IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Ingénierie des Systèmes d'Information
Vol. 26, No. 1, February, 2021, pp. 33-46
Journal homepage: http://iieta.org/journals/isi

The Purview of Blockchain Appositeness in Computing Paradigms: A Survey

Battula V. Satish Babu[1*], Kare Suresh Babu[2]

[1] JNTUH, CSE, Hyderabad 500085, India
[2] School of IT, JNUTH, CSE, Hyderabad 500085, India

Corresponding Author Email: satish@aliet.ac.in

https://doi.org/10.18280/isi.260104

Received: 28 November 2020
Accepted: 31 January 2021

Keywords:
blockchain, access control, computing paradigms, cloud, security

ABSTRACT

Blockchain technology is getting more and more pertinent to solve most of the digital problems that we face today. Blockchain is notable for its prominent features like immutability, decentralization, consensus, privacy, and security. However, blockchain is still suffering from different barriers like quantum attacks, scalability problems, integration problems, incompetence to face bigdata, storage problems, and so on. The main aim of this study was to find out the scope, various problems raised, and the applicability of blockchain technology when integrated with different computing paradigms like cloud computing, edge computing, fog computing, osmotic computing, big data computing, and quantum computing. To conduct this study, we have surveyed different research articles in the combination of blockchain technology and computing paradigms. Based on this survey, we have mentioned the contemporary research works, challenges, and a list of possible research opportunities and solutions.

1. INTRODUCTION

As a part of the Bitcoin cryptocurrency, "Satoshi Nakamoto" introduced the concept of blockchain 1.0. In the year 2015, with the advent of smart contracts in the Ethereum blockchain platform made blockchain 2.0 unconfined to the Bitcoin cryptocurrency. Later, many top MNC companies like Google, IBM, Microsoft, FedEx, Facebook, etc. started investments in developing blockchain solutions.

At present, blockchain helps to solve many digital problems that we face in our daily lives. To understand the proliferation of blockchain, in the paper [1], we have listed nine application categories with a total of 88 identified different blockchain applications.

In that paper [1], we have identified that 88 applications were implemented in one of the computing paradigms like cloud, edge, fog, osmotic, bigdata, and quantum computing paradigms. So we started our literature survey by identifying the implications of adopting blockchain along with different computing paradigms.

2. RELATED WORK

To write this survey paper, we have almost referred to 147 research articles published in the combination of computing paradigms and the blockchain. Here Figure 1 represents the time order of the literature survey, and Figure 2 represents the number of journals and conference articles referred.

As a summary of Figure 1 and Figure 2, we can understand that research on integrating computing paradigms with the blockchain and its applications is gaining more interest in the research community, but still there are so many research gaps.

The main aim of writing this survey paper is to highlight contemporary research works, challenges, and to list out the research gaps and possible research opportunities regarding blockchain appositeness in computing paradigms.

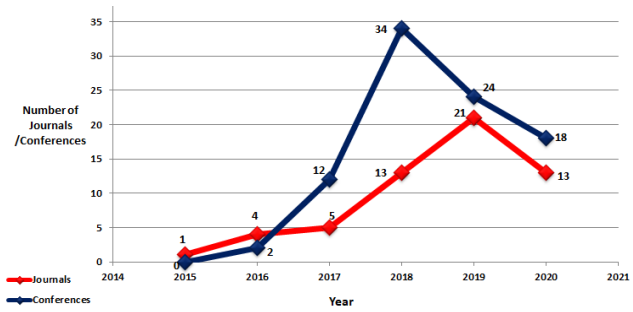

Figure 1. The time order of the literature survey

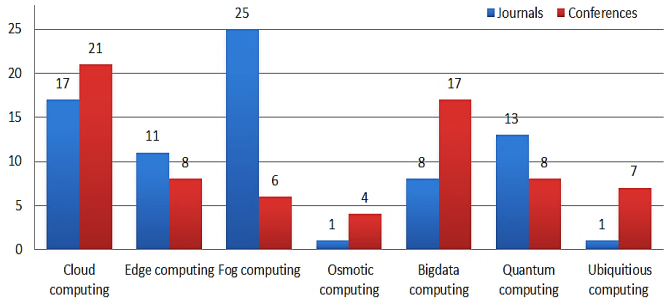

Figure 2. Number of journals and conference papers referred

In every section, we are going to mention contemporary research works, challenges, and list possible research opportunities. In Section 3, we have listed out different research works on the integration of the cloud and its services with blockchain. In Section 4, we have listed out some research works on the integration of edge computing with the blockchain framework. In Section 5, we discuss the feasibility

of integrating blockchain with the fog computing concept. Section 6 is about combining osmotic computing with blockchain. In Section 7, we have listed out different research works on combining blockchain with big computing. In Section 8, we have listed out some research works on combining blockchain with quantum computing and quantum attacks on blockchain. In Section 9, we explain the blockchain inappropriateness in particular cases. Section 10 includes the survey analysis. Finally, Section 11 is about future work and the conclusion.

3. INTEGRATING BLOCKCHAIN WITH CLOUD

The comprehensive representation of blockchain applications in cloud computing are shown in Figure 3.

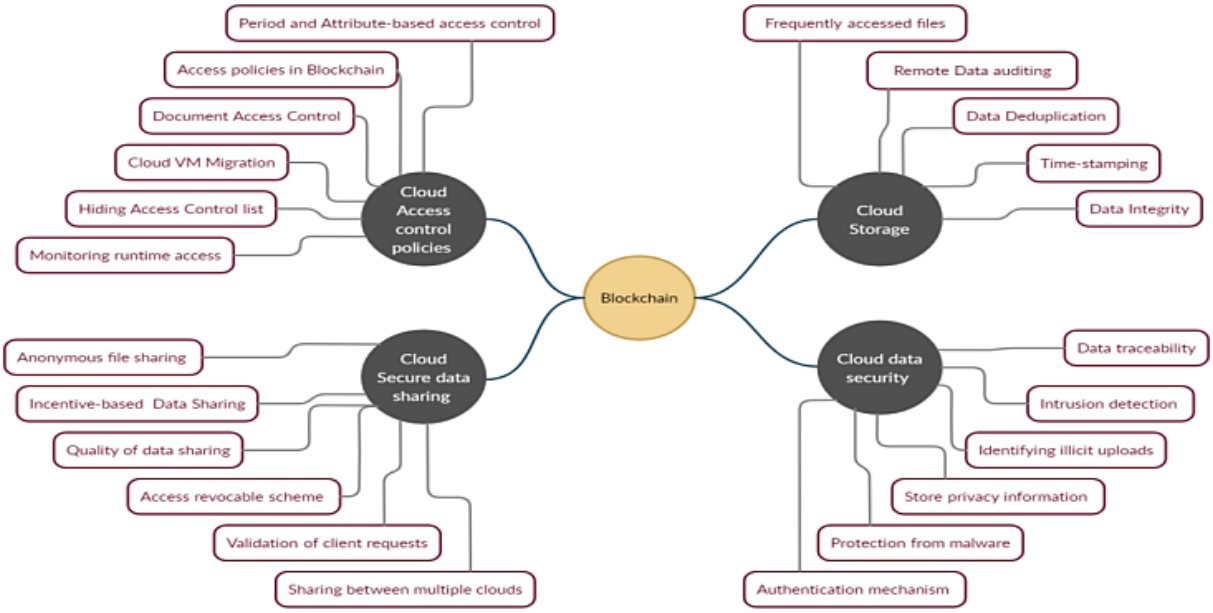

Figure 3. Comprehensive representation of blockchain applications in the cloud

When integrating blockchain with cloud, it is possible to overcome different cloud-related challenges like downtime, identifying data corruption, data security, limited access control, trust management issues, data sharing problems, and data privacy concerns.

Before integrating blockchain into the cloud, one should think of its characteristics and then decide its applicability to the cloud applications. Chan et al. [2] has given ten different characteristics and different requirement questions on the blockchain that can help anyone to decide about integration. These characteristics are immutable, data transparency, trust by smart contracts, individual identity, distribution of data, transactional system, permanent history of records, suitable for ecosystems and not for particular software, single backward-linked list, decentralized workflow architecture. But still, a few problems need to be addressed by research, among them

- Need designing of blockchain systems for the cloud that supports different data policies of different countries when cloud data moves from one country to another country data center.
- Need one common cloud blockchain IDE that supports the integration of cloud to different blockchain systems.

3.1 Blockchain combined with cloud storage

Centralized cloud storage is not secure and reliable for outsourced user data. Using a blockchain along with cloud storage will guarantee the security of user outsourced data. From the cloud storage perspective, blockchain is applied in different ways

1) Frequently accessed files: Shah et al. [3] suggested using an adaptive algorithm through which we can identify frequently accessed files and maintain their metadata in the blockchain. This procedure will make them readily available. Additionally, the credit system is introduced to prioritize peer requests based on their previously provided file access services.

2) Remote data auditing: It is a process that allows the data owner to audit the outsourced data in cloud storage and to confirm the trustworthiness of the cloud service provider. Using a blockchain for data auditing involves all peer nodes as an association to verify the correctness of outsourced data. This proposed arrangement by Huang et al. [4] decreases the data owner's cost of verification.

