International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-12, October 2019

Application of Block chain in Cloud Computing

Simanta Shekhar Sarmah

Abstract: ***Blockchain technology is recent and eminent financial technology that completely transform the business transactions. It's a decentralized network, that support and employ variety of cryptography models. This robust and flexible secured transactions is being integrated with another eminent computing paradigm, cloud computing. In this paper, we make an attempt to review about the application of blockchain in cloud computing system. Firstly, the concept of blockchain is briefly discussed with their advantages and disadvantages. Second, the concept of cloud computing is briefly demonstrated with blockchain technology. Finally, prior papers are reviewed and presented in tabular form. It dictates that the research gaps, still, pertains in field of blockchain based on cloud computing systems. This paper assists the upcoming researchers in this field for designing novel secured models.***

Keywords: ***Blockchain technology, Cloud computing, Research gaps, Security and the computational cost.***

I. INTRODUCTION

Recent developments made in information processing systems has attracted the common users for better storage of their data. The present field, cloud computing is employed as utility model for cloud users. Depends on their premises, the cloud users can access, share (or) transacts the data, at anywhere, anytime. It indirectly implies that cloud users do not have direct control on resources, after uploading to the cloud server. Based on terms and conditions, the cloud provider offers services on as-is and as-available form [1]. As we dive deeper into "information age', an immense growth can be witnessed in terms of volume, velocity and variety of data on internet. Data can be originated from multiple types of sources such as mobile devices, sensors, archives and the social networks. This kind of data explosions poses a serious research questions like 'how to efficiently and optimally administer large amounts of data and recognize the new preservation ways of unlocking information. Millions of transactions are being generated that composes of sensitive heterogenous and homogenous data that do not compromise the quality of service in end users [2]. Challenges persists in information processing units supports variant financial markets for development of next generation financial technology for secured use of network technology and the user communication. In order to deal with financial security, blockchain technology has been introduced. It is defined as public ledger network that provide better secured online transactions. The concept of blockchain model introduced since, 2008 [3]. The first cryptocurrency that make use of blockchain based approach is 'bitcoin'.

Revised Manuscript Received on October 30, 2019.
* Correspondence Author
Simanta Shekhar Sarmah*, Business Intelligence Architect, Alpha Clinical Systems Inc, USA.

The transaction process via blockchain concept are mainly done via authentication process, where the customer performs virtual transactions. This block is periodically updated and reflected in the electronic money transaction details to share the latest transaction detail block. The rest of the paper is organized as follows: Section II presents the aim and objectives of the research; Section III presents the literature review of cloud computing systems and finally, concludes in Section III with possible research gaps.

II. RESEARCH AIM AND OBJECTIVES

The purpose of the study is to identify the purpose of blockchain technology in the field of cloud computing and to identify the potential threats and challenges in the application of blockchain technology when applied in the area of cloud computing. The following objectives are stated below:

To evaluate the digital brand marketing strategies in the context of national Tourism brand marketing.

- To identify the scope of blockchain technology and its application on the area of cloud computing.
- To identify the security significance of blockchain technology on its application to cloud computing.
- To analyse the latest solution in the context of security aspects by maintaining confidentiality, integrity and authentication of public information.

III. LITERATURE REVIEW

This section deals with the literature related to the concept and algorithms of blockchain technology and cloud computing frameworks. The section encounters the various theoretical framework and algorithms in the context of blockchain technology a cloud computing.

A. Blockchain technology:

This section demonstrates the generic model and the working process of blockchain model. Generally, the blockchain architecture is developed as a reference architecture for cloud computing, edge computing and fog computing. It shall also be merged with another large-scale distributed model. In present days, it's been combined with cloud system to ensure better secured system.

- Origins of Blockchain: Blockchain technology is a sort of distributed architecture that make use of cryptographic signed transactions [4]. It operates in block-wise manner. Each block is linked with cryptographic systems. Authenticity of the transactions should validate and evaluated at each single point of failure. It employs several features of the Peer to Peer (P2P) model. This model does not incur the broker fees for authorizing the transactions. Since, this blockchain process ensures robust

- and scalable security to its end systems, the growth of blockchain technology is inclined. The hackers also find hard to exploit the vulnerabilities to the transactions systems. Thus, the transactions are easier and open access. The below fig.3.1 presents the basic components of blockchain P2P architecture.
- Hashes: It is one of the main components in blockchain model which adopts different use cases. Its main task is to encrypt the data presented in block. It computes any size of data. The changes made in input can depicts the output with that specified changes. SHA-256 algorithm is being widely used for many real-time applications.

