Contents lists available at GrowingScience

International Journal of Data and Network Science

homepage: www.GrowingScience.com/ijds

Integrated cloud computing and blockchain systems: A review

Mohammad Alshinwan[a*], Ahmed Younes Shdefat[b*], Nour Mostafa[b*], Abdullah A.M AlSokkar[c], Tamam Alsarhan[a] and Dmaithan Almajali[c]

[a]*Faculty of Information Technology, Applied Science Private University, Amman 11931, Jordan*
[b]*College of Engineering and Technology, American University of the Middle East, Egaila 54200, Kuwait*
[c]*Faculty of Business, Applied Science Private University, Amman 11931, Jordan*

C H R O N I C L E

Article history:
Received: October 12, 2022
Received in revised format: October 28, 2022
Accepted: December 17, 2022
Available online: December 18, 2022

Keywords:
Cloud Computing
Blockchain Applications
Blockchain-as-a-Service
Smart Contract
Blockchain Platforms

A B S T R A C T

Blockchain technology is one of the crypto-currency technologies that has received a lot of attention. It has also found use in various applications, including the Internet of Things (IoT) and Cloud computing. Nonetheless, Blockchain has a significant scalability issue, restricting its ability to support services with various transactions. On the other hand, cloud computing is the on-demand availability of shared computer system resources, although issues now beset it in automation, processes, management, policies, and human aspects. Combining cloud computing and blockchain technology into a single system can improve network control, task scheduling, data integrity, resource management, pricing, fair payment, and resource allocation. In this article, we offered a comprehensive and up-to-date survey of cloud computing and Blockchain integration, a critical service for business applications due to the benefits of privacy, security, and service support. The lack of a comprehensive assessment examining the significance of BaaS platforms used in cloud computing prompted this review. We focus on the various BaaS tools that are currently in use. This report also examines the most common BaaS platforms incorporating Blockchain as a cloud service, such as Alibaba, Oracle, Azure, Amazon, and IBM. Furthermore, this research highlighted some major technological issues associated with merging Blockchain with cloud computing.

1. Introduction

Cloud computing supplies computer services over the Internet, including servers, storage, databases, networking, software, analytics, and intelligence, to provide quicker innovation, adaptable resources, and scale economies (Prianga et al., 2018). There are two parts to cloud computing: the front end and the back end. The backend consists of servers, computers, databases, and central servers. At the same time, the front end allows a user to access data stored in the cloud using a web browser or cloud computing software (Al Shinwan et al., 2022). The main element of cloud computing that oversees safely keeping data and information is known as the backend. There are several advantages to cloud computing. These advantages include the services' affordability, scalability, and accessibility (Pen et al., 2023).

Regarding accessibility, cloud computing boosts mobility because most cloud services are self-service and available upon request. Accessing your documents anywhere in the world without carrying them around allows workers to access them from various locations (Sanghi et al., 2018). Scalability is made possible by cloud computing, which is a terrific solution since it

* Corresponding author.
E-mail address: m_shinwan@asu.edu.jo (M. Alshinwan) ahmed.shdefat@aum.edu.kw (A. Y. Shdefat) nour.moustafa@aum.edu.kw (N. Mostafa)

ISSN 2561-8156 (Online) - ISSN 2561-8148 (Print)

doi: 10.5267/j.ijdns.2022.12.016

enables businesses to swiftly and efficiently scale up or down their IT departments in response to changing business needs (Al Shinwan et al., 2021). Because it lowers the cost of purchasing and maintaining equipment, it is economical.

Additionally, since we will be utilizing the cloud provider's staff's knowledge, we won't need massive IT teams to manage your cloud data center operations (Alias et al., 2018). Although its many advantages, such as quick software upgrades, fewer maintenance issues, reliable data, and cost-effectiveness, cloud computing has a significant challenge regarding the security and safety of stored data. Blockchain technology is one approach to solving the security issue with cloud computing. The blockchain was initially developed for Bitcoin's trade; its applications go well beyond cryptocurrencies (AL-Sous et al., 2022). A trustworthy, challenging-to-hack record of transactions is the blockchain. Although the technology is still new, it has the potential to be revolutionary (Lokhandwala, 2018). It is based on share-out ledger technology, which uses a peer-to-peer network to store information securely. Blockchain ledgers may store various data, including manifests, identities, logistical loans, land titles, and nearly any valuable Information. The data is visible to all parties, who may use consensus techniques to accept or reject it. Verify that data is recorded into the ledger as a collection of "blocks" and kept in an immutable chronological "chain".

Furthermore, Blockchain technology is integrated with several metaheuristics algorithms (MA). Currently, the MA algorithm is implemented in different fields, such as mechanical engineering (Shehab et al., 2020), civil engineering (Abualigah, Shehab, Alshinwan, & Alabool, 2020), energy (Abualigah et al., 2021), big data (Abualigah et al., 2021), and cloud computing (Abualigah, Shehab, Alshinwan, Alabool, et al., 2020). For instance, the Salp Swarm Optimization algorithm is integrated with blockchain to solve the routing problem in wireless sensor networks (Revanesh & Sridhar, 2021). In this paper, Syafruddin et al. (2019) proposed an approach to solve the Traveling Salespersons Problem using Blockchain and Particle swarm optimization. In medical data processing, (Khan et al., 2021) presented a method to improve the quality of service based on a novel MA algorithm with a Blockchain smart contract concept.

Three essential characteristics define distributed ledgers. It is first documented by time-stamping the data that has been stored. Second, the transaction ledger is open to everyone, making it transparent. Third, the ledger is distributed among several computers, known as nodes, making it decentralized (Harshavardhan et al., 2018; Altamimi et al., 2022). It will be challenging to attack blockchain because of its share-out and encrypted features. This is encouraging for IoT and commercial security, according to (Chandrasekaran, 2014). This paper discusses cloud computing, how it functions, its most significant challenges, and how blockchain technology might help secure it. Additionally, we'll talk about how blockchain technology works and how to use it to defend cloud computing. All of it will be a review of earlier research that has been conducted.

The rest of the paper is organized as follows. In section 2, we introduce cloud computing and Blockchain. In section 3, we give an overview of Blockchain-as-a-Service. In section 4, we review the Blockchain Tools, such as Etherrum, Quorum, and Hyperledger. In section 5, we look into the Blockchain- based cloud platforms. In section 6, we outline the challenges in blockchain-Cloud integration, and the concluding remarks in section 7.

2. An Introduction to Cloud Computing and Blockchain Systems

In this section, a brief overview of Cloud computing and blockchain is presented.

2.1. Cloud Computing

The NIST defined cloud computing as a model that allows everywhere, available, on-demand network access to a distributed pool of computer resources. These resources could be storage, servers, networks, services, and applications, which can provide a service to the users with minimum service provider interaction or management potential.

2.1.1. Principles of Cloud computing

The NIST defined three primary principles for cloud computing, five of them are essential characteristics that "promote cloud computing," four deployment models, and finally, three outstanding and crucial services.

2.1.2. The five essential characteristics of cloud

There are five prerequisites for cloud computing. The phrase "vital" means that if any of these conditions aren't met, cloud computing isn't taking place (Liu et al., 2011):

1. On-demand self-service: Without contacting the providers of each service, a client can automatically provide computer resources as needed, such as network storage and server time (Alsokkar et al., 2023).

2. Wide network access: Through standardized protocols, resources are made available over networks and encouraged for use by different consumer platforms, thin or thick (e.g., personal digital assistants, laptops, and mobile phones).

3. Resource pooling: A cloud service provider's computer resources are "pooled" through virtualization or a multitenant model to serve a number of clients, "with unique virtual and physical resources dynamically assigned and reassigned according to consumer demand". In a pool-based arrangement, physical resources are effectively "unseen" by customers. As a result, the user becomes autonomous since they frequently need more control or knowledge of how exactly to place the available resources. However, they might be able to identify the location more abstractly (e.g., country, state, or datacenter). For instance, customers want assistance choosing the location in the cloud where their data will be stored.

4. Rapid elasticity: For users, the provision of capabilities shifts from being persistent to elastic and, in some situations, automatically to being quickly scaled out and released. Additionally, their resources seem limitless to them; consumption can abruptly increase to satisfy peak demands whenever necessary.

