International Journal of Innovative Research in Engineering & Management (IJIREM)
ISSN: 2350-0557, Volume-8, Issue-6, November 2021
https://doi.org/10.55524/ijirem.2021.8.6.2
www.ijirem.org

Architecture and Research Challenges in Blockchain Based Cloud Computing

Atharva Parai
Department of Computer Engineering,
NBN Sinhgad School of Engineering,
Pune, India

Shailesh Bendale
Department of Computer Engineering,
NBN Sinhgad School of Engineering,
Pune, India

ABSTRACT

Blockchain technology represents a distributed ledger that maintains a record of all transactions carried out over a network and distributes those details among the nodes involved. Bitcoin is a well-known digital money that is applied using the technology of blockchain. Instead of using the help of a local server, a cloud system uses a network of far-flung servers to store, manage, and analyze data. However, it still faces many challenges including data security, data management, compliance, and reliability. Throughout this paper, we've discussed some of the cloud's most pressing issues and proposed solutions based on blockchain technology integration. In this article, we describe a brief assessment of earlier studies that discussed the integration of blockchain and the cloud. During the study, we also developed a framework to integrate blockchain with the cloud and to demonstrate the communication between the two.

Keywords

Blockchain Technology, Cloud Computing, Data Security, Data Management

1. INTRODUCTION

Cloud computing is an explicit technology that arose from substantial, distributed computing. It helps users reduce the processing load [1]. There are many advantages to using this technology, including reduced hardware and maintenance costs, global availability, high automation, and easy scalability. IBM, Google, Amazon, and Microsoft are just a few of the companies that have adopted the cloud. A lot of applications have been developed as prototypes, including the Google App Engine, the Google Cloud Platform, the Amazon Cloud, and the Elastic computing platform [2]. With its pay-per-use policy and flexible IT architecture, it can be accessed remotely through the internet by portable devices. Cloud computing offers a variety of useful services, but organizations are slow to adopt these services due to their privacy concerns. Cloud challenges, such as security issues, have been deterring organizations from implementing the cloud. [3].

As industries strive for improved security and privacy, block-chain technology is the future. Blockchain is a distributed ledger that stores tamper-evident data in the form of a chain without a central authority. Devices that participate in block-chain technology are referred to as nodes. With blockchain, all network nodes are involved in validating and verifying data in a decentralized manner. Cryptography will be used to encipher the data in the blockchain. Every block includes an encrypted timestamp, hash and the hash of the earlier block from the chain. As a result, data in a blockchain cannot be amended. Blockchain secures the data, and participating users will be verified in the network, so data privacy concerns are eliminated [4].

Assimilation of blockchain technology with cloud computing will enable us to affect data privacy as well as security concerns. It provides superior data security and service in the running, and it can manage cloud data. The introduction to cloud computing is the antecedent part of this article. Section B explains blockchain technology, Section II analyses to us the advantages of assimilating cloud and blockchain technology, with the prospective architecture.