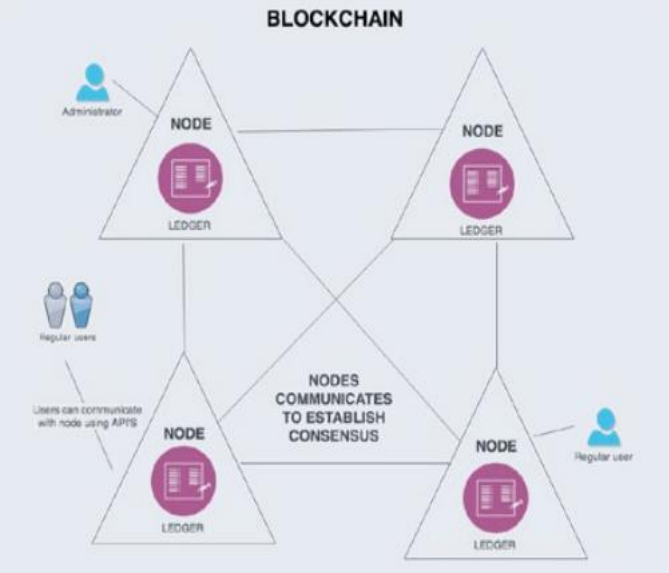

Fig.3.1. Blockchain technology in P2P architecture

- Ledgers: It composes of set of transactions. Each node has a copy of transactions i.e. Ledger. In conventional model, pen and paper are widely used for maintaining the ledgers. The same concept has been applied with adoption of new computing technologies. Hence, a centralized ledger is being used with some demerits, such as, single point of failure i.e. Sudden data loss & centralized committed transaction verifies with third party agent.
- Blocks: Each node in blocks receives a transaction id given by end users. With this transaction index, the further operations are proceeded until the process ends. The mid-operations will not save in transactional process. A transaction pool, a queue is maintained for all committed transactions. Mining nodes are responsible for updating the transaction process at every phase. Hence, a block composes of full set of transactions. The invalid transactions are rejected by blockchain mechanism. This method confirms the rigidness of data as generated hash would dramatically change by a change in single bit of the block. In addition, a copy of the hash of every block is shared among all the nodes in order to improve security. This system prevents any change since every node can check if the hash matches. The fig.3.2 presents the model of blockchain system which operates using merkle tree structure.

The blocks in blockchain model composes of following components, namely,

- Block number (or) block height.
- Hash value of present block
- Hash value of previous block
- Merkle tree root hash
- Timestamp
- Size of the block
- Transactions list in block

- Processes in blockchain: Most of the nodes in blockchain networks owned by different organizations. Depends on ledger content, the nodes are communicated. By doing so, the node agreement issue degrades the performance of the system. The blockchain receives transaction requests, which are submitted by users, to perform the operation it has been designed for. As a result of the execution of such a transaction, one or more ledgers store a record of the transaction which will never be modified or deleted. With this process, the immutability of the blockchain is achieved.

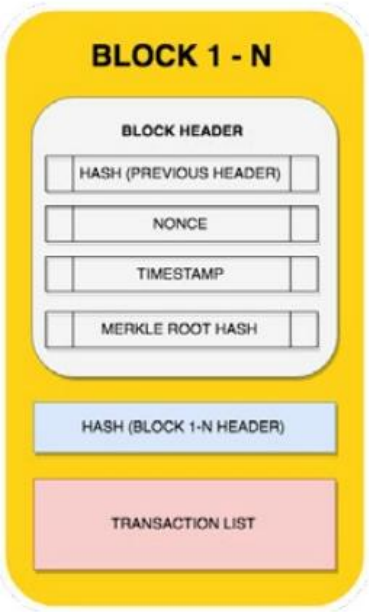

Fig.3.2 Generic blockchain model

- Blockchain security: It is a kind of network environments where transaction data and the parameters are close to business logic. Asymmetric Key Cryptography is widely used for blockchain transactions. Block of keys, viz, public and private key are used for entire transactions. Private key is used for validating the signatures on transactions. Public key checks generated signature by private key.

B. Concept of Bitcoin:

Bitcoin can be defined as an electronic cash system where each electronic coin is a chain of digital signatures. Each owner communicates by digital signing and then transfer the coin based on hash transaction of current and previous history. Depends on their ownership, a payee can verify the signatures [5]. The fig. 3.3 explain the concept of bitcoin.

