

Received October 23, 2020, accepted November 4, 2020, date of publication November 9, 2020, date of current version November 23, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3036812

Blockchain Based Cloud Computing: Architecture and Research Challenges

CH. V. N. U. BHARATHI MURTHY¹, M. LAWANYA SHRI¹,
SEIFEDINE KADRY², (Senior Member, IEEE), AND SANGSOON LIM³

¹School of Information Technology and Engineering, VIT, Vellore 632014, India

²Department of Mathematics and Computer Science, Faculty of Science, Beirut Arab University, Beirut 11072809, Lebanon

³Department of Computer Engineering, Sungkyul University, Anyang 430-742, South Korea

Corresponding author: Sangsoon Lim (slim@sungkyul.ac.kr)


This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korean Government (MSIT) under Grant NRF- 2018R1C1B5038818.

ABSTRACT Blockchain technology is a distributed ledger with records of data containing all details of the transactions carried out and distributed among the nodes present in the network. All the transactions carried out in the system are confirmed by consensus mechanisms, and the data once stored cannot be altered. Blockchain technology is the necessary technology behind Bitcoin, which is a popular digital Cryptocurrency. “Cloud computing is a practice of using a network of remote servers hosted on the internet to store, manage, and process data, rather than a local server or a personal computer.” It is still facing many challenges like data security, data management, compliance, reliability. In this article, we have mentioned some of the significant challenges faced by the cloud and proposed solutions by integrating it with blockchain technology. We tend to investigate a brief survey on earlier studies focused on blockchain integrating with the cloud to depict their supremacy. In this survey, we have also developed architecture integrating blockchain with cloud revealing the communication between blockchain and cloud.

INDEX TERMS Cloud computing, Blockchain technology, data security, decentralization, data management.

I. INTRODUCTION

Cloud computing is a well-defined technology that emerged from large-scale, distributed computing technology. Cloud computing helps to reduce the processing burden on users [52]. There are many advantages like reducing hardware and maintenance costs, availability across the globe, flexibility with a highly automated process, and easy scalability. Many major corporations have adopted cloud-like IBM, Google, Amazon, and Microsoft. Many applications are prototypes that have come up like Google App Engine, Google Cloud Platform, the Amazon Cloud, the Elastic computing platform, etc. [54]. It provides us the facility of pay-per-use policy and flexible IT architecture accessible through the internet from portable devices. Even though the cloud has many useful services, the organizations are slow in accepting this due to their privacy concerns. Security issues and the cloud's challenges are significant drawbacks of hampering the cloud [44].

The associate editor coordinating the review of this manuscript and approving it for publication was Claudio Agostino Ardagna .

Blockchain Technology is the future of the industries striving for security and privacy improvements. Blockchain is a distributed ledger that records tamper-evident data in the form of a chain without any central authority. The participants or the devices in the blockchain technology are called nodes. Blockchain provides a decentralized network in which all the network nodes have active participation to validate and verify the data. The data going to store in the blockchain will be encrypted using cryptography. Every block contains an encrypted hash, timestamp, and hash of the previous block in the chain through which the block will connect. So, the data in the blockchain is tamper-evident. Blockchain provides the data with security, and participating users will be verified in the network, eliminating the data's privacy concern [70].

To facilitate cloud computing growth, we can overcome the data's privacy and security concerns by integrating with blockchain technology. It improves data security, service availability, and it can manage cloud data. In this article, section II gives you the introduction to cloud computing concepts. Section III explains blockchain technology, its characteristics, blockchain types, blockchain layers, architecture,

working, and other leading applications. Section IV explains to us the benefits of integrating cloud with blockchain technology, with the proposed architecture.


II. CLOUD COMPUTING


In this Internet era, there are millions of websites hosted by the web. A stack of servers is needed to maintain the hosted site, which is very costly. The traffic rate of those servers must be constant, and they should be monitored and maintained continuously. There will be a need to hire more people to organize these servers and keep them. Data centers will store all the data. So, continuous efforts in maintaining the server issue, and the employees may divert us from achieving the business goals. To avoid this hectic maintenance, we are adopting “Cloud Computing.” “Cloud computing is a practice of using a network of remote servers to store, manage and process data from any corner of the world. It is used in place of a local server or a personal computer”. Cloud computing services like storing the data and applications are delivered to the organization’s devices through the internet [44]. Cloud computing provides many advantages through the services combining the data centers, resources, and servers through the internet. These services are based on pay per use regulation. The services are available anywhere globally and with significantly less cost payment, improving collaboration among employees. The software present in the cloud will be updated automatically, which makes the cloud easily manageable. The service consumer will also be having control over the documents in the cloud. It is also having some limitations [16]. As the cloud data is very flexible, there are some securities, privacy challenges to be taken care of and vulnerable to attacks. When there is a heavy load of users, there are chances of the cloud having its downtimes.

Cloud provides many services, and they are classified mainly into three delivery models. The first service is Software as a Service (SaaS), which is like an application hosted to customers provided across the internet. The Cloud Service Provider delivers the complete applications or projects as a single platform of the software running in the cloud, offering multiple services for many users. Cloud customers do not have control over the cloud infrastructure. Amazon web services, Salesforce.com, Google Mail constitute a significant example of SaaS. The second service is Platform as a Service (PaaS). The cloud service provider allows us to deploy our application and suites of programming languages within the platform. The difference between SaaS and PaaS is that SaaS hosts the whole application in the cloud, where PaaS provides the platform for the application. Google search engine is the best example for PaaS. The third service is Infrastructure as a Service (IaaS), in which it offers the user to directly access the storage, processing, and other resources over the network. Virtualization is used in IaaS to distribute the physical resources to meet the resources demand from cloud customers. The best virtualization method is to set up independent virtual machines separated from the underlying hardware and other VM’s. To provide security, they provide

TABLE 1. Comparing the Layers of Cloud Maintained by User and Cloud Provider in Different Delivery Models.

SaaS	PaaS	IaaS
Data	Data	Data
Application	Application	Application
Runtime	Runtime	Runtime
Middleware	Middleware	Middleware
Operating System	Operating System	Operating System
Virtualization	Virtualization	Virtualization
Servers	Servers	Servers
Storage	Storage	Storage
Networking	Networking	Networking

 - Layers maintained by the user

 -Layers maintained by a cloud provider

servers with a unique IP address. Amazon EC2, GoGrid, is the best example of IaaS [41].

Table 1 compares the layers of cloud maintained by the user and the cloud provider in different delivery models. In Software as a Service (SaaS), only the data layer will be held by the user, and a cloud service provider will maintain the other layers. In Platform as a Service (PaaS), the user and the cloud service provider will hold the data and application layer and support the other layers. In Infrastructure as Service (IaaS), the data layer, application layer, runtime, middleware, operating system layers are maintained by the user. The remaining layers called virtualization, servers, and the Cloud Service provider should support storage and Networking.

A. CLOUD DEPLOYMENT MODELS

Public Cloud: Public cloud is the one that can be used by different customers who need to get together on servers, and these are owned and managed by providers. The cloud infrastructure is open to use for the public and can be used by more than one enterprise when acquired dynamically. The cloud providers host and maintain these clouds. Sometimes, the cloud provider hosts the customer to lower customer risk and cost for a short-term extension. Microsoft Azure and Google App Engine are examples. [16]

Private Cloud: This is majorly built on the demand of single clients, providing ownership on data, its security, and it is client-dedicated. The infrastructure and applications which are owned by the customers are deployed in it. It is secure and expensive when compared to a public cloud. Regulations on Security, bandwidth limitations are provided in the private clouds. The clients can optimize the user’s access and can restrict the networks used in the private cloud. Eucalyptus System is the best example of a private cloud.

Hybrid Cloud: This is like merging two or more cloud deployment models. Hybrid cloud provides help on-demand and externally provisioned scale. These focus primarily on proprietary data centers but depend on public cloud resources to offer to compute. A very well constructed hybrid cloud can help provide security services, but the difficulty lies in effectively creating and governing such a solution. Amazon Web Services is a prominent example of a hybrid cloud.

Community Cloud: This is mainly built for a specific community of consumers from different organizations with shared concerns. It can be owned, managed, and operated by one or more companies in the community. This kind of cloud is useful in Educations or Banking sectors. Facebook is an example of a community cloud.

Cloud computing consists of five major characteristics. **On-demand self-service** is the one in which the users can spontaneously provide network storage capabilities. **Broad network access** offers service across the network, which can be accessed with standard mechanisms to promote different kinds of client platforms. **Resource pooling** provides most of its computing resources to serve many consumers to their demand using a multi-tenant model. **Measured service** is when resources are owned, maintained, and optimized by the metering capabilities. **Elastic Scalability** is the one that can make changes in IT resources as needed to meet changing demand. For example, when an application needs to create more servers, it can automatically scale with demand [70].

Even though the cloud provides many characteristics, there are also some disadvantages present in the cloud. Some of them are [7]:

1) SECURITY OF DATA

Most of the cloud providers ensure the security of the data holding some security mechanisms. But in some cases, leakage of data happens. A data leakage issue has come earlier in iCloud, where most of the celebrities' data got leaked to the public. It is felt like keeping the data online in the cloud gives the data access without even knowing by the user. Security is the main problem making the companies shy away from using the cloud and its services.

2) DOWNTIMES

Cloud Services are available almost 24/7, but some of the services are scheduled timeout services. They stop their services for the time being for periodic maintenance. Some of the services have been limited to a particular time in a day.

3) LIMITED CONTROL

Cloud users will be having limited control over the data in the cloud. Most control they have is in IaaS (Infrastructure as a Service), where they get control over the virtual machines and customize them according to their needs.

4) NETWORK DEPENDENCY

Cloud service availability is entirely dependent on the internet. Even though the whole world is ubiquitous in network connection, some countries have no proper network. Usage of cloud services makes the providers ignoring the parts of the world that don't have internet. Nowadays, people don't like to use mobile data for an intense application running. They prefer Wi-Fi, but it is not available everywhere.