3) Time-stamping: Time-stamping is very important when cloud data is about intellectual property rights. Zhang et al. [5] proposed a time-stamping mechanism using a blockchain, where the transaction with time-stamp will be created during the file creation in the cloud. It is not possible to change the time-stamp because the blockchain is immune to content modification.

4) Data Integrity: Blockchain is used as a perfect tool to verify the integrity of cloud data. Till now there are many proposed methods to protect the integrity of cloud data. One of them is the method proposed by Sharma et al. [6], which uses two Merkle trees to maintain owner and file information separately. This arrangement allows the verification of user request using blockchain

5) Data Deduplication: It is the process of removing the duplicated data in the cloud and reducing cloud resource costs. SP.Gochhayat et al. [7] has proposed a blockchain based tool called "Yugala", used to protect the integrity and de duplicates

the cloud data. Li [8] performed the deduplication of data from heterogeneous cloud datacenters. Here blockchain is used to maintain block indexes in the ledger.

Multiple data blocks with the same indexes will be considered as duplicates and removed from the cloud storage. But still, a few problems need to be addressed regarding the association of cloud storage along with blockchain, among them

- The problem of a byzantine node is still not addressed during the remote data audit for collaborative data verification
- In the blockchain network, every participating peer maintains the same copy of chained blocks. As time passes, the peer node may run out of storage if blockchain size increases. So there is a need for porting blockchain storage to a distributed storage solution.

3.2 Access control policies using blockchain

Controlling access to cloud assets is possible by defining the policies. There is a chance that a hostile cloud resource administrator or manager may tamper with these policies to grant illegitimate access and to pose unusual restrictions on legitimate users. Therefore, it is a dire need to protect these policies from such activities. Recently, the blockchain has emerged as a solution to protect these policies. Where policies are directly written into the blockchain. Some of the works on policy management using blockchain are listed below.

1) Cloud VM Migration: Uchibayashi et al. [9] placed policies in blockchain management host to manage cloud VM migration. This arrangement will remove restrictions on the source and destination host and speed up the migration process.

2) Document Access Control: Desai et al. [10] proposed a multi-user-based access control system. When the document is uploaded into the cloud, its encrypted link will be stored in the blockchain. Multiple clients who want to access cloud files should verify themselves and use the aggregate key to decrypt the link. Tseng et al. [11], used blockchain as a link to decrypt and encrypt the file location in the cloud, where the actual data is stored in the cloud.

3) Period and Attribute-based access control: In Wang et al. [12] method, the data owner is going to place ciphertext in blockchain and set the access period for the particular user. Users will be able to access ciphertext in blockchain only when the user provides the attributes and correct access period acceptable by access policy.

4) Access policies in Blockchain: Yang et al. [13] have proposed "AuthPrivacyChain", where access policies are written in the cloud blockchain. User access queries to access cloud data are always checked against policies in the blockchain.

5) Hiding Access Control list: Hoang et al. [14] proposed a blockchain based framework, where the data owner maintains a modifiable hidden access control list that contains consumer public keys with whom he or she wants to share the data. Additionally, smart contracts are deployed to control the location of share data located in IPFS. The consumer data retrieval request is also registered and controlled using smart contracts.

Apart from the above-mentioned methods, the research against the access control policy mechanism using the blockchain is still in the infancy.

3.3 Secure data sharing using blockchain

Data sharing through a cloud service provider is not entirely reliable and leads to different user privacy and quality issues. Choosing a blockchain is a considerable option to share data without the involvement of malicious third parties. Recent works that incorporated blockchain to share cloud data are

1) Signcryption: Liu et al. [15] used **`signcryption`** for the Internet of vehicles network data traffic sharing. The blockchain is used to maintain the vehicle's access control list. Data request from the client is validated against the blockchain ACL. On successful validation of client requests, smart contacts are used to send encrypted data storage addresses to the client. On receiving the encrypted data address, the client uses a symmetric key to get the required data.

2) Incentive-based data sharing blockchain: Shen et al. [16] proposed an incentive-based data sharing mechanism using a blockchain. When multiple clouds are involved in data sharing,**"Shapley value"** is used to determine fair incentive distribution and thereby increasing the quality of data sharing from multiple cloud participants.

3) Blockchain based academic paper sharing and peer review system: Zhou et al. [17] proposed a blockchain based academic paper sharing and peer review system. Hyper ledger Fabric platform is applied to maintain information regarding document access and reviews. For sharing documents, the blockchain is integrated with IPFS. In this method, anonymity is provided to both the reviewer and the author. This paper addressed the biased reviews using review metrics. Reviewers are automatically paid for their reviews by deploying smart contracts

4) User data-sharing categories: Shrestha and Vassileva [18] implemented incentive-based Ethereum blockchain for research data sharers users. Users need to register in a private network. A user participating in the network can describe data-sharing categories. Ethereum blockchain is used to share data among registered users. Policies regarding access and privacy are stored in the blockchain

5) Access revocable scheme: Hoang et al. [14] proposed access revocable scheme using predicate encryption, where the data owner is going to create a private key for every user that can be used for decryption. If the data owner finds malicious behavior on the user side, the data owner re-encrypts the data through a delegated storage node. After re-encryption, malicious users will become impotent to decrypt the data [19].

3.4 Achieving clouds data security using blockchain

Blockchain technology has become a promising alternative to confront different cloud data security issues because of features like immutability, distributed consensus algorithms, decentralized open ledger, using a hashing function. In this section, we are going to discuss a list of recent works that had incorporated blockchain for cloud data security:

1) Security: In the survey conducted by Xu et al. [20] and Tsai. et al. [21], have provided different solutions to secure cloud data using the blockchain. Among them

a. Public key cryptography and access control lists are used to safeguard cloud data privacy. We can use the blockchain and the public key cryptography to store data, smart contract to apply access control policies.

b. Monitoring runtime access: Smart contracts are used to specify access rights. Access logs will be collected from the cloud and compared against smart contracts to identify the

infringement.

c. Data traceability: It is possible to store cloud data access log operations in blockchain for efficient cloud data audit

d. Integrity verification: Original data will be store in cloud storage as an off-chain database. And the blockchain is used to maintain metadata like the address and hash of the cloud data. The data owners can investigate cloud data integrity using meta-data stored in the blockchain.

e. Anonymous file sharing using blockchain protect the privacy of data owners.

f.Identifying illicit uploads: A unique hash ID and other meta-data of upload files will be stored in the blockchain. Later on, this unique hash ID and authentication signatures can be used to identify illicit file uploads.

2) Kumar and Singh [22] has proposed Distributed intrusion detection using the blockchain. This method allows us to exchange log data with each other and decide the authenticity of logs from different cloud servers. If the blockchain network is growing large, then we need to face bigdata challenges.

3) Yan. et al. [23] suggested using a fuzzy algorithm based on searchable encryption through keyword. This method provides good searching results even in the case of typos in the keyword by the user. However, we can still improve this method by applying existing machine learning algorithms.

4) Albalawi and Azim [24] proposed a cloud-dependent enrollment and authentication mechanism for IoT devices using blockchain. Here blockchain is used to store IoT device-related data. However, if there is a large number of IoT devices, transactions lead to spun-out of the authentication process.

5) Malvankar et al. [25] proposed a method of restraint against malware in the cloud. Here, graph analytics are utilized to find the malicious node, and that information is shared with all other nodes that are part of the blockchain. Smarts contract is automatically applied to take appropriate action.

6) Westerlund and Jaatun [26] mentioned that using a blockchain to store privacy information does not concur with one of the GDPR privacy elements because of the immutability property of blockchain. But still, we need more research on storing and protecting user privacy data permanently in the blockchain.

4. INTEGRATING WITH EDGE COMPUTING

It was reckoned that the number of connected IoT devices would be increased to 25 billion by the end of the year 2030. Almost 130 new IoT devices per second are connected to the internet. As the velocity of data is increasing, the quantities of data that need to be processed and transferred are also increasing. Conventional centralized cloud servers can be used to store and process data originating from IoT devices. Using a centralized cloud server creates different problems.

- **Network latency from the cloud**: It is a consequential problem and critical for real-time IoT devices if there is a delayed response from the cloud, even for milliseconds.
- **Increased bandwidth**: It happens when a large volume of data is transferred with a high velocity between IoT devices and centralized cloud servers.

To overcome these problems, we can realize the distributed computing paradigm called “Edge computing”. In edge computing, instead of entirely relying on cloud services, most of the data storage and computing operations are moved and performed in the proximity of the IoT device or in the IoT device itself. When combined with the blockchain, we can even solve more problems related to edge computing. In this section, we are going to list out a few recent works on edge computing in the combination of blockchain:

1) Varghese et al. [27] has listed out different challenges regarding the integration of edge and blockchain

a. Blockchains are usually meant to store linear transactional data. But it is still obscure on how blockchain is going to handle complex data arrangements and queries that belong to edge market places.

b. It is still uncertain about the impact of different types of blockchain on edge computing models.

c. It is still uncertain about the impact of blockchains off-chain and on-chain storage on edge storage models.

