International Journal of Advance and Applied Research (IJAAR)
Peer Reviewed Bi-Monthly

ISSN – 2347-7075
Impact Factor – 7.328
Vol.9 No.4 Mar – Apr 2022

DEVOLVING A BLOCKCHAIN-BASED CLOUD COMPUTING SYSTEM: ARCHITECTURE AND RESEARCH ISSUES

Mrs Sushma Sumant
Department of Computer Science and Engineering,
JJTU, Rajasthan, India.

Dr. Vinod Vaze
Professor & Ph.D. Research Guide,
Department of Computer Science and Engineering,
JJTU, Rajasthan, India.

ABSTRACT:

It is a distributed ledger that contains all the information of the transactions that have been carried out and is spread across the nodes in the network that uses blockchain technology to keep track of them all. All of the transactions that take place in the system are confirmed by consensus procedures, and the data that has been stored cannot be changed once it is saved. Bitcoin, a prominent digital cryptocurrency, is based on blockchain technology, which is a prerequisite for its operation. It is the activity of storing, managing, and processing data on a network of distant computers that are hosted on the internet, rather than a local server or personal computer, that is known as cloud computing. It continues to face several issues, including data security, data management, compliance, and dependability. In this post, we've discussed some of the major difficulties that the cloud is facing, as well as some potential solutions that include merging the cloud with blockchain technology. We want to do a quick assessment of previous research that have focused on blockchain integration with the cloud in order to demonstrate their superiority. This study has also resulted in the development of an architecture combining blockchain with cloud computing, which reveals the connection between blockchain and cloud computing.

Keywords: *Cloud computing, Blockchain technology, data security, decentralization, data management.*

INTRODUCTION:

Enormous scope, disseminated registering innovation brought about distributed computing, which is currently a clear cut innovation with a long

history. Distributed computing might help clients by diminishing how much handling they need to do [1]. There are a few advantages, for example, lower equipment and support costs, worldwide accessibility, adaptability because of an exceptionally computerized interaction, and simplicity of increasing and down. Numerous enormous associations, like IBM, Google, Amazon, and Microsoft, have embraced distributed computing. [2] Many applications that have been created as models incorporate Google App Engine, Google Cloud Platform (counting the Amazon Cloud), the Elastic registering stage, and others. It gives us with the accommodation of a compensation for every utilization strategy as well as an adaptable IT foundation that is accessible through the web and convenient gadgets. Notwithstanding the way that the cloud gives a plenty of significant administrations, organizations have been languid to embrace it attributable to their stresses over protection. Security concerns and the challenges related with the cloud are significant negatives of undermining the cloud [3].

Blockchain When it comes to security and protection, innovation is the eventual fate of the areas that are attempting to better them. Blockchain is a disseminated record that records alter apparent information as a chain without the requirement for a focal position to keep up with track of the information. Blockchain innovation is contained hubs, which are members or gadgets that take an interest in it. Blockchain innovation makes a decentralized organization in which all organization hubs are effectively associated with approving and confirming the information they get. The information that will be put away on the blockchain will be scrambled with the assistance of cryptographic procedures. Each square incorporates a scrambled hash, a timestamp, and the hash of the previous square in the chain, by means of which the square will interface, which are all encoded. Subsequently, the information contained inside the blockchain is unalterable. [4] Blockchain empowers information security, and clients who take an interest in the organization will be affirmed in the organization, diminishing the issue about the information's classification.

By consolidating blockchain innovation with distributed computing, we can mitigate stresses over information protection and security, consequently

working with the development of distributed computing. It improves information security, increments administration accessibility, and has the ability to oversee cloud information. All through this exposition, Section II acquaints you with the essential thoughts of distributed computing. Segment III talks about blockchain innovation, including its properties, blockchain sorts, blockchain layers, engineering, working, and other driving applications. Segment IV talks about blockchain innovation in more detail. Segment IV features the benefits of consolidating distributed computing with blockchain innovation, as well as the suggested engineering for doing as such.