5) NO LEGAL LIABILITY FOR VENDORS

Even cloud providers host the data with more security; there is no liability in a potential breach. There are no legal complications involved when the data stored in the cloud from one country is used elsewhere. The question arises like laws of which country would be applied to the provision and privacy of data.

B. RESEARCH ISSUES IN CLOUD

1) RELIABILITY

Cloud services are available 24/7 to cloud users. A few times, the server stops its services due to maintenance issues or restricted time issue. Nowadays, cloud users expect more services, established standards, and best practices from the cloud providers. Servers present in the cloud are also similar to resident servers. They also experience server down-times, and also they have a high dependency on a cloud service provider. When the user chooses a particular server, they may be locked in, bringing a potential business risk [2].

2) COMPLIANCE

There are many regulations to access the storage, use the data, and require regular reporting and audit trails. In some cases, there will be special requirements from the customers regarding the data centers maintained by cloud providers that require compliance requirements.

3) SERVICE LEVEL AGREEMENTS

Cloud services will be provided based upon the Service Level Agreements that allow several instances of one application to be copied on multiple servers whenever there is a need depending upon the priority. If that is of lower priority, the cloud may shut down or minimize that application. The main challenge for cloud users is the evaluation of Service Level Agreements agreed with cloud vendors. Most vendors create SLA's making terms in favor of them while assuring minimal offers to users like data protection, outages, and price structures. These things should be dealt with with intensive care by the cloud users before signing the contract with a provider.

4) CLOUD DATA MANAGEMENT

Managing data is an important research issue as cloud data can be massive in an unstructured or semi-structured manner. Service providers rely on the infrastructure provider to achieve complete data security since they do not have access to the data centers' physical security system. Even in virtual machines, the provider can remotely set the security conditions, not aware of whether it is implemented securely. In these situations, the infrastructure provider needs to achieve terms like Auditability for attesting to the security settings of applications, confidentiality for secure data access, and transfer. Confidentiality can be achieved by using cryptographic protocols, and remote attestation techniques can achieve audibility. But, it is not possible in all situations because VM's

dynamically migrate from one place to another. So, using remote attestation will not remain the right solution.

5) DATA ENCRYPTION

Data is encrypted to provide security to the data. There are multiple levels of security supplied like low level, middle, and high level. Consider the Web services APIs used to access the cloud through a computer program or with clients written to those API. We provide SSL encryption for access, which is generally considered a standard. When the object arrives at the cloud, the data would be decrypted and stored in the cloud. The data security is being compromised while decrypting the data and storing it without prior encryption before storing the data into the cloud.

6) INTEROPERABILITY

The internal communication between the systems is very much needed to interchange information and make use of that information. The public cloud networks which are designed as closed systems are not supposed to communicate with each other. Due to the absence of internal communication amongst the cloud systems, the industry cannot combine their IT systems in the cloud. Enterprises need to take a step to develop a single toolset to integrate multiple applications across existing programs and among multiple cloud providers

C. USER CASE STUDY

Giving and supporting interoperability and cooperation among their existing and deployed cloud systems is a need for public and private companies these days. Different cloud systems are federating into goal-oriented federations. In addition to several technical issues, the development and management of cloud federations have to deal with serious security issues such as the non-disclosure of sensitive data and the implementation of confidentiality guarantees. The EU SUNFISH project aims to resolve these security issues by implementing a decentralized, democratic cloud federation system that guarantees controlled information by-design.

SUNFISH's proposal is Federation-as-a-Service (FaaS), which allows cloud data and resources to be securely created and managed. Domain federations aim to share services between members by creating controlled, safe inter-cloud interactions. Some contracts specify the rules and services provided. In one scenario, a member provides a service where specific users can only use it, and the service outputs must be masked for personal reasons. Given that the data managed by cloud federations are highly sensitive, FaaS must provide a high level of assurance about member contract compliance. FaaS must also ensure the integrity of contracts such as the fact that they cannot be manipulated and that all members involved must be aware of their existence. All interactions in the cloud must be monitored, and the logs stored ensure strong integrity. FaaS supports the absence of hierarchical governance to increase the adoption of cloud federations. There can't be a leader among the federation; instead, they form a peer network. To do this, FaaS seeks to

establish decentralized, democratic governance of the federation, so it must rely on a distributed database to ensure strong integrity guarantees. The SUNFISH project's innovative software approach for FaaS is based on blockchain [12].

III. BLOCKCHAIN TECHNOLOGY

A. EMERGENCE OF BLOCKCHAIN-BITCOIN

The introduction of Bitcoin did the introduction of Blockchain technology. Bitcoin is a form of digital currency introduced by a pseudo name called "Satoshi Nakamoto" in 2008. He published a white paper, "Bitcoin: A Peer to Peer Electronic Cash System," which presents us with the direct online payment from one party to another without using any third party [33]. This electronic cash system mainly overcomes the problem of double-spending the money, primarily the digital currency nature that allows being easily duplicated and spent more than once. This problem is solved by linking each transaction with one another in a tamper-resistant manner. The public ledger is being used to connect transactions in a tamper-resistant way. With this ledger, a network can verify the transaction history that the user submits for payment and can confirm that the coin has not already been spent [21].

In comparing Blockchain with Bitcoin, we can say that blockchain is a technology that many cryptocurrencies like Bitcoin are using for secure and anonymous transactions [71]. But blockchain is a transparent mechanism, where Bitcoin feeds on anonymity. While Bitcoin is used for online transactions, blockchain transfers data, rights, etc. So, Blockchain has a broader approach to use, while Bitcoin is limited to exchanging digital currencies [72]. "Blockchain can be defined as transparent distributed ledgers of digitally signed transactions that are grouped into blocks." Each block contains a hash value produced through cryptography, which links one block with another, a timestamp, and the transaction data. Blockchain data cannot be modified by design [35]. It is a distributed, open ledger to records transactions among the parties efficiently and permanently.

"The blockchain is an indestructible digital ledger for keeping track of economic transactions that can be programmed to maintain not only financial transactions but virtually everything that has a value." When we implement blockchain technology, no government interference is needed, and zero percent of fraud due to consensus validation. By eliminating the involvement of third-party, instant transactions can be done without paying transaction fees. These features improve financial efficiency [2]. Despite these many advantages, blockchain has some disadvantages, like it is incredibly volatile. There are chances of increasing society's crimes due to anonymous transactions that are untraceable by the person or node outside the network.

B. CHARACTERISTICS AND FUNCTIONALITIES

1) DECENTRALIZATION

In a traditional centralized network, the nodes have to be validated through a trustworthy centralized server. This approach

brings a problem of delay in communication in the whole system and increases computations' costs. The blockchain consists of peer-to-peer blocks without the need for the involvement of any third party. It means the blockchain needs not to rely on a centralized server to store and update multiple systems. In this distributed network, all the participants or nodes actively participate in transactions with a decentralized server and slash the server [1].

2) PERSISTENCY

All transactions are checked in the blockchain, and honest miners store the transaction data. If the transactions are included in the list, rolling back or erasing the transactions is difficult [67]. Moreover, these blocks are also validated by other miners, so they cannot be manipulated.

3) AUDITABILITY

All transactions in the blockchain will be signed by the sender digitally, saving the block with the timestamp, making it easy for users to track and verify the transaction information.

4) ANONYMITY

In the blockchain, data is secured by using asymmetric encryption techniques. To authenticate the recipient, all payments are digitally signed. The sender interacts with the blockchain to support a self-generated email and generates a different set of addresses to preserve their identity as a secret. Therefore, a centralized owner will retain the user's real identities; the disclosure of the sender's identity will be minimized [36].

5) AUTONOMOUS

As there is no single entity controlling the blockchain network, we can publish the signed nodes and review them if other nodes accept them in the decentralized network. The consensus base came by accepting a node by every other node in the network, ensuring that the data transfer will be done safely in the blockchain.

6) IMMUTABILITY

The transaction data is validated before it is accepted into the Block [69]. The blockchain permanently records the transactions. The data in the blocks cannot tamper. If someone tries to alter the data, it would be easily caught because data in the blocks is linked through the hash key, and change in the data would invalidate the next blocks.

7) TRANSPARENCY

Blockchain is a decentralized structure where all participants can publish their records and query the nodes' data. In this blockchain technology, the system records and maintains transaction data information in an open distributed ledger [38]. This data is open and reliable to all the nodes present in the same network to access the information.

8) TRACEABILITY

The data in the blocks of blockchain is encrypted using hashing algorithms. Each block will have a hash key. Each block

TABLE 2. Comparison Between Different Types of Blockchain.

Property	Public	Consortium	Private
Consensus Determination	All Miners	Selected Set of nodes	Limited to one organization
Read Permission	Public	Public/Restricted	Public/Restricted
Immutability	Impossible to tamper	Could be tampered	Could be tampered
Efficiency	Low	High	High
Centralized	No	Partial	Yes
Consensus Process	Permissionless	Permissioned	Permissioned

in the network contains the previous blocks' hash key and is linked through them [45]. Hence, tracing the block through the hash key is comfortable in the blockchain network.

C. TYPES OF BLOCKCHAIN

Blockchain is categorized into three major types based on the users' availability and accessibility [27].

1) PUBLIC (PERMISSIONLESS) BLOCKCHAIN

A public blockchain is a decentralized, open ledger in which any node can enter the network and can engage in the processing, storage, and validation of the transaction data through a consensus mechanism.

2) PRIVATE (PERMISSIONED) BLOCKCHAIN

The private blockchain is a limited one, where no one can quickly become a part of the network. It is a type of centralized blockchain controlled by a central authority for accessibility. The data read authorization in the private blockchain is opened to the public selectively. Private Blockchain is specific to limited organizations or small industries. Vote counting, Digital Identity, Asset Ownership, Supply chain management are different kinds of use cases of the private blockchain.

3) CONSORTIUM BLOCKCHAIN

The consortium blockchain is a partially decentralized chain. The pre-selected node will have the authority to choose the type of service in advance. Remaining nodes may have access to the blockchain transactions, but not in the consensus process. Hyperledger and R3CEV are examples of consortium blockchain.

