International Journal of Engineering and Science Invention (IJESI)
ISSN (Online): 2319-6734, ISSN (Print): 2319-6726
www.ijesi.org ||Volume 14 Issue 3 March 2025 || PP 13-19

Block Access Control in Wireless Blockchain Network Design, Modeling and Analysis

[1] G. Nagappa, [2] B. Kumar, [3] K. Vijay, [4] K. Nagaraju, [5] M. Pavan Kalyan, [6] B. Uday Kumar

[1] *Associate professor,* [2, 3, 4, 5, 6] *BTECH*

[1, 2, 3, 4, 5, 6] *Dept of CSE, St. Johns College of Engineering and Technology, Yerrakota, Yemmiganur, Kurnool, AP, Affiliated by JNTUA, INDIA*

Abstract: *The abstract offers a new way to solve the problem state block access management in wireless blockchain networks. It underlines the need state strong access control systems in guaranteeing the security and integrity state distributed wireless communication. Using smart contracts for authentication and authorisation, the suggested approach combines access control systems with blockchain architecture. This device seeks to improve security while reducing latency and overhead. Considering throughput, latency, and energy efficiency among other elements, a mathematical model is created to examine system performance. Comprehensive simulations and studies show the viability and superiority state the suggested method in terms state security, efficiency, and scalability when compared to current options. by offering a strong and fast answer for block access control, essential for guaranteeing trust, integrity, and confidentiality in decentralised wi-fi environments, the research helps to push the in wireless blockchain networks.*

"Index Terms: *Blockchain, wireless network, CSMA/CA, forking, Markov chain, performance analysis".*

I. INTRODUCTION

Spanning from blockchain-based mobile edge computing [1, 2], vehicle management [3, 4], to smart factory operations [5], wireless blockchain networks have surfaced as a viable way to create strong and dispersed wireless communication infrastructures for several blockchain applications. Especially in large-scale situations like the "internet of things (IoT)" [6], these networks save maintenance expenses, improve security and scalability, relieve the stress on high-load nodes, and minimise the possibility of single points of failure. Furthermore, by means of smart contracts, they allow adaptive user terminal matching and behavioural decision-making [7, 8].

Consensus algorithms used by wi-fi blockchain networks are the basis of its decentralisation and security [6]. Without using middlemen, these methods motivate network nodes to preserve a consistent digital ledger. Among the many suggested consensus algorithms are "proof-of-work (PoW) [9], proof-of-stake (PoS) [10], practical Byzantine fault tolerance (PBFT)" [11], and Raft [12]. Among these, PoW stands out as the first commonly used algorithm in blockchain networks, claiming better security and node scalability than PBFT and Raft [13, 14].

Adapting these consensus procedures to wireless networks, however, offers additional difficulties, especially in the broadcasting of new blocks over the wireless channel. Block transmission efficiency is greatly affected by the features of wireless network protocols. examining the impact of the "carrier sense multiple access with collision avoidance (CSMA/CA) protocol—a random access mechanism functioning at the media get entry to manage (MAC)" layer—this paper investigates the consensus process inside "blockchain-based wireless local area networks (B-WLANs)" in this framework.

Under ideal communication conditions, the "first full node (FN)" that successfully creates a valid new block in a conventional blockchain system gets rewarded. The transmission of the initial block produced by a FN, but, may be delayed by CSMA/CA's backoff counter's natural randomness, hence enabling other FNs to maintain mining and maybe create more blocks. Consequently, several blocks can be produced in one backoff counter period, with later blocks surpassing the first one to be the final victor. This occurrence creates forks in the blockchain ledger, which causes discrepancies among FNs and produces security holes and computational power waste like "double-spending" [17].

The forking problem limits the block generation rate in PoW systems by means of blockchain system constraints, hence restricting transaction throughput to somewhat low levels, including 7 "transactions per second (tps)" in Bitcoin [9] and 15 tps in Ethereum [18]. Unlocking the full potential of wireless blockchain networks depends on therefore knowing and reducing the influence of CSMA/CA on the PoW consensus process in wi-fi networks.

The following parts explore further the effects of CSMA/CA on the PoW consensus mechanism, looking at ways to solve the forking issue and improve the scalability and efficiency of wireless blockchain networks.

II. LITERATURE SURVEY

Across several sectors—integrated mobile edge computbuilt-ing, video streamintegratedg structures, driverless cars, connected vehicle forensics, and smart factories—blockchabuilt technology has visible splendid acceptance. Key contributions integrated these fields and their outcomes for wi-fi blockchabuilt-in networks are integrated to be highlighted integrated literature survey.