5. Measured service: By applying a metering capability relevant to the type of service at a particular level of abstraction, cloud systems automatically manage and optimize resource use (e.g., bandwidth, processing, storage, and active user accounts). Resource usage can be tracked, organized, and reported, which will help both the service provider and the client.

2.1.3. Four Cloud Deployment Models

The ownership of the service, the size of the cloud resources, and the restrictions on client access all affect how cloud services are distributed. The cloud community has recently described four cloud deployment models. Fig. 1 illustrated the Cloud Deployment.

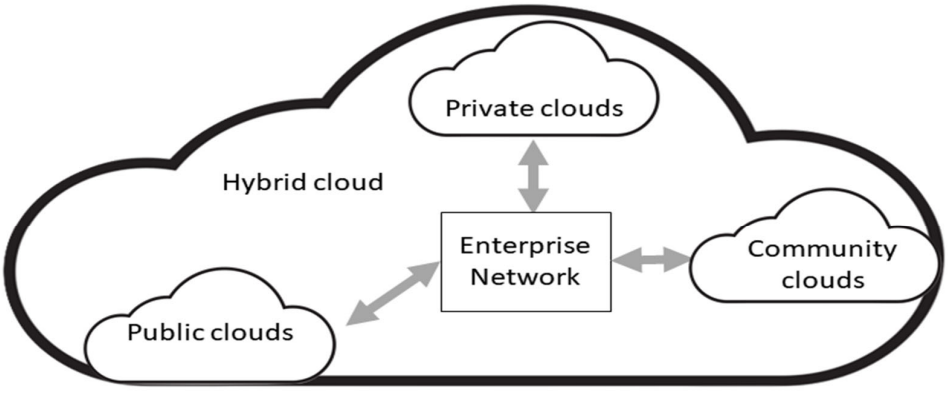

Fig. 1. Cloud Deployment

1.

1. Public clouds: Third parties' own public clouds, making the cloud substructure available for unrestricted use by everyone (Vacca, 2016). Further, this is carried out by a designated service provider under the umbrella of utilities with a pay-per-use consumption model. Numerous well-known cloud services, such as Amazon EC2, Rackspace Cloud Suite, Microsoft, and Force.com, are available on public clouds. In this situation, multiple businesses or individuals may share a physical resource, like a server, thanks to multi-tenancy and virtualization. Security is complex because cloud clients depend on the cloud computing provider to ensure data and calculate isolation across many clients (Dillon et al., 2010).

2. Private clouds are created, maintained, and controlled by institutions for internal usage only to support their business processes. It may be on- or off-site, owned, maintained, and run by organizations, individuals, or some compound. This concept is being used by public, private, and government institutions worldwide to exploit cloud benefits like flexibility, cost reduction, agility, and so on. An organization may decide to create a private cloud for a number of reasons. First, make full and efficient use of existing resources. Second, due to worries about security, particularly data protection and confidentiality, many firms opt for the private cloud. Third, moving data from a local IT system to a public cloud still costs a lot. Fourth, companies must have full control over all actions beyond their firewalls. Lastly, academics regularly create private clouds for training and research (Dillon et al., 2010).

3. Community clouds: Organizations and groups involved in collaborative projects, systems, or research commonly construct community clouds because they require a central cloud computing facility for project development, management, and execution (Dillon et al., 2010).

4. The term "hybrid cloud" refers to a cloud infrastructure that combines a variety of cloud infrastructures (private, communal, or public), each of which is a distinct entity but is interconnected to the others via common or proprietary protocols to enable data and application portability. For illustration, because the personal cloud is running at a high capacity while having a private cloud to store and manage intellectual property information, institutions may use a general cloud service to rent servers to undertake results processes. For communications between the two cloud environments, the institutions need to use a secure protocol (Dillon et al., 2010).

2.1.4 Service Offering Models

Cloud services are provided in various models, including infrastructure, platform, application, etc. These services are delivered over the Internet and consumed in real-time. These services include:

1. Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and some add Hardware as a Service (HaaS) and Data storage as a Service (DaaS).

2. Software as a Service (SaaS) is a multi-tenant platform that provides software (Harshavardhan et al., 2018). Users of applications can access the hosting medium where cloud consumers store their apps across networks using various devices (such as a web browser, PDA, etc.) (Dillon et al., 2010). Cloud service users have no effective management over how cloud software runs and how securely it accesses data, and the cloud software vendor bears full accountability. The customer can use apps from the provider running on cloud infrastructure, including network, storage, operating systems, servers, and even unique application capability, with the potential except for a small number of user-specific program configuration options (Chandrasekaran, 2014).

3. Platform as a Service (PaaS): The ability to upload programs created by the end-user or purchased by them using the services, libraries, programming languages, and tools provided by the supplier. The end-user controls the post-applications and maybe even the formation settings for the application-hosting environment. Still, they need to manage or control the fundamental cloud infrastructure. In another sense, a packaged, ready-to-use operating system or programming framework is what it means. The PaaS provider provides networks, storage, and servers, which also manage maintenance and scalability levels. The end user typically pays for services. Examples of PaaS providers are Google App Engine and Microsoft Azure Services.

4. Infrastructure as a Service (IaaS): Information technology infrastructures (processing, storage, networks, and other significant computer resources) are made available in the IaaS cloud for usage by cloud end users. In the IaaS cloud, virtualization is widely utilized to combine and separate physical resources on-demand to fulfill fluctuating resource demands from cloud end users. Setting up distinct virtual machines (VM) that are isolated from both the underlying hardware and other VMs is the fundamental strategy of virtualization. The multi-tenancy category aims to change the application software architecture so that several cases (from various cloud customers) can run on a single application; however, this strategy differs from that category in that it focuses on a single application (i.e., the same logic machine). Amazon's EC2 is an illustration of IaaS (Dillon et al., 2010).

5. Hardware as a service (HaaS) is favorable to enterprise clients since that saves them money as data centers don't need to be set up or maintained (Harshavardhan et al., 2018). IT hardware, or even a whole server farm, as a pay-as-you-go membership benefit that can be scaled up or down to address your needs (Haber & Stornetta, 1990). However, given the quick advancements in equipment virtualization, IT mechanization, and utility metering and estimating, the idea of equipment as a benefit, or what we should name HaaS, may be ready for prime time. 6. Data storage as a Service (DaaS): The DaaS can be viewed as a particular IaaS kind. The driving force behind DaaS is the ability for consumers to just pay for the services they actually use, eliminating the need for additional fees for software licenses, servers, and other services.

2.1.5. Security in Cloud Computing

Grid computing, distributed computing, parallel computing, utility computing, and simulation technology have all contributed to a new type of computational computing. Other computer technologies also have many benefits, like high expansion, virtualization, data storage, and huge computing, and they are also very affordable and dependable. The cloud computing security is-sue is essential since it slows down the industry's progress. The crucial security issue with cloud computing is the availability of services and data privacy. A single security strategy cannot resolve cloud computing security challenges; instead, a variety of established and cutting-edge technologies and techniques must be used to safeguard the entire cloud computing system. Data security can be ensured through cloud computing; thus, the user no longer needs to protect the data alone. As a result, cloud computing must guarantee the security of data kept there. Many businesses, including Google, IBM, Microsoft,

Amazon, VMware, and EMC, offer cloud computing platforms. The cloud system utilizes the internet to function, and security issues and problems with internet security can be found there. It is identical to the conventional approach used in computers. Cloud computing is concerned about the security of personal user data since it can lead to other specific and new security issues (Harshavardhan et al., 2018). On the one hand, customers' personal and business data providers are of the highest importance because security alone cannot solve the issue. Trust is a separate issue that raises additional worries when using the cloud service. Several variables affect cloud confidence, including automation, management, human factors, processes, and policies. One of the security issues with cloud computing is the usage of encryption in security computing procedures.

2.2. Blockchain

Blockchain is renowned for its decentralized method, which enables transactions to be completed without the involvement of a third party. We certify that blockchain technology can be utilized to increase the security of cloud computing. Before examining the interactions between Blockchain and Cloud computing, we will first discuss the concept of Blockchain, its structure, traits, specific applications, security challenges, and implementation (Xie et al., 2020).