2) Freitag et al. [28] proposed the community-based micro cloud over edge devices using blockchain. Here group Individual nodes part of the blockchain network denotes storage and computational resources to the edge devices. Individual nodes are going to get incentives based upon the participation in a micro-cloud service. Decentralized governance of all nodes is possible by using by materializing the blockchain.

3) Zhang et al. [29]. Used mobile edge computing to solve large intensive computational problems required for consensus. Blockchain is used to make data tamper-proof and to remove the dependency on a centralized trusted system.

4) Li et al. [30] raised the challenge that needs to be solved. Once the data is entered the blockchain, the blockchain is going to make that data immutable. But what about the protection of the same data in an edge device before it enters the chain?

5) Liu et al. [31] designed a model of blockchain and mobile edge computing to handle computationally intensive tasks related to video transcoding. Here blockchain is used to create a co-operative environment between video transcoders and provide incentives.

In their model, computationally intensive tasks are offloaded to edge devices provided with storage and computational resources. Additionally, they have introduced the concept of dynamic block size to handle different requirements of video transcoding.

6) Liu et al. [32] introduced the concept of caching the block hashes in blockchain deployed on the mobile edge computing devices. Block hashes are cached to speed the communication between edge nodes.

7) Xiong et al. [33] listed out open issues that are raised when blockchain is integrated with edge computing.

- There is a possibility of jamming attacks when the transactional data is in transit between wireless IoT devices and edger servers
- Efficient resource allocation methods are still needed when there are many resource requests from multiple IoT devices.

8) Zheng et al. [34] designed two different consensus protocols

- To improve performance of the system, message-based consensus protocol is proposed instead of hash-based consensus protocol.
- POE (Proof-of-Edge) consensus protocol is proposed to maintain consensus between edge computing nodes.

9) Xu et al. [35] proposed a resource management method. According to them, different edge devices are equipped with different levels of computational and network resources. Not all edge devices are going to afford the resources required to

maintain the blockchain. They have proposed two approaches for efficient resource utilization when dealing with bigdata on the edge. The possible solution is to develop a new mechanism that identifies the state, context, and requirements of edge devices by using some using unique identifiers.

10) The same kind of method is implemented by Seike et al. [36] in the management of ownership

- Transaction filtering: "Futile transaction theory" is applied to reduce the storage utilization of the blockchain. According to this theory, previous transactions are useless if their output is represented by the latest transactions.
- PoC (Proof of collaboration): It is a consensus protocol that requires less computational resources when compared to PoW.

11) Rahman et al. [37] proposed an anonymity scheme for each block in the edge blockchain using the open-source tool called **"tor"**. Because the address of the block is easily detectable in the public blockchain

12) Xu et al. [38] applied game theory to reduce potential attacks from edge servers. In this game, every edge server records the actions of other servers. These records are shared with the entire network. Every edge server is going to find out the Nash equilibrium value over received action records and applies a punishment scheme for identified malicious edge servers.

13) Kang et al. [39] for efficient data sharing they have implemented a consortium blockchain in a vehicular network with selected edge nodes. These prior selected edge nodes are responsible for reaching consensus.

14) Gauhar et al. [40] expounded the authentication mechanism between IoT devices installed in different places and working for variety of domains. They have created global and internal smart contracts to make them available for a variable number of users.

The synopsis of the above-mentioned recent works are listed in the Table 1.

Table 1. Recent works on Edge computing with Blockchain

Author	Purpose	Synopsis
Varghese et al. [27]	Integration Challenges	• Handle complex data arrangements and queries • impact of different types of blockchain • Impact blockchains off-chain and on-chain storage
Li et al. [30]		• Protection of data in the dge device before it enters the chain
Xiong et al. [33]		• Possibility of jamming attacks • Handling many resource requests from multiple IoT devices
Felix Freitag et al. [28]	Resource sharing and utilization	• Incentive-based storage and computational resources sharing
Xu. et al. [35]		• Resource utilization by identifying the state, context, and requirements of edge devices
Zhang et al. [29].	Intensive computational problems	• Blockchain used to make data tamper-proof
Liu et al. [31]		• Handling computationally intensive tasks related to video transcoding
Liu et al. [32]	Improving the performance of blockchain	• Caching the block hashes in blockchain
J. Zheng et al. [34]		• Message-based consensus protocol • POE(Proof-of-Edge) consensus protocol
Seike et al. [38]		• Transaction filtering to reduce the storage utilization of blockchain • Used proof of collaboration that requires less computational resources
Rahman et al. [36]	Improving the Security	• Anonymity scheme
Xu et al. [37]		• Using game theory to reduce attacks from other edge servers
Ali Gauhar et al. [40]		• Authentication mechanism between Edge devices
Kang et al. [38]	Data sharing	• Implemented a consortium blockchain for efficient data sharing

5. INTEGRATING WITH FOG COMPUTING

Fog computing is like a better version of edge computing. In edge computing, the storage and computational operations are carried out directly on edge devices. Edge computing has different cons like

- Huge amount of data generated on edge devices with less storage capacity
- Costly in terms of maintenance
- Need sophisticated infrastructure
- Security is at stake because data transferred to edge networks present outside
- Edge devices are used only for analyzing data
- Very little redundancy

Some of these problems can be solved using fog computing. Fog computing performs storage and computational operations on separate LAN-connected computers called Fog nodes. Fog nodes are equipped with more storage capacity and processing power when compared to edge devices. In turn, the fog node is connected to the cloud. Figure 4 explains the concept of Fog Computing.

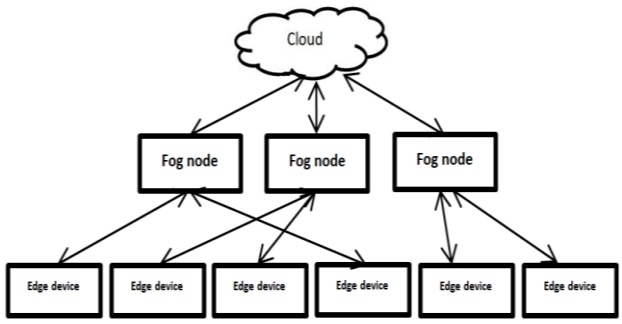

Figure 4. Fog and Edge computing

Fog computing is a solution provided by the CISCO company. Its name is given like that because fog lies just below the cloud and nearer to the ground (edge devices). When

combined with blockchain we can overcome security and privacy-related challenges. In the following section, we are going to list out a few recent works on the combination of fog computing and blockchain.

Table 2. Recent works on Fog computing with blockchain

Author	Purpose	Synopsis
Lei et al. [41]	Integration Challenges	• Need block parameters tuning to overcome scalability problems. • Computationally intensive Proof of Work (PoW) need to be addressed
Baniata et al. [50]		• Need more sophisticated security measures • Not suggested for time-critical IoT application • Lack of standardization • Problem with fast-moving clients
Yao et al. [42]	Authentication Mechanisms	• Introduced a lightweight and message-based authentication scheme using a blockchain for fast-moving vehicles
Almadhoun et al. [43]		• Proposed mutual authentication scheme between fog nodes in proximity.
Puthal et al. [53]		• Proposed lightweight blockchain consensus protocol "Proof of Authentication" for a fog node with resource constraints.
Debe et al. [45]	Reputation-based mechanisms	• Reputations of fog nodes are used either to distribute incentives and to penalize them for bad behaviour
Yu et al. [47]		• To identify and analyze storage and computing requirements
Cinque et al. [56]		• Instead of using reputation scores, fog nodes assign trust degrees to other nodes
Alshehri et al. [46]	Security	• Designed on-chain policies to control access to the data.
George et al. [48]		• Suggested using lightweight Elliptic curve cryptography
Wu et al. [49]		• Blockchain is used to store the access control list of fog nodes.
Ziegler et al. [51]	Simplifying Proof of Work (PoW)	• Creating side chains to decrease the load on blockchain caused due to PoW
Kumar et al. [52]		• Statistical-based matrix factorization is used to simplify PoW
Lee et al. [54]		• Delay Aware Tree (DAT) is constructed to free blockchain from PoW
Memon et al. [44]		• Maintained two fog layers in the system. Here the second layer is dedicated for mining operations related to PoW
Yánez et al. [55]	Data Management	• Calculated the rating of allotment (ROA) to decide on-chain data allotment for edge devices

1) Lei et al. [41] expounded problems related to fog computing like centralized and trust management and presented a solution called the blockchain. When combined with fog computing, they have suggested for block parameters tuning to overcome scalability problems of blockchain in the combination of fog computing.

Tuning block parameters like block size, block interval is going to influence blockchain properties like consistency as well as performance. The Blockchain Proof of Work is also heavy for a fog node. These problems still need to be addressed when fog computing is integrated with blockchain

2) Yao et al. [42] proposed a lightweight and one message-based authentication scheme using a blockchain for the fast-moving vehicles that are part of fog networks.

