International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 1 Volume No.8 January - February – 2024
DOI:10.46647/ijetms.2024.v08i01.038 ISSN: 2581-4621

# Integration Of Blockchain With Fog Computing To Improvise Security & Privacy Issues

**Ms. Meenu[1], Dr. Devender Kumar[2]**
*[1]Research Scholar in the department of Computer Science &Applications, Baba Mastnath University, Rohtak*
*[2]Associate Professor, Baba Mastnath University, Rohtak*

Abstract
The concept of fog computing was suggested to help cloud computing for the fast data processing of Internet of Things (IoT) based applications. Even, fog computing faces many challenges such as Security, Privacy & Storage. One way to handle these challenges is to integrate blockchain with fog computing. There are several applications of blockchain and fog computing integration that have been proposed, recently, due to their lucrative benefits such as enhancing security and privacy. Also we have to systematically review the literature on both the technologies (blockchain & fog computing). The purposes of integrating blockchain and fog computing is to tailored search criteria established from the research questions. In this research, the combination of blockchain and fog computing approach for several purposes such as security, privacy, access control, and trust management. By Insufficient laws and standard, it is difficult for blockchain and fog computing to be integrated in the future. Particularly in light of newly developed technologies like quantum computing and artificial intelligence has more power. In this paper we tried to minimize some security issues in fog computing via using the technology of blockchain.

**Keywords:** Blockchain, Cloud computing, Fog computing, PoW, Internet of things (IoT), Security, P2P

## Introduction

Fog computing is a decentralized approach to extends our computing resources closer to the edge ofthe network. This type of computing is beneficial over cloud computing as processing is very fast, because computation devices are close to network edge. These techniques allow low processing ofdata & reduced latency so make it useful for real time applications. Fog computing try to cover up the issues occurred in cloud computing like latency, efficiency of data processing & security issues. Still itfaces some issues regarding security, load balancing etc.

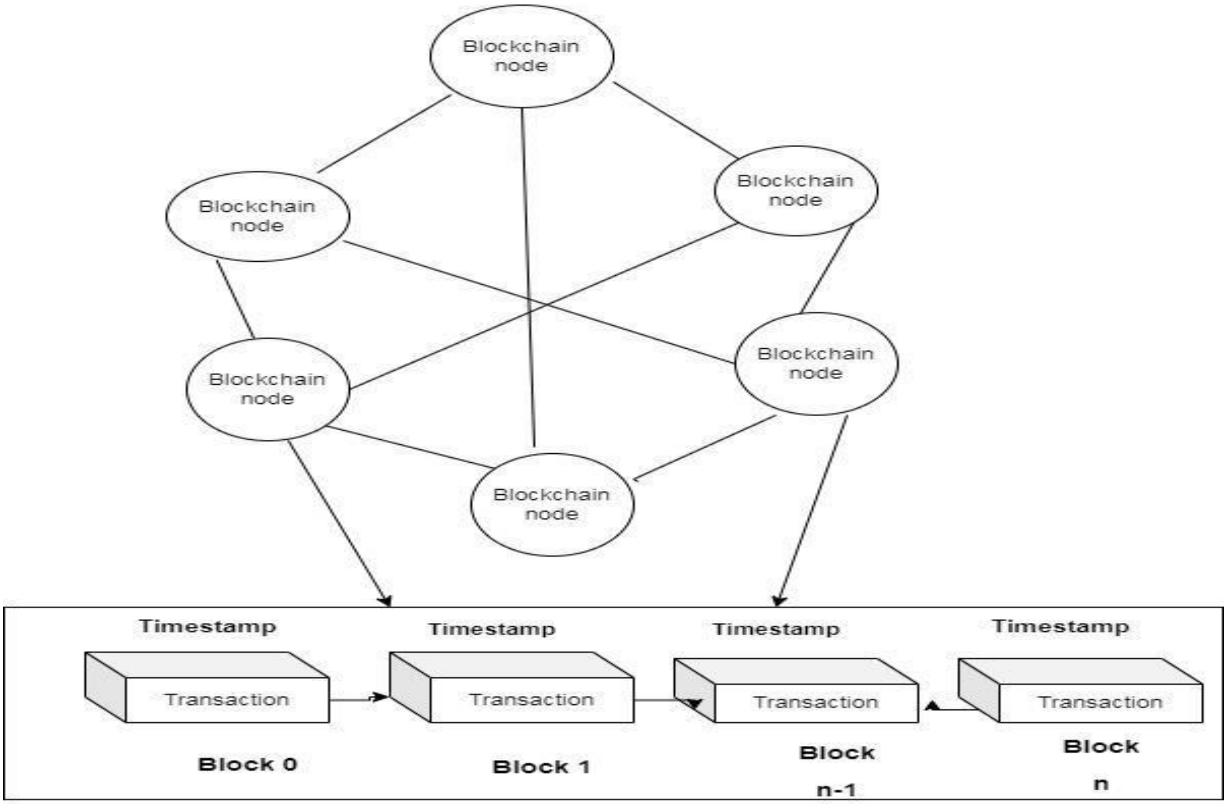
Blockchain is also a decentralized architecture which use distributed ledger technique to save records securely and also verifies its transactions over a network of computers. As blockchain operates on network of computer which collectively record & validate the transactions. In this technology, all the transactions are grouped into blocks and all the blocks were linked to the previous one to form a chain.This kind of sequential changing ensures the security and integrity of transaction history. In this paper we try to integrate both the technology to solve and atheist minimize the security issues.

