



Review

Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing

Gousia Habib ¹, Sparsh Sharma ^{1,*}, Sara Ibrahim ², Imtiaz Ahmad ¹ , Shaima Qureshi ¹ and Malik Ishfaq ³¹ Department of Computer Science and Engineering, National Institute of Technology, Srinagar 190001, India² Applied Sciences for Economics and Management, FOM University, 45127 Essen, Germany³ Department of Mathematics, University of Kashmir, South Campus, Anantnag 192101, India

* Correspondence: sparsh.sharma@nitsri.net

Abstract: The real-world use cases of blockchain technology, such as faster cross-border payments, identity management, smart contracts, cryptocurrencies, and supply chain–blockchain technology are here to stay and have become the next innovation, just like the Internet. There have been attempts to formulate digital money, but they have not been successful due to security and trust issues. However, blockchain needs no central authority, and its operations are controlled by the people who use it. Furthermore, it cannot be altered or forged, resulting in massive market hype and demand. Blockchain has moved past cryptocurrency and discovered implementations in other real-life applications; this is where we can expect blockchain technology to be simplified and not remain a complex concept. Blockchain technology's desirable characteristics are decentralization, integrity, immutability, verification, fault tolerance, anonymity, audibility, and transparency. We first conduct a thorough analysis of blockchain technology in this paper, paying particular attention to its evolution, applications and benefits, the specifics of cryptography in terms of public key cryptography, and the challenges of blockchain in distributed transaction ledgers, as well as the extensive list of blockchain applications in the financial transaction system. This paper presents a detailed review of blockchain technology, the critical challenges faced, and its applications in different fields. Blockchain in the transaction system is explained in detail with a summary of different cryptocurrencies. Some of the suggested solutions are given in the overall study of the paper.

Keywords: blockchain; cloud computing; cryptocurrency; Bitcoin

Citation: Habib, G.; Sharma, S.; Ibrahim, S.; Ahmad, I.; Qureshi, S.; Ishfaq, M. Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing. *Future Internet* **2022**, *14*, 341. <https://doi.org/10.3390/fi14110341>

Academic Editor: Sk. Md. Mizanur Rahman

Received: 18 October 2022

Accepted: 18 November 2022

Published: 21 November 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. General Introduction to Blockchain Technology

Blockchain is an especially promising and revolutionary technology because it helps to reduce security risks, eliminate fraud, and bring transparency to a scale that has never been seen before. It was originally associated with cryptocurrency and **non-fungible tokens (NFTs)** in the 2010s, but blockchain technology has since evolved into a management solution for all types of global industries. With blockchain technology, you can provide transparency for food supply chains, secure healthcare data, innovate gaming, and generally change how we handle data and ownership. Using blockchain technology (also known as distributed ledger technology, or DLT), cryptocurrencies (such as Bitcoin) and other digital information can move freely from one person to another without third-party involvement. Using blockchain technology, multiple nodes on the network verify a transaction simultaneously. Anyone with a computer can join the network and participate in the transaction validation process. Multiple devices approve the transaction, which is stored as a code block across multiple devices. Every subsequent transaction is added to a chain (hence, blockchain) to maintain a historical record on the DLT (hence distributed ledger), virtually eliminating the possibility of hacking. Taking advantage of this secure method of exchanging data without a third party makes blockchain technology so appealing [1]. In addition to financial transactions, blockchain can also be used for other transactions.

Despite its secure and transparent nature, the technology is versatile enough to be applied beyond one area of expertise. A wide range of industries are using blockchain technology. These include energy, logistics, education, and more.

The first section of the paper gives a detailed review of blockchain technology, applications platforms, and critical challenges faced by the technology. The evolution and recent technologies of blockchain are given. The transaction formats of the blockchain technology are also given in tabular form. The paper's second section mainly focuses on integrating blockchain technology with cloud computing. The applications of blockchain technology from the perspective of cloud computing are given in detail. Finally, the paper concludes with a summary of the various blockchain platforms in cloud computing. The paper also gives insight into the open challenges in this field that need to be addressed, and the future work needed to further excel the research in this integrated field.

Blockchain Evolution

Even though blockchain is a relatively new technology, it already has an extensive and fascinating history. The following section highlights blockchain development's most important and noteworthy events. Blockchain dates back to 1991, when Stuart Haber and Wakefield Scott Stornetta introduced the concept of a cryptographically protected chain of records. The technology gained traction in the following two decades and became widely used. Blockchain entered its pivotal year in 2008 when Satoshi Nakamoto gave the technology an established model and applications. As a result of the first blockchain and cryptocurrency launch in 2009, blockchain's impact on the tech sector began to unfold.

The summary of the evolution of blockchain technology is given in Table 1.

Table 1. Blockchain Evolution.

S. No.	Year of Publishing	Description	References
1	2008	A pseudonymous person or group with the name Satoshi Nakamoto published "Bitcoin: A Peer-to-Peer Electronic Cash System".	[2]
2	2009	Founder Satoshi Nakamoto and computer scientist Hal Finney execute the first successful Bitcoin transaction.	[3]
3	2010	Laszlo Hanyecz, a Florida-based programmer, purchases two Papa John's pizzas with Bitcoin. A transfer of 10,000 BTCs, worth \$60 at the time, was made by Hanyecz. Bitcoin's market cap is now over \$1 million.	[4]
04	2011	Bitcoin equals 1 USD, making it the world's most valuable cryptocurrency. Several organizations, including Wikileaks and the Electronic Frontier Foundation, have started accepting Bitcoin donations.	[5]
05	2012	There is widespread media coverage of blockchain and cryptocurrency, including in television shows such as The Good Wife, bringing blockchain into the mainstream. The Bitcoin Magazine was launched by Vitalik Buterin, a pioneering Bitcoin developer.	[6]
06	2013	The Bitcoin market cap has exceeded \$1 billion. There was a first-time rise in Bitcoin's price to \$100/BTC. The Ethereum Project paper is published, suggesting blockchain has other uses besides Bitcoin (such as smart contracts).	[7]
07	2014	A variety of companies accept Bitcoin as a payment method, including Zynga, The D Las Vegas Hotel, and Overstock.com. In an Initial Coin Offering (ICO), Buterin's Ethereum Project raises over \$18 million in Bitcoin and opens up new avenues for blockchain development. Over 200 blockchain firms form the R3 group to explore new uses of blockchain. PayPal announces a Bitcoin integration. The first-ever NFT is minted.	[7]

Table 1. Cont.