Table 2 compares different blockchain types considering the properties like the read permission of the blockchain, Immutability status, efficiency of the block, Centralization status, Consensus process, and the mechanism of consensus. Table 3 presents your comparison of different blockchain platforms, namely Bitcoin, Ethereum, and Hyperledger fabric. For **Bitcoin**, its primary purpose is Cryptocurrency, storing the transaction data. It is written in the script, and source code is available from GitHub through which anyone can participate. Its native currency is Bitcoin (BTC) with 10 minutes of block release timing, 250 bytes (avg) transaction size, 3 TXN/sec transaction rate. In Bitcoin, mining is carried out by Proof of Work. For **Ethereum**, its primary purpose is to run smart contracts, storing the cryptocurrency transaction data, digital assets, and smart contracts. It is written in

TABLE 3. Comparison of Different Blockchain Platforms.

Types	Bitcoin	Ethereum	Hyperledger fabric
Purpose	Cryptocurrency	Runs Smart Contracts	Creation of blockchain for industries
What kind of data to be stored?	Cryptocurrency transactions	Cryptocurrency, digital assets, smart contracts	Chain code, smart contracts
Scripting languages	Script	Solidity, Serpent	Go
Is the ecosystem open?	Yes	Yes	No
How can one participate?	Get source code from GitHub	Get source code from GitHub	User source code, Register for identity to the network membership services
Native currency	Bitcoin (BTC)	Ether (ETH or ETC)	N/A
Is decision making transparent?	Yes	Yes	Unknown
Does it use a managed public key infrastructure	No	No	No
Block-release timing	10 minutes	12 seconds	Configurable
Transaction size	250 bytes average	Theoretically no max	Maximum size configurable
Transaction rate	3 TXN/sec	Theoretically no max	More than 10,000 TNX/sec
Mining	Proof of Work	Proof of Work using Ethash algorithm	N/A

Solidity or Serpent, and source code is available from GitHub through which anyone can participate. Its native currency is Ether (ETH), with 12 seconds of block release timing. In Ether, mining is carried out by Proof of Work using the Ethash algorithm. For **Hyperledger fabric**, its primary purpose is creating a blockchain for industries, storing the chain code, and smart contracts. It is written in Go language, and one can participate in this by registering for identity to network membership services.

D. PHASES OR GENERATIONS OF BLOCKCHAIN

The emergence of blockchain technology is categorized into three generations. Blockchain 1.0 is the first generation as digital currency, Second generation Blockchain 2.0 is called

the digital economy, and Third generation Blockchain 3.0 is called a digital society [14].

1) FIRST-GENERATION BLOCKCHAIN

Blockchain technology is first introduced to the world through the digital currency called Bitcoin. Bitcoin is a form of digital currency introduced by the pseudo name called Satoshi Nakamoto. Blockchain technology features are more suitable for digital currencies. Transaction data is stored in the blocks, encrypted cryptographically, and these blocks are linked with each other through complex cryptographic mechanisms. The data in the blocks is immutable, and it doesn't allow updating the data. The presence of an open distributed ledger in the blockchain helps the digital currencies to avoid double-spending. Many other digital currencies are emerged using the blockchain PoW. Digital currencies help to reduce the transaction fee vastly. Their usage is also anonymous than credit cards.

2) SECOND GENERATION BLOCKCHAIN

Blockchain technology emergence proved that it could be used beyond simple payments, transactions, and transfers and includes loans, mortgages, and stocks that involve banks. Smart contracts came to existence in the second generation extending the digital currencies and turning into a digital economy. A smart contract is a self-executing line of code with terms of an agreement between the buyer and the seller are met, and it is activated with a transaction. Each of them will be having a unique address. The smart contracts execute automatically in every node present in the network based on meeting the specific code conditions. These create trust between two parties who do not know each other. It helps the involving parties to review contract code and predict the outcome as the code is executed publicly on the network, and it is verifiable. The data present in the smart contract is stored in the block of blockchain technology, which is tamper-free and anti-counterfeiting. Smart contracts are applied to many scenarios like insurance, business agreements, financial data recordings, mortgages, food supply chains, etc. Ethereum is one of the examples of a smart contract.

3) THIRD-GENERATION BLOCKCHAIN

Blockchain has been able to overcome its major problem called Scaling in the process of evolution. Blockchain 3.0 expands numerous applications not involving the currency, cash, or financial sector. It brings us smart cities with smart governance; smart resource utilization by smart citizens bringing us a smart economy. Blockchain's integration with the Internet of Things is being developed to implement smart property transactions and data payment without third party involvement. Such incorporation can also set up a market for power from machine to machine and handle electronic medical records information.

Blockchain 3.0 is beneficial in digital identity where unbanked customers can maintain their identities so that banks can complete their formalities such as Know Your

Customer and access bank accounts. In this internet era, many of the transactions are done between unknown people. Saving data in the block and carrying transactions through the blockchain network would bring trustworthy customers, which leads to a decrease in fraud rating [45].

4) MINING

Mining can be defined as adding blocks to the openly distributed ledger, which is called the blockchain. People who mine Bitcoin get rewards for more mining. Miners present in each node mine the blocks and sometimes get paid a reward for mining.

E. NODES OF BLOCKCHAIN

A node in the blockchain can be defined as the device belonging to the blockchain network. The type of node is classified based upon the task done by it. There are different kinds of nodes. They are:

1. **Mining Nodes:** Mining nodes always produce blocks for the blockchain. These nodes just verify whether the block can be added to the list in the process called mining. Mining nodes are not responsible for maintaining blocks; they only create blocks and add them to the chain. Added blocks are published over the network where full nodes validate them and add them to the blockchain.
2. **Full or Super Nodes:** Full node control maintains and sends the copies of blocks to all the network nodes. Their job is to validate transactions until the genesis block during publishing. After validation, the data is sent to all other nodes in the network to ensure the blockchains trustworthiness. When there are more nodes with a more decentralized network, it would become tough to hack it. A Node can be called a Super Node depending upon the count of exchange of transactions produced from a full node. Super Nodes are always active and connect the remaining full nodes and make them appear all over the network.
3. **Light Nodes:** Light nodes exhibit similar behavior as full nodes, but they contain only a portion of the whole block. They contain only the previous transaction blocker and validate the blockchain and inform the network's remaining nodes. Light nodes are connected to the parent node, i.e., Full node, and are not as powerful. Whenever a full node is hacked and is holding the corrupted data, the light node can capture and dismiss that blockchain as false and give the complete node information to a blockchain that should be maintaining. As these don't occupy much data space, they help make the network more decentralized and travel long distances at a lower cost than full nodes.

F. LAYERS OF BLOCKCHAIN

Blockchain doesn't contain any hierarchical structure. Six layers can explain it: data, network, consensus, contract, service, and application, as shown in figure 1. Data and Network layers gather data and validate it. In the consensus layer, con-

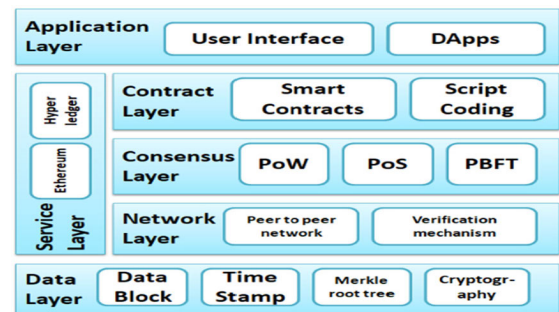


FIGURE 1. Layers of blockchain.

TABLE 4. Given Components Present in Each Layer of Blockchain.

Layer	Components
Data layer	Data Block, chain structure, timestamp, Merkle tree, cryptography
Network layer	P2P network, verification mechanism, a broadcast protocol
Consensus layer	PoW, PoS, DPoS, PBFT
Contract layer	Smart contract, script coding, incentive mechanism
Service layer	Ethereum, Hyperledger, IBM Azure BaaS, ...
Application layer	Cryptocurrency, healthcare, cloud service, ...

sensus algorithms are involved for verification [45]. Smart contracts are used in the contract layer to implement trust. The services and Application layers implement blockchain activities. In table 4, we mentioned the components present in each layer of blockchain. In the data layer, we have Data block, timestamp, Merkle root tree, hashing. In the network layer, peer-to-peer network, verification mechanism, broad protocols are the components. The consensus layer contains different consensus algorithms like Proof of Work, Proof of Stake, Byzantine Fault algorithms, etc. In the contract layer, we have smart contracts, incentive mechanisms, script coding. In the service layer, we have Ethereum, Hyperledger Fabric, IBM Azure, etc.

G. HASHING

Hashing can be defined in simple terms as identifying a specific object from a set of similar objects. A large amount of data is converted into a hash key using hash functions. The value obtained by using a hash function is stored in the data structure called a hash table. The hash function is always used to map a data set that falls into a hash table. The value obtained is called hash value or hash code [10].

H. SMART CONTRACTS

In 1994, Nick Szabo initiated smart contracts in the form of automated transaction protocol. The concept of smart contracts introduced earlier than blockchain technology. A smart contract can be defined in digital form as a series of commitments [69]. The relationship between the parties is being built by rules that build trust between the parties who do not know each other. In a blockchain, Smart Contracts are defined as a program written in programmable languages that

TABLE 5. Performance Analysis Comparison Between Bitcoin and Ethereum.

Parameter	Bitcoin	Ethereum
Block size	1 MB avg	Varies from 2000 bytes to 2800 bytes
Block time	600 secs to 10 minutes	15 Sec
No of transactions	Lower than Ethereum	Higher than Bitcoin
Difficulty	25 million Terhash per second	Not much

run in a container. The data present in the block will give be executed within the blockchain, which offers trustworthiness and uniqueness. As the data of smart contracts is present in the blockchain, the data is tamper-proof and anti-counterfeiting. The smart contract enables self-execution when a specific condition is met on all the nodes present in the network [43]. It also helps the parties predict the outcomes as the contract execution depends on the code available on a public network, and they are verifiable as they are already signed [45]. Smart contracts can maintain smart asserts and assert transactions. They are also useful during loans, mortgages, agreements between business individuals. Some research offers the results that smart contracts can have the ability to evaluate effectiveness, availability, and scalability. TDD (Test Driven Development) and BDD (Behavior Driven Development) evaluate smart contracts' accuracy. Ethereum is the best example which is building smart contracts [34].