3) Almadhoun et al. [43] proposed a mutual authentication scheme carried out by fog nodes. Instead of involving IoT devices in hefty computation required for authentication and communication, we can use fog nodes that are present in near distance to IoT devices.

4) Memon et al. [44] suggested using two fog layers in the blockchain based IoT architecture. Here layer one contains a cluster of regular fog nodes that communicate with both cloud and IoT devices. Layer two contains fog nodes that are especially dedicated to performing mining operations for IoT devices that are part of the blockchain network.

5) Debe et al. [45] implemented a reputation-based mechanism using a blockchain to identify the reputation of a fog node either to distribute incentives or to penalize them for bad behaviour.

6) Alshehri et al. [46] resist the fog nodes from infringement data security. They have maintained on-chain policies to control access to the data. Every fog node is provided with an off-chain database of data files that are accessed often.

7) Yu et al. [47] applied a reputation based framework to identify and analyze storage and computing requirements of the fog node. They have divided fog node nodes into three categories: basic, light, and full-fog nodes based on computing power. For efficient storage methods, they have also identified users with two identities in two different fog nodes.

8) George et al. [48] suggested using a lightweight Elliptic curve cryptography scheme signing transactions in the blockchain in resource constraint IoT devices. But still, lightweight ECC needs some improvements like reducing bandwidth and energy consumption.

9) Wu et al. [49] used a blockchain to store the access control list of fog nodes. In their method, fixed blockchain length is maintained in a cluster of fog nodes to save storage space. A flake of a peer-to-peer network is created as a cluster that can work with less computing power available.

10) Baniata and Kertesz [50] mentioned a few challenges regarding the integration of fog and blockchain integration that are to be addressed.

- Integration between them is not yet standardized
- Decentralization property of blockchain along with fog computing needs more sophisticated security measures.
- Their integration causes jitter, and it is not suggested for time-critical IoT application
- PoW on fog node needs more computational energy
- There will be complex situations due to fast-moving clients.

11) Ziegler et al. [51] proposed a scalable mechanism called the "Plasma framework" that can be used to integrate blockchain and fog nodes. This framework lets you create side chains from the parent chain. These side chains are used to maintain the transactions that are moved out of the parent

chain. Doing this will decrease the load on blockchain caused due to PoW and make it more suitable for fog nodes.

12) Kumar et al. [52] applied statistical-based matrix factorization to simplify "PoW". This method is used to easily obtain a solution with minimal memory and energy in a fog environment.

13) Puthal et al. [53] introduced a new lightweight blockchain consensus protocol "Proof of Authentication" for fog and IoT nodes with resource restrictions. In general PoW and other consensus protocols are applied to validate the blocks, whereas PoA is used to authenticate blocks.

14) Lee et al. [54] made a blockchain released from implementing PoW as it is computationally intensive. Here blockchain implementation is based upon the construction of Delay Aware Tree (DAT). After gathering certificates of IoT devices, now the system constructs DAT and selects as a fog device with less delay, i.e., a fog node near to the IoT device.

15) Yánez et al. [55] designed on-chain data allotment mechanism for edge devices using fuzzy logic. For every request, the method is to calculate the rating of allotment (ROA) based on different network-related parameters.

16) Cinque et al. [56] proposed a new trust management model. Instead of using reputation scores to decide the trust among nodes, this model allows every node to assign trust degree numbers (0 – No trust, 1 - Trust) to other nodes. These nodes may or may not belong to the same organization.

The synopsis of the above-mentioned recent works are listed in the Table 2.

6. INTEGRATING WITH OSMOTIC COMPUTING

Osmotic computing is a new computing paradigm inspired by the chemical osmosis process. In the chemical osmosis, process molecules move from a highly concentrated solution to a low concentrated solution to equalize the concentration of the entire solution.

Likewise, in osmotic computing micro services will be migrated to resource-constrained edge devices to the highly equipped cloud and vice versa is also possible [57].

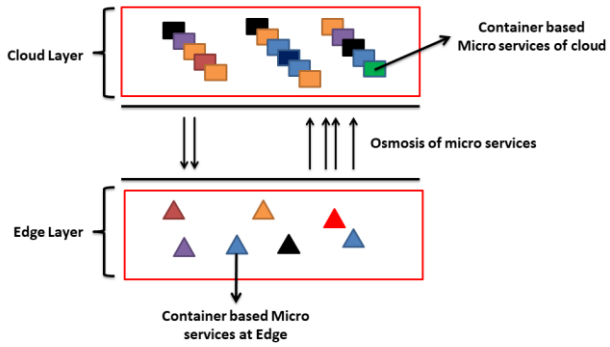

Figure 5. Osmotic computing between the edge, cloud

Osmotic computing is used to establish extensively federated and highly distributed environments in the cloud and edge. Micro services are deployed as virtualized containers using container-based technologies e.g Docker. It inherits all challenges and issues related to the edge and cloud environments. Osmotic computing is explained in Figure 5.

The following are the merits possible by integrating blockchain along with osmotic computing:

1) Supplemental analysis: Devices at the edge layer collect data from different sources and perform different types of operations on that locally stored data. The same data is transferred to the cloud layer for supplemental analysis.

2) Micro elements/Micro services: Buzachis and Villari [58] leveraged blockchain on software-defined membranes (SDMem). Micro elements/ micro services are transferred through this SDMem to enforce access control policies and to reach consensus during the osmosis.

Buzachis and Villari [58] implemented SDMem like Villari et al. [59] but with a private blockchain to ensure the integrity and ownership of data transferred and processed in micro services. A private blockchain is used to record all transactions related to micro services related to the cloud and edge.

3) Merits and challenges: Rasool et al. [60] expounded on the merits and challenges involved in the integration of blockchain. The following are the merits possible by integration.

- Openness
- Consensus-based Trust
- Smart contact-based reliability
- PoE along with access control list for privacy
- Semi-private blockchain for ownership

Challenges on integration:

- There is a dire need for research to discover the applicability of different types of blockchain in the presence of osmotic computing.
- Since Osmotic computing involves cloud, fog, edge layers, a new common consensus mechanism needs to be fabricated that requires the same level of computation resources in different layers
- Need research on possibilities of on and off-chain transactions
- Service management based on type of environments like cloud, edge, fog, IoT [61].
- Mirjana [62] stated that services would be categorized into macro services and micro services. Macro services are handled in a large cloud-based data center, whereas micro services are handled on resource-constrained IoT/Edge devices. To implement osmotic computing should have an insight into the following things.
  - Categorization of services into Macro or Micro
  - Estimating the different resource requirements for services and edge devices.

7. BIGDATA COMPUTING USING BLOCKCHAIN

Generally, the blockchain supports linear data with a small size. Recently, many scholars applied blockchain for securing bigdata in different ways like

- Bigdata Authentication
- Auditing to find interesting patterns
- Avoiding data skewness
- Data circulation in an autonomous way using blockchain
- Efficient sharing of Bigdata
- Bigdata privacy and trust
- Blockchain bloat

1) The challenges and requirements of bigdata authentication:

Abdullah et al. [63] has demonstrated the challenges and requirements necessary for bigdata authentication. The Bigdata tool Apache Hadoop uses Kerberos for the

authentication process. Already Kerberos systems are facing different challenges like

- Authentication based on password
- Having the chance of reply attacks
- Password guessed by brute-force attacks
- Exposure of session keys
- KDC (Key Distribution Center) as a single point of failure
- Time synchronization problems in a distributed environment
- Denial of service attacks

Prerequisites of bigdata authentication

- Decentralized authentication
- Anonymous and passphrase less environment
- Ignoring Session keys methods
- No single point of failure
- Immutable records

This entire list of requirements can be satisfied using a blockchain.

2) Subbiah et al. [64] proposed a querying algorithm based on blockchain technology. Traditional querying on bigdata is by using the MapReduce algorithm that causes data skewness.

To handle data skewness, the MapReduce-based querying method is replaced with a blockchain based querying method. In this method, the Map phase output is stored in the blockchain and uses caching to render the results.

3) Alexander and Wang [65] explained how blockchain 2.0 led to bigdata security in the following manner.

- Smart contracts lead to efficient bigdata circulation
- Decentralized storage of blockchain helps for efficient big data sharing
- Blockchain can be used to record the log of bigdata operations that can be used to audit.

4) Zheng et al. [66] said that when bigdata systems combined with blockchain, efficient data management schemes are possible. We can also perform data analytics on transactions of the blockchain to identify compelling patterns. (We need to check the applicability of parallel algorithms to analyze blockchain data)

5) Chen and Xue [67] stated that blockchain protects the data owner's copyrights and ownership rights by auditing the bigdata transaction logs of important documents present in the blockchain.

6) Yu et al. [68] implemented Data Auditing Blockchain (DAB), a different strategy to audit bigdata by collecting proofs of audits instead of blockchain transactions [69].

7) Karafiloski and Mishev [70] literature review suggested using access control list policies to maintain the privacy of big data. Shared encryption is applied to confidential data and sends the ciphertext to the off-chain "Distributed Hash Table" (DHT). Here blockchain is going to maintain a hash address as a link to that data.

8) Bandara et al. [71] compared blockchain storage against distributed storage and listed out a few shortcomings of blockchain.

