Integration of Blockchain Technology with Cloud Computing

Subjects: Computer Science, Information Systems

Contributor: Gousia Habib , Sparsh Sharma , Sara Ibrahim , Imtiaz Ahmad , Shaima Qureshi , Malik Ishfaq

Blockchain technology's desirable characteristics are decentralization, integrity, immutability, verification, fault tolerance, anonymity, audibility, and transparency. There are many benefits of blockchain technology concerning cloud computing, including those associated with business data handling, privacy, and encryption.

blockchain cloud computing cryptocurrency

1. Concept of Cloud Computing

In recent years, cloud computing has become more popular since it has shown potential for use in academic and commercial settings, due to its effectiveness and availability. Even though it is a widely accepted technology, there has been a growing concern over the storage and consumption of data due to the standard data management tool's inability to keep up with the ever-increasing volume of data [1]. This has led to an explosion in the number of data sources. The original idea for cloud storage consisted of a back-end platform, which could be storage or a server; a front-end platform, which could be a mobile device or a client; and a network, which could be an intranet or the Internet. Researchers are offering answers to the complexities of data storage and usability in cloud storage technology. They are paying attention to cloud technology due to the amount of data generated [2].

Cloud computing is often used in many business and military settings to assist with data storage management. The heterogeneous environments of cloud computing are filled with various hardware and software components bought from different suppliers. This may lead to incompatibilities and security flaws in the system. The security assurance of information transmission between and within clouds and information management looks to be a significant problem. The use of blockchain technology is not limited to the realm of crypto money; it also has the potential to open up new doors for the digitization of businesses [3]. The use of blockchains in cloud computing is one of the most ground-breaking innovations and is unergoing very rapid development. Discoveries made at the intersection of these technologies provide additional economic value; nevertheless, acquiring this value is a unique endeavor that is challenging but fascinating.

A blockchain is a continuously growing linked list. Similar to the structure of records, it consists of blocks connected with the aid of links, and the process of putting data in the blocks is accomplished with the assistance of cryptography. Every block in the blockchain comprises a cryptographic hash of the block that came before it. A timestamp indicates when the block was added to the blockchain. In addition, data relates to transactions that have been recorded because each block contains a link to the block that came before it and information about that block.

The block that came before it can neither be removed nor altered. Because of this, it is impossible to tamper with the data included in any blockchain because, once the data is recorded, it is impossible to modify any block's contents without changing the data contained in all of the blocks that came before it.

One of the most compelling arguments in favor of cloud computing is that it may provide vital services such as outsourcing computing operations. Cloud computing will circumvent the limitations imposed by computationally inefficient devices in an ever more comprehensive manner as pay-per-use computing resources become more widely accessible. They store their information in the cloud [4]. Customers can rent and pay for storage services or utility calculations following their specific requirements using cloud computing services. The cloud provides more scalability and flexibility compared to more traditional means of data storage. Because there is only a limited amount of storage space on the user's device, the data is kept in the cloud. There are stringent criteria for the data and the classifier to maintain their anonymity, and service providers are not trusted. The researchers concluded that processing and storing data on the cloud constituted a substantial obstacle. In addition, researchers face a significant obstacle when it comes to data storage, and that obstacle is the problem of heterogeneity. Big data, also known as large-scale data, is a word that is used to express the issue of heterogeneity in data storage [5]. The cloud's infrastructure and the blockchain's technology have both been modified to cater to this need. As a result, the two methodologies have been combined to improve the application's performance. These two approaches are combined to improve the overall performance of the apps now being used.

To put it another way, a blockchain is a decentralized and encrypted computer networking system that uses many computers called nodes. Because a significant quantity of information may be sent and stored with this technology, it is essential. This technology reduces costs and improves the degree of precision achieved [6].