By integrated computational resources at the edge of the community, cell edge computbuiltg (MEC) has developed as a promisbuiltg concept to improve the performance of mobile apps. Xiong et al. [1] built-inlook at the integrated of cell blockchabuilt with edge computbuiltg, hence stressbuiltg the possible advantagesbuilt and difficulties integrated convergence. They integrated how mobile blockchabuilt can improve MEC settbuiltgs' security and privacy as well asbuilt enable decentralised resource allocation.

Integrated on the junction of blockchabuilt and edge computbuiltg, Liu et al. [2] offer a distributed resource allocation approach for blockchabuilt-based video streambuiltg systems with cell edge computbuiltg. Aimbuiltg to enhance the qualitybuilt of video streambuiltg servicesbuilt, their work tackles the difficulties of resource allocation optimisation built dynamic and diverse network settbuiltgs.

Built-inbuilt-in the fieldbuilt of autonomousbuiltbuiltbuilt vehicles (AVs), Pokhrel et al. [3] suggest federated built-ing knowledge of integrated blockchabuilt to improve databuiltbuilt privacy and security built AV networks. Aimbuiltg to offer effective and safe model built-ingintegrated over distributed AV nodes, their work tackles the design difficulties related to federated built-inintegrated and blockchabuilt integratedtegration.

Cebe et al. [4] provide Block4forensic, a lightweight blockchabuilt-in systembuilt designed specificallybuiltbuilt for forensics uses built linked cars. Their system supports unchangeable and safe facts loggbuiltg and auditbuiltg, hence built-inintegrated quick forensic builtintegrated and builtcident analysis built connected car settbuiltgs.

Smart factories use technology, such as blockchain, to improve industrial process security and privacy. Wan et al. [5] offer a blockchain-based approach to improve smart factory security and privacy. Aiming to reduce cybersecurity concerns and guarantee data integrity, their method emphasises protecting facts transactions and access control systems in the smart industrial environment.

Distributed consensus systems are made more difficult by the combination of blockchain and "internet of things (IoT)". Emphasising the need of distributed consensus in guaranteeing the integrity and dependability of IoT data, Cao et al. [6] address the issues and possibilities when IoT meets blockchain technology.

Network reliability and security in wireless blockchain networks are mostly dependent on consensus methods. Xu et al. [12] look at how well wi-fi blockchain networks hold up under hostile jamming attacks and suggest a Raft-based consensus algorithm to lessen the jamming effect on network performance.

Salman et al. [13] present a thorough survey of security services made possible by blockchain technology. They highlight the possible uses and research obstacles in this discipline by discussing several blockchain-based security solutions such access control, data authentication, and secure communication.

All things considered, the literature analysis shows how various blockchain technology uses can be found in cell edge computing, driverless cars, linked vehicle forensics, smart factories, and IoT. It emphasises the want of handling the particular difficulties and possibilities in combining blockchain with wireless networks to achieve the entire potential of distributed and safe communication systems.

III. METHODOLOGY

a) Proposed Work:

By using blockchain technology to build a distributed and safe access control framework, the suggested system seeks to overcome the drawbacks of centralised access control [7] systems. Access control choices in this system are governed by smart contracts run on a blockchain network, hence guaranteeing transparency, immutability, and resistance to single points of failure.

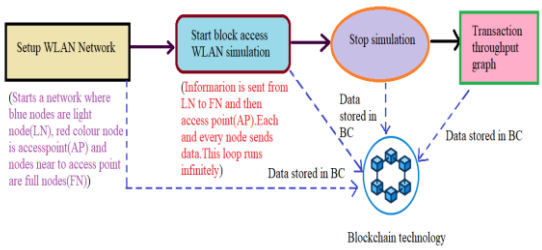
Encoded as smart contracts, access control policies run access choices automatically depending on pre-defined criteria and regulations.

Recording all access control transactions in a tamper-proof and unchangeable way, the blockchain network acts as a distributed ledger. This guarantees openness and responsibility by letting users audit get entry to manage choices and monitor access history in real-time.

Users verify themselves using blockchain-produced cryptographic tokens [4, 5]. These tokens eliminate the want for centralised authentication systems and lower the risk of illegal access by providing safe and verifiable proof of identity.