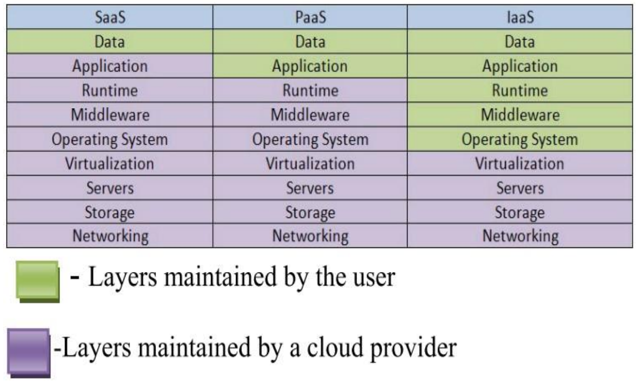
1.1 Cloud Computing

There are millions of websites presented on the web in modern Internet era. The presented site requires a large number of servers, which is highly expensive. Those servers' traffic rates must be steady, and they must be regularly checked and maintained. There will be a need to hire more people to organise and maintain these servers. All of the information will be kept in data centres. As a result, continual attempts to maintain the server issue, as well as the workers, may detract from our ability to meet our business objectives. We are using "Cloud Computing" to prevent this time-consuming upkeep. "Cloud computing is the practise of storing, managing, and processing data from anywhere in the globe utilising a network of distant servers. It replaces a local server or a personal computer". Cloud computing services, such as data storage and application delivery, are delivered to the devices of the corporation via the internet [3]. Cloud computing offers a number of advantages by merging data centres, resources, and servers across the internet. These services are governed by a pay-per-use model. The services are accessible from anywhere in the world at a substantially lower cost, allowing employees to collaborate more effectively. The firmware in the cloud will be cardinally updated, making the cloud more controllable. The cloud papers will likewise be under the control of the service consumer. It has certain restrictions as well [5]. Because cloud data is so adaptable, there are some security and privacy concerns to be addressed, as well as the potential for assaults. When there is a large number of users, there is a potential that the cloud will experience downtime.

Many services are available on the cloud, and they are categorised into three delivery methods. The first service is Software as a Service (SaaS), which is a type of internet-based programme that is hosted for consumers. The Cloud Service Provider presents the entire programme or project as a single platform of cloud-based software that provides multiple services to a large number of consumers. Customers that use cloud have no access to the framework. A prominent precedent of SaaS is Amazon Web Services, Google Mail and SalesForce.com.

Platform as a Service is the second service (PaaS). We can use the cloud service provider's platform to deploy our application and a set of programming languages. SaaS and PaaS differ in that SaaS runs the entire application on the cloud, whereas PaaS offers the application's platform. The best illustration of PaaS is Google's search engine. Infrastructure as a Service (IaaS) is the third service, which allows users to computing, directly access storage and other resources through the reticule. In IaaS, virtualization is utilised to distribute physical resources in order to fulfil the resource demands of cloud clients. The best virtualization strategy is to create distinct virtual machines from the elemental hardware and other virtual machines. To ensure security, they accredit each server an exclusive IP address. The finest representation of IaaS is Amazon EC2, GoGrid [6].

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

1.1.1 Research Issues in Cloud

1.1.1.1 Reliability

Cloud customers have passage to services 24 hours in a day, seven days from the week. The server has closed down a few times due to maintaining issues or time constraints. Cloud consumers nowadays demand cloud providers to provide more services, defined standards, and best practices. Cloud servers are similar to local servers in terms of functionality. They also have server downtimes and a strong reliance on a cloud service provider. When a user selects a certain server, they may become locked in, posing a business risk [7].

1.1.1.2 Compliance

There are numerous restrictions governing access to storage, data use, and frequent reporting and audit trails. Customers may have specific requirements for data centers managed by cloud providers, which will necessitate compliance requirements in some circumstances.

1.1.1.3 Service Level Agreements

Cloud services will be delivered in accordance with Service Level Agreements, which will allow numerous instances of the same application to be duplicated on multiple servers as needed, depending on the priority. If that program has a lower priority, the cloud may disable or minimize it. The most difficult task for cloud consumers is evaluating Service Level Agreements with cloud vendors. Most suppliers design SLAs that favor them while providing the bare minimum of services to users, such as data protection, downtime, and pricing structures. Before negotiating a contract with a provider, cloud consumers should address these issues with extreme caution.

1.1.1.4 Cloud Data Management

Because cloud data can be vast and unregulated or semi-regulated, data management is an essential study topic. Because service providers do not have access to the data centers' physical security system, they rely on the infrastructure provider to provide total data protection. Even on virtual machines, the supplier can set security conditions remotely without knowing whether they are applied securely. In these cases, the infrastructure provider must meet requirements such as auditability for attesting to application security settings, confidentiality for safe data access, and transfer. Cryptographic obligations can provide confidentiality, whereas secluded substantiation techniques can provide audibility. However, because virtual machines (VMs) dynamically drift from one location to any another, this is not always practical. As a result, remote substantiation will no longer be a viable option.

1.1.1.5 Data Encryption

To ensure data security, data is encrypted. There are several levels of security available, including low, moderate, and high. Consider Web services APIs, which can be used to access the cloud via a computer application or clients written to such APIs. For access, we use SSL encryption, which is widely accepted as a standard. When the object is delivered to the cloud, the data is decoded and stored there. While decrypting the data and storing it without prior encryption before storing it in the cloud, the data's security is jeopardized.

1.1.1.6 Interoperability

Internal intercommunication between systems is critical for exchanging and utilizing information. The public cloud networks are built as closed systems and are not meant to communicate with one another. The industry is unable to combine their IT systems in the cloud due to a lack of internal communication among cloud systems. Enterprises must take the initiative to create a single toolkit for integrating multiple apps across existing programs and cloud providers.