The working process of bitcoin is explained as follows:

a) Fresh transactions are initially broadcast to all nodes.
b) The fresh transaction is being collected by each node in block.
c) Proof-of-work on every block should assigned.
d) When proof-of-work is been find by node, then broadcast message send to all nodes in that block.
e) Only valid transactions are processed, rather than spent.
f) Nodes accept the blocks based on their hashing facilities.

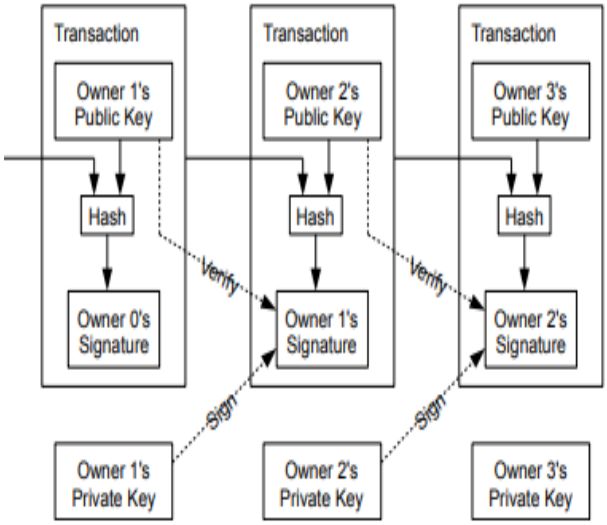

Fig.3.3 working process of bitcoin

C. Authentication- Insight on cloud computing:

An incentive and attractive computing services delivered by the cloud computing via resource pooling and virtualization techniques. Security as a service is a new concern in cloud computing paradigms. An organization can offers many application services to the end-users. E-mail and the web servers are the best instances of application service providers. The company may possess certain boundaries on their services, all services should adopt by the authorized clients. This means that the client should have security context for each application server and log in before it can consume any service [6]. Similar situation can be seen when a user accesses resources in various security domains. It is not considered as an effective solution in terms of security, system coordination and management standpoint if authentication requires several security credentials. During the cloud migration, organizations encounter similar issues as well. Variant entities are presented to acquire those services, and, thus, a proper security mechanism is required. As services grows, the management of access control becomes complex and expensive. Most of the applications focus on functionality of system and the organization value. Thus, a single security policy management ensures better authorization systems with flexible and scalable. Besides, changing a policy becomes very simple because of a single location for policy management. Compromise of authorization system has become much harder as the protection and auditing of these systems are managed separately.

D. Parameters in blockchain technology:

The parameters involved in success of blockchain technology, are:

- E-Cash and its security: e-Cash is the new concept that makes a revolution in e-commerce world. It's just replaces the paper and coin of the old systems. Credit card is one of the best e-cash systems. This system requires a trusted environment with merchants and agents. Bank or issuer stores the E-cash and during the making of a payment, consumer needs to request for it.[7]. Different from online, off-line e-cash is kept by consumer in a devise such as smart card or other type of token. Each of this implementation can be classified as identified (traceable) or anonymous (untraceable). By identified implementation, it means each transaction needs verification and validation from third party such as bank. This implementation offers better security because it uses encryption and digital signature to secure and authenticate the E-cash message respectively. The fig. 3.4 presents the workflow of e-cash processes, in which entities like bank, consumer and the merchant should be mutual trusted environment.

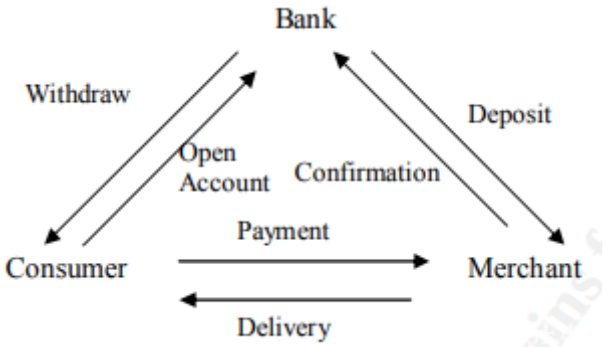

Fig.3.4. Workflow of e-cash

- Access control: It's a kind of systems that facilitate security to the data stored. The resources are valuable in terms of data, services and the computational systems. In order to create trusted environment, the entity should hold different access rights. Some scenarios require that access rights can be transferred from a subject to another for some reasons. For instance, a user could sell its access right to another user [8]. Similarly, an employee of an organization who needs to perform a required computation on a Virtual Machine deputes the task to another employee who also needs to access the same machine.