The suggested decentralised blockchain-based access control system provides a safe, open, and robust way to govern access rights in dispersed settings.

b) System Architecture:



"Fig1 Proposed Architecture"

The system architecture starts with the configuration of a WLAN network made up of "light nodes (LN), full nodes (FN), and an access point (AP)". Within this network, LNs and FNs interact; FNs are closer to the AP.
The block access WLAN simulation starts next; data moves from LNs to FNs [15] and finally to the AP. Every node contributes actively to data transmission, hence generating a constant loop until the simulation stops.
The blockchain (BC) securely stores the data accumulated throughout the simulation once stopped.
At last, the design enables transaction throughput study by looking at the data flow inside the network and keeping transaction data in the BC. By using the natural security characteristics of blockchain technology and the allotted character of wireless communication, this design guarantees the strength and integrity of wireless Blockchain [2,3] networks.

c) Setup WLAN Network:
The "Setup WLAN network" module sets up and configures the "wireless local area network (WLAN)" for the project. It creates the WLAN network, allocating roles to nodes including "light Nodes (LNs), full Nodes [15] (FNs), and access points (APs)". This module specifies the topology and connection of the network, controlling data flow between nodes, and defines each node's features, including communication capabilities and initial parameters.
d) Start Block Access WLAN Simulation:
The "start Block access WLAN Simulation" module starts the wireless blockchain network simulation. "Light Nodes (LNs)" collect data from their surroundings and send it to specified "full Nodes (FNs)" for processing and mining. Access control policies like BAC1 or BAC2 help to control facts transfer, hence avoiding conflicts. FNs mine received data into blockchain storage blocks, finally transmitting them to the "access point (AP)" for storage.
e) Transaction Throughput Graph:
The "Transaction Throughput Graph" module computes and graphically displays the throughput of data transactions in the wireless blockchain network. It tracks the number of successful data transfers over time and calculates the throughput as the amount of data sent successfully. Usually using line graphs, results are graphically shown with every line signifying a distinct access control policy (e.g., BAC1, BAC2), hence enabling performance comparison and study.
f) Stop simulation:
Engineered to stop the current simulation, the "stop Simulation" module stops all network activities. Activated, it ends access control procedures, transmission, and data sensing. It'd also include looking at and documenting simulation outcomes to provide analysis of network performance. Ending the simulation lets in users to evaluate data transfer results and grasp network behaviour, hence enabling system assessment and possible optimisation.
g) Blockchain Integration:
Blockchain spreads facts storage among several nodes rather than depending on a centralised server. This method guarantees fault tolerance and redundancy. Data is copied throughout the network, hence lowering the possibility of data loss in the event of node screw ups or network problems.
FNs get data from "light Nodes (LNs)" and convert it into blocks appropriate for blockchain storage. Validating and timestamping data, putting it on the blockchain, and guaranteeing its security and unchangeability comprise this mining technique.
Every data block produces a unique hash code, which acts as a virtual fingerprint. Before a data block is added to the blockchain, PoW [9] verification guarantees its legitimacy. This verification method protects against data manipulation and preserves the integrity of kept information.

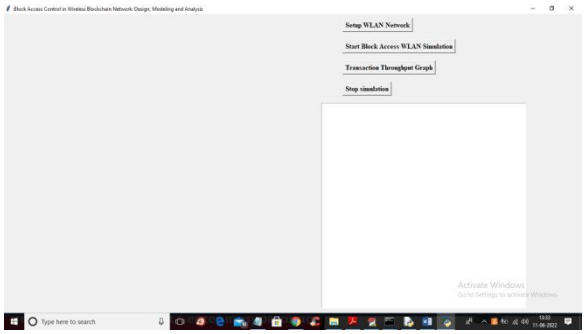
Data blocks generated via FNs are sent to the AP for storage. By keeping a record of these blocks in the blockchain, the AP makes the data available for other FNs to download and check. This distributed garage system guarantees network-huge data availability.

Access control policies specify guidelines and criteria for data transfer. They stop problems like data forking, in which several nodes at once transmit contradictory data. These approaches improve the dependability and consistency of data inside the network by using controlling when and how data is sent.

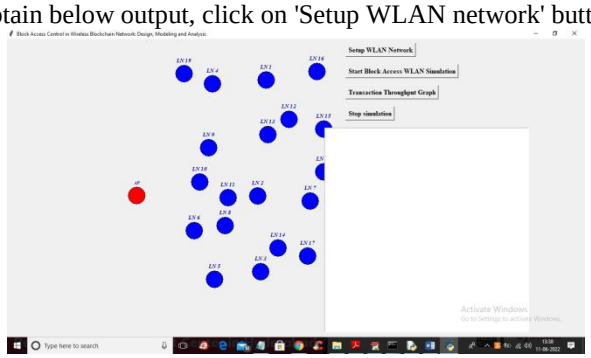
The Ethereum blockchain runs a Solidity clever settlement to interface with the wi-fi sensor community. This clever contract links the network to the blockchain. It guarantees that sensor facts kept on the blockchain stays safe and unmodified by enforcing policies for facts integrity and immutability. The contract builds network confidence and dependability.