1.2 Blockchain Technology

The innovation of Bitcoin coincided with the invention of Blockchain technology. Bitcoin is a type of digital currency created in 2008 by a personality who goes by the ananym "Satoshi Nakamoto". He published a white paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System," in which he demonstrates how to send money online without the necessity of a mediator [8]. This electronic cash system largely addresses the issue of money double-spending, owing to the digital currency's ability to be easily replicated and spent many times. This ultimatum is overcome by creating meddle-resistant links between each transaction. The public ledger is being utilized to create tamper-proof connections between transactions. A network can utilize this ledger to check the transaction history that a user presents for payment and to ensure that the coin has not been spent previously [9].

In terms of a comparison between Blockchain and Bitcoin, we can say that blockchain is a technology that several cryptocurrencies, including Bitcoin, use for secure and anonymous transactions [10]. Blockchain, on the other hand, is a transparent system, whereas Bitcoin thrives on anonymity. While Bitcoin is used for online transactions, blockchain is used to transfer data, rights, and other types of information. So, although Bitcoin is limited to trading virtual currency, Blockchain offers a broader approach to use [11]. "Blockchains are transparent distributed ledgers of digitally signed transactions organized into blocks." Each block incorporates a cryptographic hash value that hooks up one block to the next, as well as a timestamp and transaction data. By design, blockchain data cannot be altered [12]. It is a dispersed, open ledger that efficiently and permanently tabulates transactions between participants.

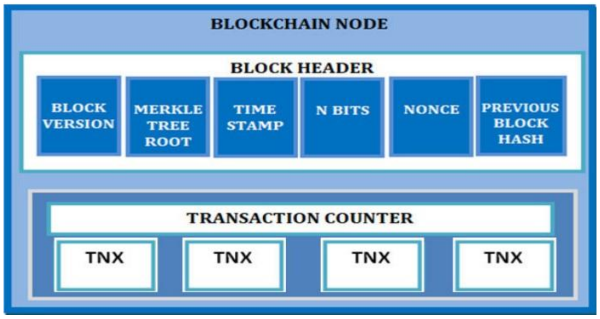


Figure 1: The general architecture of a Blockchain

"The blockchain is an unbreakable digital record for tracking economic transactions that can be modified to monitor almost anything with a value." There is no need for government intervention when we use blockchain technology, and there is no risk of fraud due to consensus confirmation. Instant transactions can be completed without incurring transaction fees by removing the need for a third-party. These characteristics help to increase financial efficiency [11]. Despite its many benefits, blockchain has several drawbacks, such as its extreme volatility. Anonymous transactions that are untraceable by a person or node outside the network have the potential to increase societal crime.

1.2.1 Challenges in Blockchain

1.2.1.1 Scalability

The number of transactions in the blockchain is growing every day, requiring more data to be kept. All nodes must store all transactions in order to legitimize them. Due to the block size constraint and the time it takes to create a new block, blockchain can only process seven transactions per second. Because miners favor transactions with a greater transaction fee, the real sufficiency of the blocks is insufficient, and many tiny transactions may be put off. As a result, scalability is a significant issue [13].

1.2.1.2 Privacy Leakage

Because users' transactions on the blockchain are performed with created addresses rather than real identities, they are considered secure. Users may generate several addresses in the event of data leaking. However, because the value of transactions is publicly viewable for each public key, the blockchain cannot guarantee transactional anonymity. The payment's anonymity must be enhanced on the blockchain [14].

1.2.1.3 Regulations and Laws

Many societal changes have resulted from the advent of blockchain, including changes in legal and legal systems. Due to a lack of legal oversight in the early phases of development, blockchain prompted a slew of legal difficulties. Only after a thorough understanding of the blockchain's properties can proper rules and regulations be strengthened. Most countries have begun to deploy blockchain as a result of strengthened regulatory procedures [15].

1.2.1.4 Governance

Blockchain offers a wide range of applications in government and infrastructure, and it is predicted to revolutionize government processes and roles. It also aids in the simplification of government organizational structures, data security, and governance and service process transparency. Because the blockchain is a distributed network without the need for a third party, it opens up more opportunities for policy progress, which is important because this is a pressing issue that requires immediate attention [16].