S. No.	Year of Publishing	Description	References
08	2015	It is estimated that more than 100,000 merchants accept Bitcoin. A partnership between NASDAQ and San Francisco-based blockchain company Chain is intended to test the technology for trading shares in private companies.	[8]
09	2016	IBM announced a blockchain strategy for cloud-based business solutions. Several government agencies recognize the legitimacy of blockchain and cryptocurrencies in Japan.	[9]
10	2017	The price of Bitcoin reaches \$1000/BTC for the first time. Cryptocurrencies have a market cap of \$150 billion. Despite Wall Street's distrust of blockchain, JP Morgan CEO Jamie Dimon said he believes in this technology. As of 19,783.21/BTC, Bitcoin has reached its all-time high. A blockchain-powered government has been announced for Dubai by 2020.	[10]
11	2018	Facebook committed to creating a blockchain group and hinted at creating a cryptocurrency itself. Large banks such as Citi and Barclays have signed up to use IBM's blockchain-based banking platform.	[11]
12	2019	President Ji Jinping embraces blockchain as the Chinese central bank announces its cryptocurrency. Twitter CEO Jack Dorsey announced Square would hire blockchain engineers as part of its cryptocurrency plans. Bakkt is a digital wallet company that offers crypto trading on the New York Stock Exchange (NYSE).	[12]
13	2020	It is estimated that BTC will reach \$30,000 by the end of 2020. From now on, Bitcoin and other cryptocurrencies will be bought, sold, and held by PayPal users. Having launched its central bank digital currency aptly called the Sand Dollar, the Bahamas became the first country in the world to do so. As part of the fight against COVID-19, blockchain technology plays a key role in securely storing the data of medical researchers and patients.	[13]
14	2021	For the first time, Bitcoin has reached a market value of more than \$1 trillion. Increasing popularity for Web3 implementation. The El Salvadorian government has adopted Bitcoin as a legal tender for the first time. The first car manufacturer to accept Bitcoin as a method of payment for automobiles, Tesla buys \$1.5 billion in BTC. As blockchain technology advances, mainstream interest is drawn to the Metaverse, a virtual environment incorporating blockchain technology.	[14]
15	2022	A \$2 trillion market value loss occurs due to economic inflation and rising interest rates. Google forms an Enterprise Digital Assets Team to serve customers on blockchain-based platforms. In the UK, the government has proposed safeguards for stablecoin holders. Blockchain technologies and NFTs are banned in the popular video game Minecraft.	[15]

2. Main Highlights of the Work

1. The paper reviews blockchain technology in detail, including applications of blockchain technology and evolution.
2. The paper highlights blockchain technology's critical challenges, and this study suggests a few solutions.
3. The paper describes blockchain technology in the transaction system and its cryptocurrencies.
4. The study integrates blockchain technology with cloud computing, and broadly discusses the application of blockchain in cloud computing.

5. Scalability and hardware issues of blockchain technology are explained in detail, and a few solutions are suggested to combat the major challenges.
6. Finally, the paper criticizes the detailed study of the paper and suggests some future directions for the study.

3. Introduction to Various Platforms of Blockchain Technology

General Overview

Blockchain is one of today's most talked-about innovations and has grown in prominence as a technology that is being used broadly across many industries. Most people see the blockchain as an accounting book or a digital distributed database [16]. Following the launch of the blockchain in 2008 [17], it has continued to evolve as a disruptive innovation that might change how people interact, make automated costs, follow up, and monitor transactions. The central authority's requirement to monitor and control transactions and interactions between various members might be eliminated using a blockchain, which could be cost-effective [18].

Other mining firms keep a copy of the full record, which includes all of the transactions, and they use that copy to validate each transfer in the blockchain cryptographically. As a result, records are kept in real-time, and are secure, synced, and cannot be altered. Aside from the software, business, and commerce sectors, blockchain technology is widely recognized as information technology [17].

With permission or not, the public A blockchain is a kind of open-source blockchain where anyone can join and participate in the network. There is no monitoring, and the rules are the same for every participating entity. The two largest public blockchains are discussed below.

Bitcoin Blockchain This is one of the largest and most popular public blockchains at present. Satoshi Nakamoto introduced it in 2008 to provide an alternative to the banking system. Its main aim was to decentralize the banking industry and implement a peer-to-peer transfer of crypto money known as Bitcoin. It uses cryptographic techniques for the regulation of cryptocurrency, which includes the verification of transactions and the creation of a chain of history of transactions in the long run. The important elements of a Bitcoin transaction address are the private key, Bitcoin software, and wallet software [19]. It is virtual, unlike conventional currencies; neither physical nor digital coins are handled. Users of Bitcoin have keys that demonstrate their ownership rights in the network. Individuals use their keys to unlock and sign transactions. The value is spent by giving it to a different key holder. Keys on user terminals are often registered in a digital wallet. Bitcoin relies on "mining", a powerful computer process that verifies and validates transactions. Every 10 min on average, the miners are paid [20]. The issue of double-spent transactions has been made worse by Bitcoin, which has been resolved [21] in digital currency.

Ethereum is another public blockchain platform developed by a programmer named Vitalik Buterin in late 2013. It also has an operating system known as EVM (Ethereum virtual machine) for executing smart contracts on participating nodes. Smart contracts are written in Solidity, which is a Turing-complete language. Ethereum is an open-source and decentralized public platform that allows anyone to build and to deploy decentralized applications. It supports a PoW type of consensus known as the Dagger Hashimoto algorithm. Ether is a cryptocurrency built on Ethereum, which can be transferred between Ethereum accounts. A Merkle tree is a bottom-up hash tree data structure that stores the transactions in a block. It uses the SHA-256 hashing algorithm to generate hashes [22].