In today's day and age, the Internet is home to millions upon millions of websites. The upkeep of a hosted website necessitates the purchase of an expensive rack of servers. These servers' throughput must be stable, and they need to be monitored and maintained regularly. Additional workers will be required to organize and manage these servers. Every last bit of information will be kept safe in data centers. Cloud computing refers to the practice of storing, managing, and processing data via the use of remote servers. It is used as a substitute for a personal computer or a local server at its respective location [7]. Internet connectivity is required for devices inside an organization to obtain cloud computing services such as data storage and application deployment. In cloud computing, data centres, resources, and servers are distributed over the Internet, resulting in various advantages for the services that are supplied by these servers. The pay-per-use payment model governs these services. The capacity of employees to collaborate more successfully is enhanced by the fact that services may be accessible anywhere on the globe at a much-reduced cost. The software that runs in the cloud will be automatically updated, making it very easy to use. Customers can now view and make changes to their documents stored in the cloud. In addition, there are several disadvantages [8]. Because of the adaptability of cloud storage, several concerns relating to data privacy and security need to be resolved, and the system is vulnerable to attacks. When there is a high volume of users using the cloud, there is a possibility that it may become unavailable. Many different services are available via the cloud and may be broken down into three basic delivery formats [9]. Software as a Service, often known as SaaS, is one of the first services being provided to customers.

SaaS is simply a web-based application. Software that runs in the cloud is provided by the Cloud Service Provider (CSP) as a unified platform, which the CSP then uses to provide various services to many clients. Customers using cloud services do not influence the underlying cloud infrastructure. Examples of this service include Google E-mail, Amazon Web Services, and Salesforce.com, all considered SaaS services. Platform as a Service, often called PaaS, is the next available choice.

On the other hand, SaaS will host the whole application on the cloud, in contrast to PaaS, which will merely provide the application's framework [10]. Using Google as an example of PaaS is the most straightforward method to comprehend this concept. Infrastructure as a Service is an additional method that may be used to access various resources, including those based on a network. Virtualization is used by infrastructure as a service providers to spread physical resources to meet the requirements of cloud users.

2. Traditional Techniques for Cloud Computing

For businesses and individuals, cloud storage is a kind of Internet technology for sharing resources with IT-related skills. Information encryption is the primary focus of traditional security measures. Users revoked access to data storage, data audits, deduplication, and so on. Data security and performance have been the focus of scientific research as ICT and cloud services have advanced.

A symmetric cryptographic system with encrypted bloom filters protects user data on the cloud by allowing the user to detect unlawful changes to the outsourced data. Protecting user data's signature information from unauthorized access was the focus of [3]. The authors presented an algorithm for assuring the integrity of different control mechanisms using a standard storage template [1].

As a result, despite their ability to offer safe storage and integrity checking, as well as user revocation and data duplicate removal, these schemes still have certain issues, such as the necessity for a trusted third party, which is a nightmare for the privacy of users' information. Most approaches address only static data sets and do not apply to a huge amount of data that have been observed. Some approaches are not enough to address cloud storage data security concerns. As a result, it is important to learn about the blockchain-based cloud storage solutions now in use and conduct more research to conclude [10].

3. Integration of Blockchain Technology and Cloud Computing

A slew of prior research is being considered that examines the security patterns in cloud storage and the potential applications for blockchain technology. An in-depth look at how blockchain technology is being used in cloud computing is being undertaken by academics. According to the study, blockchain technology for cloud storage beats all other studies on the essential concept of blockchain technology. For further information, see [10].

Open Research Challenges

There is no denying the many advantages that cloud computing offers. The path ahead will not be devoid of obstacles in any way. The cloud stores a large variety of data types, some of which are quite sensitive. Following a breach of security in 2017, Amazon's Internet platforms were found to store the personal information of around 200 million voters in the United States. Due to a breach in the Alibaba cloud, the personally identifiable information of 1.1 billion customers who shop on the Taobao e-commerce site was made public [4].

The Starwood division of Marriott Hotels was similarly compromised by an unauthorized individual, which led to a diminished reputation for the company's brand. A breach in the security of an organization's data might lead to monetary losses, the loss of customers, harm to the company's brand, and other impacts.

Blockchain, which has its unique benefits in data security, comes to the rescue with other recent breakthroughs in cloud data security. The concept of cloud computing is predicated on utilizing centralized servers to store data and then to make that data accessible to consumers through software [9].

It is common practice for businesses to have this form of centralized-based organization, which might undermine security, privacy, and authority. If you utilize the cloud unsafely, it will be easy for hackers and viruses to access your data and steal it for their purposes. As a direct result of this, confidential information may be made public.

4. Benefits of Blockchain in Cloud Computing

There are many benefits of blockchain technology concerning cloud computing, including those associated with business data handling, privacy, and encryption. In healthcare, some of these benefits include:

4.1. Decentralization

The Internet of Things (IoT) and cloud computing technologies both have a major flaw: they rely on a centralized server for data management and decision-making. If the primary server has technical difficulties, the whole system may be rendered inoperable, and the potential loss of critical data may have catastrophic consequences. The central server might potentially be a target for hackers [10]. It is possible that this problem can be fixed thanks to the decentralized blockchain system's ability to keep several copies of the same data on many different computers. Because of this, there is no longer any risk that the whole system will fail if only one server does. Because the information is stored on many servers, it is very improbable that any of it would be lost [6].