2. SYSTEM ARCHITECTURE AND RESEARCH METHODOLOGY

2.1 Integration of Cloud and Blockchain

The combination of blockchain and cloud computing ushers in a new era of data security and service availability. With its qualities, blockchain overcomes the majority of the cloud's research concerns.

2.1.1 Interoperability

Internal communication is not permitted on public clouds, which discourages many sectors from using the cloud. Consider the various clouds as nodes when integrating cloud with blockchain. The blockchain allows for inter-node communication. The data is shared across all nodes in the same network, resulting in each node having a copy of the transactions. It provides us with network transparency. They add each new transaction to the register, which is then circulate to all other nodes. Companies can add as many networks as they want while maintaining data accessibility, which adds validity to the network.

2.1.2 Data Encryption

We are all aware that data is decrypted before being stored in the cloud, raising concerns about data integrity. The blockchain network converts all block data into a hash code and produces a hash key for each block using cryptographic techniques. Consider the case when blockchain is used to keep track of cloud task scheduling. The control system that receives data from task scheduling generates hash code and records it in the blockchain network immediately to ensure timeliness and permanent data integrity. Block data integrity is preserved because to the blockchain's ability to use block discovery consensus processes. Each node in the network has a copy of each transaction, which gives us the availability and persistence we need to help the network withstand potential faults and assaults. While cloud-collected data is trustworthy, blockchain nodes maximize data availability and validity by presenting it as a 24/7 service with no downtime.

2.1.3 Service Level Agreements

These cloud agreements benefit the ISP or the user without equal justice. We can wield blockchain smart contracts to fix this issue. A blockchain smart contract facilitates the creation of trust between parties that are unfamiliar with each other. Smart Contracts are defined as a programme authored in programmable languages that runs inside a container on a blockchain. The smart contract can self-execute when a defined condition is satisfied on all nodes in the blockchain network. It also aids the parties in predicting the outcomes because contract execution is dependent on code available on a public network, and the contracts are verifiable because they have already been signed.

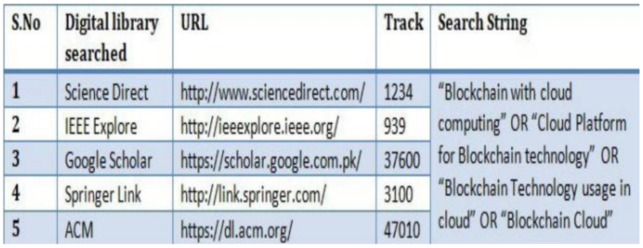
2.1.4 Cloud Data Management

The data saved in the cloud is frequently fragmented. The blockchain's data is processed in a very technical way. The data may be retrieved that used the hash key supplied for each block. Each block contains the hash key of the preceding block, as well as a key for keeping track of the network. The data in the block has been confirmed and can be accessed by the network's nodes.

2.2 Analytical Survey on Blockchain Cloud

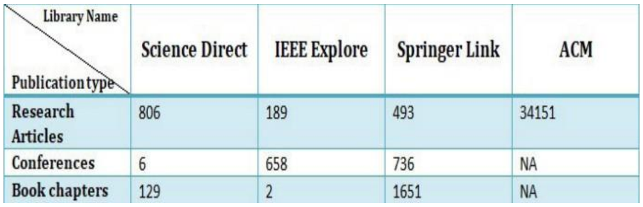
We can find a variety of papers based on Blockchain's support for cloud computing. To our knowledge, this is the first time a review of the literature on Blockchain Cloud has been accomplished. Table 2 displays a list of items available in several digital libraries, as well as our search term. Table 9 displays the publication history of various article kinds on selected literature in various libraries. We've included a bar graph below these data that shows a year-by-year examination of the number of articles published in various digital libraries. We may conclude from all of these findings that there is extensive study towards combining blockchain with cloud computing.