- Blockchain storage is not that scalable when compared to distributed databases.
- It takes so much time to confirm the transaction.
- Less transaction throughput
- Lack of proper querying features
- Not suitable for big data sets

They have proposed the **"Mystiko"** blockchain-based storage built over a distributed database called Apache Cassandra. It is capable of handling big data and provides high transaction output.

Table 3. Recent works on Bigdata computing with blockchain

Author	Purpose	Synopsis
Subbiah et al. [64]		• Kerberos for the authentication process in Apache Hadoop • Data skewness • Bigdata privacy is a problem • MapReduce based querying method is not suitable.
Bandara et al. [71]	Integration Challenges	• Blockchain storage is not scalable when compared to distributed databases. • It takes so much time to confirm the transaction • Less transaction throughput • Lack of proper querying features • Not suitable for big data sets
Alexander et al. [65]		• Bigdata circulation
Smith et al. [72]		• Blockchain bloating (suggested using a tool called "Stroj")
Preece et al. [73]		• Placing confidential data in blockchain smart contracts is not preferable.
Zhou et al. [74]	Security	• Suggested using holomorphic encryption to protect the privacy of big data.
Elena et al. [70]		• Suggested using access control list policies and DHT in to maintain the privacy of big data
Zheng et al. [66]	Data Management and Auditing	• Data analytics on transactions can be performed to identify interesting patterns
Alexander et al. [65]	Storage and Auditing	• Decentralized storage ledger of blockchain helps in bigdata sharing • Blockchain can be used to store bigdata log operations
Chen et al. [67]		• Auditing the bigdata transaction logs to protect owner's copyrights
Yu et al. [68]		• Implemented Data Auditing Blockchain (DAB) that collects audit proofs
Bandara et al. [71]		• Proposed a blockchain tool **"Mystiko"** based on distributed storage.

9) Smith [72] suggested different methodologies to cope with blockchain bloating like using a tool called "Stroj" that makes use of Merkle tree and other method is by using Distributed network coded storage.

10) Preece et al. [73] suggested that blockchain smart contracts are generally available to everyone. Placing confidential data in smart contracts like a symmetric key in unencrypted format is not at all preferable.

11) Zhou et al. [74] explained the necessity of research on holomorphic encryption suitable for Quantum algorithms. Holomorphic encryption performs special mathematical calculations on encrypted data, where data can be verified without decryption. Holomorphic encryption can be applied to protect the privacy of big data.

The synopsis of the above-mentioned recent works are listed in the Table 3.

8. INTEGRATING WITH QUANTUM COMPUTING

Quantum computing is rooted in the concept of physics quantum mechanics. In quantum mechanics, particles like a photon have a quality of spin during their travel. The spin, in the vertical position and forward diagonal position, is used to represent the binary bit "1". And the spin, in horizontal position and backward diagonal position is used to represent the binary bit "0".

Sometimes the spin position of a photon represents both "1" and "0" at the same time. This position is called "qubit", and the property is called a "Superposition" of the photon. The same superposition property is used in quantum computing.

Traditional computers represent any data only by using 1's and 0's, whereas quantum computers represent data using 1, 0, and qubit. If we have "N" qubits, then we can represent 2^N bits. For example, if we have 300 qubits, then we can represent 2^{300} bits that are almost equal to the number of particles in the world.

This property makes quantum computers and quantum computing very powerful. We can use quantum computers to solve so many complex problems in polynomial time.

8.1 Quantum attacks towards Blockchain

Attacks carried out using quantum computers are called quantum attacks. The majority of the cryptographic primitives employed inside the blockchain are vulnerable to quantum attacks because they depend upon the "Finite Abelian Group" methods like factorization of integers and discrete logarithms e.g. The RSA and Elliptical curve based signatures. Those methods can be resolved in polynomial time on quantum computers by implementing Fourier transformations (Table 4).

1) Shor.[75] designed a hypothetical algorithm that works on quantum computers to expedite the calculations of integer factors and discrete logarithms and to break the blockchain security system. That algorithm can be used to drive the private key out of the public key and use that private key to sign illegitimate transactions.

2) In 1996, Grover. [76] proposed a search-based algorithm used to exploit two vulnerabilities in blockchain hashing algorithms.

- It is used to find out a new hash value by detecting hash collisions and replace the block hash with a new hash value without disintegrating the existing blockchain.
- It fastens the calculations of the PoW puzzle hash value called "Nonce", that can be used to make a block within less time. Proof of Stake (Pos) designed as an alternative for PoW is also vulnerable to P. Shor & L.K. Grover algorithms.

3) Suhail et al. [77] stated P.Shor algorithm can be used to break public-key cryptosystems like RSA, Diffie-Hellman, DSA, and Elliptical curve-based cryptosystems like Elgamal, ECDH, ECDSA. L.K. Grover algorithm is used to break symmetric cryptographic schemes like AES and SHA-256. Finally, they expounded on the need for post-quantum cryptographic mechanisms.

8.2 Safeguard mechanisms towards quantum attacks

To safeguard blockchain against quantum attacks, it is essential to re-equip the blockchain with quantum-resistant cryptography mechanisms. In this segment, we are going to list out some of the research involved in developing anti-quantum methodologies.

1) Li et al. [78] mentioned that a few traditional cryptographic mechanisms are still viable to face quantum attacks. These mechanisms are Hash-based method, Code-based method, Multivariate method.

2) Yin et al. [79] proposed the first lattice-based cryptography scheme as an alternative for traditional public-key cryptographic mechanisms.

At present, lattice-based cryptography algorithms are mainly used as post-quantum cryptography to resist quantum attacks. At present, there are many variants of lattice-based signatures, like

- Short lattice algorithm
- Lattice-based blind signature scheme
- Bosai tree-based lattice etc.

3) Kiktenko et al. [80] suggested the concept of "Quantum key distribution inside the blockchain as a safeguard against quantum attacks.

4) Nanda et al. [81] stated that implementation of "Quantum Key Distribution (QKD)" is possible without the need for quantum computers. The QKD can be used for the secret sharing of keys with the help of qubits.

5) Jin et al. [82] incorporated the concept of "Quantum hashing" in the blockchain to defend against quantum attacks by increasing the uncertainty in hash values.

6) Yin et al. [83] stated that blockchain wallet bloat is going to happen by using lattice-based signatures. It is going to generate and store the number of private keys in the blockchain wallet from different seed keys.

In their paper, they have created a lightweight wallet based on bonsai trees and generated several private keys using a seed key.

7) Fernández-Caramés and Fraga-Lamas [84] suggested expanding the result size of the hash algorithms to face quantum attacks posed by Grover's algorithm.

8) Chalkias et al. [85] mentioned that blockchain-based solutions like Corda, Quantum resistant Ledger, and IOTA use post-quantum signatures schemes to limit the signature size and allow us the same key to sign multiple times.

9) Krendelev et al. [86] explained the required properties of the blockchain hash function to make it quantum resistant.

- Hash function should be able to define hash collision
- It should have more avalanche effect.

In their paper, they have described a quantum-resistant parametric hash function algorithm that generates hashes using a large number of parameters.

10) Suhail et al. [77] suggested the use of the "Hash-Based Signature (HBS)" scheme to defend against quantum attacks. Because HBS provides greater security with small-sized signatures and with fewer security specifications.

11) Ma and Jiang [87] proposed the smaller signature sized multi-signature approach using lattice-based cryptography and reduced memory requirements by using the aggregate public key in the place of several public keys.

Table 4. Recent works on integrating blockchain with quantum computing

Author	Purpose	Synopsis
Peter Shor.[75]	Quantum attacks on blockchain	• Designed a hypothetical algorithm that drives the private key out of the public key
Grover. [76]		• Designed a search-based algorithm to exploit vulnerabilities in blockchain hashing algorithms
Suhail et al. [77]		• Conducted survey on how Shor & Grover's algorithm affects different crypto systems
Chao-Yang et al. [78]		• Mentioned traditional methods to defend against quantum attacks
Kiktenko et al. [80], Nanda et al. [81]	Quantum Key Distribution	• Suggested the using of quantum key distribution without the need for quantum computers
Jin et al. [82]	Quantum Hashing	• Uncertainty in hash values will defend against quantum attacks
Fernández-Caramés and Fraga-Lamas [84]		• Increasing the result size of hash algorithm's will defend against Grover's algorithm
Krendelev et al. [86]		• Suggested the properties to make a quantum resistant hash function for blockchain
Yin et al. [79]	Signature Based methods	• Proposed lattice-based cryptography used as post-quantum cryptography to defend quantum attacks
Yin et al. [83]		• Proposed a method to deal with blockchain wallet bloat caused by lattice-based signatures.
Chalkias et al. [85]		• Limited the signature size and made the same key to sign multiple times.
Suhail et al. [77]		• Used Hash-Based Signature (HBS) method with small-sized signatures to defend quantum attacks
Ma and Jiang [87]		• Reduced memory requirements by using smaller signatures and aggregate key

Even though quantum computers are not real for now, by the year 2035, quantum computers may come into existence. By using quantum computers, one can fabricate and initiate different types of quantum attacks on cryptographic primitives belonging to the blockchain.