E. Integration of Blockchain in cloud computing and its security:

Cloud computing composes large networks of virtualized services, namely, hardware resources and the software resources. Any sort of services belongs to data centres and known as data farms [9]. The fig. 3.5 demonstrates the P2P based cloud architecture.

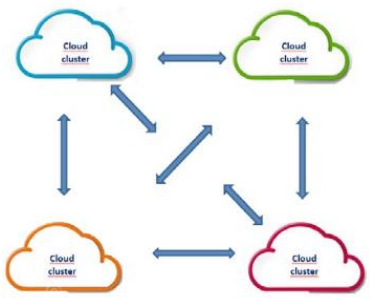

Fig.3.5. P2P based cloud architecture

There are two methods available for integrating the blockchain in cloud systems:

a) Integrating blockchain with cloud for facilitating enterprise networks like storage, replication and access to transactional database.
b) Integrating with security concepts between task, user, and data management in clouds.

The following are the challenges and requirements involved in support of cloud based blockchain transactions [10]. The transactions involved in blockchain networks are enormous in nature. Elasticity and scalability are the main function of the cloud systems in dynamic environment.

a) In view of security: From user, the data are hidden and stored in data centres. Thus, the transactional activities should be assigned with tuning purposes. It means that the cloud service allows their customers to have control over the locations in which their data is stored and processed.
b) System resilience and fault tolerance: The system should capable of finding the alternate node, if any node fails in network. Thus, a node replication mechanism in data centres and use of multiple software applications.
c) Security towards blockchain improvements: Software should centrally assign in distributed cloud environment and the use of multiple software applications.

F. Research Gap:

The research gap assists for finding the scope of the research study. The review study is given in tabular form for better convenience.

Sl. No	Paper title	Methods	Gaps	Results
1	Proof-of-Work consensus approach in Blockchain Technology for Cloud and Fog Computing using Maximization-Factorization Statistics	Statistical method with POW consensus approach for cloud and fog computing. In addition to, expectation maximization and the polynomial matrix factorization	Longer duration is required for data access. It enhanced the consensus delay by misclassified data blocks	It takes less time for converging the solutions and configures all mathematical models.
2	A Blockchain Future to Internet of Things Security: A Position Paper	This survey paper has analysed IoT datasets and its impact over blockchain mechanism since 2016 till present.	They discussed about the future of blockchain by identifying the possible threats. The system enhanced the data intervention. Possibility of hardware and software are being easily compromised.	They discussed reliability and the data distribution over public network.
3	Auction Mechanisms in Cloud/Fog Computing Resource Allocation for Public Blockchain Networks	They suggested an auction-based market models that efficiently allocates the resources to the users. A decentralized management system was introduced. It consists of two bidding schemes, namely, constant demand scheme and the multi-demand scheme which achieved the optimal social welfare.	When the level of blockchain mining increases, the blockchain developer gradually smaller the marginal gains. Though, they prevented the double spending attacks, because of adverse effect of block broadcasting process.	Winner selection problem is framed and obtained an optimal solution. Depends on miner selection, individual rationality and the truthfulness at guaranteed lower bound.
4	Controllable and Trustworthy Blockchain-based Cloud Data Management	They developed controllable blockchain data management for cloud systems. Data is being analysed in terms of bilinear pairing.	The model has limited impacts over efficiency of the document selections. The encrypted requests on modified document incurs higher computational cost.	Security and the utility of the cloud environment were improved by trustworthy parameters.
5	Integrated Blockchain and Edge Computing Systems: A Survey, Some Research Issues and Challenges	They studied the integrated blockchain and edge computing systems which faced the challenges of decentralized environment.	Mobility of the edge computing pushes the cloud resources and the services for denial of edge. It incurs excessive overheads during scalability analysis.	It enhanced the security of the systems during network server partitioning and the self- organization schemes.
6	ProvChain: A Blockchain-based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability	A decentralized and trusted cloud data provenance architecture using blockchain technology was suggested. ProvChain is architecture developed for collecting and verifying the data provenance.	It failed to develop the trusted environment. When file size increases, overhead increases the computational complexity.	It improved the security, transparency and the data accountability.