Table 2: String searching as well as result tracking in various digital libraries



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

Table 3: Track of article varieties in varied 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

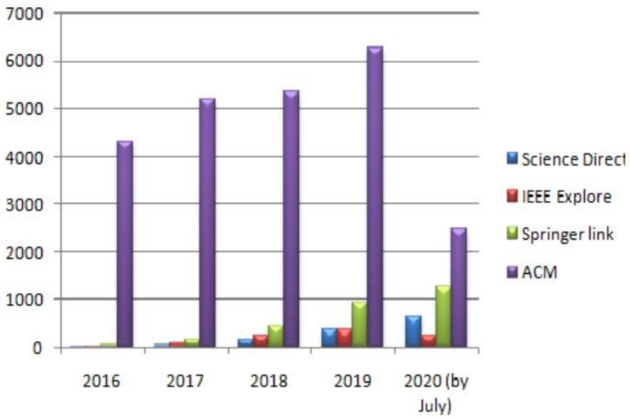


Figure 2: An assessment of publications produced in digital libraries by year

Figure 2 shows a graph that shows the year-by-year analysis of papers published in digital libraries. Cloud computing benefits from blockchain in numerous ways, including data openness, authorization, and cost-effective solutions. Figure 3 illustrates some of the most potential advantages that Blockchain could provide for cloud services. We have presented comparative research on blockchain and cloud services based on different security criteria, as we already know that blockchain may be deployed in public, private, and community modes and enable decentralization. One of the biggest challenges with cloud services is security of data. Based on this analysis, we can conclude that using the Blockchain platform would make cloud data safer.

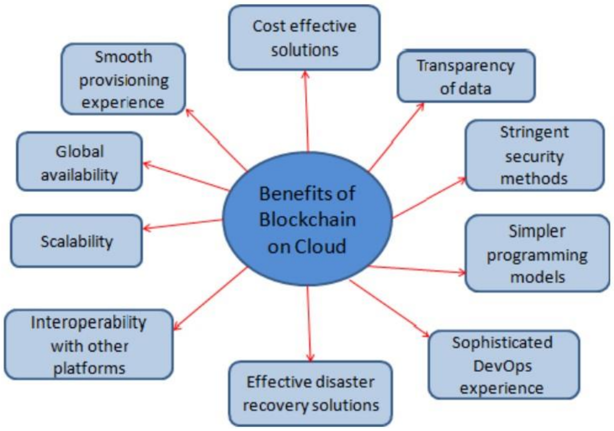

Benefits of Blockchain on Cloud
Cost effective solutions
Transparency of data
Stringent security methods
Simpler programming models
Sophisticated DevOps experience
Effective disaster recovery solutions
Interoperability with other platforms
Scalability
Global availability
Smooth provisioning experience

Figure 3: Benefits that Blockchain providing to cloud

Many Blockchain-Cloud applications can be used in our daily lives to increase the safety and security of our data. Blockchain-services Cloud's can be used in a variety of businesses. This connection can give us more storage options while also preserving the data that has been validated. The network's authorization will be monitored, and it will also improve the network's resilience. Figure 4 shows a mind map depicting several sorts of Blockchain Cloud Applications. The hereunder is the flow of blockchain with cloud data, as depicted in Figure 5. We can use blockchain services whenever there is a need to improve cloud data security.