In this paper, we tried to provides the main purposes of Blockchain-Fog Computing integration. This paper follows the evaluation of many reviewed paper. This paper comprehensively reviews the work done in the field from different perspectives (e.g., algorithms, schemes, architecture, andso on). The literature on FC with BC integration is very rare; systematically organizing the relevant literature is a significant task. We had identified main seven purposes of FC& BC integration. These are as follows:

I. Security
II. Privacy

III. Access Control
IV. Trust Management
V. Data Management
VI. Scalability
VII. Performance

Block Chain Network



We also tried to identifying some open issues in infrastructure, platform, and technical limitationsof BlockChain architecture that distress processes in specific realms. It's important to note that this analysis is by no means comprehensive since BlockChain technology continues today at breakneck speed. The paper is organized as the Blockchain with fog computing integration overview discusses the descriptive findings. Research methodology discusses Block Chain with Fog Computing integration purposes. Locating studies discusses the future challenges and open questions about BC with FC integration.

**Relevant Study**

The Blockchain technology mainly used in bitcoin BC, which is the first & most widely used Blockchain platformwhich is used in many applications. Reason for discussing Bitcoin BC integrates depth rather than other platforms such as Ethereum which is a decentralized open-source Blockchain.It has smart contract capability that is recognized for its native cryptocurrency. It is also pronounced asETH, ether, or just Ethereum. There is the extensive literature accessible on the platform. Bitcoin BC, for example, uses SHA-256 hashing and elliptic curve cryptography to provider or bust

Cryptographic evidence for data integrity and authentication. A key-based encryption named elliptic curve cryptography system that includes a pairs of private and public keys to encrypt and decrypt data.The Blockchain includes a list of all transactions and a hash to the prior block, which enables a cross- border distributed in a very trusty environment. While trusted parties or centralized authorities may misbehave and can be compromised, disrupted or hacked. The transactions in the public ledger of BC are validated by a majority consensus of miner nodes involved in the validation process. In PoW- based Blockchain, the validation occurs by calculating a hash with leading zeros to meet the difficulty target .After validating by a consensus, the transaction data are saved in a ledger that not be erased or changed (data are immutable). If any one change, then it leads to discrepancy.

Figure2describes a typical structure of the Bitcoin BC which consists of a sequence of blocks connected through the hash value. The Blockchain includes the block header & the block body which includes the transactions list. Various fields are included in the block header such as the block size, a timestamp, the number of transactions, and the version number. The hash value of the current block is represented by the field name Merkle root field. Hashing using the Merkle tree is often used in Peer-to-Peer (P2P) and distribute its arrangements as it provides effective data proof. The nonce field is included as a Proof-of-Work (PoW) algorithm (the original consensus algorithm in BC(e.g., Bitcoin and Ethereum), which is used to confirm transactions and produce new blocks in the chain), and itis used to generate the trial counter value that generates the hash with leading zeros. The number of leading zeros is specified by the difficulty target (i.e used to preserve the block time of nearly 17.5s for Ethereum and 10 min for Bitcoin. The difficulty target can be modified to increase the number of zeros if the computation power of the hardware increased. The timestamp is used for tracking the modification on the Blockchain. There are many kind of different mechanisms are used for timestamping such as signing using the private key of a trustworthy server used in the traditional schemes. There is another technique used by deploying distributed time-stamping which helps to avoid a single point of failure.