2.2.1. The concept of Blockchain

The Blockchain encourages users to update the ledgers to validate the integrity when dealing with new transactions. Further, users can maintain related information with each leader. Due to the use of the peer-to-peer communication approach in the Blockchain, high costs are eliminated through peer-to-peer transactions that a third party does not authorize. Because many individuals own the transaction information, it is more difficult to hack. Thus, it ensures promptness, reduces security costs, and approves and records transactions automatically. The system can also be easily connected, enlarged, and deployed using open-source software. Additionally, transaction records can be freely viewed, making the transactions public and lowering regulatory expenses. Blockchain technologies combine peer-to-peer networks with a distributed consensus method to solve the classic problem of synchronizing dispersed databases (Abuaddous et al., 2018). Blockchain technologies include not just one technology but cryptography, mathematics, algorithms, and economic models. A comprehensive multi-area infrastructure is being built. Blockchain technology contains six essential components, including decentralization, openness, transparency, autonomy, anonymity, and immutability, as shown in the following (Lin & Liao, 2017):

1. Decentralized: The fundamental concept in the Blockchain is that no central node can handle the transaction. Instead, the nodes are based on distributed fashion to update and register and store the data.

2. Transparent: Transparent means the nodes can see each other regarding the data record update.

3. Open Source: As an open-source technology, users can build the application easily, and the applications are accessible to everyone.

4. Autonomy: Blockchain transactions are updated and transmitted safely. Each node in the network is trusted on the entire system, and other nodes are not allowed to interfere with the transaction.

5. Immutable: Records will be preserved indefinitely and cannot be altered until more than 51%of the nodes can be taken over simultaneously.

6. Anonymity: Blockchain technologies have resolved the node-to-node trust issue, enabling anonymous data transfer or even transactions with the knowledge of a person's blockchain address.

Blockchain connects a collection of records through hashing. Each block has a header and a body, making up a structure. The preceding and current blocks' hash values and nonce values are included in the header (Raul et al., 2019; Ingole & Yamde, 2018). The consensus function is a method that forces all blockchain nodes to agree on the same message. This may ensure that the most recent block was properly added to the chain, ensure that the message saved by each node was the same, ensure that a "fork attack" will not occur, and even defend against malicious assaults. The distributed network's nodes could all instantly detect any unauthorized data alteration. The foundation of blockchain technology is decentralized, meaning the data is kept as a distributed database. Based on this architecture, data modification is very hard. In addition, the user should participate in verifying the data's validity. The data is retrieved from the database using the index method, and another hash value is used to build the chain and link the block with each other (Park & Park, 2017). Three broad categories can be used to classify blockchain technologies, according to (Lin & Liao, 2017):

1. Public blockchain: Anyone can examine a transaction, confirm it, and participate in the consensus-building process. Ethereum and Bitcoin both use public blockchains.

2. Consortium blockchains: Blockchains used in consortiums allow the authority node to be selected in advance, are

frequently used in business-to-business relationships and can be viewed as partially decentralized. R3CEV and Hyperledger are two consortium Blockchains.

3. Private Blockchain: A private blockchain will have limited nodes that can participate in it, and it will also have rigorous authority management rules for data access. Any Blockchain provides benefits, regardless of the type.

Because of its convenience, public Blockchain is sometimes required. Nevertheless, depending on the service we offer or the location where we utilize it, we can occasionally need private control, such as consortium blockchains or private Blockchain.

2.2.2 How Blockchain Works

Blockchain utilizes the ledger to save all transactions in chronological order. These transactions |transaction (The process of verifying the transaction is called Mining) (Macdonald et al., 2017). The node performs the Mining called the miner; miners verify the transaction for both the user and the transaction. Further, the first miner accomplishes the mining process and can publish the result as a new verified block to the network, and the rest of the miners will agree that the block is verified and accepted to join the chain (Nakamoto & Bitcoin, 2008). The workflow's components are described below.

Transaction request by the user

As mentioned previously, users will add their digital signature to the transaction. In addition, users use private only visible to them, and the public key is shared with the rest of the users in the network. The digital signature is generated by hashing the transaction value and the private key to start the transaction. Then, the transaction is broadcast to the miners to verify the transaction (Jimi, 2018).

Validation of transaction by the miner

Miners verify the received transaction and add the block to the ledger with the digital signature. To ensure the user's identity, miners verify the transaction based on the public key shared by the user itself. Further, the transaction is reviewed to evade the double spending problem. A digital signature is created by hashing the block data that begins with a particular number of consecutive zeroes (mining). The digital signature value of the block is used to add the new block after the verification process. The hash output should have a specific number of zeroes to check the number of zeros the Nonce is used. The Nonce is a field in the block containing 32-bit used only once in Blockchain to check the number of zeroes in the final hash output. Along with the list of transactions, the block header contains the following additional data, as shown in Fig. 2:

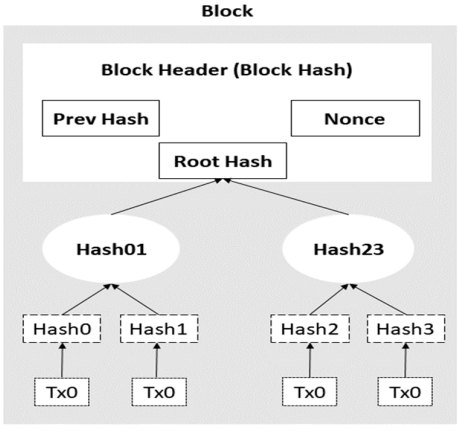

Fig. 2. Block fields

1. Previous Hash: This field is used to link the previous block and the new block, which is defined as a reference parent.
2. Time-stamp: The block's creation time.
3. Tx Root: The hash value of each block's verified transactions is contained in this field and known as the Merkle root (Merkle, 1987).
4. Version: refer to the transmission protocol utilized by the node for block inclusion in the chain.
5. This is a number used once only and refers to the hash value of the previous lock hashing result and transaction. For unique identification, the leading zeros are used.
6. Bits: This domain describes the grade of the complexity of the selected consensus approach.

After the miner verifies, the hashes block publishes the block to the rest miners in the same network. The miners who received the block will hash it again to verify its authenticity. When several miners simultaneously hash the block, they create an agreement and select the hash (Ismail et al., 2019). The network checks that the new transaction is authentic and guards against invalidating the preceding transaction in order to make sure that only legitimate transactions are added to the Blockchain. Blockchain only adds new data blocks after network computers have agreed that a transaction is genuine. Other voting mechanisms contribute to the network's consensus; the most popular of them is proof of work based on the amount of processing power provided to the system. When a block is set to the ledger, it adds permanently and can't be removed, allowing all network users to examine and verify the transactions contained therein. The hierarchical list known as the Blockchain is used to store data in a manner resembling that of a distributed database. Considering that the user of the networks store and validate the Blockchain, it is made to be easily manipulable. The ledger comprises a header and a body for each block; the header includes a timestamp, a nonce, and the hash values for the current and prior blocks. The body component is made up of transactions. The block data is retrieved using the index method (Ingole & Yamde, 2018). Such blocks, which are cryptographically sealed with a digital fingerprint created by a hashing function, are gathered into a blockchain, which is a constantly expanding, spread, shared ledger. The new block is "chained" to the previous block using the hash value. The hosts that link to the Blockchain—confirm a transaction's validity by the regulations of the governing logic or smart contract. The method by which new records are added to the ledger through verification is the distinctive feature of many blockchain platforms. Blockchain technology has several appealing features for the banking and financial services industries. These resilient systems can function as decentralized networks without a single failure point and a central server. They have integrity and don't need to trust a third party to achieve transactions because they run on spread open-source protocols (Treleaven et al., 2017).

2.2.3. Application of Blockchain

As blockchain technology develops and applications, we may use it for growth. It joins disruptive technologies that can potentially have unforeseen social effects, such as big data, the Internet of Things, intelligent personal assistants, and autonomous vehicles. Although cryptocurrencies first gained broad notice, blockchain technology has many additional applications. Smart contracts, for instance, could be used as the management framework for various documents, such as wills, conveyances, and medical records, as well as for public documents like vehicle registrations, passports, land titles, and building permits. Further, for private documents such as medical records and other legal documents. Blockchain technologies have a wide range of applications outside the financial sector (Treleaven et al., 2017).