Merkle trees are used for the efficient storage and verification of large data sets. In this type of data structure, leaf nodes contain the hash of the blockchain transaction, while non-leaf nodes contain the cryptographic hash of the labels of their child nodes. The root of the tree, also known as the Merkle root, contains the hash of all the transactions in a block [23]. The Merkle tree's root is a commitment value, and it may alternatively be thought of as a vector commitment. The Merkle tree's leaf nodes collectively convey the message. An opening proof of vector commitment is formed by every sister node along the

route from the leaf node to the root node, and by the leaf nodes themselves. A traditional blockchain verifies the data's accuracy and consistency by using the opening proof of the Merkle tree [24,25]. The figure gives the representation of the Merkle tree in Figure 1 as:

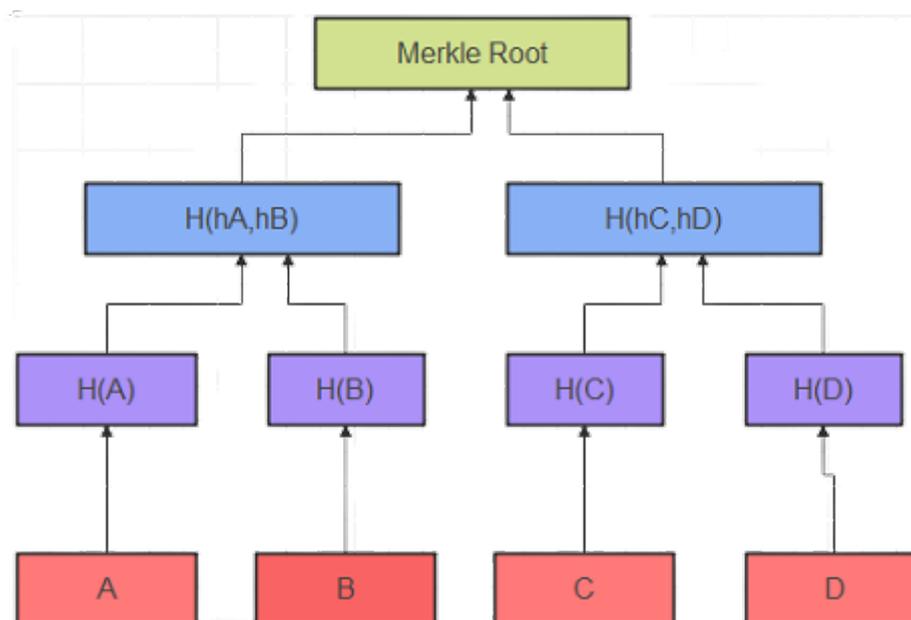


Figure 1. Representation of Merkle Tree, where hA and hB represent cryptographic hash functions of nodes A and B. $h(hA, hB)$ is the combined hash function of nodes A and B. A, B, C, and D represent the leaf nodes of the Merkle tree.

Hyperledger is an open-source, enterprise-class platform for developing blockchain solutions launched in 2016. It includes different projects for different types of blockchain needs and solutions. Some of its projects are Burrow, Composer, Fabric, Indy, etc. Hyperledger fabric is an active platform, while others are in the incubation stage. The fabric is a distributed ledger technology with smart contract functionality. The fabric's consensus mechanism can be chosen from various algorithms such as PBFT, Kafka, Solo, etc. It includes membership service functionality to develop permission blockchains [26]. One of the open-source blockchains provided by Hyperledger management is called Hyperledger Fabric. It seeks to create a decentralized setting. It involves a committed peer, a client, a certificate authority, an order, and an endorser peer. Additionally, the components communicate through channels set up to enable transactions in a private and hidden manner, dividing various application domains. Compared to privacy, a component that lacks easy access to a network cannot access a chain from a committed peer connected to the channel. To enhance the amount of data where a node is fulfilled, and to expand the quantity of data according to scalability, an individual for each channel permits the sharing of various transactions and data held within various committed nodes [27].

Multichain is another platform for building and deploying a private blockchain. It is a DIY platform for banks that hopes to build decentralized financial applications for their services. It does not use a proof of work consensus mechanism; rather, a miner is chosen from a pool of permitted miners in a round-robin fashion. There are no transaction charges or mining rewards in Multichain [28].

Blockchain technology offers a secure, transparent system that is extremely resistant to outages, and an auditable method of recording transactions or any digital interaction. The use of this technology in the commercial industry is still some years away. As a result, today's decision-makers across sectors and business functions should pay attention and begin studying this technology's potential uses. Satoshi Nakamoto invented Bitcoin in 2008. "A Peer-to-Peer Electronic Cash System" [18] has become a widely read study. The

study proposed the dispersion of electronic transactions, rather than relying on centralized organizations to facilitate trade. The term “blockchain” has a plethora of meanings [16].

To quote, “a distributed database or public ledger of all transactions or digital events performed and shared among participating parties” describes the blockchain. Most participants in the system must agree on the validity of each transaction in the public ledger. It is impossible to remove data after it has been input. Every single transaction that has ever been recorded in the blockchain may be independently verified [29]. The general architecture of blockchain technology is given in the Figure 2 as:

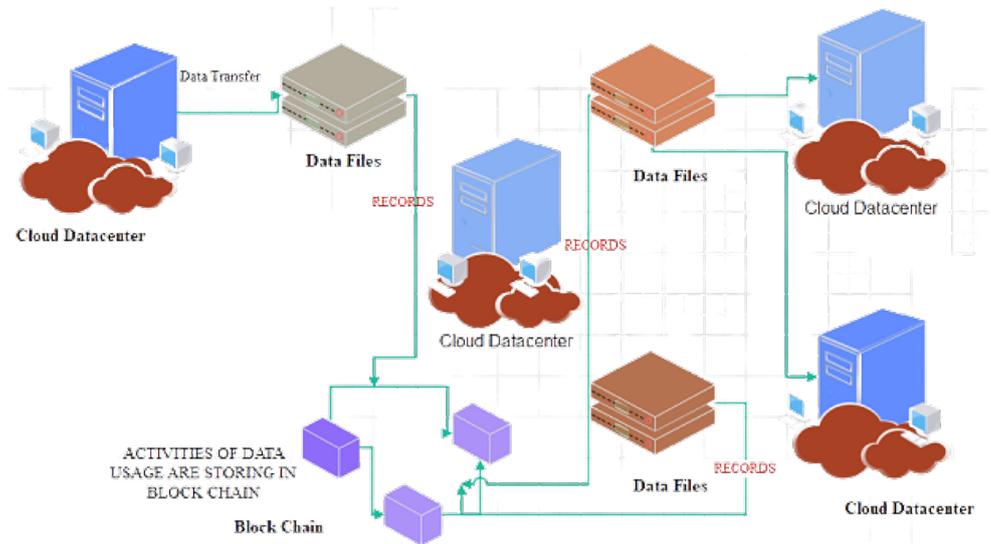


Figure 2. General architecture of the blockchain-enabled cloud computing system.

The following Figure 3 diagram explores blockchain technology in detail in distributed systems, as represented by the Merkle tree.