CLOUD COMPUTING:

These days of the Internet, there are a large number of sites that are housed on the on the web. To work the facilitated site, an enormous number of servers are required, which is very costly. This implies that the traffic rate on such servers should stay predictable, and they should be observed and kept up with on a continuous premise. It will be important to enroll more work force to orchestrate and keep up with these servers. Every one of the information will be put away in server farms. Persistent endeavors in keeping up with the server issue, as well as the endeavors of the work force, may occupy us from our central goal of accomplishing business targets. We are carrying out "Distributed computing" to dispense with this tedious upkeep. "Distributed computing is the procedure of putting away, making due, and handling information from any area in the world by means of the utilization of an organization of far off servers. Rather than a neighborhood server or PC, it's used in this present circumstance." Cloud registering administrations, like information stockpiling and application conveyance, are provided to the gadgets of the organization over the web [5]. Many advantages are given by distributed computing, which is a bunch of administrations that consolidate server farms, assets, and servers and makes them accessible through the web. The installment for these administrations depends on a for every utilization premise. The administrations are available from anyplace on the planet and at a significantly lower cost, permitting laborers to work all the more cooperatively together. The product that is accessible in the

cloud will be consequently refreshed, making the cloud a straightforward and advantageous climate to keep up with. Command over the archives put away in the cloud will be practiced by the assistance purchaser also. It additionally has a few limitations [6, for example]. Because of the way that cloud information is entirely versatile, there are different security and protection worries that should be tended to, as well as the way that it is liable to attacks. At the point when there is a high volume of clients, there is a potential that the cloud might encounter personal time.

Distributed computing offers a wide scope of administrations, which are fundamentally partitioned into three conveyance types. The principal administration is Software as a Service (SaaS), which is like an application that is facilitated and made accessible to clients through the web. The Cloud Service Provider presents the entire program or undertaking as a solitary foundation of programming working in the cloud, equipped for giving a wide scope of administrations to an enormous number of clients. Clients of cloud administrations don't approach or command over the cloud foundation. SaaS applications, for example, Amazon web administrations, SalesForce.com, and Google Mail are outstanding instances of this sort of administration. Stage as a Service (PaaS) is the second sort of administration (PaaS). The cloud specialist organization empowers us to introduce our application as well as a set-up of programming dialects on the stage given by the supplier. There is a differentiation among SaaS and PaaS in that SaaS stores the entire application in the cloud, while PaaS offers a stage on which the program might run. To act as an illustration of PaaS, the Google internet searcher is the most well known decision. It is additionally conceivable to get to capacity, handling, and different assets straight over the organization by means of Infrastructure as a Service (IaaS), which is the third assistance accessible. While giving foundation as an assistance, virtualization is used to disseminate actual assets to satisfy the asset requests of cloud clients. The best virtualization methodology is to make independent virtual machines that are disconnected from the fundamental equipment as well as from other virtual machines. To give security, they give

every server a one of a kind IP address. Amazon EC2, GoGrid, and different IaaS administrations are the best models [7].

CLOUD DEPLOYMENT MODELS:

Public Cloud:

The public cloud is a registering climate that might be shared by various clients that need admittance to similar PCs, which are possessed and overseen by specialist organizations. The cloud foundation is accessible for use by the overall population and might be utilized by a few organizations on the off chance that it is purchased in a powerful way. The cloud specialist organizations are responsible for facilitating and keeping up with these mists. In specific cases, the cloud supplier will have the client to diminish the client's gamble and expenses for a restricted timeframe. Microsoft Azure and Google App Engine are two instances of distributed computing stages. [8]

Private Cloud:

This is fundamentally founded on the longing of single clients, and it gives responsibility for, as well as information security, and it is client-committed, in addition to other things. It is utilized to have the foundation and applications that are possessed by the clients and are given to them. When contrasted with a public cloud, it is safer yet additionally more exorbitant. In private mists, guidelines about security and data transfer capacity limits are set up, also. Clients can streamline client access while additionally confining the organizations that are used in the private cloud. Private mists, like the Eucalyptus System, are the best models accessible [9].

