A study into blockchain applications for 5G and networks

Abstract – blockchain applications for 5g and networks can have an effect and impact on many areas for both by allowing development, changes, and improvement to various sectors. However, there are a great number of challenges and issues related to security, privacy, data leaks, scalability and throughput that have caused concern and halted the use of blockchain applications. After observing papers related to blockchain the use of blockchain, 5g and networks could be used to solve some issues that current technologies are facing, but to fully implement these technologies more research needs to conduct to address any complications or concerns. We'll go through some of the most common uses for this technology in the workplace, home, and city, as well as some of the issues that come with them. For this reason, we provide remedies and analyze their usefulness, as well as address future research areas that might allow the technology to overcome its difficulties and become widely adopted.

I. KEYWORDS

1. 5G Networks
2. Machine learning
3. Security and privacy
4. Blockchain
5. 5G internet of things

II. INTRODUCTION

Blockchain technology is a way of holding onto data which protects it and makes it harder for third parties or hackers to be able to try and hack the system or try to defraud it in any way any computer that is in a blockchain network has a copy of a blockchain ledger. Decentralized databases that are administered by several parties are known as Distributed Ledger Technology. Blockchain is a Decentralized Ledger Technology which is where any transactions that have been made are then recorded by something called a hash which is an immutable cryptographic signature, which is generated by a distributed computing system. In other words, if it appears that any blocks in the chain have been altered it will be known that the blockchain has been modified or compromised. A blockchain system would have to be corrupted by changing every block in the chain, across all the distributed versions of the chain, for hackers to achieve success. Cryptocurrency blockchains, such as Bitcoin and Ethereum, are constantly and continuously developing as new blocks are added to the chain, which therefore increases the security of the distributed ledger.

A. scope

in this paper multiple topics were covered in the recent advances section I have covered the background of blockchain but have not spoken about the background of 5g as the blockchain is the focus of the paper and 5g has been explained and talked about more through the paper. to explain blockchain for 5g enabling technologies I have spoken about cloud computing/cloud-RAN and have not spoken about mobile edge computing, network function virtualization, network slicing or device to device communication. For block chain 5g services I have spoken about federated learning and have not spoken about spectrum management, data sharing, network virtualization, resource management, inference management or privacy and security. Finally, for blockchain for 5g IoT applications, I choose to speak about unmanned ariel vehicles but have not spoken about smart healthcare, smart city, smart transportation, or smart grid.

B. organization

1. recent advances
   - **blockchain** – this section states what a blockchain is and the different types of blockchains and who can access them
   - **blockchain components** – this section explains the multiple components of a blockchain and explains each one showing what they do and where they can be used
   - **blockchain for cloud computing** – this section explains why cloud computing is used and the benefits of it also goes in-depth into frameworks that have been made due to blockchain and other technologies
   - **federated learning** – this section discusses the use of federated learning and how it can be used for mobile network services and how it can be used to improve mobile privacy and how it can prevent attacks from third parties.
   - **unmanned aerial vehicles –** section discusses the use of UAVs and how they can be used to support iot networks and reduce the stress and traffic on them. It discusses how the UAVs can be used and the potential risks that may come with the use of them.

2. challenges and directions
   - **challenges of blockchain and 5g integration** – this section discusses all the issues and security risks that come with blockchain
   - **blockchain performance and scalability** – this section discusses the limitations of blockchain performance as its throughput is

much slower and can handle less compared to non-blockchain applications such as visas.

- **security and privacy** – discuss the flaws of blockchain and how a minority can control 50% of the network power and can control transactions and pose great risks.
- **integration machine learning with blockchain for 5g** – explains how machine learning can be used to improve future 5g blockchain services. And how it can be integrated

III. RECENT ADVANCES

A. blockchain

blockchains are either private or public [1]. when a blockchain is public it means anyone can access them and make a transaction. The most popular blockchain application currently is bitcoin a private blockchain is a private blockchain is essentially invited only network that is regulated and managed.

