. D. Joshi, and Gail-Joon Ahn. 2010. Security and privacy challenges in cloud computing environments. *IEEE Secur. Priv.* 8, 6 (2010), 24–31.

[126] Yuzhe Tang, Qiwu Zou, Ju Chen, Kai Li, Charles A. Kamhoua, Kevin Kwiat, and Laurent Njilla. 2018. ChainFS: Blockchain-secured cloud storage. In *Proceedings of the IEEE 11th International Conference on Cloud Computing (CLOUD'18)*. 987–990.

[127] Fei Tao, Lin Zhang, V. C. Venkatesh, Y. Luo, and Ying Cheng. 2011. Cloud manufacturing: A computing and service-oriented manufacturing model. *Proc. Inst. Mech. Eng. B: J. Eng. Manufact.* 225, 10 (2011), 1969–1976.

[128] Nachiket Tapas, Giovanni Merlino, and Francesco Longo. 2018. Blockchain-based IoT-cloud authorization and delegation. In *Proceedings of the IEEE International Conference on Smart Computing (SMARTCOMP'18)*. IEEE, 411–416.

[129] Wei Tong, Xuewen Dong, Yulong Shen, and Jiawei Zheng. 2020. BC-RAN: Cloud radio access network enabled by blockchain for 5G. *Comput. Commun.* 162 (2020), 179–186. https://doi.org/10.1016/j.comcom.2020.08.020

[130] Deepak Tosh, Sachin Shetty, Peter Foytik, Charles Kamhoua, and Laurent Njilla. 2018. CloudPoS: A proof-of-stake consensus design for blockchain integrated cloud. In *Proceedings of the IEEE 11th International Conference on Cloud Computing (CLOUD'18)*. IEEE, 302–309.

[131] Deepak Tosh, Sachin Shetty, Xueping Liang, Charles Kamhoua, and Laurent L. Njilla. 2019. Data provenance in the cloud: A blockchain-based approach. *IEEE Consum. Electr. Mag.* 8, 4 (2019), 38–44.

[132] Deepak K. Tosh, Sachin Shetty, Xueping Liang, Charles A. Kamhoua, Kevin A. Kwiat, and Laurent Njilla. 2017. Security implications of blockchain cloud with analysis of block withholding attack. In *Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID'17)*. IEEE, 458–467.

[133] Toshihiro Uchibayashi, Bernady Apduhan, Takuo Suganuma, and Masahiro Hiji. 2018. Toward a secure VM migration control mechanism using blockchain technique for cloud computing environment. In *Proceedings of the International Conference on Computational Science and Its Applications*. Springer, 177–186.

[134] Hui Wang, Yuanyuan Cen, and Xuefeng Li. 2017. Blockchain router: A cross-chain communication protocol. In *Proceedings of the 6th International Conference on Informatics, Environment, Energy and Applications*. 94–97.

[135] Hao Wang and Yujiao Song. 2018. Secure cloud-based EHR system using attribute-based cryptosystem and blockchain. *J. Med. Syst.* 42, 8 (2018), 152.

[136] Jia Wang, Fang Peng, Hui Tian, Wenqi Chen, and Jing Lu. 2019. Public auditing of log integrity for cloud storage systems via blockchain. In *Proceedings of the International Conference on Security and Privacy in New Computing Environments*. Springer, 378–387.

[137] Shangping Wang, Xu Wang, and Yaling Zhang. 2019. A secure cloud storage framework with access control based on blockchain. *IEEE Access* (2019).

[138] Yong Wang, Aiqing Zhang, Peiyun Zhang, and Huaqun Wang. 2019. Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain. *IEEE Access* 7 (2019), 136704–136719. https://doi.org/10.1109/ACCESS.2019.2943153

[139] Q. I. Xia, Emmanuel Boateng Sifah, Kwame Omono Asamoah, Jianbin Gao, Xiaojiang Du, and Mohsen Guizani. 2017. MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. *IEEE Access* 5 (2017), 14757–14767.

[140] Shaoan Xie, Zibin Zheng, Weili Chen, Jiajing Wu, Hongning Dai, and Muhammad Imran. 2020. Blockchain for cloud exchange: A survey. *Comput. Electr. Eng.* 81 (2020), 106526.