7	Hierarchical Edge-Cloud Computing for Mobile Blockchain Mining Game	They presented a two-layer computation offloading model that comprised the service of edge computing and the cloud computing. Two case study was analysed, a fixed miner number and the dynamic miner number.	Different communication delays alter the security model of the environment. Maximized the profit of the limited resources.	With the help of reinforcement learning, the blockchain protocols discarded the administration of blockchain's security and privacy.
8	Secure data storage based on blockchain and coding in edge computing	Combing blockchain with regeneration coding was suggested to enhance the security and reliability of data stored under edge computing.	Analysis on redundant hash values changes the integrity of the data. Shortcoming of bandwidth decreased the value of single cloud server.	Security and reliability of the coding environment is ensured. Ensured the integrity of the data.
9	FogBus: A Blockchain-based Lightweight Framework for Edge and Fog Computing	FogBus is the mechanism introduced which facilitated end-to -end IoT fog-cloud integration. This blockchain technology ensures the sensitivity of the data.	It failed to support services for both users and the providers. Though, a centralized programming module is incorporated, the task of applying security features dislike the dealing with diverse applications	The simplified process reduced the cost and scalability of the data. Based on situation, the data are communicated.
10	Blockchain-Based Public Integrity Verification for Cloud Storage against Procrastinating Auditors	They employed a certificateless public verification scheme against procrastinating auditors using blockchain technology. It demands the auditors for verification process via blockchain transaction.	Though it's a certificateless photography, the performance of auditors during verifications is of poor. If auditor is being compromised, the chance of attack rate is of high.	They analysed the computational overhead and communication overhead. Likewise, the computational costs on server side is not wiser due to its poor auditing services.
11	SmartProvenance: A Distributed, Blockchain Based Data Provenance System	They suggested blockchain as a trustworthy platform for data provenance collection, verification and the management. They also studied smart contracts and the open provenance models for interpreting the data trails.	Allocation of each updated document consumes higher computational costs, because it maintains the old memory of documents. Utilization of public address reveals identity of the process.	The use of randomized voting reduces the centralization of the verification process. Therefore, there is no need for a physical verifier as the verification script verifies the changes before voting on the change
12	A Blockchain-enabled Thrustless Crowd-Intelligence Ecosystem on Mobile Edge Computing	They developed a crowd intelligence model for platform, workers and the task publishers. They resolved the trust issue between publisher and the workers by reward-penalty models.	It created excessive latency fluctuation. It doesn't reduce the location uncertainty. It doesn't reduce the worker shortage issue.	Eliminated the network congestion. It also maximized the strong nash equilibrium that interests the edge servers.
13	A Blockchain Enabled Cyber-Physical System Architecture for Industry 4.0 Manufacturing Systems	Potential impacts of blockchain technology and the realization of Cyper-Physical Production Systems (CPSS) with three level architecture was developed.	To develop a learning agent, a greater number of training data is required.	They ensured interoperability, data integrity, security and the privacy.
14	Permissioned Blockchain and Edge Computing Empowered Privacy-preserving Smart Grid Networks	They introduced a Permissioned Blockchain Edge Model for Smart Grid Network model that resolved smart grid, privacy protections and the energy security.	Covert channel attack is a type of adversarial approach that uses latency time to leak critical information. It must be focussed using top-up and bottom-down approaches.	It avoided the energy related attacks.
15	Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain	They framed a secure cloud assisted e-health systems which eliminated the illegal modification.	The collusion between data server and its corresponding transactions are processed as blockchain. Absence of central authority request multiple tokens creates non-trusted environment.	They analysed communication overhead and computational overhead with reduced computational time.
16	CKshare: secured cloud-based knowledge-sharing blockchain for injection mold redesign	Secured Cloud-based knowledge is suggested for private and blockchain technology. It's a redesign knowledge sharing platform that has its own privacy and data format requirements. Similarly, retrieval mechanism developed using k-nearest neighbour.	Due to the immutability of the blockchain, its labelling is critical. This will help in reducing the risks of fake knowledge	The security of the system was tested.
17	Privacy-preserving Energy Trading Using Consortium Blockchain in Smart Grid	A consortium blockchain oriented approach was studied for privacy leakage problem. The model mines the behaviour users for privacy modelling	Analysis on fake accounts creation is not examined.	The developed account generation and bound detection algorithms validated the trust between user and service providers.