Digital Currency. Bitcoin's data structure and transaction mechanism are constructed using blockchain technologies, which is how Bitcoin is extended to be an online payment system and a digital currency. It is possible to transfer money via encrypted methods without relying on a central bank. Bitcoin logged the transaction, sent, and received payments using public key addresses, and protected user identities. To reach a consensus, the transaction confirms procedure utilizes the processing power of other users before recording the transaction to the network.

Smart Contract. Smart contracts are a container for the code that executes and reflects real-world transactions in the digital realm. The smart contract offers a contract for two or more parties, where each item complies with each party's obligations under the contract. However, in the BaaS, the third parties are replaced by the smart contract; the smart contract plays the agent's role between the contract members. Generally, the agreements are executable by law via a centralized permitted item. This function is done by automatically running shared and verified code by all Blockchain network nodes (Macrinici et al., 2018).

Hyperledger. The Linux Foundation launched the open-source Hyperledger blockchain technology in December 2015 to support distributed ledgers based on the blockchain. To enhance many areas of performance and dependability, it is concentrated on ledgers created to facilitate international commercial transactions, including those of significant technology, financial, and supply chain firms. By offering a modular framework that supports various components for various uses, Hyperledger seeks to unify numerous distinct efforts to build open protocols and standards. Various blockchains with their respective consensus and storage structures, as well as services for identity, access control, and contracts, would be included in this (Tsai et al., 2016; Luu et al., 2016).

Digital Identity. Blockchain digital identification minimizes business worries while giving identity owners more control over their personal information. It provides identity issuers and verifies with a place to collaborate on the same platform (Taneja, 2018). It creates a decentralized system where point-to-point information exchange is enabled by Blockchain. The identity bearers, issuers, and auditors uphold privacy and adhere to the code of conduct.
Registry. The registry is a reliable database for things. Public authorities, whose authority ensures the legitimacy of the registered things, organize, and oversee many public registers. Every modification to a logbook is marked with a digital fingerprint that can be independently controlled (Tran et al., 2017). A register must maintain a record of all modifications and be accessible for evaluation 340 by a third party. To lessen duplications and errors, a register may refer to other records (Blockchain and the Internet of Things: The IoT Blockchain Picture, 2018).

Internet of Things (IoT). Blockchain technology for IoT data opens up new possibilities for automating commercial operations

between partners without building an elaborate and expensive centralized IT infrastructure. IoT can now take part in blocking transactions thanks to this (Treleaven et al., 2017; Mashal et al., 2015). Recall the most critical business relationships in the world; widen the door to new forms of digital communication; facilitate implementation expenditures and sophistication (KSI Blockchain Technology, 2018; Sharma et al., 2018; Qutqut et al., 2018).

Other Applications. Blockchain technologies have a wide range of applications, including protecting intellectual property, supply chain traceability, identity validation, insurance, international payments, the Internet of Things, patient privacy in medical care, and prediction markets (Tsai et al., 2016; Luu et al., 2016).

2.2.4. Consideration for Blockchain Security: Challenges

Blockchain is effective for transactions; however, there are questions about the security of those transactions. Cybercriminals have been targeting exchanges and businesses since 2014 using digital currencies and the Blockchain, which can be hacked like any other platform or protocol. For instance, if the private keys and bitcoin are kept on a computer that is connected to the internet, they could be taken. No matter how secure the architecture or encryption features are set up, they are lost forever if these private keys are stolen (Kuebler, 2018). The consensus protocol of the blockchain system, which enables different nodes that are mutually unreliable and uncoordinated to concur on blocks and transactions in the network on which the blockchain is running, is crucial to the distribution process of the system. Numerous research on consensus in distributed systems resilient to node failures and corrupted messages have been conducted. Every node must concur on a constant global state, and any compromised or malfunctioning nodes must be addressed by consensus on the blockchain. Based on three crucial aspects, the applicability and efficiency of blockchain consensus are evaluated.

Safety property declares that all verified hosts provide the same output, called the value v, and the output v produced by verified hosts is genuine. Valid hosts cannot reach contradictory conclusions. The Blockchain protocol has safety mechanisms, so if one legal host provides a proper output, all other legal hosts must either produce the identical output or attest to the accuracy of the production they have already received. Verified hosts won't accept a fake value that dishonest hosts provide. The perspective relates to the consistency of the shared state, which is essential in many Blockchain protocols like PBFT and legitimate and identical to all verified hosts at a given time (Baliga, 2017).

Liveness, in Blockchain, guarantees that all accurate requests are eventually fulfilled and that all valid nodes participating in a consensus will eventually yield a value. Since there is no time-bound restriction on determining a value, only some nodes have the same state at any time. Fault Tolerance refers to a node's capacity to bounce back (perform effectively) after errors or complex behavior. As long as the number of faulty nodes is limited, the consensus can still be obtained. According to the Fischer Lynch Paterson (FLP) paradigm, any knowable consensus mechanism that manifests in an asynchronous framework can only have two of these three characteristics (Lynch et al., 1982). The situation is said to be asynchronous when operation and delay times have an undetermined upper bound. It is essential to follow the asynchronous model because it captures the Internet, where nodes might fail, and communications can be discarded at any time accurately. The importance of fault tolerance over the other two factors is that most Blockchain systems prefer to choose between safety and liveness (Baliga, 2017).

Security of Transaction. Because the script used for inputs and outputs is written in a flexible programming language, different transaction forms can be generated. A bitcoin contract is a method for incorporating bitcoin into the present banking and authentication systems. Using a script that generates the contract utilizing the multiple-signature technique is a frequent solution. The scripts are used to solve a range of bitcoin-related issues, but as the complexity of the scripts increases, so does the chance of a transaction that is not adequately configured. No one can use a bitcoin if the locking script is specified properly since an unlocking script cannot be produced. To check the integrity of a transaction's script, some research advises employing models of bitcoin contract-type transactions.

3. Blockchain as a Service (BaaS)

The Blockchain-as-a-service (BaaS) term refers to a combination of the Blockchain and cloud computing that allows clients to use cloud computing solutions to create, host, and manage Blockchain applications such as smart contracts and other Blockchain network functions. BaaS service is based on the Software-as-a-Service (SaaS) model and works in the same way. Furthermore, BaaS con-sider as a third-party control and create cloud-based networks for the cloud service provider in the business of creating Blockchain applications (Zheng et al., 2019). Currently, BaaS platforms providers focus on keeping the infrastructure flexible and easy to access and operate by managing the required activities and tasks. Many BaaS service provider offers the essential Blockchain networks and the required infrastructure for a fee. After the client creates his system, the service provider manages the complicated back-end procedures for the client. The BaaS operator provides several services like managing resource allocation, application hosting, data security characteristics, and bandwidth management.

4. Blockchain Tools

In this section we will review the most well-known Blockchain Tools.

4.1 Etherrum

Etherrum is a platform used to develop generalized technology, which means to build all state machine transactions. Further, the platform provides an integrated end-to-end method for developers for building applications on a previously unexplored compute model and creating a secure object messaging system. Another goal of this platform is to accelerate the transaction process between authorized users who don't trust one another, due to the separated location, communication problem, or difficulties because of the legal systems. In the Ethereum platform, all users of the network must agree to join the consensus, and this method is known as permissionless. Moreover, the Proof of Work (POW) method is used to allow the user to join the consensus. To assist in the procedure of mining blocks to join the consensus, Ethereum uses the virtual currency "Ether" to pay the nodes. Besides, Ethereum can be appropriate in various industry scenarios, because of the nature of the framework as a generic blockchain system. The object-oriented programming language Solidity is used to write the smart contract (Wood, 2014).

4.2 Quorum

Quorum is a permissioned Blockchain platform built based on Go Ethereum. Quorum functions are very similar to Ethereum but with some differences such as the voting-based consensus techniques, network and peer permissions management, enhanced transaction and contract privacy, higher performance. Consensus uses a voting protocol called Quorum Chain, where a group of nodes in the Blockchain network can vote on blocks.

4.3 R3 Corda

The R3 Corda platform is a private or permissioned blockchain system; Corda guarantees data is distributed only with parties that join the transaction. Two types of consensuses in Corda are considered the Validity consensus (all requisite signer verifies this before they sign the transaction by running the smart contracts) and Uniqueness consensus (verifies by official service). The smart contract validates the transaction to be acceptable or not through checking the states of all input and output. Kotlin and Java are used to write the contracts.