Hybrid Cloud:

Consolidating at least two cloud organization strategies is practically equivalent to doing as such. The half and half cloud offers on-request help as well as remotely conveyed adaptability. These are to a great extent zeroed in on private server farms, albeit additionally depend on open cloud assets to offer computational types of assistance. It is feasible to convey security administrations by means of the utilization of an all around planned half and half cloud, however the test is in productively constructing and controlling such a

framework. Amazon Web Services [10] is a notable illustration of a half and half cloud engineering.

Community Cloud:

This site is fundamentally expected for a specific gathering of clients addressing an assortment of associations that have normal issues. It very well may be possessed, made due, and worked by a solitary organization or by a gathering of firms from the neighborhood local area. This sort of cloud is exceptionally compelling in the instruction and banking enterprises. A people group cloud, like Facebook, is an illustration of this [11].

RESEARCH ISSUES IN CLOUD:

Reliability:

Cloud administrations are available to cloud clients whenever of day or night. There have been a couple of occurrences when the server has needed to suspend its administrations attributable to support concerns or a period limitation. Cloud purchasers have come to expect more contributions, laid out guidelines, and best practices from the cloud specialist organizations of yesterday. The servers that are available in the cloud are in like manner indistinguishable from the servers that are accessible on-premises. They additionally experience server personal times, and they depend vigorously on a cloud specialist organization for an assortment of reasons. It is conceivable that assuming a client chooses a specific server, they will be tied onto that server, representing a potential business risk [12].

Compliance:

There are a few limitations administering admittance to capacity and utilization of information, as well as prerequisites for successive announcing and review trails. In specific conditions, clients might have explicit requirements for the server farms oversaw by cloud suppliers, which would require the execution of consistence guidelines [13].

Service Level Agreements:

Cloud administrations will be given as per Service Level Agreements, which will empower a few duplicates of an equivalent application to be cloned on

various servers at whatever point there is a need, contingent upon the need, to be made accessible. In the event that the program is considered to be insignificant, the cloud might decide to close it down or diminish its usefulness. The most troublesome trouble for cloud clients is assessing the Service Level Agreements (SLAs) that have been settled upon with cloud providers. Most organizations foster assistance level arrangements (SLAs) that favor them while giving the absolute minimum as far as client advantages like information security, personal time, and estimating structures. The cloud clients ought to take extraordinary watchfulness in managing these issues prior to going into an agreement with a cloud specialist organization [14].

Cloud Data Management:

Information the executives is a fundamental review subject since cloud information might be tremendous and unstructured or semi-organized in nature, making it a provoking issue to address. Since they don't approach the actual security arrangement of the server farms, specialist organizations should rely upon the foundation supplier to give far reaching information insurance to their clients. Indeed, even on virtual PCs, the supplier can somewhat set the security boundaries without monitoring whether the safety efforts are being executed securely. In these cases, the foundation supplier should achieve prerequisites, for example, auditability to bear witness to the security settings of utilizations, classification with the end goal of secure information access and move, and accessibility to offer dependable assistance. Classification might be acquired by the utilization of cryptographic conventions, while discernibility can be achieved using distant authentication instruments. Notwithstanding, this isn't generally practicable because of the way that virtual machines (VMs) progressively move starting with one area then onto the next. Subsequently, taking on distant authentication will at this point not be a suitable choice [15].

Data Encryption:

Information is scrambled to guarantee the information's protection and security. There are numerous levels of safety accessible, including low, moderate, and significant levels. Consider the Web administrations APIs that are utilized to arrive at the cloud either by means of a PC program or through clients that

are made to use those APIs to speak with the cloud. SSL encryption is utilized for access, and being a traditional practice is generally accepted. At the point when the thing is shipped off the cloud, the information would be scrambled and kept in the cloud till the article is returned. Unscrambling and putting away information without first scrambling it prior to placing it in the cloud [16] are two manners by which information security is compromised [14, 15].