18	SecLaaS: Secure Logging-as-a-Service for Cloud Forensics	They introduced secure logging as a service model that provides access to forensic for ensuring confidentiality of the users. Based on past logs, the dishonest behaviours are analysed.	Usage of bloom filter process like probabilistic data structure consumes higher time for membership verification.	They analysed past log of generation of data accumulators. Average execution time were analysed for all sorts of CPU.
19	Secure and Reliable IoT Networks Using Fog Computing with Software-Defined Networking and Blockchain	They developed an IOT framework which serves both fog layer and the edge layer for nodes with distributed controllers and resource constraints.	The SDN network achieves lower system performance in terms of network management, flexibility and latency performances. Moreover, a data offloading algorithm was not organized and managed the offloading scheme.	They achieved high reliability and availability.
20	Blockchain Radio Access Network (B-RAN): Towards Decentralized Secure Radio Access Paradigm	They introduced a Blockchain radio access network (B-RAN) architecture and developed decentralized, secure, and efficient mechanisms to manage network access and authentication among inherently trust less network entities	The secured multi-party computation can be further incorporated to avoid unauthorized access of sensitive data but can instead still provide distributed computing directly.	They analysed throughput vs traffic load, throughput vs block size and latency vs security and proved better performances.
21	A Blockchain-Based Solution for Enhancing Security and Privacy in Smart Factory	They introduced blockchain architecture that support distributed networks and reconfigure the conventional IioT architecture. A novel design interaction module was developed for enhancing the security technologies.	Maintenance of whitelist and blacklist nodes used in equipped and users.	Data processing due to network settings degraded the performances. It utilized the resources and efficiency of the data interaction.
22	Resource Trading in Blockchain-based Industrial Internet of Things	They resolved resource management and pricing problem between cloud providers and miners. A multi-agent learning environment that searches the near-optimal policy in Stackelberg game.	Unexpected data rewards the miners with greater financial loss. This financial loss distorts the relationship between expected reward and service demand.	They studied convergence time, no of miners and the service demand.
23	Proofware: Proof of Useful Work Blockchain Consensus Protocol for Decentralized Applications	There are variant protocols available in blockchain technology, namely, Proof of work, Proof of Stake, Proof of space and Proof of activities. Proofware model was developed for computing resources and administers the incentive system.	Real time application and the service over peer to peer network are not processed properly. In some cases, the distributed infrastructure is interrupted during unlimited no of nodes assessment.	Compared to centralised solution, cost and reliability of the video application was analysed.
24	Cloud-based Manufacturing Knowledge Sharing for Injection Mould Redesign	They introduced cloud based manufactured knowledge sharing for injection mould redesign. K-nearest neighbour algorithm was used for proper organization of the document. The developed knowledge layer acted as knowledge sharing environment for all phases.	Most relevant knowledge cases are not properly extracted the shared information. Similarly, the search results also degraded the ranking performances.	This system reduces the keyword extraction time.
25	Blockchains in operations and supply chains: a model and reference implementation	They reviewed the blockchain technology and possible solution for immutable distributed ledgers in operations and supply chains.	Scalability and data privacy failed to support the blockchain transactions.	They discussed about the lifecycle development-based capability of blockchain.

IV. CONCLUSION

Recently, blockchain is a popular financial technology which support variety of Information Processing Units (IPU) on virtual financial transactions. The customers of blockchain stores their data in their P2P networks for effective utilization of the computing resources. The two main algorithms like proof-of- work and proof- of -stake are mainly used for assuring security to the blockchain transactions. This paper reviews about the applications of blockchain in cloud computing. Initially, we briefly discussed the integration of blockchain network with cloud systems. The main aim of this integrated system is to ensure and enhance the trust between data server, data users and the data security. We discussed the origin of blockchain, and its advantages and disadvantages are discussed. A review of prior techniques have been analysed for identifying the challenges involved in this integration. The review states that the study on blockchain based cloud systems is still in development process. Access control is one of the core issues faced by the researchers. In view of rewarding the data, the communication between multi- party computations disrupts the networks as well as unexpected financial loss. Creation of fake accounts also degrades the scalability of the system. In future, the designed model should try to resolve the above-mentioned issues.

REFERENCES

1. Il-Kwon, L.; Young-Hyuk, K.; Jae-Gwang, L.; Jae-Pil, L. The Analysis and Countermeasures on Security Breach of Bitcoin. In Proceedings of the International Conference on Computational Scienceand Its Applications, Guimarães, Portugal, 30 June–3 July 2014; Springer International Publishing:Cham, Switzerland, 2014.