I. DIGITAL SIGNATURES

A digital signature can be defined as digitally signed data sent from one-to-one or one-to-many, ensuring no data loss. Every client will have a private key and a public key. If a client wants to send any data, they must generate the hash value from the transaction data and then use their private key to encrypt the hash value. This process is called 'digital signing,' and the stage is called 'signing.' The digitally signed transactions are distributed throughout the network to nodes present. The payment information received will be decrypted using the public key of the recipient [20]. The decrypted hash value is checked by comparing it with the hash value obtained from the sender's data. This phase is called the verification phase. Elliptic Curve Digital Signature Algorithm (ECDSA) is used for verification in the blockchain [60].

J. PERFORMANCE ANALYSIS OF BLOCKCHAIN PLATFORMS

1) PERFORMANCE ANALYSIS COMPARISON BETWEEN BITCOIN AND ETHEREUM

In table 5, the comparison between the blockchain platforms called Bitcoin and Ethereum is shown. We have considered Block size, Block time, number of transactions, and difficulty creating the block [62].

Block Size: the average size of Bitcoin is 1 MB, and the Ethereum block size varies from 2000 bytes to 2800 bytes.

Block Time: The time taken by Bitcoin to create a block is 600 seconds to 10 minutes, whereas Ethereum can create within 15 seconds

TABLE 6. Comparison Between Hyperledger Fabric and Ethereum.

Parameter	Hyperledger Fabric	Ethereum
Average throughput	High	Low
CPU Utilization	Low	High
Memory Utilization	High	Low
Network Utilization	High	Low
Execution time	Low	High
Average Latency	Low	High

No of Transactions: As Bitcoin takes more time to create a block and transact, the number of transactions are significantly less than Ethereum, and also Ethereum has become popular recently

Difficulty: The difficulty in creating the block in Bitcoin takes 25 million Terhash per second, and the creation of Ethereum will not be much.

2) COMPARISON BETWEEN HYPERLEDGER FABRIC AND ETHEREUM

In table 6, the comparison between blockchain platforms called Hyperledger fabric and Ethereum is shown. We have considered parameters called Average throughput, CPU Utilization, Memory Utilization, Network Utilization, Execution time, and Average latency [62].

K. BLOCKCHAIN APPLICATIONS

Various blockchain applications are emerging in our day-to-day lives. The applications include food supply chain, Asset management, Insurance claims, smart car, smartphone, e-passport, smart appliances, health care management, and personal health record-keeping, and so on.

1) BLOCKCHAIN IN FINANCE

Bank activities are intermediaries in the traditional method and system transactions. Such payments are prone to errors as many intermediary parties maintain the record. This whole process takes time and costs more [69]. This problem is simplified by introducing blockchain technology that uses a distributed public ledger in which miners verify the transactions using "Proof-of-work." The blockchain provides many services to the financial world. Some of them are:

- 1. Cryptocurrency:** Like Bitcoin, many cryptocurrencies are introduced to the world that uses blockchain technology. There is no need for a trusted third-party like a bank in traditional systems. All payments can be checked and unchanged.
- 2. Global Payments:** Global payments are time-consuming because many intermediaries will verify the transactions. Blockchain technology is beneficial in these situations. It reduces the complexity of verifying by introducing the decentralized public ledger. With the peer-to-peer network's help, global payments are made faster, verifiable, immutable, and safer.
- 3. Insurance Claims and Processing:** Many fraudulent claims are coming up in the insurance sector. These

TABLE 7. Comparison Between Different Consensus Algorithms.

Property	PoW	PoS	PBFT	DPOS	Ripple	Tendermint
Node Identity Management	Open	Open	Permissioned	Open	Open	Permissioned
Energy Saving	No	Partial	Yes	Partial	Yes	Yes
Tolerated power of adversary	<25% computing power	<51% stake	<33.3% faulty replicas	<51% validators	<20% faulty nodes	<33.3% byzantine voting power
Example	Bitcoin	Peer coin	Hyperledger fabric	Bitshares	Ripple	Tendermint

defective claims can be avoided in a secure manner using Blockchain distributed ledger technology.

2) BLOCKCHAIN IN HEALTHCARE

Blockchain is useful for personal health databases and information sharing centers', is a smart platform for medical assistance and an in-depth analysis of the medical challenges. The patient's necessary information, medical history, test results, treatment records, drug prescriptions, and diagnostic effects are stored in a digital record called The Electronic Health Record (EHR). Continuous processing of data on cloud servers helps reduce the risk of medical data failure and increases the safety and accuracy of medical information. Health data and medical records are helpful for clinicians to verify the health status of a person. The health database allows doctors to understand the condition of the patient quickly. The medical database is for extensive data analysis and mining for hospitals and medical research centers. The smart contracts in the blockchain can help build a smart medical management system to form medical contracts and vouchers [45].

3) BLOCKCHAIN IN DATA PROVENANCE

Data provenance means data processing management, addressing data status, and source. The provenance of data is carried out in managing scientific data, data storage, and data assets. Blockchain technology and smart contracts can be used to enforce data provenance and to check the asset's integrity and ownership. It also helps with the traceability of the product and can also have a multi-stakeholder traceability chain. It is also useful for applications such as forensics and accountability.

4) BLOCKCHAIN IN 5G NETWORK

In 5G networks, Heterogeneous devices and applications need to be coordinated to improve energy efficiency, network capacity, and resource accessibility. We could build a business model combining blockchain and smart contracts to collaborate industrial automation processes and related manufacturing equipment to achieve efficient operations. In the traditional approach, there is a need for a network slice broker for resource allocation facilities [8]. However,

using blockchain, we could have cloud radio over an optical fiber network to adopt an anonymous access identification mechanism to reduce the cost of operating and connecting the network and make a joint agreement between the parties.

5) BLOCKCHAIN IN AVIATION SYSTEMS

Blockchain will provide digital operator and product provider alliances to provide secure decentralized travel services and products. Smart contracts can also work together between companies and different units within the company.

6) BLOCKCHAIN IN SUPPLY CHAIN SYSTEMS

Smart sensors are used in traditional supply chain systems to collect information about the supply chain as it is transported. Shortly, the number of sensors is expected to rise rapidly. Blockchain technology would, therefore, help maintain the massive amount of data to be collected and analyzed. The information in a distributed network would be robust and stable.

7) BLOCKCHAIN IN SMART HOMES

Blockchain integration with the Internet of Things will help make smart home appliance operations efficient and safe.

8) BLOCKCHAIN IN SMART PROPERTY

In the distributed ledger technology, all properties such as home, property, cars, and smart devices can be represented. Blockchain keeps track of all devices and their operations. The records can be shared with legit persons whenever we want and can establish contacts between multiple parties [20].

1. Hard money lending: Hard money lending is very common nowadays. The borrower needs to have a property to keep it as collateral to lend the money. Borrowers can do fraud using illicit assets as collateral or by borrowers if they are using dishonest policies as part of the agreement. The property can be checked before it is taken as collateral by using Blockchain technology, and smart contracts can agree. It improves trust, brings transparency and security even among strangers.

2. Cars and Phones: Using authentication keys,

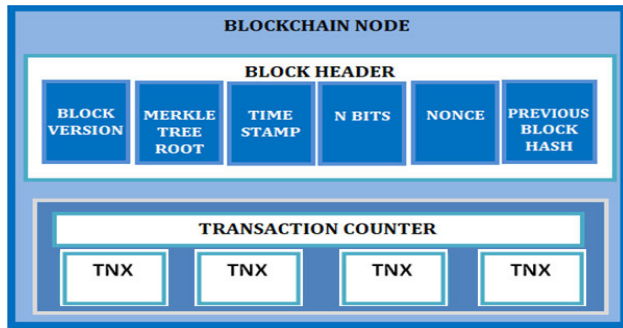


FIGURE 2. The general architecture of a blockchain.

personal devices are protected, and cars are accessible only to owners using smart keys. Using cryptography, this can be kept safe. But if the authentication key is stolen or copied, or transferred, there are chances of failure. Using a blockchain ledger to replace and replicate lost credentials would fix this.

9) BLOCKCHAIN IN OTHER INDUSTRIES

Blockchain has numerous applications such as Energy Cyber-Physical System, Vehicular Cyber-Physical System in the Internet of Things, on the Internet of Battle-field Things (IoBT), Cyber Security, Smart Appliances, Asset Management, Cloud Storage, Intellectual Property, Food Safety, Blockchain Notary, Fundraising and transparency, wireless networks and Virtualization, Real estate, Identity management like Academic records, Blockchain Music, Birth, Marriage and Death Certificates, Passports, Personal Identity and Privacy, Voting, etc. Because the blockchain is a decentralized, stable, open, and scalable network, it will supply future energy internet growth.

10) BLOCKCHAIN ARCHITECTURE

Blockchain would be like a sequence of blocks that hold the entire data belonging to a network in an open public ledger. There are a block header and a block body in each block. As shown in figure 2, there are six main components in the block header [24]. They are:

1. **Block version:** This allows us to follow the set of block validation rules.
2. **Merkle tree root hash:** The data is encrypted with hashing algorithms when a transaction occurs, and then it is transmitted to each node. Because it could contain thousands of transaction records in the block of each node, the Merkle tree function was used by the blockchain to produce a final hash value and Merkle tree root.
3. **Timestamp:** Produces timestamp with the current time as seconds for every block
4. **Difficulty target:** threshold of a valid hash block.
5. **Nonce:** A 4-byte field that usually begins at zero and increases with each hash calculation
6. **Parent block hash:** The value of 256-bit hash points to the previous block.