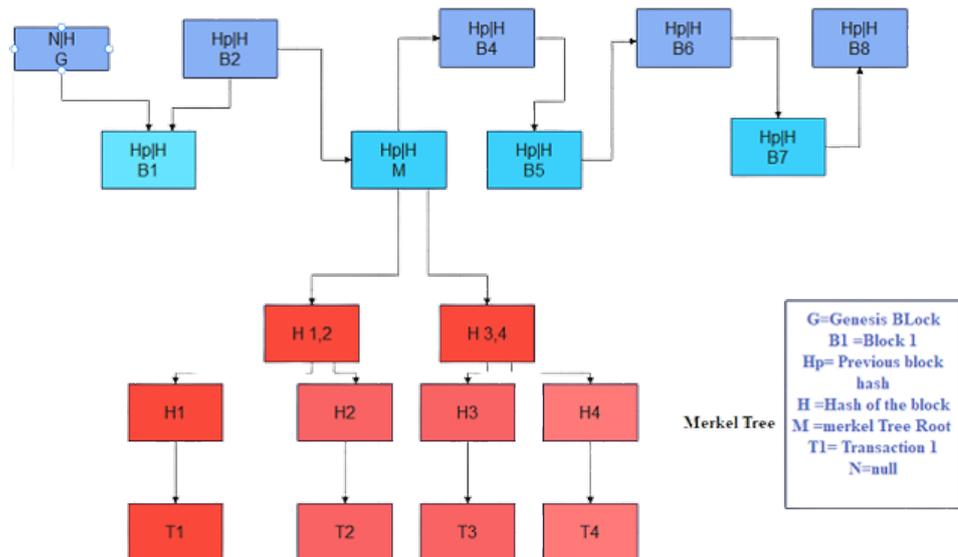


Figure 3. Distributed blockchain technology visualization using the Merkle tree, where H 1,2 represent the cryptographic hash function applied to the Merkle nodes 1 and 2. H 3,4 represents a cryptographic hash function applied to nodes 3 and 4. Hp | H represents a previous header hash and B1 represents block1.

A transaction is a data structure that defines a transfer of any value or information. In the blockchain, a transaction can perform some operation such as storing any information to the block, querying any information from the block, or a transaction may denote a

transfer of value from one entity to another. Transactions are grouped into fixed-sized blocks and then appended to the blockchain. A Merkle, or hash tree, is a data structure that is used to store transactions inside a block in a verifiable and efficient way. A Merkle tree can be considered as a bottom-up hash tree data structure that stores the transactions in a block. It uses the SHA-256 hashing algorithm for the generation of hashes. Merkle trees are used for the efficient storage and verification of large data sets. In this type of data structure, leaf nodes contain the hash of the blockchain transaction, while non-leaf nodes contain the cryptographic hash of the labels of their child nodes. The root of the tree, also known as the Merkle root, contains the hash of all the transactions in a block. A transaction has several fields associated with it that are given in the table below, and the fields may vary according to the type of transaction. A simple transaction format can be represented by the Table 2 given as:

Table 2. Simple Transaction Format.

Size	Field	Description
4 bytes	Version	The version of rules followed
1–9 bytes (Var-Int)	Input Counter	Number of transaction inputs
Variable	Inputs	Transaction inputs
1–9 bytes (Var-Int)	Output Counter	Number of transaction outputs
Variable	Outputs	Transaction outputs
4 bytes	Lock time	Timestamp of block number

Below are some of the characteristics of the blockchain that makes it a revolutionary technology:

- Consensus:** All participating nodes in the network must agree on the validity of a transaction.
- Provenance:** All the participants in the network can know the lineage of an asset recorded on the blockchain.
- Immutability:** It is impossible to tamper with any transaction on the blockchain. If any transaction is wrongly executed, a new transaction must be issued to right the wrongs of the previous transaction.
- Distributed:** The blockchain network is a peer-to-peer distributed network. There is no single point of failure. If some of the nodes fail to work, that will not affect the functioning of the network. No single authority can control the whole network.
- Security:** The security of the transactions is achieved through public key cryptography. Every network participant has public and private keys to encrypt the data and issue digital signatures.
- Coherence:** There will always exist a single value of truth in the blockchain. Every participant in the network sees the same copy of the distributed ledger.
- Decentralization:** A conventional centralized transaction structure requires transactions to be approved by a trusted entity (e.g., the National Bank), causing cost and execution bottlenecks on central servers. The blockchain eliminates the need for outsiders, contrary to the previously introduced centralized mode. In blockchain networks, agreement calculations are used to preserve details.
- Persistency:** There is a quick way to check transactions, and fair miners will not admit to fraudulent transactions. As soon as a transaction is recorded in the blockchain, it is hard to reverse or erase. It is possible to instantly identify blocks that contain invalid transactions.

- Anonymity:** There is a possibility that a client can sign up for a blockchain and use a generated address that does not reveal the client's real identity. We should be aware of blockchain technology.
- Auditability:** A Bitcoin blockchain stores information about client adjustments based on the UTXO (Unused Transaction Performance): Every transaction applies to previously unused exchanges. If the present transaction is registered in the blockchain, the unspent transactions are changed from unspent to spent when the transaction is registered. There is also the possibility of effortlessly confirming transactions.

4. Demanding Applications of Blockchain Technology and the Motivation behind Them

The various important applications of blockchain technology and the main motivation behind using them are described in the following subsection.

4.1. The Cost of the Reduction of Data Breaches

Blockchain technology can reduce data breach costs for organizations. Companies can avoid litigation, losses, compromised data, and interruption costs by preventing breaches. Over 20% of organizations' IT budgets are allocated to security and data protection. Many of these costs are due to malware, which averages \$2.4 million per year. Additionally, the affected systems need to be fixed for months. According to IBM's recent report, data breaches now cost \$3.2 million per year, a 12 per cent increase in five years.

4.2. Increasing Cross-Border Remittances and Reducing Trans-Border Transaction Costs

A major problem facing banks and other organizations is the high cost of cross-border transactions. In most cases, models take three days or longer to complete these transactions. Cryptocurrencies and blockchain technology are now used by companies such as Ripple to overcome these barriers. There are now over 40 countries on six continents on Ripple's network. Blockchain technology allows cross-border transactions to be completed at near-real-time, at a fraction of the cost.

4.3. Inefficient Supply Chains Can Be Eliminated, and Costs Can Be Reduced

After documents are verified, several days are required to complete supply chain and trade finance transactions. There is a manual documentation process behind this. Aside from inefficiencies, fraud, and the high cost of the process, it is also rated for its high inefficiency. A variety of blockchain platforms are being used to solve this problem. These include IBM's Batavia, R3's Marco Polo, the Digital Trade Chain operated by various banks, and the Hong Kong Trade Finance Platform. These transactions can be completed in a few minutes for a fraction of the cost.