4.4 Hyperledger Fabric

The Hyperledger Fabric platform is an open-source built by Linux, and it's the first distributed ledger platform (DLT) platform to assist the smart contracts. The smart contracts are written in general programming languages such as Go and Java. Further, Hyperledger follows the permissioned method, which means that all users are known to each other. The Hyperledger is efficiently customized to suit trust forms and use cases because it implements pluggable consensus protocols (A Blockchain Platform for the Enterprise: Hyperledger Fabric, 2020).

4.5 CREDITS

The CREDITS is a permissioning blockchain platform interaction system between the users based on the peer-to-peer network, and it is a decentralized financial approach for users. The method allows users to use financial services based on self-running smart contracts, CREDITS cryptocurrency, and shared ledger. All the participants of the Blockchain network can provide service whenever they use various services. Delegated Proof-of-Stake (DPoS) and Byzantine Fault Tolerance (BFT) algorithms are used to be the consensus approach for the platform ("Decentralized Financial System CREDITS," 2018). The following Table 1 summarizes the Blockchain tools.

Table 1
Summary of the Blockchain Tools

Characteristic	Etherrum	Quorum	R3 Corda	Hyperledger Fabric	CREDITS
Description	platform provides an integrated end-to-end method for developers for building applications on a previously unexplored compute model	A permissioned Blockchain platform and built based on Go Ethereum.	Corda guarantees data is distributed only with parties join the transaction.	Platform that suits trust forms and use cases because it implements pluggable consensus protocols	A platform permissioning blockchain platform interaction system between the users based on the peer-to-peer network
Operation Approach Consensus	Permissionless the Proof of Work (POW) method is used to allow the user to join the consensus.	permissioned Consensus uses a voting protocol (QuorumChain)	permissioned The Validity consensus and Uniqueness consensus.	permissioned General understanding of consensus that enables various methods.	permissioning Delegated Proof-of-Stake (DPoS) and Byzantine Fault Tolerance (BFT).
Smart Contract	Solidity	Go Ethereum	Kotlin and Java	Go and Java	Self-running smart contracts
Open-Source Currency	Yes Ether	Yes JPM Coin	Yes None	Yes None, Currency can be developed by chaincode	Yes Private cryptocurrency
Privacy	No	Yes	Yes	Yes	Yes

5. Blockchain-based database to secure data integrity in Cloud Computing

Blockchain can be used to secure the data integrity of distributed replicas of a database, such as storing determined information of the database transactions that cannot be discarded. Further, the Blockchain can ensure fully distributed data control related to the database. Gaetani et al. propose an approach to secure the distributed database based on Blockchain (Gaetani et al., 2017). The introduced work is used in the context of Federation-as-a-Service (FaaS), FaaS is a service that ensures production and management the cloud services and data (Schiavo et al., 2016). Figure 3 illustrated the blockchain-based database shared on three different cloud systems of federation.

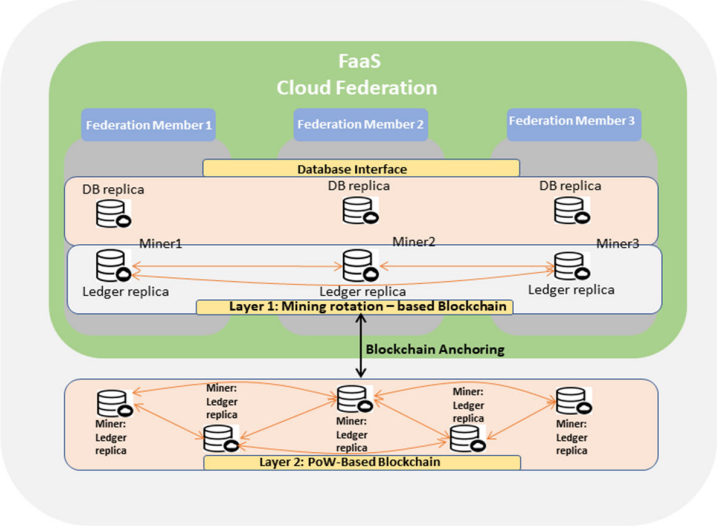

Fig. 3. Blockchain-based database shared for cloud environment

The database interface is used with the clouds to operate on the database problem. Operations are initially registered with proper evidence using the Blockchain's first stage, and then they are carried out on distributed database replicas. As a result, the Blockchain is permissioned in the first stage and uses a single miner for each cloud member. The miners use public and private keys to identify the messages and perform consensus using the mining rotation strategy, which divides the time into cycles and selects one miner as the leader. New transactions will be received by the miner leader, who will then mark them with a secret key and distribute them to the other miners. Each miner's actions will be added to the Blockchain after completion. The second layer uses the Blockchain anchoring approach and is proof of work (PoW) based. An operation in the first layer might link with a block from the second layer according to the time-based anchoring technique. The suggested study can thereby enhance the measurement of data stability, performance, and integrity.

6. Blockchain based cloud platforms

In this section, we presented the most well-known cloud platforms integrated with Blockchain, known as Blockchain-as-a-Service.

6.1 IBM Blockchain Platform

IBM company introduces a platform based on open source for blockchain for cloud computing. The proposed platform is built on the Hyperledger Fabric tools from Linux. Using the open-source code support for on-premises bases and giving a choice to utilize third-party clouds to help the user avoid the vendor lock-in restriction (IBM Blockchain Platform, 2020). IBM Blockchain works based on three levels, service level, Hyperledger Fabric, and Hyperledger Composer. Furthermore, the IBM platform accelerates blockchain applications' development process by implementing an application development framework. The Hyperledger Composer affords a suitable layer and business stage to help the users to generate the smart contract and implement them on Hyperledger Fabric (Novotny et al., 2018). Fig. 4 illustrates the IBM Blockchain platform.

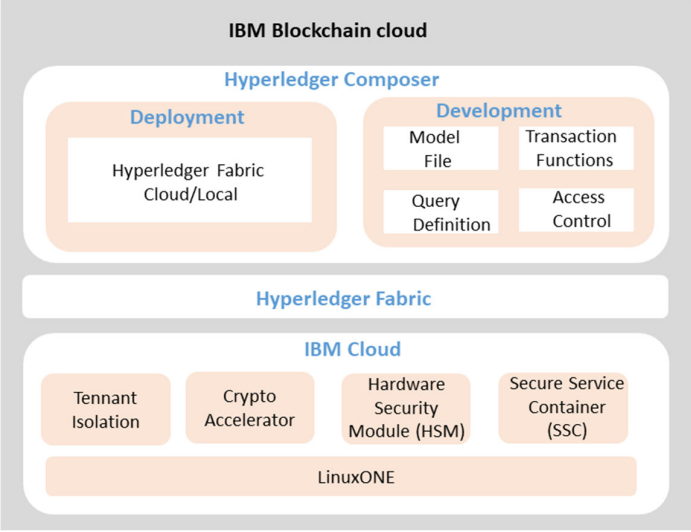

Fig. 4. IBM Blockchain platform architecture (Novotny et al., 2018)

6.2 AWS Blockchain Platform

AWS is a Blockchain service provided by Amazon. AWS uses templates and an open- source system to create and deploys Blockchain networks effectively. AWS users use the templates to create different Blockchain applications. Several AWS blockchain models use the blockchain structure selected in containers similar to Amazon Elastic Container Service (Amazon ECS) cluster or within Amazon Elastic Compute Cloud (Amazon EC2). Each Blockchain network is built on a private network, allowing the user to use the access control list and subnets. Further, the user can allocate permissions to limit with system resources accessed (Coutinho et al., 2020).

AWS blockchain deploys two open-source frameworks, the Ethereum and Hyperledger Fabric. So, templates can be implemented in various Blockchain infrastructures. Templates using Ethereum give the user the ability to build and run blockchain applications without downtime, fraud, supervision or third parties interference. Users can perform peer transactions on the Ethereum network to accomplish the transaction. In AWS, users can initiate smart contracts using Ethereum's Solidity language. Further, The Hyperledger Fabric enables users to create Blockchain applications while providing access control lists and permissions for Blockchain data. Users can utilize the Hyperledger Fabric to create a private Blockchain network and limit the transactions that different parties can see (AWS Blockchain Templates, 2020).