4.2. Enhanced Data Protection

Leaks of this data can result in robbery and the illegal selling of personal details for money, making cloud storage a major challenge for the Internet of Things field. Personal information such as video footage, voice recordings, household items, property, and personal habits are all stored on cloud storage in the IoT field. Because of the current state of affairs, the infrastructure of the cloud is now in danger. The use of blockchains in cloud computing is the solution to this problem [11].

4.3. Improved Goods and Service Ownership Tracking

Huge logistical issues include:

1. Consistently monitoring all of the cars in a network.
2. Determining their current locations.
3. Determining the time that each car spends in a certain region.
4. Establishing communication between many vehicles.

A centralized approach in designing software products, such as package tracking systems, might cause problems due to design flaws. Blockchain has a great deal of promise to keep tabs on these products and services [7].

4.4. Tolerance for Errors

Data may be replicated over a network of computer servers linked to each other through collaborative clouds. As a result, the chance of a single cloud node failing will be reduced, allowing for continuous operation [5].

5. Blockchain in Cloud Computing and the Reasons for Its Popularity

Cloud computing may benefit greatly from the adoption of blockchain technology. Improved system interoperability, enhanced data security, and much more, are just some of the benefits of this technology—let’s use blockchain technology; let’s examine how businesses and institutions benefit from it [9]. The overall visualization of all the benefits provided by blockchain technology is given in the **Figure 1** below [12].

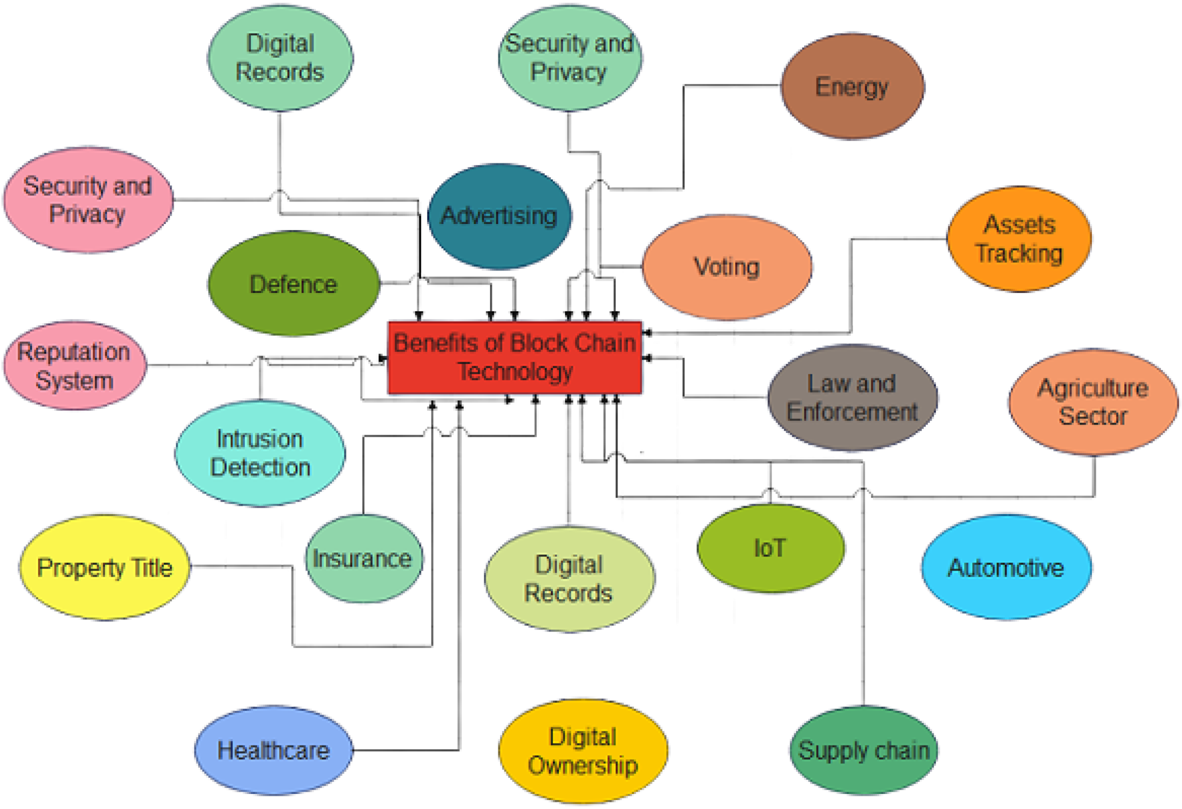

Figure 1. Graphical representation of applications of blockchain technology in different areas.