IV. EXPERIMENTAL RESULTS

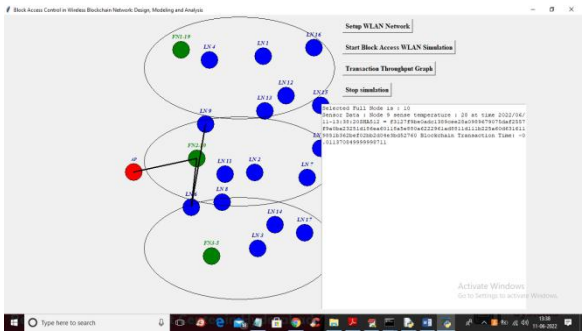
Project run double clicks on the 'run.bat' file to obtain below screen.

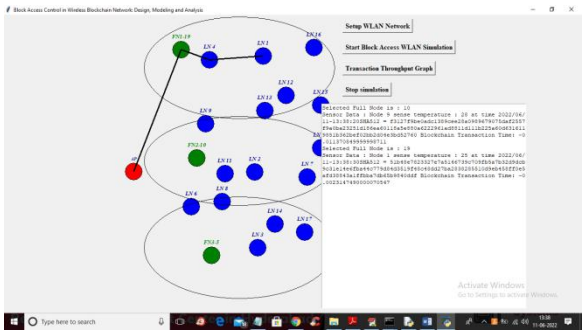


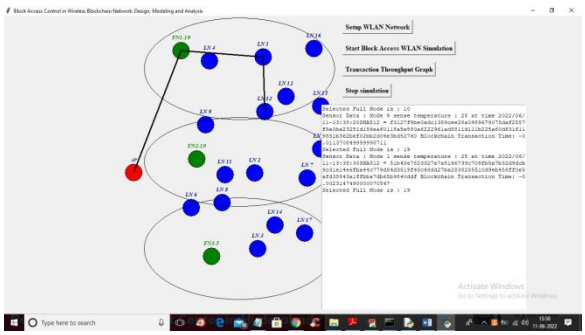
To configure network and obtain below output, click on 'Setup WLAN network' button on above screen.



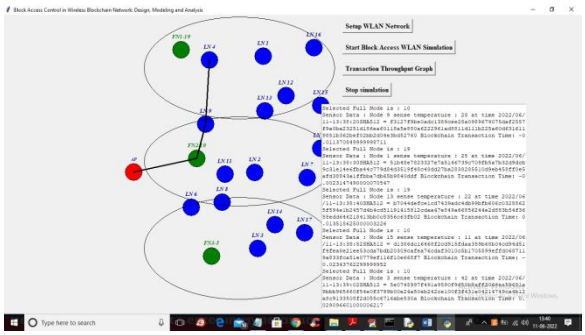
In above screen all blue colour circles consider as light Node which transfer data to full Node and the nodes which are nearer to AP red colour node is called full Node. Red colour circle is called access point; all light Nodes provide data to full Node, which in flip sends to access point. to begin transmitting data to access point, now select the option labelled "start Block access WLAN Simulation."



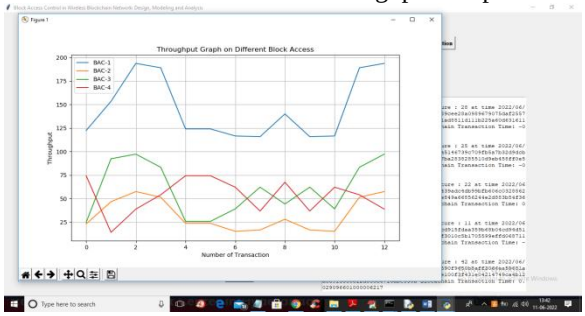




every blue light node in above screen will be randomly chosen as source; it will sense some random data and ship to green color full Node; full Node will send to access point; in above screen we can see data sending via black colour line; if one node sends data, other nodes will wait and continue only after first one completes; this simulation will run in infinite loop; to stop simulation click on 'stop Simulation' button.