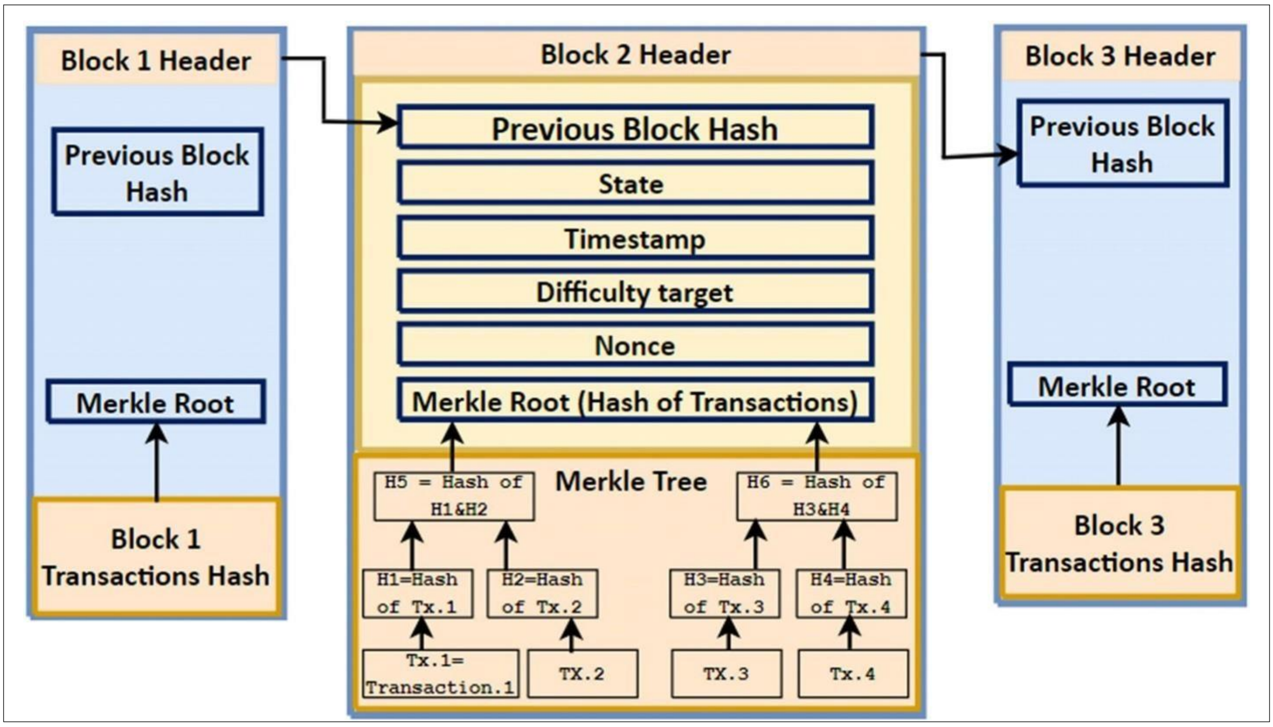


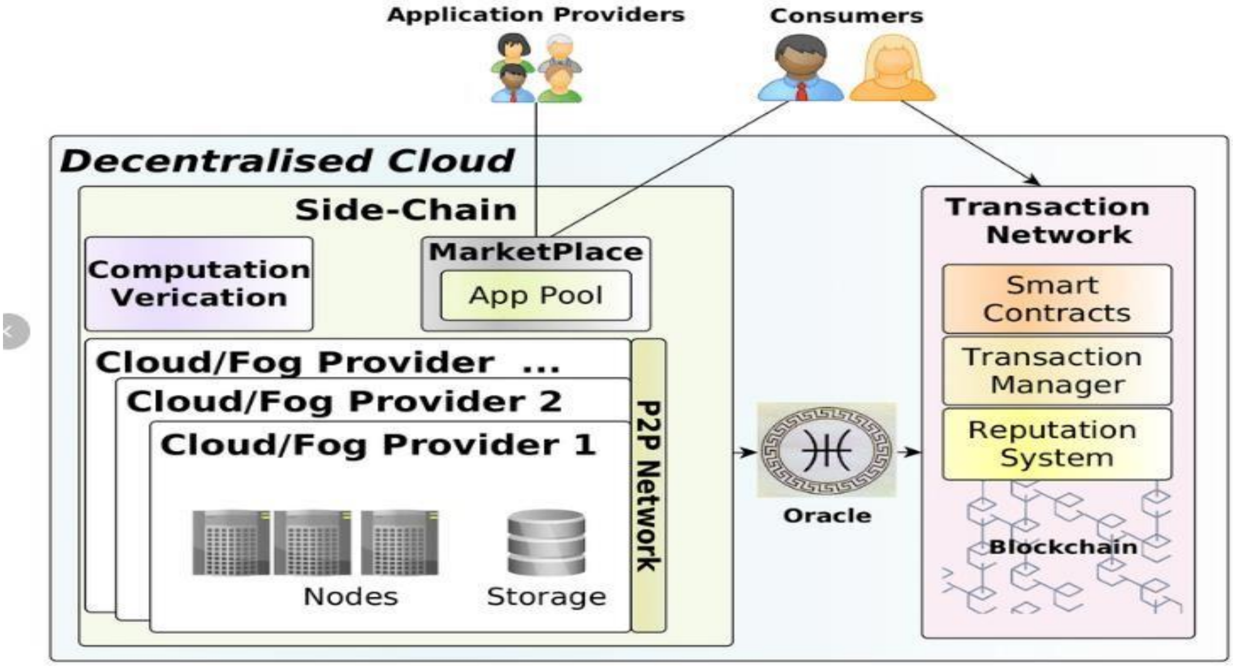
figure 2:Transaction in bitcoin by sequence of block

The Blockchain network achieves consensus by a method is referred to as a consensus mechanism or algorithm. As we know, there is no any central authority like RBI, It is a public Blockchain (used decentralized approach) is constructed as a distributed mechanism, with distributed nodes agreeing on the validity of transactions using a consensus algorithm. In other words, Blockchain depends on distributed consensus to validate the transactions. It guarantees the consistency & integrity of the transactions. The different consensus mechanisms result the Blockchain system differently. The ideal consensus mechanism giving the same weight to all miners for the validation process and the deciding mechanism is based on the majority. This ideal scenario may be applicable in a controlled or we can say that private environment. However, in public contexts, this may increase the chance of Sybil attacks as users can share multiple identities. In distributed architecture such as Fog Computing, only one random user will add every block whichmay lead to several attacks, but time stamp ordering can preserve it.

Bitcoin is the most well-known crypto-currency. After that, in 2015, Ethereum Blockchain was introduced, which can execute smart contracts and store data. The smart contracts are the programs which are written and uploaded by the parties to be executed in the Blockchain which includes the terms of the contract. Soon later, other BC platforms were launched such as Stellar (a digital money protocol that's distributed and open- source), Hyper-ledger (a worldwide business BC initiative that provides the structure, tools, and rules for creating open-source BCs and apps), Ripple (a BC-based digital payment system and mechanism with its cryptocurrency, XRP), Eris (an open-source software that enables anybody to create low-cost, safe, and portable apps utilizing smart contract and BC technology), and **Tendermint** , it is an algorithm for securely andconsistently replicating applications over many devices. On the part of data management, the availability of that data & the actions taken by different types of Blockchain, it can be identified. It is worth mentioning here that some authors refer to public/permission lessand private/permission, interchangeably. This can be applied in the case of cryptocurrencies; however, in other applications there is need to distinguish between authentication & authorization, it's not applicable. Although, the naming is still in debate among authors. Note that Bitcoin is used to track digital assets, while smart contracts used in Ethereum enable certain logic. Moreover, while some system like Ripple makes use of tokens, others like Hyper-ledger do not.