L. WORKING OF BLOCKCHAIN

Blockchain technology suggests building blocks containing data and is linked to the chain. Blocks are linked together through each block containing the previous block header [27]. If some data is changed in the previous block, the hash key will change, and hence the mismatch of the hash key will happen in the chain of blocks. It prevents the data from tampering. When a user wants to send some transaction data to others, that transaction will be represented as a block. The block must be broadcast to all other nodes on the network to add the blockchain block. Miners of the node need to approve the transaction. The miners get the authority to approve a block by solving computationally challenging problems when the block is created. The block is added to the blockchain after authentication, which completes the transaction. The next step is to decide which user published the next block. The collection of validated blocks is combined into a chain that forms a blockchain network [69].

M. CONSENSUS ALGORITHMS

When a block is needed to be added into the blockchain, that block needs to be verified as a valid one by all the nodes in the network. Consensus algorithms are a kind of protocol that maintains the nodes involved in the blockchain network to reach a transaction order decision and filter invalid transactions. More than one transaction is competing with each other to get published to obtain the reward of the transaction. To solve the decision problem, consensus algorithms came into existence. It is also difficult for the miners to reach a consensus because, without a central authority, the blockchain network is distributed [69].

1) PROOF-OF-WORK

The user power is directly proportional to the system's total computational power in this proof-of-work consensus model. The main target of the consensus models is to remove the fraudulent nodes, including honest nodes. In the decentralized network, to record all transactions, one of the nodes must be chosen. One-way is a random selection to pick the node, but it is vulnerable to attack. Therefore, if a user or node decides to record transactions, they must show that their network is not vulnerable to attacks.

In this, the user needs to face the challenge of solving a computationally difficult problem to get the incentive when a node is added to the blockchain. That network node will use a block header and a nonce to measure a cryptographic hash function SHA-256. To get different hash values, the miners are likely to change the nonce. The miners will calculate the value that is equal to or less than the value of a consensus. When a miner hits the target value, the miner block is transmitted to all other nodes in the network, and all other nodes need to confirm the validity of the hash value to each other. If the new block is approved, it will be connected to its blockchain by the other miners. Sometimes valid blocks can be generated in parallel when the target value is found almost

simultaneously by multiple miners. Branches of blocks that are called competing forks will be formed in these cases. In this PoW protocol, the longer the chain is, it would be considered an authenticate one. In PoW, miners have to use a lot of computation power to do many computer calculations [24]. This process wastes too much of its resources. Some side applications are designed from the PoW protocol, such as Prime Coin, which searches for prime number chains used in mathematical research.

2) PROOF-OF-STAKE

Proof-of-Stake is PoW's best alternative without a waste of resources. It is known that miners with more blocks are less likely to attack the PoS protocol network. And, with more coins, the miner will be given the ability to produce the next one. This selection is unfair as the wealthiest miner in the network would begin to dominate the others. Most solutions are suggested using a miner's number of blocks compared to the network number. One of the solutions is the Peer coin that favors selection based on the age of the coin. The probability of mining the next block is a larger or older set of coins in peer coin. Another example is Blackcoin, which predicts the next block generator using randomization. It selects the equation in conjunction with the stake size, that gives the lowest hash value. Many blockchains are planning to move from PoW to PoS gradually [9].

3) PRACTICAL BYZANTINE FAULT TOLERANCE (PBFT)

PBFT is like a set of principles that can withstand Byzantine flaws. As PBFT handles up to one-third of Byzantine replicas, Hyperledger Fabrics uses PBFT as its consensus algorithm. A new block is decided in each round, and a primary node is chosen according to specific rules responsible for ordering the transaction. The PBFT process can be divided into three phases, such as prepared, prepared, and committed. The node enters the next phase in every phase when two-thirds of all nodes receive votes. Here, PBFT requires every node in the network to be familiar. Antshares must implement delegated byzantine fault tolerance (dPBFT) based on the PBFT protocol in which some professional nodes are supposed to vote to record the transactions.

4) DELEGATED PROOF OF STAKE

PoS and DPoS differ in that PoS is democratic, and DPoS is a democratic representative. The network stakeholders elect the delegate to publish the blocks and validate them. The block could be checked easily if there are fewer nodes to verify the transactions, which leads to early confirmation of the transaction. Delegates can adjust the parameters such as block size and block interval. DPoS is used mainly by Bitshares.

5) RIPPLE

In Ripple, we use sub-networks that are collectively trusted within the extensive network. Nodes can be divided into two types in this network. One is a Consensus Process Participating Server and the other is the client to transfer funds

only. Each server will have an essential Unique Node List (UNL). The database will ask the nodes present in the UNL to determine whether to publish a transaction in the ledger and if it obtained an agreement of more than 80%, the transaction would be packed into the ledger. So long as the number of nodes in UNL is less than 20 percent, the ledger will authenticate node.

6) TENDERMINT

Tendermint is similar to the algorithm of PBFT consensus. If a new block is added in a round to broadcast an unconfirmed block, a proposer would be selected. This method is divided into three stages: Prevote, Precommit, and Commit. Validators determine in the prevote process whether to broadcast the forecast for the proposed frame. The Precommit phase sends precommit to the block if the node receives more than two-thirds of prevotes on the proposed block. The node receives more than two-thirds of precommitments; it joins the process of the commit. The node validates the block in the commit phase and transmits a commit do to the block. If the node receives more than two-thirds of commitments, the block will be accepted.

7) COMPARISON OF CONSENSUS ALGORITHMS

In the study of comparison between different consensus algorithms, it showed that there are different advantages and disadvantages [2]. These were explained in table 7 using properties like:

a: NODE IDENTITY MANAGEMENT

In PBFT, each user's identity is required to select a primary user for each round, while in each round, Tendermint knows all validators to select a proposer. The nodes freely join the network in the remaining algorithms.

b: ENERGY-SAVING

PoW consumes more energy as the miners continuously make calculations to reach the target value. In contrast, PoS and DPoS do not consume much energy as the target value's search space is minimal. The energy is much saved by the rest of the algorithms, as there is no mining concept.

c: TOLERATED POWER OF ADVERSARY

In general, the node's threshold to gain control of the network is considered to be 51 percent of the hash power. Because of a selfish mining strategy in PoW, by having only 25 percent of the hashing power, miners can gain more revenue. In ripple, if the faulty nodes in a UNL are less than 20 percent, consistency is retained, and up to one-third of faulty nodes can be managed by PBFT and Tendermint.

Through this comparison, we can understand that these mechanisms are implied to improve either decentralization or efficiency. There are some advantages to each algorithm that brings us to Proof of Work, highly scalable in comparison [2]. Proof of Stake decreases the power consumption compared to Proof of Work, with faster processing of

Stake decreases the power consumption compared to Proof of Work, with faster processing of transactions, and require less hardware. In PBFT, energy utilization is significantly reduced compared to others due to the absence of hashing energy to enter the next block. Among all the algorithms, DPoS provides better distribution of rewards with real-time voting security and minimizes costs for blockchain network support. Ripple is more decentralized than other networks and uses less energy while enabling the instant verification of the transactions.

N. CHALLENGES IN BLOCKCHAIN

There is no doubt that Blockchain is a promising emerging technology, yet it faces some challenges. These challenges sometimes limit the usage of blockchain. There are many problems, such as consensus processes, data management, storage, chain systems, legislation, governance, etc. [20]. Some of the main challenges are:

1) SCALABILITY

There are several transactions increasing day by day in the blockchain, making more data to be stored. All the nodes have to store all the transactions for validation. Because of the block size restriction and the time taken to create a new block, blockchain can only process seven transactions per second. The blocks' actual capacity is deficient, and many small transactions could be delayed as miners prefer transactions with a higher transaction fee. The problem of scalability is, therefore, high [9].

2) PRIVACY LEAKAGE

In the blockchain, users' transactions are considered safe as they are made with created addresses instead of real identities. In the event of data leakage, users may produce multiple addresses. However, the blockchain cannot guarantee transactional privacy since the value of transactions is publicly visible for each public key. The anonymity of the payment must be strengthened in the blockchain [29]

3) REGULATIONS AND LAWS

The introduction of blockchain has brought many societal changes, including in legal and law systems. Blockchain triggered a series of legal issues by lagging legal supervision in the early stages of development. Proper laws and regulations can only be strengthened after a quick understanding of the blockchain characteristics. Through strengthening regulatory measures, most countries started to implement blockchain [69].

4) GOVERNANCE

Blockchain has vast implementation possibilities in terms of government and infrastructure and can be expected to transform government functions and roles. It also helps make less complex government organizational structures, the security of government data, and transparency of governance and service processes. Since the blockchain is a distributed network without a third party's need, it provides broader possibilities

TABLE 8. String Searching in Various Digital Libraries Along With Tracking Result.

S.No	Digital library searched	URL	Track	Search String
1	Science Direct	http://www.sciencedirect.com/	1234	"Blockchain with cloud
2	IEEE Explore	http://ieeexplore.ieee.org/	939	computing" OR "Cloud Platform
3	Google Scholar	https://scholar.google.com.pk/	37600	for Blockchain technology" OR
4	Springer Link	http://link.springer.com/	3100	"Blockchain Technology usage in
5	ACM	https://dl.acm.org/	47010	cloud" OR "Blockchain Cloud"

for policy advancement as it is a critical issue that needs immediate resolution [14].

IV. INTEGRATION OF CLOUD AND BLOCKCHAIN

A. BLOCKCHAIN SUPPORT FOR CLOUD COMPUTING

Blockchain integration with cloud computing brings us into the next era of data security and service availability. Blockchain overcomes most of the research issues of the cloud with its characteristics.