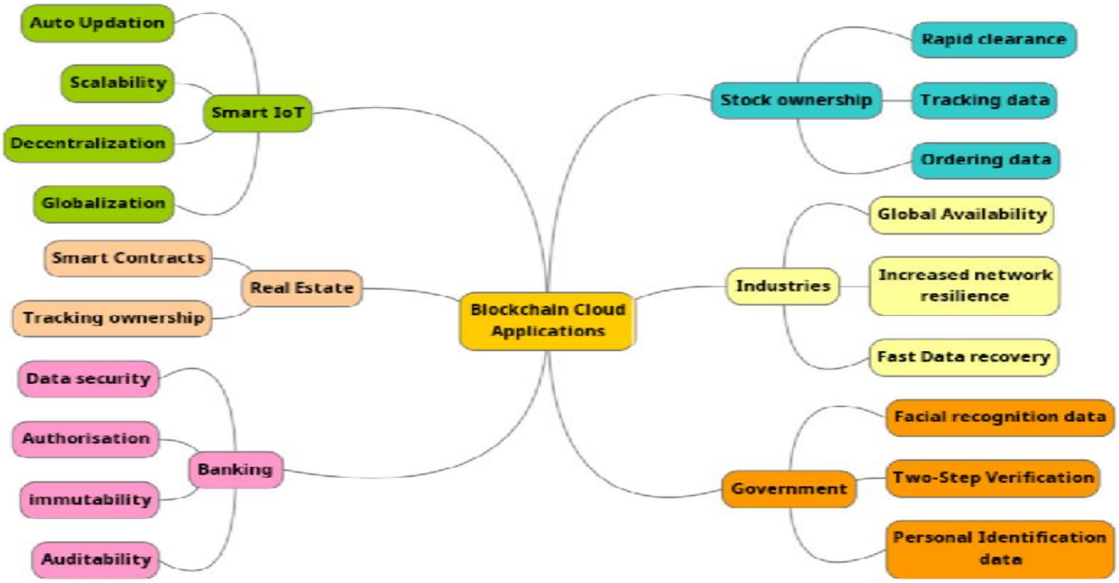


Figure 4: The many forms of Blockchain Cloud applications are depicted in a mind map

2.3 Model of Integrated Architecture

Figure 6 depicts the architecture of cloud computing and blockchain technology integration. The application layer sends the information to the server. Assume that when a user requests a transaction via the application layer, the details of the transaction are saved by establishing a block for each transaction. The blockchain network's data would be confirmed by blockchain network validating nodes before the block could be added to the network. Consensus will be used to validate the results. All other network nodes would be connected to the network and data would be transferred after the block is deemed authentic.

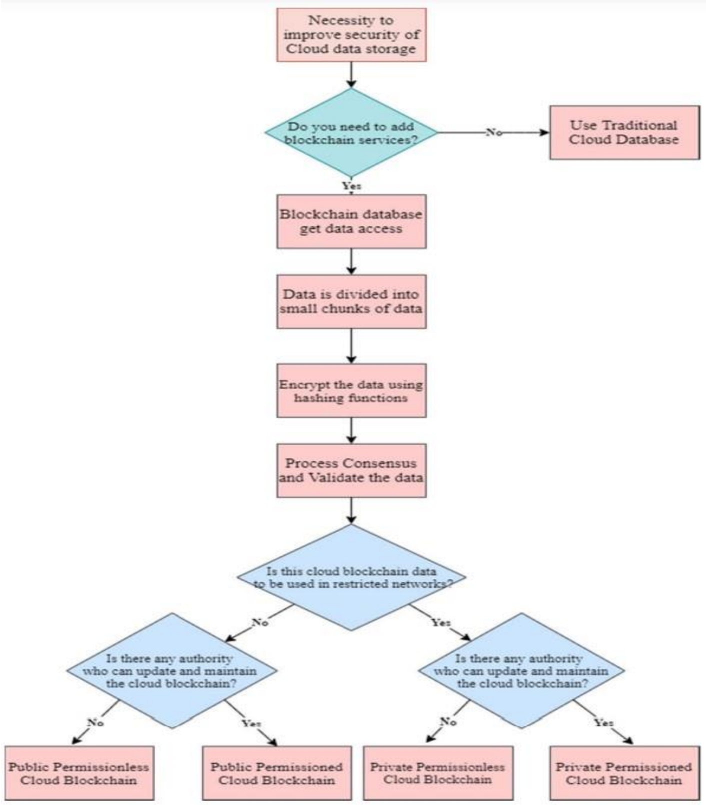

Necessity to improve security of Cloud data storage
Do you need to add blockchain services?
No
Use Traditional Cloud Database
Yes
Blockchain database get data access
Data is divided into small chunks of data
Encrypt the data using hashing functions
Process Consensus and Validate the data
Is this cloud blockchain data to be used in restricted networks?
No
Yes
Is there any authority who can update and maintain the cloud blockchain?
Is there any authority who can update and maintain the cloud blockchain?
No
Yes
No
Yes
Public Permissionless Cloud Blockchain
Public Permissioned Cloud Blockchain
Private Permissionless Cloud Blockchain
Private Permissioned Cloud Blockchain