So there is a dire need for post-quantum cryptographic algorithms and techniques to prevent quantum attacks on the blockchain. Currently, there are very few works available on making blockchain quantum resistant.

9. INAPPROPRIATENESS OF BLOCKCHAIN

One should not prefer blockchain because of its hype or due to its prominent features like immutability. One should understand its appositeness from different functional requirements of the application.

In this section, we are going to list out possible scenarios where the blockchain is not appropriate [88, 89].

- It is not efficient for applications that deal with transactions that are huge in volume and less in profit.
- Blockchain is used to store a small amount of linear data, and it is still challenging for bigdata applications
- It is not suitable for time-critical applications. Because of the propagation delay and slow transaction confirmation.
- If your application depends on a compulsory third party, then blockchain is not a correct option.
- Blockchain is not a correct option if the application is not for storing the data related to the system state.
- It is not suitable for applications where only one node is going to act as a writer to the ledger
- It is not necessary for the applications where the identity of peers is already known and they completely trust each other.

Blockchain is not suitable for applications where validation of collected data is critical. Because using blockchain, we can make data immutable, but it doesn't guarantee the correctness of data.

10. SURVEY ANALYSIS

Based on the recent works mentioned in this survey paper, we have taken synopsis points from Figure 3 and synopsis points from Tables 1-4 of different computing paradigms to identify the most appropriate computing paradigm with the blockchain

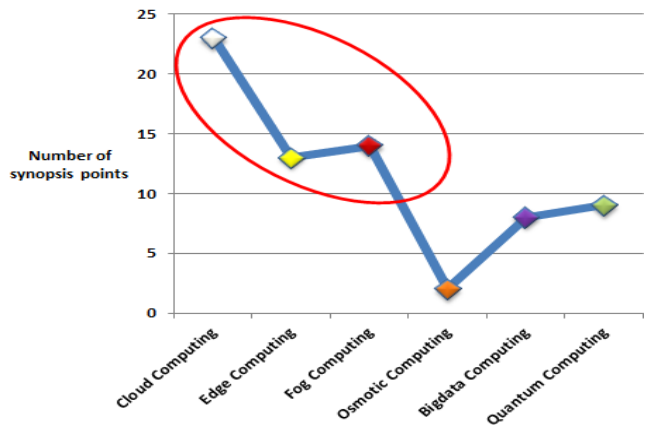

Figure 6. Mapping Computing paradigms with blockchain

Therefore, from Figure 6. We can identify that most of the research innovation of blockchain technology is done along with cloud, Edge, and fog computing paradigms. It is also identified that the suitability of inducing blockchain with different computing paradigms depends upon the context of the application and the type of framework we have selected to implement blockchain.

11. FUTURE WORK AND CONCLUSION

The main focal point of this survey paper is to identify the scope of the blockchain and its appropriateness and inappropriateness. In this paper, as a part of a literature survey, we have identified challenges and possible research opportunities involved in the integration of blockchain with different computing paradigms. In future work, further, we want to survey the role of blockchain in data management, access control policies and we want to address some of the challenges that we have mentioned in this survey paper.

REFERENCES

[1] Babu, B.S., Babu, K.S. (2020). Materializing block chain technology to maintain digital ledger of land records. In Proceedings of the Third International Conference on Computational Intelligence and Informatics, 1090: 201-212. https://doi.org/10.1007/978-981-15-1480-7_16

[2] Chan, K.C., Zhou, X., Gururajan, R., Zhou, X., Ally, M., Gardiner, M. (2020). Integration of blockchains with management information systems. In Proceedings of the 2019 International Conference on Mechatronics, Robotics and Systems Engineering (MoRSE 2019), 157-162). https://doi.org/10.1109/MoRSE48060.2019.8998694

[3] Shah, M., Shaikh, M., Mishra, V., Tuscano, G. (2020). Decentralized cloud storage using blockchain. In 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI), 48184: 384-389. https://doi.org/10.1109/ICOEI48184.2020.9143004

[4] Huang, P., Fan, K., Yang, H., Zhang, K., Li, H., Yang, Y. (2020). A collaborative auditing blockchain for trustworthy data integrity in cloud storage system. IEEE Access, 8: 94780-94794. https://doi.org/10.1109/ACCESS.2020.2993606

[5] Zhang, Y., Xu, C., Cheng, N., Li, H., Yang, H., Shen, X. (2019). Chronos^{+}+: An accurate blockchain-based time-stamping scheme for cloud storage. IEEE Transactions on Services Computing, 13(2): 216-229. https://doi.org/10.1109/TSC.2019.2947476

[6] Sharma, P., Jindal, R., Borah, M.D. (2019). Blockchain-based integrity protection system for cloud storage. In 2019 4th Technology Innovation Management and Engineering Science International Conference (TIMES-iCON), 1-5. https://doi.org/10.1109/TIMES-iCON47539.2019.9024583

[7] Gochhayat, S.P., Bandara, E., Shetty, S., Foytik, P. (2019). Yugala: Blockchain based encrypted cloud storage for IoT data. In 2019 IEEE International Conference on Blockchain (Blockchain), pp. 483-489. https://doi.org/10.1109/Blockchain.2019.00073

[8] Li, L.J. (2019). Secured cloud storage scheme based on blockchain. In 2019 IEEE 2nd International Conference on Electronic Information and Communication Technology (ICEICT), pp. 137-142. https://doi.org/10.1109/ICEICT.2019.8846406

[9] Uchibayashi, T., Apduhan, B.O., Shiratori, N., Suganuma, T., Hiji, M. (2019). Policy management technique using blockchain for cloud VM migration. In 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), pp. 360-362. https://doi.org/10.1109/DASC/PiCom/CBDCom/CyberSciTech.2019.00073

[10] Desai, S., Deshmukh, O., Shelke, R., Choudhary, H., Sambhare, S.S., Yadav, A. (2019). Blockchain based Secure Data Storage and Access Control System using Cloud. In 2019 5th International Conference on Computing, Communication, Control and Automation (ICCUBEA), pp. 1-6. https://doi.org/10.1109/ICCUBEA47591.2019.9129015

[11] Tseng, M.H.R., Chang, S.E., Kuo, T.Y. (2019). Using blockchain to access cloud services: A case of financial service application. In 2019 Federated Conference on Computer Science and Information Systems (FedCSIS), pp. 565-568. https://doi.org/10.15439/2019F296

[12] Wang, S., Wang, X., Zhang, Y. (2019). A secure cloud storage framework with access control based on blockchain. IEEE Access, 7: 112713-112725. https://doi.org/10.1109/ACCESS.2019.2929205

[13] Yang, C., Tan, L., Shi, N., Xu, B., Cao, Y., Yu, K. (2020). AuthPrivacyChain: A blockchain-based access control framework with privacy protection in cloud. IEEE Access, 8: 70604-70615. https://doi.org/10.1109/ACCESS.2020.2985762

[14] Hoang, V.H., Lehtihet, E., Ghamri-Doudane, Y. (2020). Privacy-preserving blockchain-based data sharing platform for decentralized storage systems. In 2020 IFIP Networking Conference (Networking), pp. 280-288.

[15] Liu, J., Zhang, G., Sun, R., Du, X., Guizani, M. (2020). A blockchain-based conditional privacy-preserving traffic data sharing in cloud. In ICC 2020-2020 IEEE International Conference on Communications (ICC), pp. 1-6. https://doi.org/10.1109/ICC40277.2020.9148864

[16] Shen, M., Duan, J., Zhu, L., Zhang, J., Du, X., Guizani, M. (2020). Blockchain-based incentives for secure and collaborative data sharing in multiple clouds. IEEE Journal on Selected Areas in Communications, 38(6): 1229-1241. https://doi.org/10.1109/JSAC.2020.2986619

[17] Zhou, I., Makhdoom, I., Abolhasan, M., Lipman, J., Shariati, N. (2019). A blockchain-based file-sharing system for academic paper review. In 2019 13th International Conference on Signal Processing and Communication Systems (ICSPCS), pp. 1-10. https://doi.org/10.1109/ICSPCS47537.2019.9008695

[18] Shrestha, A.K., Vassileva, J. (2018). Blockchain-based research data sharing framework for incentivizing the data owners. In International Conference on Blockchain, 259-266. https://doi.org/10.1007/978-3-319-94478-4_19

[19] Yadav, D., Shinde, A., Nair, A., Patil, Y., Kanchan, S. (2020). Enhancing data security in cloud using blockchain. In 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), pp. 753-757. https://doi.org/10.1109/ICICCS48265.2020.9121109

[20] Xu, H., Cao, J., Zhang, J., Gong, L., Gu, Z. (2019). A survey: Cloud data security based on blockchain technology. In 2019 IEEE Fourth International Conference on Data Science in Cyberspace (DSC), pp. 618-624. https://doi.org/10.1109/DSC.2019.00100

[21] Tsai, W.Y., Chou, T.C., Chen, J.L., Ma, Y.W., Huang, C.J. (2020). Blockchain as a platform for secure cloud computing services. In 2020 22nd International Conference on Advanced Communication Technology (ICACT), pp. 155-158. https://doi.org/10.23919/ICACT48636.2020.9061435

[22] Kumar, M., Singh, A.K. (2020). Distributed intrusion detection system using blockchain and cloud computing infrastructure. In 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184), pp. 248-252. https://doi.org/10.1109/ICOEI48184.2020.9142954

[23] Yan, X., Yuan, X., Ye, Q., Tang, Y. (2020). Blockchain-based searchable encryption scheme with fair payment. IEEE Access, 8: 109687-109706. https://doi.org/10.1109/ACCESS.2020.3002264

[24] Albalawi, K., Azim, M.M.A. (2019). Cloud-based IoT Device authentication scheme using blockchain. In 2019 IEEE Global Conference on Internet of Things (GCIoT), pp. 1-7. https://doi.org/10.1109/GCIoT47977.2019.9058391

[25] Malvankar, A., Payne, J., Budhraja, K.K., Kundu, A., Chari, S., Mohania, M. (2019). Malware containment in cloud. In 2019 First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), pp. 221-227. https://doi.org/10.1109/TPS-ISA48467.2019.00036

[26] Westerlund, M., Jaatun, M.G. (2019). Tackling the cloud forensic problem while keeping your eye on the GDPR. In CloudCom, 418-423.