1) INTEROPERABILITY

In public clouds, internal communication is not allowed, and it makes many industries back off from using the cloud. When cloud integrated with blockchain, consider the different clouds as nodes. Inter-node communication is possible in the blockchain. All the nodes present in the same network share the data among themselves so that every node contains a copy of transactions. It brings us transparency into the network. They update every next transaction into the ledger, which publishes to all other nodes. In this way, companies can add any number of networks and can preserve the accessibility of the data, which brings authenticity into the network

2) DATA ENCRYPTION

We all know the data is decrypted before storing it in the cloud, which questions the data integrity. In the blockchain network, all the block data is turned into a hash code using cryptographic algorithms, and it generates a hash key for each block. Let us consider a scenario in which blockchain is used to preserve task scheduling in the cloud. To ensure timeliness and permanent data integrity, the control system that collects data from the task scheduling produces hash code and records it in the blockchain network immediately. Because the blockchain has the facility for block discovery consensus mechanisms, block data integrity is maintained. Each node in the network contains a copy of each transaction that provides us with the availability and persistence that helps the network withstand potential fault points and attacks. While cloud-collected data is reliable, the blockchain nodes maximize data availability and data validity by projecting it as an on-demand service with no downtime.

3) SERVICE LEVEL AGREEMENTS

These agreements in the cloud are favorable to the service provider or customer without equal justice. To solve this issue, we can make use of blockchain smart contracts. A smart

TABLE 9. Track of Article Types in Various Libraries on Selected String.

Library Name Publication type	Science Direct	IEEE Explore	Springer Link	ACM
Research Articles	806	189	493	34151
Conferences	6	658	736	NA
Book chapters	129	2	1651	NA

contract in blockchain helps to build trust between the parties who do not know each other. In a blockchain, Smart Contracts are defined as a program written in programmable languages that run in a container. The smart contract allows self-execution when a specific condition is met on all nodes present in the blockchain network. It also helps the parties predict the outcomes as the contract execution depends on the code available on a public network, and they are verifiable as they are already signed.

4) CLOUD DATA MANAGEMENT

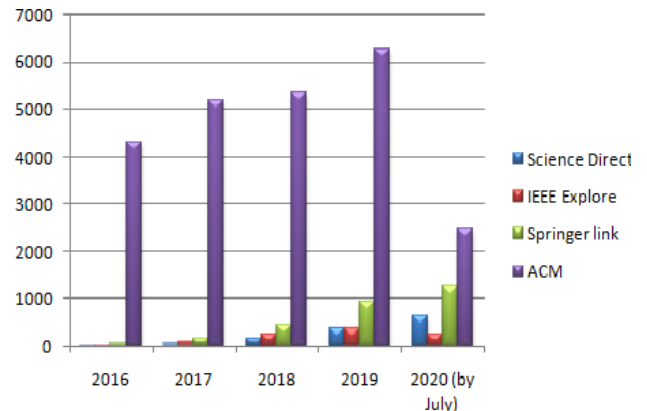
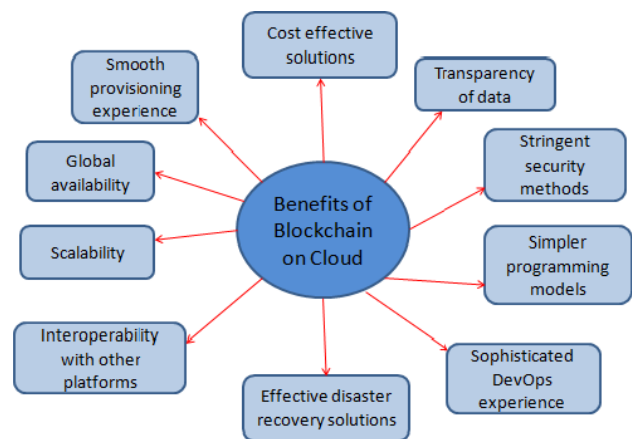
The data stored in the cloud is in a very unstructured manner. The data stored in the blockchain is a very structured manner. The data can be traced using the hash key generated for every block. Each block contains the previous block's hash key, and it's key to keep track of the network. The data in the block is validated and can be accessed by the nodes present in the network.

Cloud supports elasticity and can handle the fluctuations in computational loads when required. Using a Distributed ledger, this can be easily handled by managing a large number of events that cause a variety of smart contracts, ensuring service quality. Blockchain also ensures the user's anonymity, and the user's record can be safely removed from the system to prevent third party access to the user's information. The integration of the cloud with blockchain will also ensure that many businesses have confidence, and it would become an on-demand service.

B. ANALYTICAL SURVEY ON BLOCKCHAIN CLOUD

Based on Blockchain's supporting cloud computing, we can find different articles. To the best of our knowledge, we have conducted a literature survey for the first time on Blockchain-Cloud. Table 8 shows the track of articles available in different digital libraries along with our search string. Table 9 shows the track of different article types published in various libraries on selected literature. Below these tables, we have provided a bar graph depicting a year-wise analysis of the numbers of articles that have been published in different digital libraries. From all these analyses, we can conclude that there is exquisite research for merging blockchain with cloud computing.

In figure 3, we provided you with a graph depicting the year-wise analysis of articles published in digital libraries. Blockchain provides many essential benefits to cloud computing like data transparency, Authorization, and also provide cost-effective solutions. Some of the main benefits

**FIGURE 3.** Year-wise analysis of articles being published in digital libraries.**FIGURE 4.** Benefits that Blockchain providing to cloud.

that Blockchain is providing cloud services are depicted in Figure 4. As we already know that blockchain can be deployed in public, private, and community modes and provide decentralization, we have provided a comparative study on blockchain and cloud services based on different security requirements. One of the significant gaps in cloud services is Data Security. By this analysis, we could conclude that the data in the cloud would be more secure by adopting the Blockchain platform. In table 10, we provided this comparative analysis of Blockchain and Cloud-based on different security requirements.

Many Blockchain-Cloud applications can be applied in our daily activities, making our data more safe and secure. Various industries can use the services of Blockchain-Cloud. This integration can provide us with more storage flexibility, and at the same time, it keeps the validated data. Authorization to the network will be monitored, and also it increases the network resilience. In figure 5, we provided a mind map with different types of Blockchain Cloud Applications.

In figure 6, we depicted the flow of blockchain with cloud data as follows. Whenever there is a necessity to improve cloud data security, we can add blockchain services. The data that needs to be stored in the blockchain is divided into small chunks and then encrypted using hashing algorithms. Before adding the data to the chain, it is verified and

TABLE 10. Comparative Analysis of Blockchain and Cloud-Based on the Requirement.

Requirement	Cloud			Blockchain			Cloud	Blockchain
Design pattern	Deployment type						Centralized	Decentralized
	Public	Private	Community	Public	Private	Community		
Data Integrity	Less likely	Neutral	Less likely	More likely	Less likely	Neutral	Less likely	More likely
Trust	Less likely	Neutral	Less likely	More likely	Less likely	Neutral	Less likely	More likely
Non-repudiation	Less likely	Neutral	Less likely	More likely	Less likely	Neutral	Less likely	More likely
Privacy	Less likely	Neutral	Less likely	More likely	Less likely	Neutral	Less likely	More likely
Utilization	More Likely	NA	Neutral	More likely	Less Likely	Neutral	More Likely	Less likely
Immutability	Less likely	Neutral	Less Likely	More likely	Less likely	Neutral	Less likely	More likely
Scalability	More likely	NA	Neutral	More likely	Less likely	Neutral	More likely	More likely
Privacy	Less likely	Neutral	Less likely	More likely	Less likely	Neutral	Less likely	More likely
Flexibility	More likely	Less likely	Neutral	Less likely	More likely	Neutral	More likely	Less likely

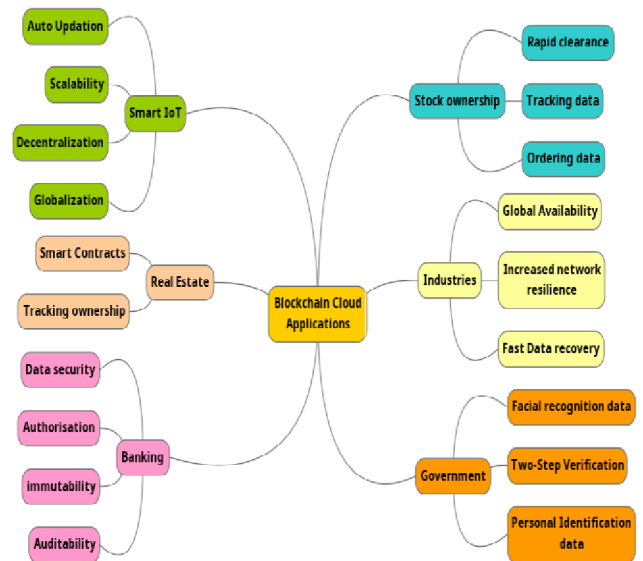


FIGURE 5. Mind map depiction of the different types of Blockchain Cloud applications.

validated by a consensus mechanism. Based on the requirement, the provider can use a Permissioned or Permissionless blockchain or public or private blockchain.

C. MODEL OF INTEGRATED ARCHITECTURE

In figure 7, we have shown the architecture of the integration of cloud computing with blockchain technology. The user interacts with the server with the help of the application layer. Suppose, when a user requests a transaction through the application layer, the transactions' details are stored by creating a block for each transaction. To add the block into the blockchain network, the blockchain network's data would be verified by blockchain network validating nodes. The validation will be done based on consensus. Once the block is considered legitimate, all other network nodes would be connected to the network and data sent. All blockchain data

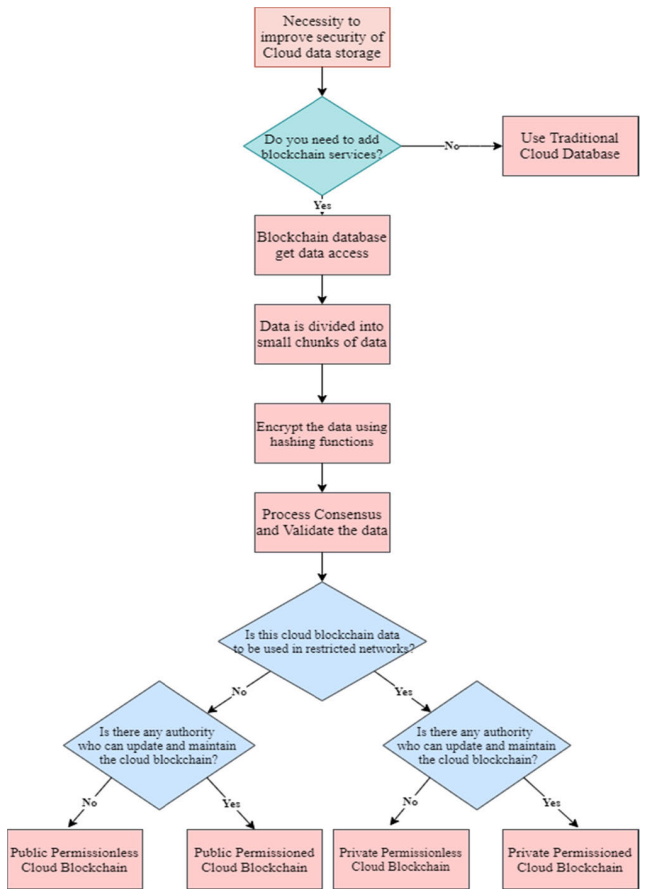


FIGURE 6. Flowchart providing process of Blockchain with cloud data.