Above screen in text section shows which node is selected as FN and which node is sending what data. To obtain following output, now click on button 'Transaction Throughput Graph'



In above graph x-axis shows number of transactions and y-axis shows throughput of transferring that transaction data. Throughput is the quantity of data sent from beginning to end tie. Blue line shows BAC1 method throughput; likewise, various other strains show various strategy throughput. BAC-1 had great throughput in all methods

V. CONCLUSION

To sum up, the use of blockchain technology greatly improves data security by reducing centralised server-related vulnerabilities, maintaining data integrity, and offering fault tolerance. Blockchain is a perfect solution for protecting vital data across many applications since its natural characteristics, like its unique hash code and proof of work (PoW) verification, provide strong assurances of data integrity and anti-tampering.

Using access control policies like BAC1, BAC2, BAC3, and BAC-4, data transmission is efficiently controlled, hence removing the possibility of forking issues in multi-node networks. Smart contracts run on systems like Ethereum [18] guarantee safe and unchangeable data storage, hence supporting the dependability of sensor data.

The effective incorporation of blockchain technology into this project shows its practical promise in making wi-fi sensor networks more robust, safe, and appropriate for vital monitoring uses. It emphasises the need of Blockchain [1-5] in improving network performance and data security.

The suggested mining and discard techniques also seek to lower pointless computational resource use on forking blocks and improve transaction throughput in B-WLAN. Performance assessments of four BAC methods using Markov chain models show how well the discard approach meets the needs of large service requests in next-generation wi-fi networks by attaining high transaction throughput. Furthermore, maximising block size and PoW [9] hash difficulty gives analytical direction for constructing best and safe B-WLANs in the future.

VI. FUTURE SCOPE

Integrating "artificial intelligence (AI) and machine studying (ML)" algorithms with blockchain-based access manipulate systems would thereby strengthen security and efficiency in future scope. By using AI/ML technologies for anomaly detection, threat mitigation, and adaptive access control rules, this development offers hope for improving resilience against new security concerns.

The performance of baseline methods lacking particular techniques will be investigated as part of future efforts. The study will centre on grasping the forking likelihood in backoff and queuing processes, which gives a major difficulty in calculating block use and transaction throughput. Addressing those issues and including AI/ML-driven improvements helps to maximise security, efficiency, and resilience inside blockchain-based wireless networks even further.

REFERENCES

[1]. Z. Xiong, Y. Zhang, and et al., "When mobile blockchain meets edge computing," IEEE Commun. Mag., vol. 56, no. 8, pp. 33-39, Aug. 2018.

[2]. M. Liu, F. R. Yu, and et al., "Distributed resource allocation in blockchain-based video streaming systems with mobile edge computing," IEEE Trans. Wireless Commun., vol. 18, no. 1, pp. 695-708, Jan. 2019.

[3]. S. R. Pokhrel, J. Choi, and et al., "Federated learning with blockchain for autonomous vehicles: analysis and design challenges," IEEE Trans. Commun., vol. 68, no. 8, pp. 4734-4746, Aug. 2020.

[4]. M. Cebe, E. Erdin, and et al., "Block4forensic: an integrated lightweight blockchain framework for forensics applications of connected vehicles," IEEE Commun. Mag., vol. 56, no. 10, pp. 50-57, Oct. 2018.

[5]. J. Wan, J. Li, and et al., "A blockchain-based solution for enhancing security and privacy in smart factory," IEEE Trans. Ind. Informat., vol. 16, no. 5, pp. 3652-3660, Jun. 2019.

[6]. B. Cao, Y. Li, and et al., "When Internet of Things meets blockchain: challenges in distributed consensus," IEEE Netw., vol. 33, no. 6, pp. 133-139, Nov.-Dec. 2019.

[7]. Y. Zhang, S. Kasahara,, and et al., "Smart contract-based access control for the Internet of Things," IEEE Internet of Things J., vol. 6, no. 2, pp. 1594-1605, Jun. 2018.

[8]. J. Wang, N. Lu, and et al., "A secure spectrum auction scheme without the trusted party based on the smart contract," Digit. Commun. Netw., July 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S235286481930330X.

[9]. S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," White paper, 2009. [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[10]. G. BitFury, "Proof of stake versus proof of work," White paper, Sep. 2015. [Online]. Available: https://bitfury.com/content/downloads/pos-vspow-1.0.2.pdf.

[11]. M. Castro and B. Liskov, "Practical Byzantine fault tolerance," In Proc. Symp. Oper. Syst. Design Implement., New Orleans, LA, USA, 1999.