4.4. Data on National Identity Is Being Protected Using Blockchain by Governments

Furthermore, blockchain is being used by governments for the management of digital identities. For example, Estonia uses blockchain-based digital identity to digitize national identity records, secure citizen data, and to reduce the inefficiencies of legacy digital ID management platforms, such as high costs.

4.5. Protection of Copyright Through Blockchain Technology

Several startups are using blockchain to protect their customers' intellectual property rights. Customers can protect their artwork on the platform from being used illegally without permission, once registered. Owners can also seek a legal injunction if their platforms are violated using the certificates provided. Companies such as Blockai and Copyrobo use blockchain technology and artificial intelligence to help artists protect their art online in seconds. Creating a timestamp or fingerprint on the blockchain will obtain a copyright certificate to prove their rights. It is through these platforms that copyright in-

fringement interoperability has been demonstrated in the U.S. Drug Supply Chain Security Act Interoperability Pilot programs are discouraged, and licensing is encouraged.

4.6. A Blockchain-Based Solution for Tracking Drugs throughout Supply Chains and Securing Data in Healthcare

In pharmaceutical supply chains, blockchain technology is utilized for tracking and tracing prescription drugs. Interoperability has been demonstrated in the U.S. Drug Supply Chain Security Act Interoperability Pilot program. This program can easily and quickly prevent and control the distribution of counterfeit drugs, as well as recall ineffective and harmful drugs.

4.7. Blockchain Technology in Cybersecurity

The blockchain can explicitly mitigate cyberattacks to strengthen the 5G application's security. Among the different blockchains, the public blockchain is highly secure compared with the consortium and private blockchains due to the nature of the members and the consensus mechanism. The members of the public blockchain can be anonymous, whereas only the trusted nodes can be members of the consortium and private blockchains. The consensus mechanism followed in the public blockchain is proof of work. In contrast, multi-party voting in the consortium blockchain and strictly pre-approved nodes in the private blockchain are followed as a consensus mechanism.

4.8. Blockchain Technology in Smart Contracts

The smart contract is a computer program based on transaction protocol that executes the term of a contract. Smart contracts allow the execution of programs without the intervention of any third party. The sale of goods or services can be realized through a transaction, cryptically signed by the seller and the purchaser, and joining a smart contract for sales transactions.

4.9. Blockchain in Business Data Privacy and Threats

A database where all transactions are visible to the public is a less travelled route and is not very inviting to cybercriminals. The blockchain stores data in a highly encrypted way thanks to cryptography, which reduces vulnerability and ensures data ownership by providing a higher level of encryption. As all transactions are recorded across all nodes, hackers cannot steal, hack, or tamper with data unless a platform-level vulnerability exists. A cyberattack is a common occurrence. Every other day, thousands of users are affected by a breach of a company's data. Despite blockchain's ability to secure user data, there is the issue of the outage that results from it. Blockchain's decentralized servers ensure that the servers will continue to run uninterrupted even if an attack occurs. In addition, DOS attacks are generally not possible with blockchain technology.

Blockchain-based applications are still in the nascent stage from various perspectives, which are seen as future research problems. Many SG applications operate in real-time, and the blockchain should not overburden the applications. The resource requirements for computation are a major challenge in blockchain-based systems. Blockchain must be developed to work on a lighter framework while retaining its security features. Additionally, regulatory bodies must develop standardization procedures to make this technology interoperable and popular. Some of these research problems can be solved in the future by thoroughly revolutionizing blockchain-based applications.

5. Major Challenges

The major challenges faced by blockchain technology are summarized in the following sections.

5.1. Hardware and Energy Consumption for Blockchain Applications Are a Major Challenge

Blockchain is used widely on the Internet for a variety of purposes. Due to its decentralized nature can be viewed as a viable alternative to many traditional transaction systems. Blockchain systems must be offloaded to an accelerating system for scalability, interoperability, and sustainability (scalability, interoperability, and sustainability). Public key operations such as signature generation and verification can be offloaded as one of the solutions, a secure public key infrastructure engine. They have combined a load dispatcher with our Public Key Crypto Engine (BA414EP) to design our blockchain hardware accelerator. Because the transaction load is distributed among several components, the overall transaction speed and output accuracy increase. The architecture provides a high-performance offloading architecture and support for all cryptographic algorithms, such as ECC. The ECDSA operations supported by us include those used by Ethereum, Ripple, Bitcoin, Hyperledger, and EdDSA using the Edwards 25519 curve for the Libra blockchain [18]. In terms of electricity consumption, Bitcoin is estimated to consume 127 terawatt-hours (TWh) per year.

This usage exceeds Norway's entire annual electricity consumption. The average energy consumption of Bitcoin per transaction is 707 kilowatt-hours (kWh), 11 times more than Ethereum. Bitcoin requires computers to solve ever more complicated math problems to verify transactions. The miner who completes the mathematical equation the fastest certifies the transaction and receives a small reward in the form of Bitcoins in return. The proof of work consensus mechanism uses much more energy than many people realize. This is accomplished by having many competitors race to the finish line to see who can package the transactions quickly and solve the small mathematical problem, says Paul Brody, global blockchain leader at EY. In addition, Bitcoin transactions take upwards of 10 min, so this process takes a considerable amount of time. This is the length of time it takes to mine a new block. Compared to other digital transactions, such as those powered by Visa, Visa transactions are faster and require less energy.

Compared to Bitcoin's 4 transactions per second (TPS), Visa can handle around 1700 transactions per second (TPS). Bitcoin's huge energy consumption problem cannot be solved by returning to centralized networks such as Visa. After all, the central promise of Bitcoin is to eliminate intermediaries such as the card networks and their concentrated power over finance. Bitcoin's advocates, however, have several other options as well. We can switch to renewable energy, transitioning to proof of stack systems, embrace pre-mining and introduce carbon credits [30].

5.2. Scalability

Blockchain networks can handle a high number of transactions on large-scale blockchain applications. Data processing services are essential for scalable blockchain services because high transaction execution requires sophisticated data processing services. On-demand computer resources for blockchain activities may be provided through the cloud because of its capacity to grow. As a result, a highly scalable integrated system may be achieved by combining cloud computing with the blockchain.