When the users want to use the AWS blockchain, initially they choose the model. Then, select an Amazon platform ECS or EC2 to deploy the blockchain network. Next, users select a blockchain platform (Ethereum or Hyperledger Fabric) to improve deployment speed. Finally, users find the AWS blockchain application (AWS Blockchain Platform, 2020). Fig. 5 shows the AWS blockchain procedures flow.

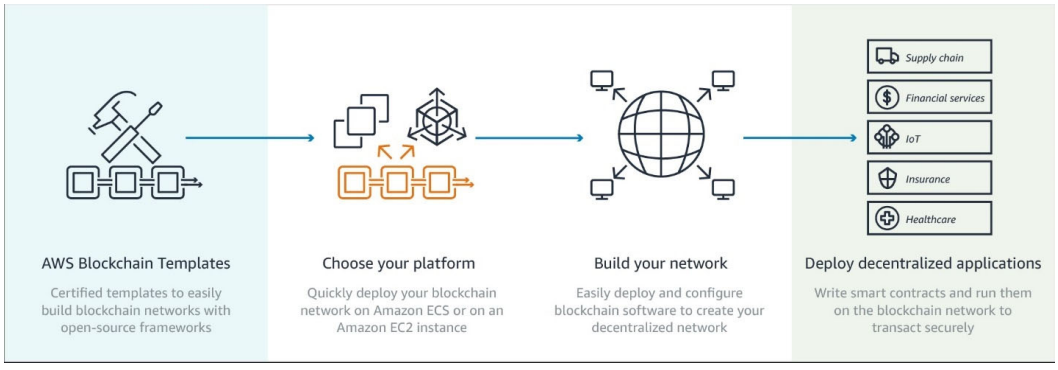

Fig. 5. AWS blockchain procedures flow (AWS Blockchain Platform, 2020)

6.3 Azure Blockchain Service

Microsoft introduced its blockchain services for its cloud resources based on Azure Blockchain (What Is Azure Blockchain Service?, 2020). Azure Blockchain Service is a managed ledger service to build and develop any Blockchain networks which

allow clients to operate and grow their network. Furthermore, Azure Blockchain provides cohesive control for blockchain network governance and infrastructure management. Users will have the ability to build, control, and extend Azure Blockchain networks with simple development, governance, and management.

Several features provided by Azure block such as: create different blockchain network applications with trusted tools; use the blockchain data manager to capture and store ledger data without chain, easy management for Blockchain networks; scale management control is based on codeless consortium and internal management (What Is Azure Blockchain Service?, 2020). The Azure Blockchain network deployment is done by Azure CLI, Azure Blockchain, or using the Azure Blockchain extension in Visual Studio. The deployment process is simplified by providing validator nodes and transactions and security isolation by deploying the Azure Virtual Networks and service-managed storage. Furthermore, when a new Blockchain member implements, users will join or create a consortium. The consortiums facilitate multiple nodes in various Azure subscriptions to communicate with one another on a shared blockchain securely. To build the Azure Blockchain Service application, users use Quorum Ethereum ledger, which is an open-source code platform. Moreover, users can use the Visual Studio development tools to build a smart contract. Several Azure capabilities are used to keep the data secure. For example, the Azure Blockchain services are isolated through a private virtual network. Every validation node and transaction reserve a virtual machine (VM). Each group of VMs in a specific virtual network is not allowed to communicate directly to different VMs in other virtual networks in terms of isolating the communication and keeping it private within a particular virtual network (Azure Blockchain Service Security, 2020). Figure 6 demonstrates the isolation process in Azure Blockchain.

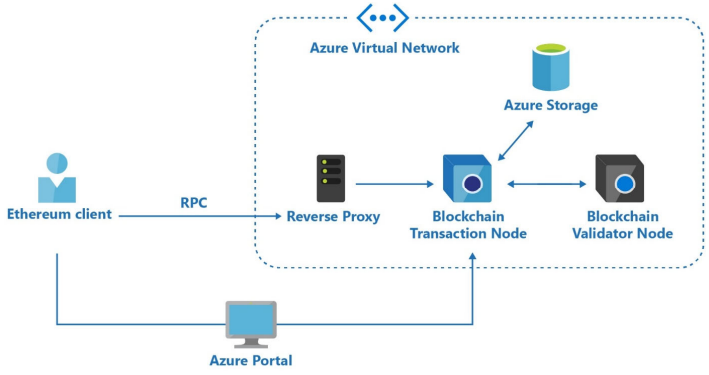

Fig. 6. Azure blockchain isolation procedures (Azure Blockchain Service Security, 2020)

6.4 Oracle Blockchain Cloud Service

In 2017 Oracle introduced their Blockchain Cloud Service, a platform-as-a-service (PaaS) that offers a distributed ledger system operating in the cloud and created based on the Hyperledger Fabric and Oracle improvements to offer an enterprise-grade blockchain application. Oracle Blockchain enables the user to enroll members, create Blockchain networks, deployment, and execute smart contracts (Oracle Autonomous Blockchain Cloud Service, 2020).

As shown in figure, Oracle Blockchain service is a PaaS service that provides a distributed ledger system executed in the cloud. It contains the validating network members (called peers), which update and validate the leger when getting any transaction and reply to queries by run the smart contract. The user can choose the validated nodes when designing the network. Applications on the client can interact with transactions and queries through SDKs and Representational state transfer (REST) software (Van Mölken, 2018).

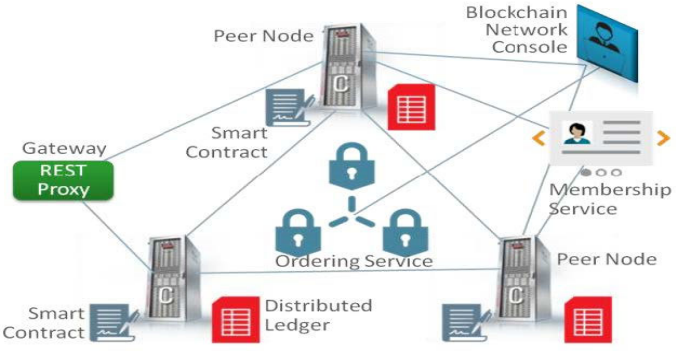

Fig. 7. Oracle Blockchain Cloud Service (Oracle Autonomous Blockchain Cloud Service, 2020)

6.5 Alibaba Cloud BaaS

It is a BaaS service from Alibaba cloud Container for Kubernetes clusters. It provides users with the ability to utilize Alibaba services in security, computing, database, and Cloud. Services are offered based on several architectures like the private cloud and public cloud deployments. Furthermore, the Alibaba Cloud BaaS support different open-source systems for Blockchain, such as Enterprise Ethereum - Quorum and Hyperledger Fabric; on the other side, also the system supports Blockchain financial-grade approach Ant Blockchain. Users can create and deploy a Blockchain network quickly, and Alibaba Cloud BaaS affords a graphical interface to let users efficiently manage and operate the Blockchain network. Businesses and Enterprises add dynamically to the network (Alibab Cloud Blockchain as a Service, 2020). Fig. 8 demonstrates the Alibaba Cloud architecture.

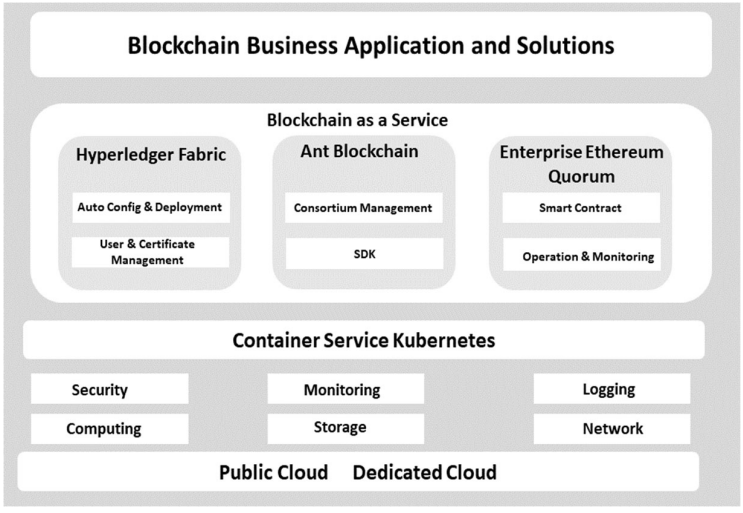

Fig. 8. Alibaba Cloud architecture (Alibaba Cloud Blockchain as a Service, 2020)

7. Challenges in blockchain–Cloud integration

In this section, we analyze the challenges to be addressed when implementing the Blockchain to cloud computing. The integration of Blockchain with the cloud is not an easy job. Transaction over any Blockchain network must be digitally signed; therefore, any cloud computing system should be able to operate this function. Some of the integration challenges are presented in this section.