[27] Varghese, B., Villari, M., Rana, O., James, P., Shah, T., Fazio, M., Ranjan, R. (2018). Realizing edge marketplaces: challenges and opportunities. IEEE Cloud Computing, 5(6): 9-20. https://doi.org/10.1109/MCC.2018.064181115

[28] Freitag, F. (2018). On the collaborative governance of decentralized edge microclouds with blockchain-based distributed ledgers. In 2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI), pp. 709-712. IEEE. https://doi.org/10.1109/WI.2018.000-7

[29] Zhang, X., Li, R., Cui, B. (2018). A security architecture of VANET based on blockchain and mobile edge computing. In 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), pp. 258-259. https://doi.org/10.1109/HOTICN.2018.8605952

[30] Li, Y., Shi, W., Kumar, M., Chen, J. (2018). Dycrem: Dynamic credit risk management using edge-based blockchain. In 2018 IEEE/ACM Symposium on Edge Computing (SEC), pp. 344-346. https://doi.org/10.1109/SEC.2018.00039

[31] Liu, M., Yu, F.R., Teng, Y., Leung, V.C., Song, M. (2018). Distributed resource allocation in blockchain-based video streaming systems with mobile edge computing. IEEE Transactions on Wireless Communications, 18(1): 695-708. https://doi.org/10.1109/TWC.2018.2885266

[32] Liu, M., Yu, F.R., Teng, Y., Leung, V.C., Song, M. (2018). Computation offloading and content caching in wireless blockchain networks with mobile edge computing. IEEE Transactions on Vehicular Technology, 67(11): 11008-11021. https://doi.org/10.1109/TVT.2018.2866365

[33] Xiong, Z., Zhang, Y., Niyato, D., Wang, P., Han, Z. (2018). When mobile blockchain meets edge computing. IEEE Communications Magazine, 56(8): 33-39. https://doi.org/10.1109/MCOM.2018.1701095

[34] Zheng, J., Dong, X., Zhang, T., Chen, J., Tong, W., Yang, X. (2018). Microthingschain: Edge computing and decentralized iot architecture based on blockchain for cross-domain data shareing. In 2018 International Conference on Networking and Network Applications (NaNA), pp. 350-355. https://doi.org/10.1109/NANA.2018.8648780

[35] Xu, C., Wang, K., Li, P., Guo, S., Luo, J., Ye, B., Guo, M. (2018). Making big data open in edges: A resource-efficient blockchain-based approach. IEEE Transactions on Parallel and Distributed Systems, 30(4): 870-882. https://doi.org/10.1109/TPDS.2018.2871449

[36] Seike, H., Hamada, T., Sumitomo, T., Koshizuka, N. (2018). Blockchain-based ubiquitous code ownership management system without hierarchical structure. In 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), pp. 271-276. https://doi.org/10.1109/SmartWorld.2018.00081

[37] Rahman, M.A., Hossain, M.S., Loukas, G., Hassanain, E., Rahman, S.S., Alhamid, M.F., Guizani, M. (2018). Blockchain-based mobile edge computing framework for secure therapy applications. IEEE Access, 6: 72469-72478. https://doi.org/10.1109/ACCESS.2018.2881246

[38] Xu, D., Xiao, L., Sun, L., Lei, M. (2017). Game theoretic study on blockchain based secure edge networks. In 2017 IEEE/CIC International Conference on Communications in China (ICCC), pp. 1-5. https://doi.org/10.1109/ICCChina.2017.8330529

[39] Kang, J., Yu, R., Huang, X., Wu, M., Maharjan, S., Xie, S., Zhang, Y. (2018). Blockchain for secure and efficient data sharing in vehicular edge computing and networks. IEEE Internet of Things Journal, 6(3): 4660-4670. https://doi.org/10.1109/JIOT.2018.2875542

[40] Gauhar, A., Ahmad, N., Cao, Y., Khan, S., Cruickshank, H., Qazi, E.A., Ali, A. (2020). xDBAuth: Blockchain based cross domain authentication and authorization framework for Internet of Things. IEEE Access, 8: 58800-58816. https://doi.org/10.1109/ACCESS.2020.2982542

[41] Lei, K., Du, M., Huang, J., Jin, T. (2020). Groupchain: Towards a scalable public blockchain in fog computing of IoT services computing. IEEE Transactions on Services Computing, 13(2): 252-262. https://doi.org/10.1109/TSC.2019.2949801

[42] Yao, Y., Chang, X., Mišić, J., Mišić, V.B., Li, L. (2019). BLA: Blockchain-assisted lightweight anonymous authentication for distributed vehicular fog services. IEEE Internet of Things Journal, 6(2): 3775-3784. https://doi.org/10.1109/JIOT.2019.2892009

[43] Almadhoun, R., Kadadha, M., Alhemeiri, M., Alshehhi, M., Salah, K. (2018). A user authentication scheme of IoT devices using blockchain-enabled fog nodes. In 2018 IEEE/ACS 15th international conference on computer systems and applications (AICCSA), pp. 1-8. https://doi.org/10.1109/AICCSA.2018.8612856

[44] Memon, R.A., Li, J.P., Nazeer, M.I., Khan, A.N., Ahmed, J. (2019). Dualfog-iot: Additional fog layer for solving blockchain integration problem in internet of things. IEEE Access, 7: 169073-169093. https://doi.org/10.1109/ACCESS.2019.2952472

[45] Debe, M., Salah, K., Rehman, M.H.U., Svetinovic, D. (2020). Blockchain-Based Decentralized Reverse Bidding in Fog Computing. IEEE Access, 8: 81686-81697. https://doi.org/10.1109/ACCESS.2020.2991261

[46] Alshehri, M., Panda, B. (2019). A Blockchain-Encryption-Based approach to protect fog federations from rogue nodes. In 2019 3rd Cyber Security in Networking Conference (CSNet), pp. 6-13. https://doi.org/10.1109/CSNet47905.2019.9108975

[47] Yu, Y., Liu, S., Guo, L., Yeoh, P.L., Vucetic, B., Li, Y. (2020). CrowdR-FBC: A distributed fog-blockchains for mobile crowdsourcing reputation management. IEEE Internet of Things Journal, 7(9): 8722-8735.