Many blockchains struggle to support countless users on that machine. Because of a large increase in clients, Bitcoin and Ethereum, the major blockchain systems, experienced modest exchange rates and higher exchange fees. Although this reality has prompted top-to-bottom research about making both these systems and blockchains more proportional, the discussion around the recommendations is exceptionally changed. It is likely to take a long time to conclude. In addition, scaling techniques should be verified and thoroughly tested before being applied to a record. A wide adoption of the blockchain will require successfully addressing concerns about its versatility. BCH was created to solve some of Bitcoin's existing problems, especially scalability and transaction fees. IOTA offers the biggest advantage over other cryptocurrencies in the form of zero transaction fees. IOTA's technology promises infinite scalability, unlike all other cryptocurrencies struggling with scaling problems [31].

The scalability of blockchain data chains, data security in the download process, and confidentiality are challenges that are yet to be addressed. The major challenge of peer-to-peer technologies is the processing of energy transactions and the anonymity of information. The high resource requirement and transaction cost in energy consumption plagued the use of blockchain technology for EV applications with WSN infrastructure. Overcoming these limitations would make blockchain technology the main key factor for EVs. The development of lightweight blockchain algorithms for reaching consensus in real-time can be a probable solution.

At the end of the detailed introduction of blockchain technology in general, we would like to summarize the technology platforms used in the current research era. **The summary is given [31]** in Table 3 as:

Table 3. Different Types of Blockchain Technology.

Blockchain Technology	Bitcoin	Ethereum	Hyperledger Fabric
Main Purpose	Used for cryptocurrency	Employed for smart contracts	Deploys block chain technology for fabric industries
Data storage type	Transactions of cryptocurrencies	Transactions of cryptocurrencies, smart contract history	Chain coding and smart contract transactions
Languages used	Script	Solidity Serpent	Go
Choice of ecosystem	Open	Open	Restricted
Participation choice	Open-source code from GitHub	Open-source code from GitHub	Needs network membership for user source code
Naïve currency	Bitcoin (BTC)	Ether (ETC) or (ETH)	N/A
Decision-making	Yes	Yes	Unknown
Block release timing	10 min	12 s	Configurable
Size of transaction	250 B	No upper bound	Configurable
Rate of transaction	3TXN/s	No upper bound	>10,000 TNX/s
Mining	Needs proof of work	Needs proof of work using Ethash algorithm	N/A

6. 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 [16]. 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 [18].

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 [32]. The use of blockchains in cloud computing is one of the most groundbreaking innovations and is undergoing 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. We could not stay one step ahead of the competition, so we compiled a guide for anyone interested in capitalizing on the trend. Read through it to learn about the blockchain technology used in cloud computing, its benefits to businesses, and how to successfully implement blockchain technology into the cloud so your business may thrive [29].

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 [29]. 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 [31]. 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 [33].

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. Therefore, if we continue to concentrate on the issue with the server and the members of our team, it is possible that we will not be able to achieve our business goals [34]. We are transitioning to "cloud computing" to eliminate the burden of doing maintenance on-site. 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 [35]. 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 [36]. 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 [37]. 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 (PaaS). Because our company uses a cloud service provider, we have access to various programming languages and apps.

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 [38]. 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.

7. 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 [32]. The authors presented an algorithm for assuring the integrity of different control mechanisms using a standard storage template [16].

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 [38].

8. 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. Since this paper does not focus on any specific application of blockchain technology for cloud storage, it addresses current trends, classifications, and unresolved difficulties that previous studies have not addressed. An in-depth look at how blockchain technology is being used in cloud computing is being undertaken by academics. According to our study, blockchain technology for cloud storage beats all other studies on the essential concept of blockchain technology. For further information, see [38].

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 [29].

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 [37].

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.

9. 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:

9.1. 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 [38]. 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 [33].

9.2. 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 [39].

9.3. 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 [35].

9.4. 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 [31].

10. 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 [37]. The overall visualization of all the benefits provided by blockchain technology is given in the Figure 4 below [40].

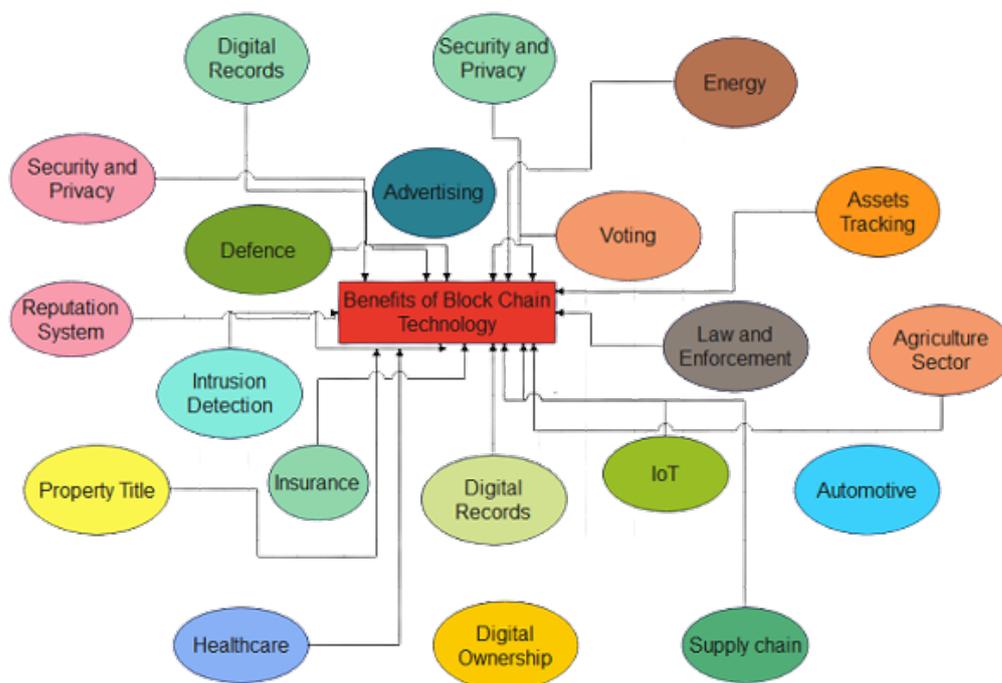


Figure 4. Graphical representation of applications of blockchain technology in different areas.

11. 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 [41]. Applications in society (blockchain music and blockchain government), include advertising, and defense, mobile apps, supply chain, automotive [42], advertising [43], agriculture [44], voter registration, identity management, education, and law and monitoring, digital documents, and asset tracking [45]. Intrusion detection [19], computerized ownership management, registers of property titles, and others.

11.1. 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 [38].

11.2. 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 [35]. 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 [39]. A decentralized data integrity architecture built on blockchain technology may effectively ensure the safety and stability of the whole system.

11.3. 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 [18].