**Blockchain with fog computing Integration**

FC is a highly dispersed computing structure with a set of assets made up of one or more pervasively linked embedded systems (which include IoT devices) sup- ported by cloud computing, to cooperatively offer storage, computation, storage, connectivity, and other services to a sizable number of IoT devices nearby. Fog Computing is a cloud extension that is more closely connected to IoT devices. Fog Computing is a bridge betweenedge devices like sensors, actuators & the cloud. A fog node could be any device which has processing power, storage capabilities & network connection including routers, security cameras, switches, and control devices. Fog Computing has many characteristics like Distribution, flexibility, proximity to IoT devices, low latency, real-time transactions and analysis, and heterogeneity. All of the qualities made Fog Computing a very appealing solution for cloud computing problems, particularly excessivelatency and centralized authority. figure 3 shows this secure integration.



Smart contracts and blockchain have the capability to change the current market of cloud by enabling the development of completely decentralized cloud/fog solutions. It also provides us a solution like lower costs and enforces predictable results without requiring any intermediary.
Blockchain-Fog Computing Purpose
By examining the literature and existing fog computing based technology which facing some security based issues can be solved by above given scenario of block chain technology. We tried to show some basic purpose which are listed below by the integration of both the technologies.
□ Security
□ Confidentiality
□ Integrity
□ Fraud detection
□ Confidentiality
□ Privacy
□ Availability
□ Authentication
□ Authorization
□ Key management
□ Trust Management
□ Qos(Quality of Services)
□ Storage

**Open Issues & Future Trends**
There are several terms noticed which awareus the limitations of the Blockchain with Fog Computing integration and the usefulness of BC across a wide range of purposes may be gained from this SLR.As mentioned above, BC with FC integration is presently use wide range of disciplines and businesses, giving unlimited exploration potential. However,difficulties and obstacles occur, just as they do with any other new technology. We highlight some of the limitations of the BC with FC integration in this part, as well as various options for future research initiatives. Because of the FC and BC features, the stated challenges of BC with FC integration have risen. The following challenges of BC with FC integration, as mentioned

above, are mainly based on the Bit coin BC drawbacks, according to the available literature. While scalability challenge is mainly caused by a lack of FC resources, security, privacy, and standards issues are primarily caused by a lack of BC capabilities and rules. On the other hand, quantum, AI, and big data are affected both BC and FC capabilities in any of these scenarios, these challenges will have an impact on FC’s performance. As a result, it’s essential to investigate the BC-based challenges that impact FC performance.