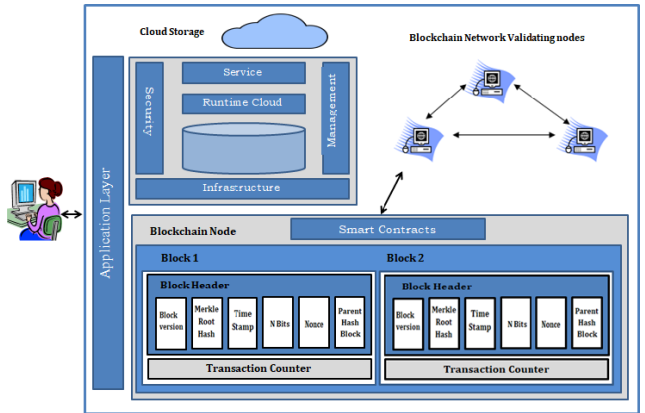


FIGURE 7. The architecture of cloud integrated with Blockchain.

is stored in blockchain protection cloud storage. Blockchain incorporation of the cloud provides data protection, transparency and also improves services.

V. CONCLUSION

Cloud computing is a well-known technology as it has existed for many years. But people are still struggling to overcome some challenges of cloud computing like data security, data management, interoperability, etc. Blockchain technology is an emerging technology well known for its security and authenticity, which are the main characteristics that are mak-

ing the world turn to its side. By integrating blockchain with cloud computing, there will be many advantages in usability, trust, security, scalability, data management, and many other advantages.

In this article, we briefly introduced cloud computing, blockchain technology. We discussed the benefits of integrating the blockchain network with a scalable cloud environment to enhance confidence, server service, data security, and user data management.

REFERENCES

- [1] A. Vatankeh Barenji, H. Guo, Z. Tian, Z. Li, W. M. Wang, and G. Q. Huang, "Blockchain-based cloud manufacturing: Decentralization," 2019, *arXiv:1901.10403*. [Online]. Available: <http://arxiv.org/abs/1901.10403>
- [2] A. Harshavardhan, T. Vijayakumar, and S. R. Mugunthan, "Blockchain technology in cloud computing to overcome security vulnerabilities," in *Proc. 2nd Int. Conf. I-SMAC (IoT Social, Mobile, Anal. Cloud)(I-SMAC) I-SMAC (IoT Social, Mobile, Anal., Cloud)(I-SMAC) 2nd Int. Conf.*, Aug. 2018, pp. 408–414.
- [3] A. Jabbari and P. Kaminsky, "Blockchain and supply chain management," Dept. Ind. Eng. Oper. Res., Univ. California, Berkeley, CA, USA, Tech. Rep., 2018.
- [4] M. K. R. Ingole and M. S. Yamde, "Blockchain technology in cloud computing: A systematic review," Sipna College Eng. Technol., Maharashtra, India, Tech. Rep., 2018.
- [5] C. Qiu, H. Yao, C. Jiang, S. Guo, and F. Xu, "Cloud computing assisted blockchain-enabled Internet of Things," *IEEE Trans. Cloud Comput.*, early access, Jul. 23, 2019, doi: [10.1109/TCC.2019.2930259](https://doi.org/10.1109/TCC.2019.2930259).
- [6] D. Dujak and D. Sajter, "Blockchain applications in the supply chain," in *SMART Supply Network*. Cham, Switzerland: Springer, 2019, pp. 21–46.
- [7] D. A. Fernandes, L. F. Soares, J. V. Gomes, M. M. Freire, and P. R. Inácio, "Security issues in cloud environments: A survey," *Int. J. Inf. Secur.*, vol. 13, no. 2, pp. 113–170, 2014.
- [8] D. B. Rawat, V. Chaudhary, and R. Doku, "Blockchain: Emerging applications and use cases," 2019, *arXiv:1904.12247*. [Online]. Available: <https://arxiv.org/abs/1904.12247>
- [9] D. K. Tosh, S. Shetty, X. Liang, C. Kamhoua, and L. Njilla, "Consensus protocols for blockchain-based data provenance: Challenges and opportunities," in *Proc. IEEE 8th Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON)*, Oct. 2017, pp. 469–474.
- [10] D. Tosh, S. Shetty, X. Liang, C. Kamhoua, and L. L. Njilla, "Data provenance in the cloud: A blockchain-based approach," *IEEE Consum. Electron. Mag.*, vol. 8, no. 4, pp. 38–44, Jul. 2019.
- [11] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," 2019, *arXiv:1906.11078*. [Online]. Available: <http://arxiv.org/abs/1906.11078>
- [12] E. Gaetani, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, "Blockchain-based database to ensure data integrity in cloud computing environments," Res. Center Cyber Intell. Inf. Secur., La Sapienza Univ. Rome, Rome, Italy, Univ. Southampton, Southampton, U.K., Tech. Rep., 2017.
- [13] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, and A. Peacock, "Blockchain technology in the energy sector: A systematic review of challenges and opportunities," *Renew. Sustain. Energy Rev.*, vol. 100, pp. 143–174, Feb. 2019.
- [14] D. Efanov and P. Roschin, "The all-pervasiveness of the blockchain technology," *Procedia Comput. Sci.*, vol. 123, pp. 116–121, 2018, doi: [10.1016/j.procs.2018.01.019](https://doi.org/10.1016/j.procs.2018.01.019).
- [15] F. Knirsch, A. Unterweger, and D. Engel, "Implementing a blockchain from scratch: Why, how, and what we learned," *EURASIP J. Inf. Secur.*, vol. 2019, no. 1, p. 2, Dec. 2019.
- [16] S. Sharma, G. Gupta, and P. R. Laxmi, "A survey on cloud security issues and techniques," 2014, *arXiv:1403.5627*. [Online]. Available: <http://arxiv.org/abs/1403.5627>
- [17] G. J. Katuwal, S. Pandey, M. Hennessey, and B. Lamichhane, "Applications of blockchain in healthcare: Current landscape & challenges," 2018, *arXiv:1812.02776*. [Online]. Available: <http://arxiv.org/abs/1812.02776>
- [18] H. Kaur, M. A. Alam, R. Jameel, A. K. Mourya, and V. Chang, "A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment," *J. Med. Syst.*, vol. 42, no. 8, p. 156, Aug. 2018.
- [19] H. Zhu, Y. Wang, X. Hei, W. Ji, and L. Zhang, "A blockchain-based decentralized cloud resource scheduling architecture," in *Proc. Int. Conf. Neww. Netw. Appl. (NaNA)*, Oct. 2018, pp. 324–329.
- [20] Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.
- [21] J. Kołodziej, A. Wilczynski, D. Fernandez-Cerero, and A. Fernandez-Montes, "Blockchain secure cloud: A new generation integrated cloud and blockchain platforms—general concepts and challenges," *Eur. Cybersecurity*, vol. 4, no. 2, pp. 28–35, 2018.
- [22] J. Park and J. Park, "Blockchain security in cloud computing: Use cases, challenges, and solutions," *Symmetry*, vol. 9, no. 8, p. 164, Aug. 2017.
- [23] J. Singh and J. D. Michels, "Blockchain as a service (BaaS): Providers and trust," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops (EuroSPW)*, Apr. 2018, pp. 67–74.
- [24] K. Bendiab, N. Kolokotronis, S. Shialeles, and S. Boucherka, "WiP: A novel blockchain-based trust model for cloud identity management," in *Proc. IEEE 16th Int. Conf. Dependable, Autonomic Secure Comput., 16th Int. Conf. Pervasive Intell. Comput., 4th Int. Conf. Big Data Intell. Comput. Cyber Sci. Technol. Congr. (DASC/PiCom/DataCom/CyberSciTech)*, Aug. 2018, pp. 724–729.
- [25] K. Chandrasekaran, *Essentials of Cloud Computing*. Boca Raton, FL, USA: CRC Press, 2014.
- [26] J. Truby, "Decarbonizing bitcoin: Law and policy choices for reducing the energy consumption of blockchain technologies and digital currencies," *Energy Res. Social Sci.*, vol. 44, pp. 399–410, Oct. 2018.
- [27] M. Niranjanamurthy, B. N. Nithya, and S. Jagannatha, "Analysis of blockchain technology: Pros, cons and SWOT," *Cluster Comput.*, vol. 22, no. 6, pp. 14743–14757, Nov. 2019.
- [28] M. Risius and K. Spohrer, "A blockchain research framework," *Bus. Inf. Syst. Eng.*, vol. 59, no. 6, pp. 385–409, 2017.
- [29] C. V. N. U. B. Murthy and M. L. Shri, "A survey on integrating cloud computing with blockchain," in *Proc. Int. Conf. Emerg. Trends Inf. Technol. Eng. (IC-ETITE)*, Feb. 2020, pp. 1–6.
- [30] N. Sanghi, R. Bhatnagar, G. Kaur, and V. Jain, "BlockCloud: Blockchain with cloud computing," in *Proc. Int. Conf. Adv. Comput., Commun. Control Netw. (ICACCCN)*, Oct. 2018, pp. 430–434.
- [31] N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain-based publicly verifiable cloud storage," in *Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP)*, Jun. 2019, pp. 381–386.
- [32] M. Westerlund and N. Kratzke, "Towards distributed clouds: A review about the evolution of centralized cloud computing, distributed ledger technologies, and a foresight on unifying opportunities and security implications," in *Proc. Int. Conf. High Perform. Comput. Simulation (HPCS)*, Jul. 2018, pp. 655–663.
- [33] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Bitcoin, Saint Kitts, Saint Kitts and Nevis, Tech. Rep., 2008.
- [34] S. Nanayakkara, S. Perera, and S. Senaratne, "Stakeholders' perspective on blockchain and smart contracts solutions for construction supply chains," in *Proc. CIB World Building Congr.*, 2019, pp. 1–11.
- [35] L. Popovski, G. Soussou, and P. B. Webb, "A brief history of blockchain," Patterson Belknap Webb & Tyler, New York, NY, USA, Tech. Rep., 2014.
- [36] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, "A survey on privacy protection in blockchain system," *J. Netw. Comput. Appl.*, vol. 126, pp. 45–58, Jan. 2019.
- [37] Q. K. Nguyen and Q. V. Dang, "Blockchain technology for the advancement of the future," in *Proc. 4th Int. Conf. Green Technol. Sustain. Develop. (GTSD)*, Nov. 2018, pp. 483–486.
- [38] G. Zhao, S. Liu, C. Lopez, H. Lu, S. Elgueta, H. Chen, and B. M. Boshkoska, "Blockchain technology in agri-food value chain management: A synthesis of applications, challenges and future research directions," *Comput. Ind.*, vol. 109, pp. 83–99, Aug. 2019.
- [39] A. Rathore and N. Lakhnotra, *Blockchain: Consensus Protocols, Attacks, and Mitigation*. [Online]. Available: <https://www.academia.edu>
- [40] H. A. Reddy, K. R. Bhat, M. Pavithra, N. Mandara, and S. Ramya, "Blockchain for financial applications using IoT," *Int. Res. J. Comput. Sci.*, vol. 6, no. 6, pp. 369–377, 2019.
- [41] S. Kirkman, "A data movement policy framework for improving trust in the cloud using smart contracts and blockchains," in *Proc. IEEE Int. Conf. Cloud Eng. (IC2E)*, Apr. 2018, pp. 270–273.