11.4. 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 [17]. 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.

11.4.1. 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 [29], 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 [33]. 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 [46].

11.4.2. 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 [39]. 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 [16]. 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 [18].

11.4.3. 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 [47]. 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 [36].

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 4 below.

Table 4. 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.	[48]
02.	Mobile Blockchain Mining Game with Hierarchical Edge-Cloud Computing	This model combines edge computing with cloud computing to offload computations. Two case studies were examined, a fixed miner number and a dynamic miner number.	Although profitable, use of limited resources. Different communication delays alter the security model of an environment.	[49]
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.	[50,51]
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.	[52–55]
05.	Fog Bus	We 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.	[56]

Table 4. Cont.

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.	[57]
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.	[58]
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.	[59]
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.	[60]
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, 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.	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.	[61,62]

12. Conclusions, Limitations, and Future Work

Regarding security concerns, the cloud computing approach differs from centralized data centers. Although the cloud has several advantages over conventional data centers, it also has several disadvantages, such as user administration (including CSP management) and device management (many CSPs). Cloud computing security may benefit from combining blockchain technology and the cloud computing concept. Scalability and thorough analysis are enhanced by using the cloud platform. Blockchain technology may make the cloud computing paradigm more secure and trustworthy. Cloud computing has the computer power and storage capacity to handle the demands of the blockchain.

An overview of blockchain technology and the cloud computing approach is provided in this article. We looked at recent studies examining the advantages and problems of

integrating cloud computing with blockchain technology. Based on the most current and relevant publications in the literature, we have conducted an extensive review of cloud computing.

Security services. The following are the results of the investigation as a whole, setting the stage by providing an overview of blockchain and cloud computing integration designs and models, as well as an explanation of the responsibilities played by clouds in the blockchain. Different blockchain security services in the cloud computing concept are being classified and discussed. We only look at how cloud computing may enhance the blockchain. The fourth part of the supplemental materials provides major cloud providers' current positions in merging cloud and blockchain. Blockchain and cloud computing may work together to overcome the most common roadblocks. We recommend how blockchain and cloud systems may be integrated for future study and enhancement.

Limitations of the Study. These include drastic energy consumption and expensive hardware requirements. In addition, the transaction consumes a considerable amount of time. This is a critical challenge that needs to be addressed. The mining industry may benefit from more efficient coin creation by increasing profitability, but it may also contribute to the widespread adoption of blockchain technology. Integrating blockchain technology into all aspects of economic life could reduce many businesses' carbon footprints.

Future of Blockchain in Cloud Computing. A 2018 Gartner study found that cloud computing was the top rising business risk. A high dependence on the cloud and related hazards may be dangerous and unsafe in today's corporate environment. There is a significant danger in the cloud's security, compliance, and centralized paradigm. Additionally, in the wake of the panic of COVID-19, businesses have rushed to adopt cloud computing solutions and services without ensuring that they meet all of the necessary legal and regulatory criteria. This has placed their data in jeopardy. The use of blockchain technology is in improving the security, speed, and dependability of data storage, transactions, and business operations. A combination of blockchain and cloud computing is the best path forward since it provides more security and decentralization while allowing for better authorization and privacy. It is necessary to continue working on issues such as data storage at every node, additional security, etc., in the future as the blockchain encounters them. Research on how to use this combination may assist businesses in battling threats to data, which is critical to their ability to operate and make choices in today's ever-competitive world.

Author Contributions: G.H., S.S., S.I., I.A., S.Q. and M.I. conceptualization. Formal analysis, original draft making, writing review, and editing. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable: The study does not report any data.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Krdzalic, Y. Blockchain Explained: The Complete Guide [2018 Update—Part 2]. 2021. Available online: <https://www.trentonsystems.com/blog/blockchain-explained-the-complete-guide-part-2> (accessed on 17 October 2022).
2. Harvey, C.R. Bitcoin Myths and Facts. Available at SSRN 2479670. 2014. Available online: <https://www.semanticscholar.org/paper/Bitcoin-Myths-and-Facts-Harvey/992342c42002b5952df16f8236b1c80072135496> (accessed on 17 October 2022).
3. Hayes, A. The socio-technological lives of bitcoin. *Theory Cult. Soc.* **2019**, *36*, 49–72. [CrossRef]
4. Rose, C. The evolution of digital currencies: Bitcoin, a cryptocurrency causing a monetary revolution. *Int. Bus. Econ. Res. J.* **2015**, *14*, 617–622. [CrossRef]
5. Jeong, S. The Bitcoin Protocol as Law, and the Politics of a Stateless Currency. Available at SSRN 2294124. 2013. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2294124 (accessed on 17 October 2022).
6. DuPont, Q. *Cryptocurrencies and Blockchains*; John Wiley & Sons: Hoboken, NJ, USA, 2019.
7. French, L.A. The Effects of Blockchain on Supply Chain Trust: A Thesis Presented in Partial of the Requirements for the Master of Supply Chain Management at Massey University, Palmerston North, New Zealand. Ph.D. Thesis, Massey University, Palmerston North, New Zealand, 2022.