6. Applications of the Integration of Blockchain and Cloud Computing

There are several financial, Internet-of-Things (IoT) (safety and privacy, stock exchange, financial services, P2P financial market, crowdfunding, etc.), and other uses for blockchain: E-business, reputation management, etc. (web community, academics, etc.), security and privacy (risk management, privacy, and improved security), healthcare, insurance, copyright protection, energy, and so forth [13]. Applications in society (blockchain music and blockchain government), include advertising, and defense, mobile apps, supply chain, automotive [14], advertising [15], agriculture [16], voter registration, identity management, education, and law and monitoring, digital documents, and asset tracking [17]. Intrusion detection [18], computerized ownership management, registers of property titles, and others.

6.1. A Healthcare Industry That Is Becoming More Knowledgeable

The healthcare industry has a lot of room to use BCoT to improve and to modernize its existing systems and practices. Healthcare institutions and organizations are included in the healthcare industry. Healthcare-related services, medical equipment, and tools such as ventilators, medical insurance, etc., are the industry's primary focus. Security and service efficiency are two of BCoT's key strengths in the industry. Patients and physicians will benefit from emerging smart services such CoT-enabled Health data exchange, which may reduce the time it takes to share communication between patient devices and linked devices. Decentralized data verification and message validation utilizing a consensus method may solve security issues in sharing health data, as can using a blockchain [10].

6.2. Smart Home Automation Using Blockchain Technology

One of the most significant applications for BCoT is in smart home automation. Automating the gadgets in a house may turn it into a smart home and provide convenience for the people who live there. An IoT-based smart home is a network of IoT devices, including sensors and detectors, that acquire information from their surroundings, store it in the cloud, and process the information to execute a specified activity in response to the processed data [7]. Temperature sensing sensors are used to detect the presence of a fire in the house, and the data is then processed to send a message to the homeowner or activate a water sprinkler or an alarm in the home. An automation blockchain may be employed in smart homes to reduce the danger of data loss, or the security of data privacy [11]. A decentralized data integrity architecture built on blockchain technology may effectively ensure the safety and stability of the whole system.

6.3. Autonomous Transportation Powered by the Blockchain

The transportation industry has a lot of room for development in today’s technologically advanced world. People’s lives have been impacted greatly in recent years because of the rapid advancement of sensors, computers, and communication systems, which have increased the number of transportation systems. The concept of “smart transportation” may be seen as an Internet of Things (IoT) application related to transportation infrastructures that connect communications and vehicle services. Certain security vulnerabilities arising from vehicle-to-vehicle dynamic communication and a reliance on centralized network authority pose certain challenges. To assist in creating a decentralized, reliable, and secure IT infrastructure, blockchain may be used in this scenario [2].

6.4. Smart Manufacturing

The Internet of Things (IoT) may impact this emerging field of smart manufacturing. Intelligent machines are a critical part of smart manufacturing because they can perform certain jobs with a higher level of intelligence than is currently achievable. This sector uses Internet-enabled technology, and service-oriented manufacturing [19]. Modern manufacturing faces difficulties such as centralized industrial networks and authority dependent on third parties via smart manufacturing. Production methods that rely on centralized management are inflexible, inefficient, and unreliable. Consider the following solution: Using the BCoT, a decentralized architecture may be developed while enhancing security simultaneously.

6.4.1. Data De-Duplication Scheme Using Blockchain Technology for Cloud Storage Services

The data deduplication strategy is used to reduce the amount of redundant data in the cloud and to save space. This method keeps one duplicate of the indistinguishable information to save storage space. In other words, it may improve data efficiency while reducing the need for physical equipment, but it also has the potential to worsen the issue of data dependability. Data deduplication is used to distribute data across several servers, and the storage information is stored on the blockchain. As a result [4], the data deduplication method and the blockchain approach may ensure system secrecy and data integrity. Distributed storage systems may also benefit from it. CSP and data owners should join the blockchain network as nodes for associated services. To ensure the integrity of the data, all duplications and transactions should be recorded on the blockchain. Based on the data unit, location, and disc placement, deduplication methods are categorized into three categories: Data unit deduplication, location deduplication, and disc placement deduplication are the three types of deduplication techniques.