[141] Xiaolan Xie, Tao Huang, and Zhihong Guo. 2018. Research on the security protection scheme for container-based cloud platform node based on blockchain technology. In *Proceedings of the International Conference of Pioneering Computer Scientists, Engineers and Educators*. Springer, 24–32.

[142] Cipai Xing, Zhuorong Chen, Lexin Chen, Xiaojie Guo, Zibin Zheng, and Jin Li. 2020. A new scheme of vulnerability analysis in smart contract with machine learning. *Wireless Netw.* (2020), 1–10. https://doi.org/10.1007/s11276-020-02379-z

[143] Zehui Xiong, Shaohan Feng, Wenbo Wang, Dusit Niyato, Ping Wang, and Zhu Han. 2018. Cloud/fog computing resource management and pricing for blockchain networks. *IEEE IoT J.* 6, 3 (2018), 4585–4600. https://doi.org/10.1109/JIOT.2018.2871706

[144] Zehui Xiong, Jiawen Kang, Dusit Niyato, Ping Wang, and H. Vincent Poor. 2019. Cloud/edge computing service management in blockchain networks: Multi-leader multi-follower game-based ADMM for pricing. *IEEE Trans. Serv. Comput.* 13, 2 (2019), 356–367.

[145] Chenhan Xu, Kun Wang, and Mingyi Guo. 2017. Intelligent resource management in blockchain-based cloud datacenters. *IEEE Cloud Comput.* 4, 6 (2017), 50–59.

[146] Mengtian Xu, Guorui Feng, Yanli Ren, and Xinpeng Zhang. 2020. On cloud storage optimization of blockchain with a clustering-based genetic algorithm. *IEEE IoT J.* 7, 9 (2020), 8547–8558.

[147] Changsong Yang, Xiaofeng Chen, and Yang Xiang. 2018. Blockchain-based publicly verifiable data deletion scheme for cloud storage. *J. Netw. Comput. Appl.* 103 (2018), 185–193.

[148] Hui Yang, Haowei Zheng, Jie Zhang, Yizhen Wu, Young Lee, and Yuefeng Ji. 2017. Blockchain-based trusted authentication in cloud radio over fiber network for 5G. In *Proceedings of the 16th International Conference on Optical Communications and Networks (ICOCN'17)*. IEEE, 1–3.

[149] Mu Yang, Andrea Margheri, Runshan Hu, and Vladimiro Sassone. 2018. Differentially private data sharing in a cloud federation with blockchain. *IEEE Cloud Comput.* 5, 6 (2018), 69–79.

[150] Bo Yin, Lishi Mei, Zexun Jiang, and Kai Wang. 2019. Joint cloud collaboration mechanism between vehicle clouds based on blockchain. In *Proceedings of the IEEE International Conference on Service-Oriented System Engineering (SOSE'19)*. IEEE, 227–2275.

[151] Chunxia Yu, Luping Zhang, Wenfan Zhao, and Sicheng Zhang. 2019. A blockchain-based service composition architecture in cloud manufacturing. *Int. J. Comput. Integr. Manufact.* (2019), 1–11.

[152] Dongdong Yue, Ruixuan Li, Yan Zhang, Wenlong Tian, and Chengyi Peng. 2018. Blockchain based data integrity verification in P2P cloud storage. In *Proceedings of the IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS'18)*. IEEE, 561–568.

[153] Victor Zakhary, Divyakant Agrawal, and Amr El Abbadi. 2019. Atomic commitment across blockchains. arXiv:1905.02847. Retrieved from https://arxiv.org/abs/1905.02847.

[154] Sherali Zeadally and Jacques Bou Abdo. 2019. Blockchain: Trends and future opportunities. *Internet Technol. Lett.* 2, 6 (2019).

[155] Huaqing Zhang, Yanru Zhang, Yunan Gu, Dusit Niyato, and Zhu Han. 2017. A hierarchical game framework for resource management in fog computing. *IEEE Commun. Mag.* 55, 8 (2017), 52–57.

[156] Peng Zhang, Zehong Chen, Kaitai Liang, Shulan Wang, and Ting Wang. 2016. A cloud-based access control scheme with user revocation and attribute update. In *Proceedings of the Australasian Conference on Information Security and Privacy*. Springer, 525–540.