Interoperability:

Interior correspondence between frameworks is fundamental for the trading of data and the utilization of that data inside the framework. Not at all like private cloud organizations, public cloud networks are intended to work as shut frameworks and are not expected to associate with each other. As a result of an absence of interior correspondence across cloud frameworks, the business can't consolidate its data innovation frameworks in the cloud climate. Fostering a solitary tool compartment to associate different applications across current frameworks and across various cloud suppliers [17] is a fundamental initial step for undertakings.

NODES OF BLOCKCHAIN:

A hub in the blockchain is a gadget that is associated with the blockchain network and might be portrayed accordingly. The work performed by a hub decides the sort of hub that it is classified as. Hubs might be characterized into numerous classifications. They are as per the following:

Mining Nodes:

Mining hubs are continually producing blocks for the blockchain, regardless of anything else. These hubs simply check whether the square might be added to the rundown, which is essential for the interaction known as mining. Mining hubs are not answerable for block support; they are essentially liable for making blocks and adding them to the chain. Blocks that have been added to the blockchain are communicated all through the organization, where full hubs confirm them and integrate them into the blockchain.

Full or Super Nodes:

Full hub control is answerable for keeping up with and sending duplicates of squares to all organize hubs. Their obligation is to approve exchanges up to the beginning square, which happens during the distributing system. Following approval, the information is shipped off any remaining hubs in the organization to confirm the unwavering quality of the blockchain. At the point when there are more hubs associated with a more decentralized network, it turns out to be more challenging to hack into the framework. It is feasible to assign a Node as a Super Node in light of the quantity of exchanges made by the hub when it is completely functional. Super Nodes are continually dynamic and connection the leftover complete hubs, making them show up all through the organization [19]. They are otherwise called "super hubs."

Light Nodes:

Light hubs act along these lines as full hubs, then again, actually they just hold a negligible portion of the entire square of information. They essentially hold the past exchange blocker and are answerable for approving the blockchain and illuminating different hubs in the organization. Since they are attached to the parent hub, i.e., the Full hub, they are less strong than full hubs. When a full hub is hacked and the adulterated information it contains is caught and excused by the light hub, the light hub might give the entire hub data to the blockchain that ought to be responsible for keeping up with the blockchain being referred to. Since they don't occupy a lot of information room, they add to the decentralization of the organization and the capacity to navigate tremendous distances at a lesser expense than complete hubs [20].

WORKING OF BLOCKCHAIN:

Blockchain innovation proposes making blocks that hold information and are associated with the chain of exchanges. Blocks are associated together by the way that each square contains the square header from the previous square [21]. In the event that any information in the earlier square is modified, the hash key will change also, bringing about a crisscross of the hash key happening in the following chain of squares subsequently. It safeguards the data from being

messed with. At the point when a client wishes to move specific exchange information to another client, that exchange will be recorded as a square on the blockchain. To add the blockchain block, the square should be communicated to any remaining hubs on the organization [22, 23]. The exchange should be supported by the excavators of the hub. At the point when a square is framed, the excavators are provided the capacity to endorse it by addressing computationally extreme difficulties that are introduced to them. After effective confirmation, the square is transferred to the blockchain, along these lines finishing up the exchange. Following, we should figure out which client distributed the following square in the chain of occasions. Blocks that have been confirmed are joined into a chain, which thusly makes a blockchain network [24].