## References

1. Mouradian C, Naboulsi D,Yangui S, Glitho RH, Morrow MJ, Polakos PA (2017)A comprehensive survey on fog computing: state-of-the-artand research challenges. IEEE Commu Surv Tutor20:416–464
2. Xiao M, Zhou J, Liu X, Jiang M (2017) A hybrid scheme for fine-grained search and access authorization in fog computing environment. Sen- sors17:1423
3. Atlam HF,Walters RJ,Wills GB (2018) Fog computing and the internet ofthings:areview.BigDataCognComput2:10
4. Bellavista P,Berrocal J,Corradi A,D as SK,FoschiniL, ZanniA(2019)A survey on fog computing forthe internet of things. Pervasive Mob Comput52:71–99
5. Dastjerdi AV, Gupta H, Calheiros RN, Ghosh SK, Buyya R (2016) Fog com-puting: Principles, architectures, and applications. In: Buyya R, Dastjerdi AV(eds) Internet of things :PrinciplesandParadigms.Elsevier,Morgan Kaufmann,Burlington,Massachusetts,ed,pp61–75
6. FrancisT, Madhiajagan M (2017) A comparison of cloud execution mechanisms: fog, edge and clone cloud computing. ElectrEngComput SciandInfor4:446–450
7. Yousef pour A ,Fung C,Nguyen T,Kadiyala K,JalaliF, Niakanlahiji Aetal (2019) All one needs toknow about fog computing and related edge computing paradigms: a complete survey. J Syst Archit 98:289–330
8. Naha RK, Garg S, Georgakopoulos D, Jayaraman PP, Gao L, XiangY et al (2018)Fog computing :survey of trends ,architectures, requirements, and research directions. IEEE access 6:47980– 48009
9. ElazharyH(2019)Internet of things (IoT), mobile cloud, cloudlet, mobile IoT, IoT cloud, fog, mobile edge, and edge emerging computing paradigms: disambiguation and research directions. J Netw Comput Appl128:105–140
10. PereiraJ, Ricardo L,LuísM,Senna C,SargentoS(2019)Assessingthe reliability of fog computing forsmart mobility applications in VANETs.FuturGenerComputSyst94:317–332
11. Roman R,LopezJ ,Mambo M(2018) Mobileed gecomputing ,fog etal.: as urvey and analys is ofsecurity threats and challenges. FuturGener Comput Syst 78:680–698
12. KhalidT,AbbasiMAK,ZuraizM,KhanAN,AliM,AhmadRWetal(2021) A survey on privacy andaccess control schemes in fog computing .IntJ CommunSyst34:e4181
13. ZhangP,ZhouM,FortinoG(2018)Securityandtrustissuesinfogcomputing:asurvey.FuturGenerC omputSyst88:16–27
14. AlzoubiYI,OsmanajVH,JaradatA,Al-AhmadA(2021)Fogcomputing security and privacy for theinternet of thing applications: state-of-the- art. Security and Privacy 4:e145
15. ChiangM,ZhangT(2016)FogandIoT:anoverviewofresearchoppor- tunities. IEEE InternetThings J 3:854–864
16. PuthalD, Mohanty SP , Bhavake SA,Morgan G,RanjanR(2019)Fog com- putting security challenges and future directions [energyandsecurity]. IEEEConsum.Electron.Mag.8:92–96
17. SinghA,PariziRM,HanM,DehghantanhaA,KarimipourH,ChooK-KR (2020) Public blockchains scalability: An examination of sharding
18. andsegregatedwitness.In:ChooK,DehghantanhaA,PariziR(eds)
19. Fernández-CaramésTM,Fraga-LamasP(2019)Designofafogcomput- ing, blockchain and IoT- based continuous glucose monitoring system forcrowdsourcingmHealth.Proceedings4:37
20. Fernández-Caramés TM, Fraga-Lamas P (2019) Towards next generation teaching, learning, and context-aware applications for higher educa- tion: a review on blockchain, IoT, fog and edge computing enabled smartcampusesanduniversities.ApplSci9:4479
21. NkenyereyeL,AdhiTamaB,ShahzadMK,ChoiY-H(2020)Secureand blockchain-

basedemergencydrivenmessageprotocolfor5Genabled vehicularedgecomputing.Sensors20:154
22. RenY,ZhuF,QiJ,WangJ,SangaiahAK(2019)Identitymanagement andaccesscontrolbasedonblockchainunderedgecomputingforthe industrial internet of things. ApplSci 9:2058
23. Tariq N, Asim M, Al-Obeidat F, Zubair Farooqi M, BakerT, HammoudehM et al (2019)The securityof big data in fog-enabled IoT applicationsincludingblockchain:asurvey.Sensors19:1788
24. DuY,Wang Z, LeungV (2021) Blockchain-enabled edge intelligence for IoT: background,emerging trends and open issues. Future Internet13:48
25. ShahbaziZ,ByunY-C(2021)Improvingtransactionaldatasystembased onanedgecomputing–blockchain–machinelearningintegrated framework.Processes9:92
26. JainV, Kumar B (2022) Auction based cost-efficient resource allocation byutilizingblockchaininfogcomputing.Trans.Emerg.Telecommun. Technol33:e4469
27. Kamruzzaman M,Yan B, Sarker MNI, Alruwaili O,Wu M, Alrashdi I (2022) Blockchain and fog computing in IoT-driven healthcare services for smartcities.J.Healthc.Eng.2022.https://doi.org/10.1155/2022/9957888
28. Huang X, Deng X, Liang C, FanW (2021) Blockchain-enabled task offloadingandresourceallocationinfogcomputingnetworks.Wirel Commun Mob Comput 2021. https://doi.org/10.1155/2021/7518534
29. SilvaCA,AquinoGS,MeloSR,EgídioDJ(2019)Afogcomputing-based architecture for medical records management. Wirel Commun Mob Comput2019:1–16