7.1 Integration Aspects

Cloud computing systems provide various tools, applications, and services for clients, developers, and service providers. Further, the integration between cloud computing and Blockchain in terms of applications and environments will be pervasive among users when the feature and the benefits are known. As the number of applications and technologies is very large in cloud computing, there is a risk of integration of these systems. For example, some PaaS services offering programming language for the fast expansion of an application apply Blockchain features. The integration features are numerous, demanding awareness of the solution architecture (Coutinho et al., 2020).

7.2. Storage capacity and Scalability

One of the main problems in the Blockchain is storage capacity and scalability. In the Blockchain, the chain is continuously increasing at a rate of one megabit for each block every ten minutes in Bitcoin; moreover, many copies will be stored amongst the network nodes. However, only the nodes that validate transactions are called a full node; only the full node can store the full chain, so the storage obligations are essential. As long as the size increases, the network requires more resources, diminishing the system capability scale. Besides, the performance affected by the chain with big size, it raises the synchronization time for clients (Reyna et al., 2018).

7.3 Blockchain Security

The Blockchain facing several attacks including the 51% attack, fork after withholding attacks, distributed denial-of-service attacks, DNS attacks, selfish mining, consensus delay, and eclipse at tacks (Leelavimolsilp et al., 2018). For example, the selfish mining attack is an approach opted for some miners who try to grow their recompense through carefully putting their blocks private. Instead of publishing blocks to other users upon discovery, the selfish miners keep mining the private blocks

to select a longer than the public one, resulting in a block race between the private chain of selfish miners and the public chain authentic miners (Saad et al., 2019).

These kinds of attacks can create unwanted effects for the rest of the Blockchain network by revoking the blocks of authentic miners who join the Blockchain network. Also, all the transactions in the authentic miner's block declined.

7.4 Smart Contract

The smart contract provides an agreement for two or more parties and replaces the intermediaries between the parties. Besides, the smart contract will play the leading role in Cloud computing's future market by providing the users to build Blockchain-based applications on the Cloud. The development of BaaS services for cloud computing has only newly begun and concentrated on commercial targets. Several difficulties arise in this context, such as the application cost that is running inside and outside the Blockchain, the security of access, data management, and performance analysis (Uriarte & DeNicola, 2018).

8. Conclusion

In this paper, we presented an extended and up-to-date survey of cloud computing and Blockchain's integration, a very important service for companies' applications due to the benefits in privacy, security, and service support. This review was motivated by the lack of a comprehensive survey reviewing the significance of BaaS platforms implemented in cloud computing. We began dis-cussing the Blockchain explanation with security issues and architecture and present the Cloud computing architecture and related security issues. We particularly focus on the various BaaS Tools, such as Etherrum, Quorum, R3 Corda, Hyperledger Fabric, and CREDITS. Further, this survey reviews the most common BaaS platforms that adopted Blockchain as a cloud service, including Alibaba, Oracle, Azure, Amazon, and IBM. Besides, this paper highlighted some of the key technical challenges in integrating Blockchain and cloud computing.

References

A Blockchain Platform for the Enterprise: Hyperledger Fabric. (2020). https://hyperledger-fabric.readthedocs.io/en/release-1.2/whatis.html

Abuaddous, H. Y., Al Sokkar, A. A. M., & Abualodous, B. I. (2018). The impact of knowledge management on organizational performance. *International Journal of Advanced Computer Science and Applications*, *9*(4).

Abualigah, L., Gandomi, A. H., Elaziz, M. A., Hamad, H. Al, Omari, M., Alshinwan, M., & Khasawneh, A. M. (2021). Advances in meta-heuristic optimization algorithms in big data text clustering. *Electronics*, *10*(2), 101.

Abualigah, L., Shehab, M., Alshinwan, M., & Alabool, H. (2020). Salp swarm algorithm: a comprehensive survey. *Neural Computing and Applications*, *32*(15), 11195–11215.

Abualigah, L., Shehab, M., Alshinwan, M., Alabool, H., Abuaddous, H. Y., Khasawneh, A. M., & Al Diabat, M. (2020). Ts-gwo: Iot tasks scheduling in cloud computing using grey wolf optimizer. In *Swarm intelligence for cloud computing* (pp. 127–152). Chapman and Hall/CRC.

AL-Sous, N., Alsokkar, A., Majali, T., Mansour, A., Alsherideh, A., Masadeh, R., Dahali, Z., & others. (2022). Antecedents of e-commerce on intention to use the international trade center: An Exploratory Study in Jordan. *International Journal of Data and Network Science*, *6*(4), 1531–1542.

Al Shinwan, M., Abualigah, L., Huy, T.-D., Younes Shdefat, A., Altalhi, M., Kim, C., El-Sappagh, S., Abd Elaziz, M., & Kwak, K. S. (2022). An Efficient 5G Data Plan Approach Based on Partially Distributed Mobility Architecture. *Sensors*, *22*(1), 349.

Al Shinwan, M., Abualigah, L., Le, N. D., Kim, C., & Khasawneh, A. M. (2021). An intelligent long-lived TCP based on real-time traffic regulation. *Multimedia Tools and Applications*, *80*(11), 16763–16780.

Alias, J. S., Manasa, M., Pallavi Krishna, B. R., & Asha Rani, M. (2018). Security System for Cloud Based Services. *3rd National Conference on Image Processing, Computing, Communication, Networking and Data Analytics*, 132.

Alibab Cloud Blockchain as a Service. (2020). http://docs-aliyun.cn-hangzhou.oss.aliyun-inc.com/pdf/baas-product_intro-intl-en-2020-04-28.pdf

Alsokkar, A., Law, E., Almajali, D., & Alshinwan, M. (2023). The effect of multimodality on customers' decision-making and experiencing: A comparative study. *International Journal of Data and Network Science*, *7*(1), 1–14.

Altamimi, A., Al-Bashayreh, M., AL-Oudat, M., & Almajali, D. (2022). Blockchain technology adoption for sustainable learning. *International Journal of Data and Network Science*, *6*(3), 983–994.

AWS blockchain platform. (2020). https://aws.amazon.com/blockchain/templates/

AWS Blockchain Templates. (2020). https://docs.aws.amazon.com/blockchain-templates/latest/developerguide/blockchain-templates-dg.pdf#what-are-blockchain-templates

Azure Blockchain Service security. (2020). https://docs.microsoft.com/en-us/azure/blockchain/service/data-security

Baliga, A. (2017). Understanding blockchain consensus models. *Persistent*, *4*, 1–14.

Blockchain and the Internet of Things: the IoT blockchain picture. (2018). https://www.iscoop.eu/blockchain-distributed-ledger-technology/blockchain-iot/

Chandrasekaran, K. (2014). *Essentials of cloud computing*. CrC Press.

Coutinho, E. F., Paulo, D. E., Abreu, A. W., & Carla, I. M. B. (2020). Towards Cloud Computing and Blockchain Integrated Applications. *2020 IEEE International Conference on Software Architecture Companion (ICSA-C)*, 139–142.

Decentralized financial system CREDITS. (2018). *White Paper*. http://195.58.33.24:8080/Content/Docs/TechnicalWhitePaperCREDITSEng.pdf

Dillon, T., Wu, C., & Chang, E. (2010). Cloud computing: issues and challenges. *2010 24th IEEE International Conference on Advanced Information Networking and Applications*, 27–33.

Gaetani, E., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., & Sassone, V. (2017). *Blockchain-based database to ensure data integrity in cloud computing environments*.

Haber, S., & Stornetta, W. S. (1990). How to time-stamp a digital document. *Conference on the Theory and Application of Cryptography*, 437–455.

Harshavardhan, A., Vijayakumar, T., & Mugunthan, S. R. (2018). Blockchain Technology in Cloud Computing to Overcome Security Vulnerabilities. *2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), 2018 2nd International Conference On*, 408–414.