[157] Yinghui Zhang, Robert H. Deng, Ximeng Liu, and Dong Zheng. 2018. Blockchain based efficient and robust fair payment for outsourcing services in cloud computing. *Inf. Sci.* 462 (2018), 262–277.

[158] Yuan Zhang, Xiaodong Lin, and Chunxiang Xu. 2018. Blockchain-based secure data provenance for cloud storage. In *Proceedings of the International Conference on Information and Communications Security*. Springer, 3–19.

[159] Yong Zhang, Songyang Wu, Bo Jin, and Jiaying Du. 2017. A blockchain-based process provenance for cloud forensics. In *Proceedings of the 3rd IEEE International Conference on Computer and Communications (ICCC'17)*. IEEE, 2470–2473.

[160] Yuan Zhang, Chunxiang Xu, Xiaodong Lin, and Xuemin Sherman Shen. 2019. Blockchain-based public integrity verification for cloud storage against procrastinating auditors. *IEEE Trans. Cloud Comput.* (2019).

[161] Yuan Zhang, Chunxiang Xu, Jianbing Ni, Hongwei Li, and Xuemin Sherman Shen. 2019. Blockchain-assisted public-key encryption with keyword search against keyword guessing attacks for cloud storage. *IEEE Trans. Cloud* https://doi.org/10.1109/TCC.2019.2923222

[162] Bo Zhao, Peiru Fan, and Mingtao Ni. 2018. Mchain: A blockchain-based VM measurements secure storage approach in iaas cloud with enhanced integrity and controllability. *IEEE Access* 6 (2018), 43758–43769.

[163] Rongyue Zheng, Jianlin Jiang, Xiaohan Hao, Wei Ren, Feng Xiong, and Yi Ren. 2019. bcBIM: A blockchain-based big data model for BIM modification audit and provenance in mobile cloud. *Math. Probl. Eng.* 2019, (03 2019), 1–13. https://doi.org/10.1155/2019/5349538

[164] Xiaochen Zheng, Raghava Rao Mukkamala, Ravi Vatrapu, and Joaqun Ordieres-Mere. 2018. Blockchain-based personal health data sharing system using cloud storage. In *Proceedings of the IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom'18)*. IEEE, 1–6.

[165] Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Xiangping Chen, and Huaimin Wang. 2018. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* 14, 4 (2018), 352–375.

[166] Huan Zhou, Cees de Laat, and Zhiming Zhao. 2018. Trustworthy cloud service level agreement enforcement with blockchain based smart contract. In *Proceedings of the IEEE International Conference on Cloud Computing Technology and Science (CloudCom'18)*. IEEE, 255–260.

[167] Huan Zhou, Xue Ouyang, Zhijie Ren, Jinshu Su, Cees de Laat, and Zhiming Zhao. 2019. A blockchain based witness model for trustworthy cloud service level agreement enforcement. In *Proceedings of the IEEE Conference on Computer Communications (INFOCOM'19)*. IEEE, 1567–1575.

[168] He Zhu, Yichuan Wang, Xinhong Hei, Wenjiang Ji, and Li Zhang. 2018. A blockchain-based decentralized cloud resource scheduling architecture. In *Proceedings of the International Conference on Networking and Network Applications (NaNA'18)*. IEEE, 324–329.

[169] Liehuang Zhu, Yulu Wu, Keke Gai, and Kim-Kwang Raymond Choo. 2019. Controllable and trustworthy blockchain-based cloud data management. *Fut. Gener. Comput. Syst.* 91 (2019), 527–535.

[170] Zhiqin Zhu, Guanqiu Qi, Mingyao Zheng, Jian Sun, and Yi Chai. 2019. Blockchain based consensus checking in decentralized cloud storage. *Simul. Model. Pract. Theory* (2019), 101987.

[171] Dimitrios Zissis and Dimitrios Lekkas. 2012. Addressing cloud computing security issues. *Fut. Gener. Comput. Syst.* 28, 3 (2012), 583–592.

[172] Weiqin Zou, David Lo, Pavneet Singh Kochhar, Xuan-Bach D. Le, Xin Xia, Yang Feng, Zhenyu Chen, and Baowen Xu. 2019. Smart contract development: Challenges and opportunities. *IEEE Trans. Softw. Eng.* (2019). https://doi.org/10.1109/TSE.2019.2942301

Received March 2020; revised January 2021; accepted March 2021