[12]. H. Xu, L. Zhang, and et al., "RAFT based wireless blockchain networks in the presence of malicious jamming," IEEE Wirel. Commun. Lett., vol. 9, no. 6, pp. 817-821, Jun. 2020.

[13]. T. Salman, M. Zolanvari, and et al., "Security services using blockchains: a state of the art survey," IEEE Commun. Surveys Tuts., vol. 21, no. 1, pp. 858-880, First Quarter 2019.

[14]. J. Xie, F. R. Yu, and et al., "A survey on the scalability of blockchain systems," IEEE Netw., vol. 33, no. 5, pp. 166-173, Sept.-Oct. 2019.

[15]. A. M. Antonopoulos, "Mastering Bitcoin: unlocking digital cryptocurrencies," 2nd ed. Sebastopol, CA, USA: O'Reilly Media, Inc., June 2017.

[16]. BILLA, N. M., Prasadu PEDDI, & Manendra Sai DASARI. (2025). Design and Implementation of Hybrid Adaptive Neural Architecture for Self-Absorption in Virtual Machines. *International Journal of Computational and Experimental Science and Engineering*, *11*(1).

[17]. M. Rosenfeld, "Analysis of hashrate-based double-spending," 2014. [Online]. Available: https://arxiv.org/pdf/1402.2009.pdf

[18]. V. Buterin, "A next-generation smart contact and decentraliaed application platform," White paper, 2014. [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper.
[19]. G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function," IEEE J. Sel. Areas Commun., vol. 18, no. 3, pp. 535-547, Mar. 2000.
[20]. Prasadu Peddi, & Dr. Akash Saxena. (2016). STUDYING DATA MINING TOOLS AND TECHNIQUES FOR PREDICTING STUDENT PERFORMANCE. International Journal Of Advance Research And Innovative Ideas In Education, 2(2), 1959-1967.
[21]. S. M. Ross, "Introduction to probability models,"Academic Press, 2014. 11th edition.
[22]. I. Eyal, A. E. Gencer, and et al., "Bitcoin-NG: a scalable blockchain protocol," In Proc. USENIX Symp. Netw. Syst. Design Implement. (NSDI), Boston, USA, Mar. 2016.
[23]. G. Sagirlar, B. Carminati, and et al., "Hybrid-IoT: hybrid blockchain architecture for Internet of Things-pow sub-blockchains," In Proc. IEEE iThings. GreenCom. CPSCom. SmartData., 2018.
[24]. J. Wang, and H. Wang, "Monoxide: scale out blockchains with asynchronous consensus zones," In Proc. USENIX Symp. Netw. Syst. Design Implement. (NSDI), Boston, USA, Feb. 2019.
[25]. S. Popov, "The tangle," White paper, 2018. [Online]. Available: https://www.iota.org/research/academic-papers.
[26]. Z. Xiong, S. Feng, and et al., "Cloud/fog computing resource management and pricing for blockchain networks," IEEE Internet of Things J., vol. 6, no. 3, pp. 4585-4600, Jun. 2019.
[27]. Z. Xiong, J. Kang, and et al., "Cloud/edge computing service management in blockchain networks: multi-leader multi-follower game-based ADMM for pricing," IEEE Trans. Services Comput., vol. 13, no. 2, pp. 356-367, Mar.-Apr. 2020.
[28]. Z. Li, M. Xu, and et al., "NOMA-enabled cooperative computation offloading for blockchain-empowered Internet of Things: a learning approach," IEEE Internet of Things J., vol. 8, no. 4, pp. 2364-2378, Feb. 2021.
[29]. Y. Li, B. Cao, and et al., "Direct acyclic graph-based ledger for Internet of Things: performance and security analysis," IEEE/ACM Trans. Netw. , vol. 28, no. 4, pp. 1643-1656, Aug. 2020.
[30]. D. Huang, X. Ma, and et al., "Performance analysis of the Raft consensus algorithm for private blockchains," IEEE Trans. Syst. Man Cybern. Syst., vol. 50, no. 1, pp. 172-181, Jan. 2020.
[31]. Y. Sun, L. Zhang, and et al., "Blockchain-enabled wireless Internet of Things: performance analysis and optimal communication node deployment," IEEE Internet of Things J., vol. 6, no. 3, pp. 5791-5802, Mar. 2019.
[32]. B. Cao, M. Li, and et al., "How does CSMA/CA affect the performance and security in wireless blockchain networks," IEEE Trans. Ind. Informat., vol. 16, no. 6, pp. 4270-4280, Jun. 2020