2. Beikverdi, A.; JooSeok, S. Trend of centralization in Bitcoin's distributed network. In Proceedings of the 2015 16th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), Takamatsu, Japan, 1–3 June 2015.
3. Bonneau, J.; Miller, A.; Clark, J.; Narayanan, A.; Kroll, J.A.; Felten, E.W. Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In Proceedings of the 2015 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 17–21 May 2015.
4. Christidis, K.; Michael, D. Blockchains and Smart Contracts for the Internet of Things. IEEE Access 2016, 4,2292–2303.
5. Huang, H.; Chen, X.; Wu, Q.; Huang, X.; Shen, J. Bitcoin-based fair payments for outsourcing computation of fog devices. Future Gener.Comput.Syst. 2016.
6. Huh, S.; Sangrae, C.; Soohyung, K. Managing IoT devices using blockchain platform. In Proceedings of the 2017 19th International Conference on Advanced Communication Technology (ICACT), Bongpyeong, Korea, 19–22 February 2017.
7. Armknecht, F.; Karame, G.; Mandal, A.; Youssef, F.; Zenner, E. Ripple: Overview and Outlook. In Trust and Trustworthy Computing; Conti, M., Schunter, M., Askoxylakis, I., Eds.; Springer International Publishing: Cham, Switzerland, 2015; pp. 163–180.
8. Vasek, M.; Moore, T. There's No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scams. In Proceedings of the International Conference on Financial Cryptography and Data Security, San Juan, Puerto Rico, 26–30 January 2015; Springer: Berlin/Heidelberg, Gemany, 2015.
9. Zhang, J.; Nian, X.; Xin, H. A Secure System For Pervasive Social Network-based Healthcare. IEEE Access 2016, 4, 9239–9250.
10. Singh, S.; Jeong, Y.-S.; Park, J.H. A survey on cloud computing security: Issues, threats, and solutions. J. Netw. Comput. Appl. 2016, 75, 200–222
11. Kumar, G., Saha, R., Rai, M. K., Thomas, R., & Kim, T. H. (2019). Proof-of-Work consensus approach in Blockchain Technology for Cloud and Fog Computing using Maximization-Factorization Statistics. IEEE Internet of Things Journal.
12. Verma, V. K. (2019). Blockchain Technology: Systematic Review of Security and Privacy Problems and Its Scope with Cloud Computing. Journal of Network Security, 7(1), 1-6.
13. Jiao, Y., Wang, P., Niyato, D., & Suankaewmanee, K. (2019). Auction mechanisms in cloud/fog computing resource allocation for public blockchain networks. IEEE Transactions on Parallel and Distributed Systems.
14. Zhu, L., Wu, Y., Gai, K., & Choo, K. K. R. (2019). Controllable and trustworthy blockchain-based cloud data management. Future Generation Computer Systems, 91, 527-535.
15. Yang, R., Yu, F. R., Si, P., Yang, Z., & Zhang, Y. (2019). Integrated blockchain and edge computing systems: A survey, some research issues and challenges. IEEE Communications Surveys & Tutorials.
16. Liang, X., Shetty, S. S., Tosh, D., Njilla, L., Kamhoua, C. A., & Kwiat, K. (2019). ProvChain: Blockchain-based Cloud Data Provenance. Blockchain for Distributed Systems Security, 69.
17. Jiang, S., Li, X., & Wu, J. (2019, July). Hierarchical Edge-Cloud Computing for Mobile Blockchain Mining Game. In Proc. of the 39th IEEE International Conference on Distributed Computing Systems (ICDCS 2019) (Vol. 15).
18. Nadeem, S., Rizwan, M., Ahmad, F., & Manzoor, J. (2019). Securing Cognitive Radio Vehicular Ad Hoc Network with Fog Node based Distributed Blockchain Cloud Architecture. INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS, 10(1), 288-295.
19. Tosh, D., Shetty, S., Liang, X., Kamhoua, C., & Njilla, L. L. (2019). Data Provenance in the Cloud: A Blockchain-Based Approach. IEEE Consumer Electronics Magazine, 8(4), 38-44.
20. Tuli, S., Mahmud, R., Tuli, S., & Buyya, R. (2019). FogBus: A Blockchain-based Lightweight Framework for Edge and Fog Computing. Journal of Systems and Software.
21. Zhang, Y., Xu, C., Lin, X., & Shen, X. S. (2019). Blockchain-Based Public Integrity Verification for Cloud Storage against Procrastinating Auditors. IEEE Transactions on Cloud Computing.
22. Xu, J., Wang, S., Bhargava, B., & Yang, F. (2019). A Blockchain-enabled Trustless Crowd-Intelligence Ecosystem on Mobile Edge Computing. IEEE Transactions on Industrial Informatics.