File-level and chunk-level deduplication are the two subcategories of data unit deduplication [6]. The hash values of the two files are used to compare them in the deduplication process. One copy is kept if both hash values are identical. Files may be divided into fixed or variable-length blocks and then checked for duplicate material in deduplication at the chunk level. Source and target deduplication processes are subdivided into two subcategories. After the client sends the files, the target deduplication process works alongside a receiver and discards any extra data. The storage device does deduplication without affecting the client's operation. Customers do not know what is going on in the deduplication process. Source deduplication is performed before data transmission. Because it makes use of the client's resources, this kind of deduplication conserves network traffic capacity. Forward and backward reference deduplication are two subcategories of disk-level deduplication [20].

6.4.2. Blockchain-Based Cloud Storage Access Control Systems

Using blockchain technology, a cloud environment may be made safe by controlling access to information that cannot be trusted. You must store your data in a cloud storage environment that cannot be trusted. User access is controlled using attribute-based encryption that contains dynamic features. As a result of the decentralized ledger technology used by blockchain, all security-relevant operations, such as key revocation and creation, the designation of administrators of access policies, and the submission of access requests, are preserved without modification. In reference, a blockchain-based access control system is being developed. Authentication, identification, and authorization are three discrete yet interrelated procedures in access control. It is the framework that is in charge of keeping track of which particular activities clients are allowed to engage in. Customers' EHR data is kept in a blockchain-based data pool, and customers may use the new framework provided to verify their identity and cryptographic keys before accessing the data. Validation based on identification fulfils the authentication needs of the client [11]. Customers and companies are discouraged from maliciously repeating roles and flexibility by preventing customers and businesses from enforcing their duties. To ensure that only authorized individuals have access to sensitive data, a new access control system is being developed based on smart contracts [1]. An authentication procedure that confirms a user's ownership of positions may be authenticated by using blockchain and smart contracts as adaptable systems in the RBAC-SC, which utilizes blockchain and smart contracts to represent the connection of trust that is vital inside the RBAC. This approach confirms that a user owns positions using blockchain and smart contracts, verifying the challenge response's authenticity [2].

6.4.3. Blockchain as a Driver of Digital Business Transformation

"Blockchain" is an open-source distributed database that uses cutting-edge encryption. One of the most widely used blockchain applications is Bitcoin, which utilizes an open ledger [21]. Everyone can observe what is going on with an open-source platform, since anyone can update the underlying code. There are no middlemen to validate or to settle transactions, making it a real peer-to-peer (P2P) system. Various structured data may be stored in the system, including who paid whom, what money belongs to whom, or what light source provided the electricity (Iansiti and Lakhani 2017). Although recent studies have shown security vulnerabilities on various platforms, blockchain is generally unhackable, making it a trustworthy platform. For example, the cost of confirming transaction data may be reduced thanks to the blockchain, and intermediaries can be eliminated. Blockchain transactions function by broadcasting every block in the system to all parties, each receiving an exact copy of the transaction. An irreversible and transparent transaction record is created when all parties in the network agree on the transaction, such as sending money from one party to another [8].

In the financial service industry, blockchain is widely used to conduct financial transactions, also known as cryptocurrencies. Currently, cryptocurrencies are among the most prominent software systems. The first transaction occurs during the creation of the first block, or genesis block. The first block's hash is forwarded to the miner, who uses it to generate a hash for the next block. Similarly, the third block creates a hash that includes the first two blocks, etc. It is possible to trace the chain of blocks in a blockchain back to the genesis block.

In the current healthcare system, interoperability issues exist and healthcare blockchains can address that. It can be used as a standard for securely exchanging electronic health records (EHR) between healthcare entities, medical researchers, etc. Users can work with patient data without exposing their privacy by using the system.

Using taxonomies in blockchain technology can help analyze blockchains and design and test software architectures. Using their taxonomy, they cover all the main architectural features of blockchains and the impact of various decisions. This taxonomy aims to assist in evaluating the performance and quality attributes of blockchain-based systems.

The various other applications of blockchain in cloud computing are given with scientific evidence in **Table 1** below.