- [42] S. Nayak, N. C. Narendra, A. Shukla, and J. Kempf, "Saranyu: Using smart contracts and blockchain for cloud tenant management," in *Proc. IEEE 11th Int. Conf. Cloud Comput. (CLOUD)*, Jul. 2018, pp. 857–861.
- [43] S. Wang, X. Wang, and Y. Zhang, "A secure cloud storage framework with access control based on blockchain," *IEEE Access*, vol. 7, pp. 112713–112725, 2019.
- [44] W. Venters and E. A. Whitley, "A critical review of cloud computing: Researching desires and realities," *J. Inf. Technol.*, vol. 27, no. 3, pp. 179–197, Sep. 2012.
- [45] Y. Lu, "The blockchain: State-of-the-art and research challenges," *J. Ind. Inf. Integr.*, vol. 15, pp. 80–90, Sep. 2019.
- [46] D. Yadav and S. Behera, "A survey on secure cloud-based E-health systems," *EAI Endorsed Trans. Pervas. Health Technol.*, vol. 5, no. 20, May 2020, Art. no. 163308.
- [47] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data (BigData Congress)*, Jun. 2017, pp. 557–564.
- [48] L. Zhu, K. Gai, and M. Li, "Exploring topics in blockchain-enabled Internet of Things," in *Blockchain Technology in Internet of Things*. Cham, Switzerland: Springer, 2019, pp. 109–114.
- [49] S. Kumar, N. Darshini, S. Saxena, and P. Hemavathi "VOTEETH: An E-voting system using blockchain," *Int. Res. J. Comput. Sci.*, vol. 6, no. 6, pp. 11–18, Jun. 2019.
- [50] C. Surianarayanan and P. R. Chelliah, *Essentials of Cloud Computing: A Holistic Perspective*. New York, NY, USA: Springer, 2019.
- [51] S. Mukherji and S. Srivastava, "Pros and cons of cloud computing technology," *Int. J. Sci. Res.*, vol. 5, no. 7, pp. 848–851, Jul. 2016.
- [52] M. R. Prasad, R. L. Naik, and V. Bapuji, "Cloud computing: Research issues and implications," *Int. J. Cloud Comput. Services Sci.*, vol. 2, no. 2, p. 134, Jan. 2013.
- [53] C. T. S. Xue and F. T. W. Xin, "Benefits and challenges of the adoption of cloud computing in business," *Int. J. Cloud Comput., Services Archit.*, vol. 6, no. 6, pp. 1–15, Dec. 2016.
- [54] M. Nazir, "Cloud computing: Overview & current research challenges," *IOSR J. Comput. Eng.*, vol. 8, no. 1, pp. 14–22, 2012.
- [55] H. Alzahrani, "A brief survey of cloud computing," *Global J. Comput. Sci. Technol.*, vol. 16, no. 3, pp. 11–16, 2016.
- [56] S. Sindhu and D. Sindhu, "Cloud computing models and security challenges," *Int. J. Eng. Sci.*, vol. 7, no. 4, p. 10934, 2014.
- [57] C. R. Cunha, E. P. Morais, J. P. Sousa, and J. P. Gomes, "The role of cloud computing in the development of information systems for SMEs," *J. Cloud Comput.*, vol. 2017, pp. 1–7, Feb. 2017.
- [58] S. Kumar and R. H. Goudar, "Cloud computing-research issues, challenges, architecture, platforms, and applications: A survey," *Int. J. Future Comput. Commun.*, vol. 1, no. 4, p. 356, 2012.
- [59] J. Y. Astier, I. Y. Zhukov, and O. N. Murashov, "Smart building management systems and the Internet of Things," *Inf. Technol. Secur.*, vol. 3, pp. 17–28, 2017.
- [60] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *Int. J. Inf. Secur.*, vol. 1, no. 1, pp. 36–63, 2001.
- [61] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2016, pp. 3–16.
- [62] P. S. Maharjan, "Performance analysis of blockchain platforms," Howard R. Hughes College Eng., Univ. Nevada, Las Vegas, Las Vegas, NV, USA, Tech. Rep., 2018.
- [63] S. Pongnumkul, C. Siripanpornchana, and S. Thajchayapong, "Performance analysis of private blockchain platforms in varying workloads," in *Proc. 26th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul. 2017, pp. 1–6.
- [64] M. Scherer, "Performance and scalability of blockchain networks and smart contracts," Umeå Univ., Umeå, Sweden, Tech. Rep., 2017.
- [65] J. R. Q. Verkleij, "A decision support system for blockchain platform selection," Utrecht Univ., Utrecht, The Netherlands, Tech. Rep., 2018.
- [66] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Gener. Comput. Syst.*, vol. 88, pp. 173–190, Nov. 2018.
- [67] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Integration of blockchain and cloud of things: Architecture, applications and challenges," 2019, *arXiv:1908.09058*. [Online]. Available: <http://arxiv.org/abs/1908.09058>
- [68] M. Numan, F. Subhan, W. Z. Khan, S. Hakak, S. Haider, G. T. Reddy, A. Jolfaei, and M. Alazab, "A systematic review of clone node detection in static wireless sensor networks," *IEEE Access*, vol. 8, pp. 65450–65461, 2020.
- [69] L. Zhu, K. Gai, and M. Li, "Blockchain and the Internet of Things," in *Blockchain Technology in Internet of Things*. Cham, Switzerland: Springer, 2019, pp. 9–28.
- [70] D. Agrawal, A. A. El Abbadi, S. Das, and A. J. Elmore, "Database scalability, elasticity, and autonomy in the cloud," in *Proc. Int. Conf. Database Syst. Adv. Appl. Berlin, Germany: Springer*, 2011, pp. 2–15.
- [71] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, "Bitcoin-NG: A scalable blockchain protocol," in *Proc. 13th USENIX Symp. Netw. Syst. Design Implement.*, 2016, pp. 45–59.
- [72] H. Halaburda and G. Haeringer, "Bitcoin and blockchain: What we know and what questions are still open," NYU Stern School Business, New York, NY, USA, Tech. Rep., 2019.



CH. V. N. U. BHARATHI MURTHY is currently a Research Associate with the School of Information Technology and Engineering, VIT, Vellore. Her current research interests include cloud computing, Blockchain technology, and the Internet of Things.



M. LAWANYA SHRI is currently an Associate Professor with the School of Information Technology and Engineering, VIT, Vellore, India. She has published more than 40 research articles in international journals and 15 conference proceedings. She has published several books chapters and coauthored one book *Computer Architecture for Beginners*. Her research interests include Blockchain technology, artificial intelligence, cloud computing, web services, and the Internet of Things. She serves as an Editorial Board Member for *Informatics in Medicine Unlocked* (Elsevier).



SEIFEDINE KADRY (Senior Member, IEEE) received the bachelor's degree in applied mathematics from Lebanese University, in 1999, the M.S. degree in computation from Reims University, France, in 2002, and also from EPFL, Lausanne, the Ph.D. degree from Blaise Pascal University, France, in 2007, and the HDR degree in engineering science from Rouen University, in 2017. His current research interests include education using technology, system simulation, operation research, system prognostics, stochastic systems, and probability and reliability analysis. He is an IET Fellow. He is an ABET Program Evaluator, an ACBSP Program Reviewer, and a NTCM Program Reviewer.



SANGSOON LIM received the Ph.D. degree in electrical engineering and computer science from Seoul National University, South Korea, in 2013. From 2013 to 2017, he has been a Senior Engineer with Samsung Research, Seoul, South Korea. He is currently an Assistant Professor with the Department of Computer Engineering, Sungkyul University, Anyang, South Korea. His current research interests include wireless/mobile networks, the Internet of Things, network management, resource optimization, machine learning, and big data analysis.

...