23. Yin, B., Mei, L., Jiang, Z., & Wang, K. (2019, April). Joint Cloud Collaboration Mechanism between Vehicle Clouds Based on Blockchain. In 2019 IEEE International Conference on Service-Oriented System Engineering (SOSE) (pp. 227-2275). IEEE.
24. Ren, Y. J., Leng, Y., Cheng, Y. P., & Wang, J. (2019). Secure data storage based on blockchain and coding in edge computing. Math. Biosci. Eng, 16, 1874-1892.
25. Barenji, A. V., Guo, H., Tian, Z., Li, Z., Wang, W. M., & Huang, G. Q. (2019). Blockchain-Based Cloud Manufacturing: Decentralization. arXiv preprint arXiv:1901.10403.
26. Lee, J., Azamfar, M., & Singh, J. (2019). A blockchain enabled Cyber-Physical System architecture for Industry 4.0 manufacturing systems. Manufacturing Letters, 20, 34-39.
27. Gai, K., Wu, Y., Zhu, L., Xu, L., & Zhang, Y. (2019). Permissioned Blockchain and Edge Computing Empowered Privacy-preserving Smart Grid Networks. IEEE Internet of Things Journal.
28. Cao, S., Zhang, G., Liu, P., Zhang, X., & Neri, F. (2019). Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain. Information Sciences, 485, 427-440.
29. Li, Z., Liu, X., Wang, W. M., Vatankhah Barenji, A., & Huang, G. Q. (2019). CKshare: secured cloud-based knowledge-sharing blockchain for injection mold redesign. Enterprise Information Systems, 13(1), 1-33.
30. Wu, A., Zhang, Y., Zheng, X., Guo, R., Zhao, Q., & Zheng, D. (2019). Efficient and privacy-preserving traceable attribute-based encryption in blockchain. Annals of Telecommunications, 1-11.
31. Farhadi, M., Miorandi, D., & Pierre, G. (2019). Blockchain enabled fog structure to provide data security in IoT applications. arXiv preprint arXiv:1901.04830.
32. Gai, K., Wu, Y., Zhu, L., Qiu, M., & Shen, M. (2019). Privacy-preserving Energy Trading Using Consortium Blockchain in Smart Grid. IEEE Transactions on Industrial Informatics.
33. Rane, S., & Dixit, A. (2019, January). BlockSLaaS: Blockchain Assisted Secure Logging-as-a-Service for Cloud Forensics. In International Conference on Security & Privacy (pp. 77-88). Springer, Singapore.
34. Wang, J., Peng, F., Tian, H., Chen, W., & Lu, J. (2019, April). Public Auditing of Log Integrity for Cloud Storage Systems via Blockchain. In International Conference on Security and Privacy in New Computing Environments (pp. 378-387). Springer, Cham.
35. Muthanna, A., A Ateya, A., Khakimov, A., Gudkova, I., Abuarqoub, A., Samouylov, K., & Koucheryavy, A. (2019). Secure and Reliable IoT Networks Using Fog Computing with Software-Defined Networking and Blockchain. Journal of Sensor and Actuator Networks, 8(1), 15.
36. Ling, X., Wang, J., Bouchoucha, T., Levy, B. C., & Ding, Z. (2019). Blockchain Radio Access Network (B-RAN): Towards Decentralized Secure Radio Access Paradigm. IEEE Access, 7, 9714-9723.
37. Wan, J., Li, J., Imran, M., & Li, D. (2019). A Blockchain-Based Solution for Enhancing Security and Privacy in Smart Factory. IEEE Transactions on Industrial Informatics.
38. Yao, H., Mai, T., Wang, J., Ji, Z., Jiang, C., & Qian, Y. (2019). Resource Trading in Blockchain-based Industrial Internet of Things. IEEE Transactions on Industrial Informatics.
39. Muthanna, A., Ateya, A. A., Khakimov, A., Gudkova, I., Abuarqoub, A., Samouylov, K., & Koucheryavy, A. (2019). Secure IoT Network Structure Based on Distributed Fog Computing, with SDN/Blockchain.
40. Dong, Z., Lee, Y. C., & Zomaya, A. Y. (2019). Proofware: Proof of Useful Work Blockchain Consensus Protocol for Decentralized Applications. arXiv preprint arXiv:1903.09276.

AUTHORS PROFILE

Simanta Shekhar Sarmah is currently working as a BI Consultant at National Science Foundation, USA. He has published several research papers in various International Journals. His area of interests is Cloud Computing, Blockchain Technology, Internet of Things, Data Security, Artificial Intelligence, etc.

He did his Bachelors of Engineering in Computer Technology from Nagpur University, India and completed his Masters in Science degree from Texas A&M University-Commerce. He is actively involved in various research works and also has over eleven years of professional experience in his field.