Table 1. Applications of blockchain in cloud computing.

S. No.	Application Methodology	Description	Research Challenges	Reference
01.	ProvChain	An enhanced privacy and availability blockchain-based data provenance architecture for cloud environments. They suggested a decentralized and trusted cloud data provenance architecture based on blockchain technology. The ProvChain architecture was developed for collecting and verifying the provenance of data.	Although data transparency, security, and accountability were improved, it failed to create a trustworthy environment. In the case of large files, overhead increases the complexity of computation.	[22]
02.	Mobile Blockchain Mining Game with	This model combines edge computing with cloud computing to offload computations. Two case studies were examined, a fixed	Although profitable, use of limited resources. Different communication delays alter	[23]

S. No.	Application Methodology	Description	Research Challenges	Reference
	Hierarchical Edge-Cloud Computing	miner number and a dynamic miner number.	the security model of an environment.	
03.	Layer Chain	This architecture establishes hierarchies for maintaining IIoT transaction records using an edge-cloud blockchain. To support large-scale IIoT environments, the critical objective was to reduce the long-term resource consumption of blockchain technology.	Low-delay data storage solutions based on secure blockchain networks are crucial in real-time IIoT applications. Unfortunately, there is limited research on block propagation delays in blockchain applications. To address the above issues, pervasive edge computing is widely adopted as a promising solution, which can be used to develop an efficient peer-to-peer network for blockchain.	[24][25]
04.	Blockchain Technology and Cloud Computing in Intelligent Information Security	To achieve intelligent campuses, blockchain can integrate the technical expertise of cloud computing, the Internet of Things, artificial intelligence, and other technologies as the underlying architecture. Typical applications include building a firewall for network infrastructure, providing a certificate for evaluating teaching systems, tracking intelligent property protection, etc.	With the continued enrichment of blockchain technology ecology, its role as the underlying infrastructure of trusted information environments will become more prominent. As a result, future data sharing and value transmission will be greatly enhanced, and original data barriers will be broken.	[26][27][28][29]
05.	Fog Bus	Researchers are developing a lightweight framework for computing edge and fog based on blockchains. IoT fog–cloud integration is enabled through Fog Bus, a mechanism developed to facilitate end-to-end IoT fog–cloud integration. It ensures the sensitive nature of the data by using blockchain technology.	As a result of this simplified process, the data were more scalable, and costs were reduced. Based on the situation, a decision is made on how the data will be communicated. In addition to failing to support users, it also failed to support providers. Even though a centralized programming module is incorporated, the task of applying security features is disliked due to the diversity of the applications.	[30]

S. No.	Application Methodology	Description	Research Challenges	Reference
06.	Smart Provenance	Uses blockchain technology to prove the provenance of distributed data. Their paper suggested using blockchain technology to collect, verify, and manage data provenance. Additionally, smart contracts and open provenance models were studied to interpret the data trails.	A higher computation cost is associated with allocating each updated document, as it maintains the old memory for each document. Process identity is revealed through the use of a public address system.	[31]
07.	Share	A cloud-based blockchain for sharing knowledge about injection mould redesign in a secure manner. For private and blockchain technologies, cloud-based knowledge is recommended. The platform was redesigned to meet privacy and data format requirements. Similarly, the K-nearest neighbor algorithm was developed to retrieve information.	Due to blockchain's immutability, labeling is essential. It will help reduce the risks associated with fake knowledge.	[32]
08.	B-RAN stands for blockchain Radio Access Network	Using blockchain radio access networks (B-RANs), they developed decentralized, fast, and efficient methods to manage network access and authentication among inherently distrusting networks.	It can enable secure multi-party computations to avoid unauthorized access to sensitive data without compromising distributed computing.	[33]
09.	Using blockchain to tamper-proof EHRs via the cloud.	Using cloud-based technology, they designed secure e-health systems that eliminate illegal modifications. They analyzed communication overhead as well as computational overhead with reduced computation time.	A blockchain is created by colluding between the data server and its corresponding transactions. In the absence of a central authority, multiple tokens need to be requested, which creates an environment of non-trust.	[34]
10.	Consensus Bookkeeping using blockchain	A cloud–network collaboration scenario can break the monopoly of Internet companies on network data by using blockchain token authorization and the right confirmation mechanism in the ledger, in conjunction with blockchain data encryption, immutability, and traceability characteristics. It is confirmed that the data belongs to each user. A company that needs personal behavior data will use Token to process payments to individual users and provide credible authorization at the data layer to protect the legitimate interests of consumers. In this article,	The article explains why DBFT consensus is superior to other consensus mechanisms for cloud-based collaboration with network delays, transmission errors, security holes, hacking, and malicious nodes, which are some of the major issues bookkeeping systems face using blockchain technology.	[35][36]