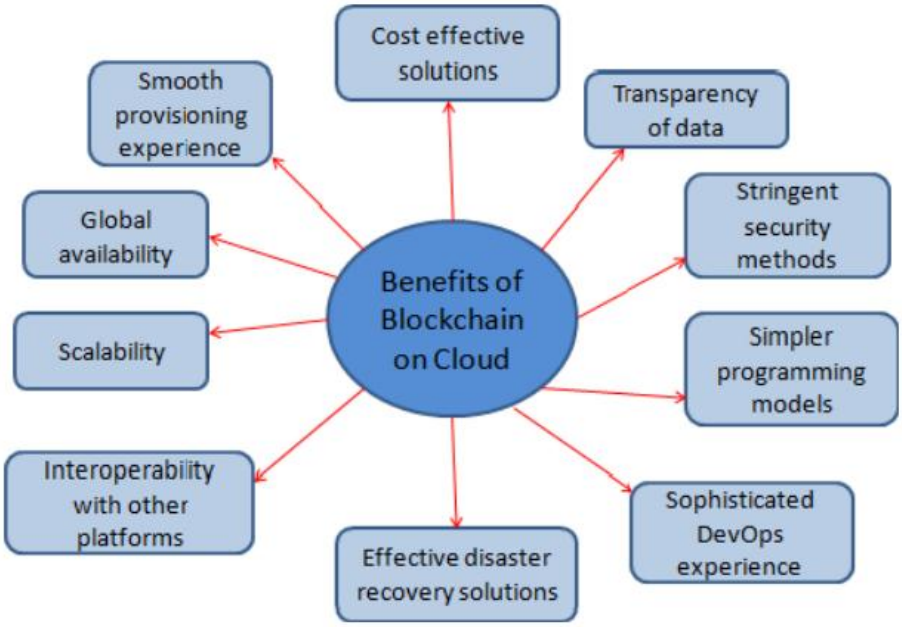

Figure 1. Benefits That Blockchain Providing to Cloud

CONCLUSION:

Distributed computing is a notable innovation that has been around for a significant stretch of time. Be that as it may, various distributed computing concerns, like information security, information the executives, interoperability, etc, keep on being a wellspring of dissatisfaction for some people. Blockchain innovation is a new and creating innovation that is notable for its security and genuineness, which are the essential characteristics that are making the world shift to its side. Blockchain innovation is an innovation that is still in its

beginning phases. By consolidating blockchain innovation with distributed computing, there will be a few advantages concerning convenience, trust, security, adaptability, information the executives, and an assortment of different perspectives. In this exposition, we made sense of distributed computing and blockchain innovation in a fundamental way. We talked about the benefits of associating the blockchain network with an adaptable cloud climate to further develop certainty, waiter administration, information security, and client information the executives, in addition to other things.

REFERENCES:

[1]. A. Vatankhah Barenji, H. Guo, Z. Tian, Z. Li, W. M. Wang, and G. Q. Huang, "Blockchain-based cloud manufacturing: Decentralization," 2019, arXiv:1901.10403. [Online]. Available: http://arxiv.org/ abs/1901.10403

[2]. A. Harshavardhan, T. Vijayakumar, and S. R. Mugunthan, "Blockchain technology in cloud computing to overcome security vulnerabilities," in Proc. 2nd Int. Conf. I-SMAC (IoT Social, Mobile, Anal. Cloud)(ISMAC) I-SMAC (IoT Social, Mobile, Anal., Cloud)(I-SMAC) 2nd Int. Conf., Aug. 2018, pp. 408–414.

[3]. A. Jabbari and P. Kaminsky, "Blockchain and supply chain management," Dept. Ind. Eng. Oper. Res., Univ. California, Berkeley, CA, USA, Tech. Rep., 2018.

[4]. M. K. R. Ingole and M. S. Yamde, "Blockchain technology in cloud computing: A systematic review," Sipna College Eng. Technol., Maharashtra, India, Tech. Rep., 2018.

[5]. C. Qiu, H. Yao, C. Jiang, S. Guo, and F. Xu, "Cloud computing assisted blockchain-enabled Internet of Things," IEEE Trans. Cloud Comput., early access, Jul. 23, 2019, doi: 10.1109/TCC.2019.2930259.

[6]. D. Dujak and D. Sajter, "Blockchain applications in the supply chain," in SMART Supply Network. Cham, Switzerland: Springer, 2019, pp. 21–46.

[7]. D. A. Fernandes, L. F. Soares, J. V. Gomes, M. M. Freire, and P. R. Inácio, "Security issues in cloud environments: A survey," Int. J. Inf. Secur., vol. 13, no. 2, pp. 113–170, 2014.