Figure 5: Flowchart providing process of Blockchain with cloud data

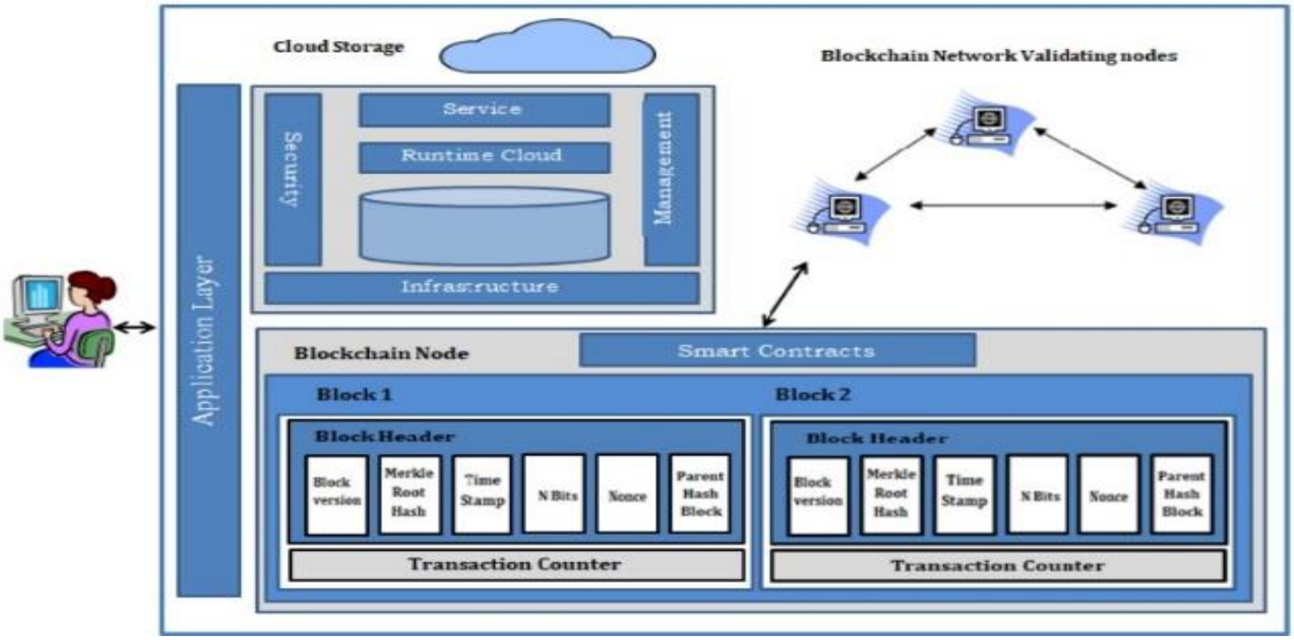


Figure 6: The architecture of cloud integrated with Blockchain

3. CONCLUSION

Cloud computing is a well-known and very well-established technology that has been around for a long time. However, key cloud computing concerns, such as data security, data management, and interoperability, remain unsolved. Blockchain technology is a new technology that is known for its security and authenticity, which are the major features that are causing the world to take notice of it. There will be numerous benefits in terms of usability, trust, security, scalability, data management, and other factors if blockchain and cloud computing are combined.

We briefly discussed blockchain technologies and cloud computing in this piece. The advantages of combining the blockchain network with a scalable cloud environment to improve confidence, server service, data security, and user data management were explored.

ACKNOWLEDGMENTS

My first and biggest gratitude goes to my mentor and adviser, Prof. Shailesh P. Bendale. During the long journey of this study, he/she supported me in every aspect. He was the one who helped and motivated me to propose re-search in this field and inspired me with his/her enthusiasm on research, his/her experience, and his/her lively character.

Prof. Shailesh Bendale, my guide, deserves a heartfelt thank you, for his excellent and valuable advice, as well as his constant support and encouragement.

I'd also want to express my gratitude to our department's leader, Prof. Shailesh P. Bendale, principal and management inspiring me and providing all lab and other facilities, which made this seminar presentation very convenient.

I'm really thankful to all those who rendered their valuable help for successful completion on seminar presentation.

REFERENCES

[1] 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.

[2] M. Nazir, ‘‘Cloud computing: Overview & current research challenges,’’ IOSR J. Comput. Eng., vol. 8, no. 1, pp. 14–22, 2012.

[3] 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.

[4] 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.

[5] 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

[6] 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.

[7] 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.

[8] S. Nakamoto, ‘‘Bitcoin: A peer-to-peer electronic cash system,’’ Bitcoin, Saint Kitts, Saint Kitts and Nevis, Tech. Rep., 2008.

[9] 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.

[10] 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

[11] 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.

[12] L. Popovski, G. Soussou, and P. B. Webb, ''A brief history of blockchain,'' Patterson Belknap Webb & Tyler, New York, NY, USA, Tech. Rep., 2014.

[13] 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.

[14] 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.

[15] 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.

[16] 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.