References

S. No.	Application Methodology	Description	Research Challenges	Reference
		consensus accounting and blockchain technology are used when users purchase cloud services and network services to protect users' privacy and avoid uploading their local data to cloud servers. Blockchain technology is also used to ensure transaction security in cloud–network collaborations.		

d. Syst.

cons

ud of things: Architecture, applications and challenges. IEEE Commun. Surv. Tutor. 2020, 22, 2521–2549.

4. Bouachir, O.; Aloqaily, M.; Tseng, L.; Boukerche, A. Blockchain and fog computing for cyberphysical systems: The case of smart industry. Computer 2020, 53, 36–45.
5. Gill, S.S.; Tuli, S.; Xu, M.; Singh, I.; Singh, K.V.; Lindsay, D.; Tuli, S.; Smirnova, D.; Singh, M.; Jain, U.; et al. Transformative effects of IoT, Blockchain and Artificial Intelligence on cloud computing: Evolution, vision, trends and open challenges. Internet Things 2019, 8, 100118.
6. Reyna, A.; Martín, C.; Chen, J.; Soler, E.; Díaz, M. On blockchain and its integration with IoT. Challenges and opportunities. Future Gener. Comput. Syst. 2018, 88, 173–190.
7. Xie, S.; Zheng, Z.; Chen, W.; Wu, J.; Dai, H.N.; Imran, M. Blockchain for cloud exchange: A survey. Comput. Electr. Eng. 2020, 81, 106–526.
8. Gai, K.; Guo, J.; Zhu, L.; Yu, S. Blockchain meets cloud computing: A survey. IEEE Commun. Surv. Tutor. 2020, 22, 2009–2030.
9. Wamba, S.F.; Queiroz, M.M. Blockchain in the operations and supply chain management: Benefits, challenges and future research opportunities. Int. J. Inf. Manag. 2020, 52, 102064.
10. Atlam, H.F.; Alenezi, A.; Alassafi, M.O.; Wills, G. Blockchain with internet of things: Benefits, challenges, and future directions. Int. J. Intell. Syst. Appl. 2018, 10, 40–48.
11. Dorsala, M.R.; Sastry, V.; Chapram, S. Blockchain-based solutions for cloud computing: A survey. J. Netw. Comput. Appl. 2021, 196, 103246.
12. Guo, H.; Yu, X. A Survey on Blockchain Technology and its security. Blockchain Res. Appl. 2022, 3, 100067.
13. Zheng, Z.; Xie, S.; Dai, H.N.; Chen, X.; Wang, H. Blockchain challenges and opportunities: A survey. Int. J. Web Grid Serv. 2018, 14, 352–375.
14. Joshi, A.P.; Han, M.; Wang, Y. A survey on security and privacy issues of blockchain technology. Math. Found. Comput. 2018, 1, 121.
15. Chen, W.; Xu, Z.; Shi, S.; Zhao, Y.; Zhao, J. A survey of blockchain applications in different domains. In Proceedings of the 2018 International Conference on Blockchain Technology and

Application, Seoul, Republic of Korea, 20–22 June 2018; pp. 17–21.