[8]. D. B. Rawat, V. Chaudhary, and R. Doku, "Blockchain: Emerging applications and use cases," 2019, arXiv:1904.12247. [Online]. Available: https://arxiv.org/abs/1904.12247

[9]. D. K. Tosh, S. Shetty, X. Liang, C. Kamhoua, and L. Njilla, "Consensus protocols for blockchain-based data provenance: Challenges and opportunities," in Proc. IEEE 8th Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON), Oct. 2017, pp. 469–474.

[10]. D. Tosh, S. Shetty, X. Liang, C. Kamhoua, and L. L. Njilla, "Data provenance in the cloud: A blockchain-based approach," IEEE Consum. Electron. Mag., vol. 8, no. 4, pp. 38–44, Jul. 2019

[11]. D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," 2019, arXiv:1906.11078. [Online]. Available: http://arxiv.org/abs/1906.11078

[12]. E. Gaetani, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, "Blockchain-based database to ensure data integrity in cloud computing environments," Res. Center Cyber Intell. Inf. Secur., La Sapienza Univ. Rome, Rome, Italy, Univ. Southampton, Southampton, U.K., Tech. Rep., 2017.

[13]. M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, and A. Peacock, "Blockchain technology in the energy sector: A systematic review of challenges and opportunities," Renew. Sustain. Energy Rev., vol. 100, pp. 143–174, Feb. 2019.

[14]. D. Efanov and P. Roschin, "The all-pervasiveness of the blockchain technology," Procedia Comput. Sci., vol. 123, pp. 116–121, 2018, doi: 10.1016/j.procs.2018.01.019.

[15]. F. Knirsch, A. Unterweger, and D. Engel, "Implementing a blockchain from scratch: Why, how, and what we learned," EURASIP J. Inf. Secur., vol. 2019, no. 1, p. 2, Dec. 2019.

[16]. S. Sharma, G. Gupta, and P. R. Laxmi, "A survey on cloud security issues and techniques," 2014, arXiv:1403.5627. [Online]. Available: http://arxiv.org/abs/1403.5627

[17]. G. J. Katuwal, S. Pandey, M. Hennessey, and B. Lamichhane, "Applications of blockchain in healthcare: Current landscape & challenges," 2018, arXiv:1812.02776. [Online]. Available: http://arxiv.org/abs/1812.02776

[18]. H. Kaur, M. A. Alam, R. Jameel, A. K. Mourya, and V. Chang, "A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment," J. Med. Syst., vol. 42, no. 8, p. 156, Aug. 2018.

[19]. H. Zhu, Y. Wang, X. Hei, W. Ji, and L. Zhang, "A blockchain-based decentralized cloud resource scheduling architecture," in Proc. Int. Conf. Netw. Netw. Appl. (NaNA), Oct. 2018, pp. 324–329.

[20]. Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," Int. J. Web Grid Services, vol. 14, no. 4, pp. 352–375, 2018.

[21]. J. Kołodziej, A. Wilczynski, D. Fernandez-Cerero, and A. Fernandez-Montes, "Blockchain secure cloud: A new generation integrated cloud and blockchain platforms–general concepts and challenges," Eur. Cybersecurity, vol. 4, no. 2, pp. 28–35, 2018.

[22]. J. Park and J. Park, "Blockchain security in cloud computing: Use cases, challenges, and solutions," Symmetry, vol. 9, no. 8, p. 164, Aug. 2017.

[23]. J. Singh and J. D. Michels, "Blockchain as a service (BaaS): Providers and trust," in Proc. IEEE Eur. Symp. Secur. Privacy Workshops (EuroS PW), Apr. 2018, pp. 67–74.

[24]. K. Bendiab, N. Kolokotronis, S. Shiaeles, and S. Boucherkha, "WiP: A novel blockchain-based trust model for cloud identity management," in Proc. IEEE 16th Int. Conf. Dependable, Autonomic Secure Comput., 16th Int. Conf. Pervasive Intell. Comput., 4th Int. Conf Big Data Intell. Comput. Cyber Sci. Technol. Congr. (DASC/PiCom/DataCom/CyberSciTech), Aug. 2018, pp. 724–729.