https://doi.org/10.1109/JIOT.2020.2996229
[48] George, G., Sankaranarayanan, S. (2019). Light weight cryptographic solutions for fog based blockchain. In 2019 International Conference on Smart Structures and Systems (ICSSS), pp. 1-5. https://doi.org/10.1109/ICSSS.2019.8882870
[49] Wu, D., Ansari, N. (2020). A cooperative computing strategy for blockchain-secured fog computing. IEEE Internet of Things Journal, 7(7): 6603-6609. https://doi.org/10.1109/JIOT.2020.2974231
[50] Baniata, H., Kertesz, A. (2020). A survey on blockchain-fog integration approaches. IEEE Access, 8: 102657-102668. https://doi.org/10.1109/ACCESS.2020.2999213
[51] Ziegler, M.H., Groβmann, M., Krieger, U.R. (2019). Integration of fog computing and blockchain technology using the plasma framework. In 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 120-123. https://doi.org/10.1109/BLOC.2019.8751308
[52] Kumar, G., Saha, R., Rai, M.K., Thomas, R., Kim, T.H. (2019). Proof-of-work consensus approach in blockchain technology for cloud and fog computing using maximization-factorization statistics. IEEE Internet of Things Journal, 6(4): 6835-6842. https://doi.org/10.1109/JIOT.2019.2911969
[53] Puthal, D., Mohanty, S.P., Nanda, P., Kougianos, E., Das, G. (2019). Proof-of-authentication for scalable blockchain in resource-constrained distributed systems. In 2019 IEEE International Conference on Consumer Electronics (ICCE), pp. 1-5. https://doi.org/10.1109/ICCE.2019.8662009
[54] Lee, J.L., Kerns, S.C., Hong, S. (2019). A secure IoT-fag-cloud framework using blockchain based on DAT for mobile IoT. In 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), pp. 0213-0218. https://doi.org/10.1109/UEMCON47517.2019.8993056
[55] Yánez, W., Mahmud, R., Bahsoon, R., Zhang, Y., Buyya, R. (2020). Data allocation mechanism for Internet-of-Things systems with blockchain. IEEE Internet of Things Journal, 7(4): 3509-3522. https://doi.org/10.1109/JIOT.2020.2972776
[56] Cinque, M., Esposito, C., Russo, S. (2018). Trust management in fog/edge computing by means of blockchain technologies. In 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 1433-1439. https://doi.org/10.1109/Cybermatics_2018.2018.00244
[57] Villari, M., Fazio, M., Dustdar, S., Rana, O., Ranjan, R. (2016). Osmotic computing: A new paradigm for edge/cloud integration. IEEE Cloud Computing, 3(6): 76-83. https://doi.org/10.1109/MCC.2016.124
[58] Buzachis, A., Villari, M. (2018). Basic principles of osmotic computing: secure and dependable microelements (MELs) orchestration leveraging blockchain facilities. In 2018 IEEE/ACM International Conference on Utility and Cloud Computing Companion (UCC Companion), pp. 47-52. https://doi.org/10.1109/UCC-Companion.2018.00033
[59] Villari, M., Galletta, A., Celesti, A., Carnevale, L., Fazio, M. (2018). Osmotic computing: software defined membranes meet private/federated blockchains. In 2018 IEEE Symposium on Computers and Communications (ISCC), pp. 01292-01297. https://doi.org/10.1109/ISCC.2018.8538546
[60] Rasool, S., Saleem, A., Iqbal, M., Dagiuklas, T., Bashir, A.K., Mumtaz, S., Al Otaibi, S. (2020). Blockchain-EnaBlEd REliaBlE osmotic computing for cloud of things: applications and challEngEs. IEEE Internet of Things Magazine, 3(2): 63-67. https://doi.org/10.1109/IOTM.0001.1900101
[61] Carnevale, L., Celesti, A., Galletta, A., Dustdar, S., Villari, M. (2018). From the cloud to edge and IoT: a smart orchestration architecture for enabling osmotic computing. In 2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA), pp. 419-424. https://doi.org/10.1109/WAINA.2018.00122
[62] Maksimović, M. (2018). The role of Osmotic computing in Internet of Things. In 2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH), pp. 1-4. https://doi.org/10.1109/INFOTEH.2018.8345538
[63] Abdullah, N., Hakansson, A., Moradian, E. (2017). Blockchain based approach to enhance big data authentication in distributed environment. In 2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN), pp. 887-892. https://doi.org/10.1109/ICUFN.2017.7993927
[64] Subbiah, S., Mala, S., Nayagam, S. (2017). Job starvation avoidance with alleviation of data skewness in Big Data infrastructure. In 2017 2nd International Conference on Computing and Communications Technologies (ICCCT), pp. 137-142. https://doi.org/10.1109/ICCCT2.2017.7972264
[65] Alexander, C.A., Wang, L. (2019). Cybersecurity, information assurance, and big data based on blockchain. In 2019 SoutheastCon, pp. 1-7. https://doi.org/10.1109/SoutheastCon42311.2019.9020582
[66] Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In 2017 IEEE international congress on big data (BigData congress), pp. 557-564. https://doi.org/10.1109/BigDataCongress.2017.85
[67] Chen, J., Xue, Y. (2017). Bootstrapping a blockchain based ecosystem for big data exchange. In 2017 IEEE International Congress on Big Data (Bigdata Congress), pp. 460-463. https://doi.org/10.1109/BigDataCongress.2017.67
[68] Yu, H., Yang, Z., Sinnott, R.O. (2018). Decentralized big data auditing for smart city environments leveraging blockchain technology. IEEE Access, 7: 6288-6296. https://doi.org/10.1109/ACCESS.2018.2888940
[69] Zhang, F., Liu, M., Shen, W. (2017). Operation modes of smart factory for high-end equipment manufacturing in the Internet and Big Data era. In 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), pp. 152-157. https://doi.org/10.1109/SMC.2017.8122594
[70] Karafiloski, E., Mishev, A. (2017). Blockchain solutions for big data challenges: A literature review. In IEEE EUROCON 2017-17th International Conference on Smart Technologies, pp. 763-768. https://doi.org/10.1109/EUROCON.2017.8011213
[71] Bandara, E., Ng, W.K., De Zoysa, K., Fernando, N.,

Tharaka, S., Maurakirinathan, P., Jayasuriya, N. (2018). Mystiko—blockchain meets big data. In 2018 IEEE International Conference on Big Data (Big Data), pp. 3024-3032. https://doi.org/10.1109/BigData.2018.8622341

[72] Smith, T.D. (2017). The blockchain litmus test. In 2017 IEEE International Conference on Big Data (Big Data), pp. 2299-2308. https://doi.org/10.1109/BigData.2017.8258183

[73] Preece, J.D., Easton, J.M. (2018). Towards encrypting industrial data on public distributed networks. In 2018 IEEE International Conference on Big Data (Big Data), pp. 4540-4544. https://doi.org/10.1109/BigData.2018.8622246

[74] Zhou, X., Lin, P., Li, Z., Wang, Y., Tan, W., Huang, M. (2019). Security of big data based on the technology of cloud computing. In 2019 4th International Conference on Mechanical, Control and Computer Engineering (ICMCCE), pp. 703-7033. https://doi.org/10.1109/ICMCCE48743.2019.00163

[75] Shor, P.W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Review, 41(2): 303-332. https://doi.org/10.1137/S0036144598347011

[76] Grover, L.K. (1996). A fast quantum mechanical algorithm for database search. In Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, 212-219. https://doi.org/10.1145/237814.237866

[77] Suhail, S., Hussain, R., Khan, A., Hong, C.S. (2020). On the role of hash-based signatures in quantum-safe internet of things: Current solutions and future directions. IEEE Internet of Things Journal. 8(1): 1-17. https://doi.org/10.1109/JIOT.2020.3013019

[78] Li, C.Y., Chen, X.B., Chen, Y.L., Hou, Y.Y., Li, J. (2018). A new lattice-based signature scheme in post-quantum blockchain network. IEEE Access, 7: 2026-2033. https://doi.org/10.1109/ACCESS.2018.2886554

[79] Yin, W., Wen, Q., Li, W., Zhang, H., Jin, Z. (2018). An anti-quantum transaction authentication approach in blockchain. IEEE Access, 6: 5393-5401. https://doi.org/10.1109/ACCESS.2017.2788411

[80] Kiktenko, E.O., Pozhar, N.O., Anufriev, M.N., Trushechkin, A.S., Yunusov, R.R., Kurochkin, Y.V., Fedorov, A.K. (2018). Quantum-secured blockchain. Quantum Science and Technology, 3(3): 035004. https://doi.org/10.1088/2058-9565/aabc6b

[81] Nanda, A., Puthal, D., Mohanty, S.P., Choppali, U. (2018). A computing perspective of quantum cryptography [energy and security]. IEEE Consumer Electronics Magazine, 7(6): 57-59. https://doi.org/10.1109/MCE.2018.2851741

[82] Jin, M., Yoo, C.D. (2009). Quantum hashing for multimedia. IEEE Transactions on Information Forensics and Security, 4(4): 982-994. https://doi.org/10.1109/TIFS.2009.2033221

[83] Yin, W., Wen, Q., Li, W., Zhang, H., Jin, Z. (2018). An anti-quantum transaction authentication approach in blockchain. IEEE Access, 6: 5393-5401. https://doi.org/10.1109/ACCESS.2017.2788411

[84] Fernández-Caramés, T.M., Fraga-Lamas, P. (2020). Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. IEEE Access, 8: 21091-21116. https://doi.org/10.1109/ACCESS.2020.2968985

[85] Chalkias, K., Brown, J., Hearn, M., Lillehagen, T., Nitto, I., Schroeter, T. (2018). Blockchained post-quantum signatures. In 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 1196-1203. https://doi.org/10.1109/Cybermatics_2018.2018.00213

[86] Krendelev, S., Sazonova, P. (2018). Parametric hash function resistant to attack by quantum computer. In 2018 Federated Conference on Computer Science and Information Systems (FedCSIS), pp. 387-390.

[87] Ma, C., Jiang, M. (2019). Practical lattice-based multisignature schemes for blockchains. IEEE Access, 7: 179765-179778. https://doi.org/10.1109/ACCESS.2019.2958816

[88] Wüst, K., Gervais, A. (2018). Do you need a blockchain? In 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), pp. 45-54. https://doi.org/10.1109/CVCBT.2018.00011

[89] Nofer, M., Gomber, P., Hinz, O., Schiereck, D. (2017). Blockchain. Business & Information Systems Engineering, 59(3): 183-187. https://doi.org/10.1007/s12599-017-0467-3