B. Blockchain components

Blockchain has multiple components for example:

1. Data block – is where a chain of blocks, starting with a genesis block, connects every newly updated block to form a blockchain. Every block that is added is closely linked to the previous one by a hash label, preventing any alteration risks. One transaction record per data block, plus a blockchain header [2]. Merkle tree design of a combination of all transactions is used to organize and store the records of transactional activity. Furthermore, the block header is composed mostly of four minor components: the hash value, the Merkle root, the nonce value, and the timestamp.
2. Consensus algorithms - To prevent security difficulties, the block-transaction chain shouldn't be under the control of just one person or company but rather every block is managed equally by all parties involved [3]. Consensus is one way to do this. The consensus method ensures that entities agree on each data blockchain. For example, Bitcoin utilizes the Proof of Work method to manage transactions. Nodes that have a high computational capability are allowed to go through the mining process in which they have to go against other nodes to verify a block of data first to receive a reward. [4]
3. Smart contracts - A smart contract is a self-executing blockchain application. Since the first Ethereum smart contract was established in 2015, this technology has grown rapidly. Smart contracts can automatically execute provisions defined in the contract. Inputs from users can be used to execute smart contracts. Nothing in the smart contract may be changed, and its functionality is not dependent on a third party [4]. Smart contracts are frequently employed in applications such as money transfer, healthcare data sharing, and supply chain management because of their unique features [5].

C. The use of blockchain technology in cloud computing

Cloud computing has gained popularity in recent years due to its unlimited storage and computing capacity, allowing for on-demand, powerful and efficient services with minimal administrative work. Cloud computing has been intensively explored and integrated with 5G networks, paving the path for cloud-assisted multi-dimensional huge data processing applications. To realize 5G services, there are several options available through cloud computing paradigms, including streamlining communication and storage processes for 5G data content capture, as well as resource allocation for cloud-enabled small cells for 5G media services [6]. For example, the cloud radio access network architecture is seen to be the most ideal and best when it comes to managing a large number of small cells through the centralized cloud controller as a baseband unit pool so that it can keep up to speed with the growing and much-needed demand for user association and allocating resources in cellular 5g networks. In addition, Cloud-RAN is capable of providing interconnection at a high-speed level and shared powerful processing to make it easier for multicell cooperation alongside also making it easier for real-time cloud computing.[7]

Currently, a blockchain-based approach is being analyzed and slowly interpreted with cloud computing so that it can be used to address any security issues successfully that have been previously mentioned.

With the help of blockchain, [8] developed BlockONet, a framework designed to increase the network's credibility and security in 5G fronthaul scenarios. Verification between IoT devices, BBU units and the manufacturer is made possible using blockchain technology and smart contracts, which save user access information in an immutable database on the blockchain. When using blockchain cloud-RAN it has 2 main advantages the first being that there is a reduction in single-point failure bottlenecks due to decentralized fair agreement using blockchain consensus platform. The second advantage is that using a decentralized blockchain and having no third parties with it optimizes resources consumption and reduces signaling and connection costs. According to the same line of thinking, the research conducted by [9] uses blockchain to create a reliable and trusted authentication architecture for cloud radio access networks in the 5G era.

Due to its centralized architecture, existing cloud computing models pose unaddressed security, networking, and computing performance issues. A large amount of data traffic from IoT devices to the cloud has created new security concerns such as data availability, privacy management, and data integrity [23] in the 5G era. 5G data transmission to the cloud and data interchange between cloud service providers and mobile consumers, for instance, can be compromised by third parties. Unauthorized access to personal information is possible even among network organizations that are curious about the data that is being shared.

D. Federated learning

Federated learning is now being seen as a viable machine learning technique when it comes to mobile network situations on a great scale, particularly in the context of social networks [10]. When employing federated learning, distributed model training can be accomplished through the use of local datasets from distributed nodes. However, not all data is shared the only information that is shared is model updates. It utilizes the computing power that the device has untapped private data through decentralizing model training and storing data locally. This developing technique promises to serve 5G applications which will be privacy sensitive while protecting mobile device privacy. Recently, the use of blockchain and federated learning to solve complicated issues in 5G wireless networks has been discussed. [11] provide an on-device machine learning architecture that does not require centralized training data or coordination can be provided. An incentive mechanism on the blockchain also speeds up training, promoting pervasive device collaboration.

The study by [12] proposes a reputation strategy that picks reputable mobile devices for federated learning. Blockchain technology and contract theory enable an incentive mechanism that promotes high-quality data workers that participate in model training, hence reducing attacks in throughout federated learning systems.

[13], the writers combine blockchain and federated learning to determine data relevance in mobile device networks. This is to encourage mobile users to gather relevant information on a certain topic while interacting with other users. This decreases the risk of centralized data storage. The Proof of Common Interest consensus technique verifies data before it is added to the blockchain ledger.