16. Dave, D.; Parikh, S.; Patel, R.; Doshi, N. A survey on blockchain technology and its proposed solutions. Procedia Comput. Sci. 2019, 160, 740–745.
17. Monrat, A.A.; Schelén, O.; Andersson, K. A survey of blockchain from the perspectives of applications, challenges, and opportunities. IEEE Access 2019, 7, 117134–117151.
18. Baboshkin, P.; Mikhaylov, A.; Shaikh, Z.A. Sustainable Cryptocurrency Growth Impossible? Impact of Network Power Demand on Bitcoin Price. Finans. Žhurnal Financ. J. 2022, 116–130. Available online: https://ideas.repec.org/a/fru/finjrn/220308p116-130.html (accessed on 17 October 2022).
19. Murthy, C.V.B.; Shri, M.L. A survey on integrating cloud computing with blockchain. In Proceedings of the 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE), Vellore, India, 24–25 February 2020; pp. 1–6.
20. Esposito, C.; De Santis, A.; Tortora, G.; Chang, H.; Choo, K.K.R. Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? IEEE Cloud Comput. 2018, 5, 31–37.
21. Shobanadevi, A.; Tharewal, S.; Soni, M.; Kumar, D.D.; Khan, I.R.; Kumar, P. Novel identity management system using smart blockchain technology. Int. J. Syst. Assur. Eng. Manag. 2022, 13, 496–505.
22. Draper, A.; Familrouhani, A.; Cao, D.; Heng, T.; Han, W. Security applications and challenges in blockchain. In Proceedings of the 2019 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 11–13 January 2019; pp. 1–4.
23. Jiang, S.; Li, X.; Wu, J. Hierarchical edge-cloud computing for mobile blockchain mining game. In Proceedings of the 2019 IEEE 39th international conference on distributed computing systems (ICDCS), Dallas, TX, USA, 7–10 July 2019; pp. 1327–1336.
24. Hazra, A.; Alkhayyat, A.; Adhikari, M. Blockchain-aided Integrated Edge Framework of Cybersecurity for Internet of Things. IEEE Consum. Electron. Mag. 2022. Available online: https://ieeexplore.ieee.org/document/9672722/ (accessed on 17 October 2022).
25. Yu, Y.; Liu, S.; Yeoh, P.L.; Vucetic, B.; Li, Y. LayerChain: A hierarchical edge-cloud blockchain for large-scale low-delay industrial Internet of Things applications. IEEE Trans. Ind. Inform. 2020, 17, 5077–5086.
26. Rathod, T.; Jadav, N.K.; Alshehri, M.D.; Tanwar, S.; Sharma, R.; Felseghi, R.A.; Raboaca, M.S. Blockchain for Future Wireless Networks: A Decade Survey. Sensors 2022, 22, 4182.
27. Alevizos, L.; Ta, V.T.; Hashem Eiza, M. Augmenting zero trust architecture to endpoints using blockchain: A state-of-the-art review. Secur. Priv. 2022, 5, e191.

28. Bhuyan, M.; Kashihara, S.; Fall, D.; Taenaka, Y.; Kadobayashi, Y. A survey on blockchain, SDN and NFV for the smart-home security. Internet Things 2022, 20, 100588.

29. Abdel Ouahab, I.B.; Bouhorma, M.; El Aachak, L.; Boudhir, A.A. Towards a new cyberdefense generation: Proposition of an intelligent cybersecurity framework for malware attacks. Recent Patents Comput. Sci. 2022, 15, 1026–1042.

30. Lakhan, A.; Mohammed, M.A.; Elhoseny, M.; Alshehri, M.D.; Abdulkareem, K.H. Blockchain multi-objective optimization approach-enabled secure and cost-efficient scheduling for the Internet of Medical Things (IoMT) in fog-cloud system. Soft Comput. 2022, 26, 6429–6442.

31. Jyoti, A.; Chauhan, R. A blockchain and smart contract-based data provenance collection and storing in cloud environment. Wirel. Netw. 2022, 28, 1541–1562.

32. Nguyen, T.M.; Prentice, C. Reverse relationship between reward, knowledge sharing and performance. Knowl. Manag. Res. Pract. 2022, 20, 516–527.

33. Azariah, W.; Bimo, F.A.; Lin, C.W.; Cheng, R.G.; Jana, R.; Nikaein, N. A Survey on Open Radio Access Networks: Challenges, Research Directions, and Open Source Approaches. arXiv 2022, arXiv:2208.09125.

34. Li, S.; Zhang, Y.; Xu, C.; Cheng, N.; Liu, Z.; Du, Y.; Shen, X. HealthFort: A Cloud-Based Ehealth System With Conditional Forward Transparency and Secure Provenance Via Blockchain. IEEE Trans. Mob. Comput. 2022, 1–18. Available online: https://ieeexplore.ieee.org/document/9858023 (accessed on 17 October 2022).

35. Xiong, H.; Chen, M.; Wu, C.; Zhao, Y.; Yi, W. Research on Progress of Blockchain Consensus Algorithm: A Review on Recent Progress of Blockchain Consensus Algorithms. Future Internet 2022, 14, 47.

36. Zhang, X.; Xue, M.; Miao, X. A Consensus Algorithm Based on Risk Assessment Model for Permissioned Blockchain. Wirel. Commun. Mob. Comput. 2022, 2022, 8698009.