8. Burniske, C.; White, A. Bitcoin: Ringing the Bell for a New Asset Class. Ark Invest (January 2017). 2017. Available online: https://research.ark-invest.com/hubfs/1_Download_Files_ARK-Invest/White_Papers/Bitcoin-Ringing-The-Bell-For-A-New-Asset-Class.pdf (accessed on 17 October 2022).
9. Mougayar, W. *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*; John Wiley & Sons: Hoboken, NJ, USA, 2016.
10. Notaro, A. All that is solid melts in the Ethereum: The brave new (art) world of NFTs. *J. Vis. Art Pract.* **2022**, 1–24. [[CrossRef](#)]
11. KiliÇarslan, S.K. Bitcoin Özelinde Kripto paraların Edinilmiş mallara katılma rejiminde tasfiyesi sorunu. *Kırıkkale Hukuk Mecmuası* **2023**, 3, 1–27.
12. Strilets, B. Current state and prospects for the legal regulation of cryptocurrencies in the European Union. *Actual Probl. Law* **2022**, 70–76. [[CrossRef](#)]
13. Ramadoss, R. Blockchain technology: An overview. *IEEE Potentials* **2022**, 41, 6–12. [[CrossRef](#)]
14. Hocaoğlu, M.; Habbal, A. NFT-based model to manage educational assets in Metaverse. *Avrupa Bilim Teknol. Derg.* **2022**, 20–25. Available online: <https://dergipark.org.tr/tr/download/article-file/2709574> (accessed on 17 October 2022).
15. Trimborn, S.; Peng, H.; Chen, Y. Influencer Detection Meets Network AutoRegression-Influential Regions in the Bitcoin Blockchain. Available at SSRN. 2022. Available online: <https://www.ml-quant.com/42546603-d6fd-493a-8736-5130928e127b> (accessed on 17 October 2022).
16. Kaur, H.; Alam, M.A.; Jameel, R.; Mourya, A.K.; Chang, V. A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment. *J. Med. Syst.* **2018**, 42, 156. [[CrossRef](#)]
17. 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.
18. Nirananamurthy, M.; Nithya, B.; Jagannatha, S. Analysis of Blockchain technology: Pros, cons and SWOT. *Clust. Comput.* **2019**, 22, 14743–14757. [[CrossRef](#)]
19. Baboshkin, P.; Mikhaylov, A.; Shaikh, Z.A. Sustainable Cryptocurrency Growth Impossible? Impact of Network Power Demand on Bitcoin Price. *Finans. Zhurnal Financ. J.* **2022**, 116–130. Available online: <https://ideas.repec.org/a/fru/finjrn/220308p116-130.html> (accessed on 17 October 2022).
20. Jabbar, R.; Dhib, E.; ben Said, A.; Krichen, M.; Fetais, N.; Zaidan, E.; Barkaoui, K. Blockchain Technology for Intelligent Transportation Systems: A Systematic Literature Review. *IEEE Access* **2022**, 10, 20995–21031. [[CrossRef](#)]
21. Pagnotta, E.S. Decentralizing money: Bitcoin prices and blockchain security. *Rev. Financ. Stud.* **2022**, 35, 866–907. [[CrossRef](#)]
22. Salem, H.; Mazzara, M.; Saleh, H.; Husami, R.; Hattab, S.M. Development of a Blockchain-Based Ad Listing Application. In Proceedings of the International Conference on Advanced Information Networking and Applications, Sydney, NSW, Australia, 13–15 April 2022; Springer: Berlin/Heidelberg, Germany, 2022; pp. 37–45.
23. Rajashekar, M.; Sundaram, S. Dynamic Attribute Tree for the Data Encryption and Third Party Auditing for Cloud Storage. *Indian J. Sci. Technol.* **2022**, 15, 798–805. [[CrossRef](#)]
24. Wang, J.; Chen, J.; Xiong, N.; Alfarraj, O.; Tolba, A.; Ren, Y. S-BDS: An effective blockchain-based data storage scheme in zero-trust IoT. *ACM Trans. Internet Technol.* **2022**. [[CrossRef](#)]
25. Maalla, M.A.; Bezzateev, S.V. Efficient incremental hash chain with probabilistic filter-based method to update blockchain light nodes. *Sci. Tech. J. Inf. Technol. Mech. Opt.* **2022**, 22, 538–546. [[CrossRef](#)]
26. Agrawal, D.; Minocha, S.; Namasudra, S.; Gandomi, A.H. A robust drug recall supply chain management system using hyperledger blockchain ecosystem. *Comput. Biol. Med.* **2022**, 140, 105100. [[CrossRef](#)] [[PubMed](#)]
27. Sammeta, N.; Parthiban, L. Hyperledger blockchain-enabled secure medical record management with deep learning-based diagnosis model. *Complex Intell. Syst.* **2022**, 8, 625–640. [[CrossRef](#)]
28. Mirtskhalava, L.; Iavich, M.; Razmadze, M.; Gulua, N. Securing Medical Data in 5G and 6G via Multichain Blockchain Technology using Post-Quantum Signatures. In Proceedings of the 2021 IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), Odesa, Ukraine, 29 November–3 December 2021; pp. 72–75.
29. 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. [[CrossRef](#)]
30. Sedlmeir, J.; Buhl, H.U.; Fridgen, G.; Keller, R. The energy consumption of blockchain technology: Beyond myth. *Bus. Inf. Syst. Eng.* **2020**, 62, 599–608. [[CrossRef](#)]
31. 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. [[CrossRef](#)]
32. Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. Integration of blockchain and cloud of things: Architecture, applications and challenges. *IEEE Commun. Surv. Tutor.* **2020**, 22, 2521–2549. [[CrossRef](#)]
33. 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. [[CrossRef](#)]
34. Al-Jaroodi, J.; Mohamed, N. Blockchain in industries: A survey. *IEEE Access* **2019**, 7, 36500–36515. [[CrossRef](#)]
35. 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. [[CrossRef](#)]

36. Gai, K.; Guo, J.; Zhu, L.; Yu, S. Blockchain meets cloud computing: A survey. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 2009–2030. [CrossRef]
37. 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. [CrossRef]
38. 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. [CrossRef]
39. Dorsala, M.R.; Sastry, V.; Chapram, S. Blockchain-based solutions for cloud computing: A survey. *J. Netw. Comput. Appl.* **2021**, *196*, 103246. [CrossRef]
40. Guo, H.; Yu, X. A Survey on Blockchain Technology and its security. *Blockchain Res. Appl.* **2022**, *3*, 100067. [CrossRef]
41. 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. [CrossRef]
42. Joshi, A.P.; Han, M.; Wang, Y. A survey on security and privacy issues of blockchain technology. *Math. Found. Comput.* **2018**, *1*, 121. [CrossRef]
43. 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.
44. Dave, D.; Parikh, S.; Patel, R.; Doshi, N. A survey on blockchain technology and its proposed solutions. *Procedia Comput. Sci.* **2019**, *160*, 740–745. [CrossRef]
45. 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. [CrossRef]
46. 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. [CrossRef]
47. 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. [CrossRef]
48. 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.
49. 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.
50. 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).
51. 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. [CrossRef]
52. 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. [CrossRef] [PubMed]
53. 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. [CrossRef]
54. 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.
55. 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. [CrossRef]
56. 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. [CrossRef]
57. Jyoti, A.; Chauhan, R. A blockchain and smart contract-based data provenance collection and storing in cloud environment. *Wirel. Netw.* **2022**, *28*, 1541–1562. [CrossRef]
58. Nguyen, T.M.; Prentice, C. Reverse relationship between reward, knowledge sharing and performance. *Knowl. Manag. Res. Pract.* **2022**, *20*, 516–527. [CrossRef]
59. 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.
60. 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).
61. 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. [CrossRef]
62. Zhang, X.; Xue, M.; Miao, X. A Consensus Algorithm Based on Risk Assessment Model for Permissioned Blockchain. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 8698009. [CrossRef]