[14] takes on a blockchain-enabled safe data sharing architecture for dispersed devices in IoT. Incorporating federated learning allows for data exchange while maintaining privacy. The federated learning paradigm ensures data privacy by sharing the data model without releasing the actual data.

E. Unmanned ariel vehicles

Unmanned Aerial Vehicles [15] are rapidly evolving, opening new business opportunities. UAVs are flying IoT devices that have been utilized for military, vehicle networks, and smart cities. While 5G networks accommodate billions of IoT devices, the quick expansion of IoT data traffic is seen as a serious difficulty to current network architecture with static base stations. So, deploying UAVs to support IoT networks is logical. With its mobility and flexibility, UAV can provide unparalleled IoT services such as dynamic traffic unloading and object monitoring. To operate UAVs in the skies poses various privacy and security hazards affecting data accountability, integrity, permission, and reliability.

Recent research has focused on combining blockchain and UAVs to address crucial UAV network difficulties and enable new 5G IoT applications. For example, [16] use consortium blockchain to create a spectrum sharing platform for UAV-based cellular networks. To ensure spectrum trading and sharing between mobile network operators and drone operators, a distributed shared database must be established. Security threats associated with UAV-based spectrum trading caused by malevolent UAVs abusing the spectrum and privacy leaks because of a centralized sharing architecture are two of the most pressing concerns addressed by the model under consideration.

UAVs could be used to create an independent economic system where blockchain serves as a protocol for independent business activities in current industrial and corporate processes, according to [17]. With the use of multi-agent systems, IoT devices such as robots and unmanned aerial vehicles may exchange data and work together in an unattended fashion. In order to maintain the system's integrity and safety, any agent can join and carry out block verification tasks. The distributed network that blockchain creates allows any agent to join and execute block verification, ensuring that the system will continue to run correctly and safely in the long term. [18] propose the use of blockchain technology to address the challenges of data leakage and data loss that might occur during the transfer of data between UAVs. The data transfer process takes place within the blockchain, which allows for the storage of all user information as well as the exchange of records for security management.

Blockchain technology is being studied and is currently integrated with cloud/edge computing to enable new UAV-based applications. Using UAV swarms to collect data from IoT devices, [19] investigate the security of a blockchain-enabled data collecting system for UAV swarm networks. When establishing the security mechanism, UAVs uses a unique shared key so they can communicate to the IoT devices. Data gathering from IoT devices and missions is handled by a smart contract.

IV. CHALLENGES AND FUTURE DIRECTIONS

A. The difficulties associated with the integration of blockchain technology and 5G

Before deploying blockchain with 5G, significant obstacles must be addressed. First, existing 5G systems need infrastructure for blockchain integration. Smart contract software for blockchain integration in 5G are not provided by most 5G wireless providers. The absence of standardization and rules also hinders the integration of blockchain and 5G [20]. Due to lack of coordination between blockchain enterprises and governments, existing blockchain operations are deregulated. It is difficult to implement blockchain in real-world 5G networks without standardization, needs to be resolved before implementation.

B. Blockchain performance and scalability

Throughput - When put up against non-blockchain apps, the throughput of blockchain applications is much lower. Consider the following comparison: Bitcoin can only manage four transactions per second, whereas Visa can handle up to 1667 transactions per second. [21]. The present blockchain systems have major scalability issues with replicas and performance issues with throughput and transaction delay (22). This because the block size restriction, many blockchains have significant queues for adding transactions. Thus, a rapid rise in block production time can lower total system throughput.

Storage - 5G networks employ blockchain technology to analyze enormous volumes of data generated by Internet of Things devices in order to provide 5G services such as data sharing, resource management, and user transaction monitoring. A copy of the whole transaction data is typically processed and stored by each blockchain node in the normal course of events. IoT devices with low resources may experience storage and processing challenges as a result of this. [24]

C. Concerns about the security and privacy of blockchain technology

Blockchain is regarded as a secure database platform to protect the security and privacy of 5G networks. However, recent studies have found blockchain has underlying security vulnerabilities that are mostly connected to 5G networks [25]. In blockchain mining, a 51 percent attack happens when a group of miners controls more than 50 percent of the network's computational power, preventing the block from being properly transacted and mined. Adversaries can take advantage of this weakness to gain control of the blockchain and change transactional information. In addition, the functioning of smart contracts raises some security risks, such as the possibility of data leakage or the alteration of system logic, among other things. All these vulnerabilities would raise additional worries about the database security of blockchain-based 5G networks. Several recent security upgrades, such as SmartPool, which was proposed to increase transaction validation efficiency for blockchain mining, have the potential to reduce security bottlenecks, such as a 51 percent vulnerability in blockchain mining, by reducing the number of transactions validated. Smart contracts' security may now be better assessed with the use of new security techniques introduced in recent research [26]. These efforts would increase the security and performance of blockchain 5G environments.