IBM Blockchain Platform. (2020). https://www.ibm.com/blockchain/platform

Ingole, M. K. R., & Yamde, M. S. (2018). *Blockchain Technology in Cloud Computing: A Systematic Review*.

Ismail, L., Hameed, H., AlShamsi, M., AlHammadi, M., & AlDhanhani, N. (2019). Towards a blockchain deployment at uae university: Performance evaluation and blockchain taxonomy. *Proceedings of the 2019 International Conference on Blockchain Technology*, 30–38.

Jimi, S. (2018). *Blockchain: How Mining Works and Transactions are Processed in Seven Steps*.

Khan, A. A., Shaikh, Z. A., Baitenova, L., Mutaliyeva, L., Moiseev, N., Mikhaylov, A., Laghari, A. A., Idris, S. A., & Alshazly, H. (2021). QoS-ledger: smart contracts and metaheuristic for secure quality-of-service and cost-efficient scheduling of medical-data processing. *Electronics*, *10*(24), 3083.

KSI Blockchain Technology. (2018). https://guardtime.com/technology/ksitechnology

Kuebler, R. G. (2018). *Application of Blockchain for Authentication, Verification of Identity and Cloud Computing*. Utica College.

Leelavimolsilp, T., Tran-Thanh, L., & Stein, S. (2018). On the preliminary investigation of selfish mining strategy with multiple selfish miners. *ArXiv Preprint ArXiv:1802.02218*.

Lin, I.-C., & Liao, T.-C. (2017). A survey of blockchain security issues and challenges. *IJ Network Security*, *19*(5), 653–659.

Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D. (2011). NIST cloud computing reference architecture. *NIST Special Publication*, *500*(2011), 1–28.

Lokhandwala, F. A. (2018). *A Heuristic Approach to Improve Task Scheduling in Cloud Computing using Blockchain technology*. Dublin, National College of Ireland.

Luu, L., Narayanan, V., Zheng, C., Baweja, K., Gilbert, S., & Saxena, P. (2016). A secure sharding protocol for open blockchains. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 17–30.

Lynch, N. A., Fischer, M. J., & Fowler, R. (1982). *A Simple and Efficient Byzantine Generals Algorithm.*

Macdonald, M., Liu-Thorrold, L., & Julien, R. (2017). The blockchain: A comparison of platforms and their uses beyond bitcoin. *COMS4507-Adv. Computer and Network Security*.

Macrinici, D., Cartofeanu, C., & Gao, S. (2018). Smart contract applications within blockchain technology: A systematic mapping study. *Telematics and Informatics*, *35*(8), 2337–2354.

Mashal, I., Alsaryrah, O., Chung, T.-Y., Yang, C.-Z., Kuo, W.-H., & Agrawal, D. P. (2015). Choices for interaction with things on Internet and underlying issues. *Ad Hoc Networks*, *28*, 68–90.

Merkle, R. C. (1987). A digital signature based on a conventional encryption function. *Conference on the Theory and Application of Cryptographic Techniques*, 369–378.

Nakamoto, S., & Bitcoin, A. (2008). A peer-to-peer electronic cash system. *Bitcoin.--URL: Https://Bitcoin. Org/Bitcoin. Pdf*.

Novotny, P., Zhang, Q., Hull, R., Baset, S., Laredo, J., Vaculin, R., Ford, D. L., & Dillenberger, D. N. (2018). Permissioned blockchain technologies for academic publishing. *Information Services \& Use*, *38*(3), 159–171.

Oracle Autonomous Blockchain Cloud Service. (2020). https://www.oracle.com/a/ocom/docs/blockchain-cloud-service-data-sheet.pdf

Park, J. H., & Park, J. H. (2017). Blockchain security in cloud computing: Use cases, challenges, and solutions. *Symmetry*, *9*(8), 164.

Pen, L. Z., Xian Xian, K., Yew, C. F., Hau, O. S., Sumari, P., Abualigah, L., Ezugwu, A. E., Shinwan, M. Al, Gul, F., & Mughaid, A. (2023). Artocarpus Classification Technique Using Deep Learning Based Convolutional Neural Network. In *Classification Applications with Deep Learning and Machine Learning Technologies* (pp. 1–21). Springer, Cham.

Prianga, S., Sagana, R., & Sharon, E. (2018). Evolutionary Survey On Data Security In Cloud Computing Using Blockchain. *2018 IEEE International Conference on System, Computation, Automation and Networking (ICSCA)*, 1–6.

Qutqut, M. H., Al-Sakran, A., Almasalha, F., & Hassanein, H. S. (2018). Comprehensive survey of the IoT open-source OSs. *IET Wireless Sensor Systems*, *8*(6), 323–339.

Raul, A., Kalyanaraman, S., Yerande, K., & Devadkar, K. (2019). Blockchain Technology for Decentralized Data Storage on P2P Network. In *Soft Computing and Signal Processing* (pp. 101–110). Springer.

Revanesh, M., & Sridhar, V. (2021). A trusted distributed routing scheme for wireless sensor networks using blockchain and meta-heuristics-based deep learning technique. *Transactions on Emerging Telecommunications Technologies*, *32*(9), e4259.

Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future generation computer systems*, *88*, 173-190.

Saad, M., Spaulding, J., Njilla, L., Kamhoua, C., Shetty, S., Nyang, D., & Mohaisen, A. (2019). Exploring the attack surface of blockchain: A systematic overview. *ArXiv Preprint ArXiv:1904.03487*.

Sanghi, N., Bhatnagar, R., Kaur, G., & Jain, V. (2018). BlockCloud: Blockchain with Cloud Computing. *2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*, 430–434.

Schiavo, F. P., Sassone, V., Nicoletti, L., & Margheri, A. (2016). Faas: Federation-as-a-service. *ArXiv Preprint ArXiv:1612.03937*.

Sharma, S. G., Ahuja, L., & Goyal, D. P. (2018). Building secure infrastructure for cloud computing using blockchain. *2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS)*, 1985–1988.

Shehab, M., Abualigah, L., Al Hamad, H., Alabool, H., Alshinwan, M., & Khasawneh, A. M. (2020). Moth--flame optimization algorithm: variants and applications. *Neural Computing and Applications*, *32*(14), 9859–9884.

Syafruddin, W. A., Dadkhah, S., & Köppen, M. (2019). Blockchain scheme based on evolutionary proof of work. *2019 IEEE Congress on Evolutionary Computation (CEC)*, 771–776.

Taneja, A. (2018). *In blockchain we trust? Testing the promise of blockchain as a means of identity management against the challenges raised by Aadhaar.*

Tran, A. B., Xu, X., Weber, I., Staples, M., & Rimba, P. (2017). Regerator: a Registry Generator for Blockchain. *CAiSE-Forum-DC*, 81–88.

Treleaven, P., Brown, R. G., & Yang, D. (2017). Blockchain technology in finance. *Computer*, *50*(9), 14–17.

Tsai, W.-T., Blower, R., Zhu, Y., & Yu, L. (2016). A system view of financial blockchains. *2016 IEEE Symposium on Service-Oriented System Engineering (SOSE)*, 450–457.

Uriarte, R. B., & DeNicola, R. (2018). Blockchain-Based Decentralized Cloud/Fog Solutions: Challenges, Opportunities, and Standards. *IEEE Communications Standards Magazine*, *2*(3), 22–28.

Vacca, J. R. (2016). *Cloud computing security: foundations and challenges*. CRC Press.

Van Mölken, R. (2018). *Blockchain across Oracle: Understand the details and implications of the Blockchain for Oracle developers and customers*. Packt Publishing Ltd.

What is Azure Blockchain Service? (2020). https://docs.microsoft.com/en-us/azure/blockchain/service/overview#publish-blockchain-data

Wood, G., (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*, *151*(2014), 1–32.

Xie, S., Zheng, Z., Chen, W., Wu, J., Dai, H.-N., & Imran, M. (2020). Blockchain for cloud exchange: A survey. *Computers \& Electrical Engineering*, *81*, 106526.

Zheng, W., Zheng, Z., Chen, X., Dai, K., Li, P., & Chen, R. (2019). NutBaaS: A Blockchain-as-a-Service Platform. *IEEE Access*, *7*, 134422–134433.