D. Using machine learning in conjunction with blockchain for 5G

Revolutionary machine learning technology can be used to improve the most recent 5G services by offering data-driven insights to support decision-making activities or data forecasts, enabling 5G services to become more intelligent. Future networks could benefit from blockchain-5G services thanks to machine intelligence advancements. Machine learning, for example, can be used to improve resource management and user communication, among other things. The discovery of data features to predict data usage behavior for the purpose of creating control algorithms, such as data traffic estimation to reduce network congestion or user access tracking to maintain privacy, also shows great promise. For 5G use case domains, machine learning and blockchain are increasingly being combined. Deep reinforcement learning [27] is being studied and integrated with blockchain so it can provide secure and intelligent resource management and orchestration in the 5G network. Blockchain-Deep Reinforcement Learning architectures have also been proposed in other key publications for flexible and secure compute offloading, dependable networks, as well as network optimization and network management.

V. CONCLUSION

blockchain has first been described and then labelled as being both private and public and who can access them. The Blockchain has further been explained and the different components have been explained. The data block is how a blockchain is formed and how each newly updated block is added by a hash label to from at blockchain. Conscious algorithms are used to prevent a security risk. Smart contracts are used as a self-executing blockchain application.

Cloud computing is used due to its great number of features. Cloud computing and blockchain have been used together to improve security and credibility. Federate learning can be used to improve security and prevent attacks from third parties. UAVs can be sued alongside IoT networks and ease the pressure on the networks. However, UAVs pose big security and privacy risk. UAVs can be used to address network issues and enable new 5g IoT applications by combining with blockchain.

5g systems do not have the infostructure needed for blockchain integration. Due to centralized architecture cloud computing has many issues. Blockchain has a low throughput non-blockchain application that can handle more transactions. Blockchain requires a lot of storage due to the need of making copies. Blockchain has a lot of vulnerabilities when it comes to security. Machine learning can be used to improve current 5g services using data-driven insights.

VI. REFERENCES

[1]W. Wang et al., “A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks,” IEEE Access, vol. 7, pp. 22328–22370, 2019, doi: 10.1109/access.2019.2896108.

[2]T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, “Untangling Blockchain: A Data Processing View of Blockchain Systems,” IEEE Transactions on Knowledge and Data Engineering, vol. 30, no. 7, pp. 1366–1385, Jul. 2018, doi: 10.1109/tkde.2017.2781227.

[3]S. Zhang and J.-H. Lee, “Double-Spending With a Sybil Attack in the Bitcoin Decentralized Network,” IEEE Transactions on Industrial Informatics, vol. 15, no. 10, pp. 5715–5722, Oct. 2019, doi: 10.1109/tii.2019.2921566.

[4]J. Liu and Z. Liu, “A Survey on Security Verification of Blockchain Smart Contracts,” IEEE Access, vol. 7, pp. 77894–77904, 2019, doi: 10.1109/access.2019.2921624.

[5]S. Rouhani and R. Deters, “Security, Performance, and Applications of Smart Contracts: A Systematic Survey,” IEEE Access, vol. 7, pp. 50759–50779, 2019, doi: 10.1109/access.2019.2911031.

[6]P. Paglierani et al., “Techno-economic analysis of 5G immersive media services in cloud-enabled small cell networks: The neutral host business model,” Transactions on Emerging Telecommunications Technologies, Sep. 2019, doi: 10.1002/ett.3746.

[7]X. Wang et al., “Virtualized Cloud Radio Access Network for 5G Transport,” IEEE Communications Magazine, vol. 55, no. 9, pp. 202–209, 2017, doi: 10.1109/mcom.2017.1600866.

[8]H. Yang, Y. Wu, J. Zhang, H. Zheng, Y. Ji, and Y. Lee, “BlockONet: Blockchain-based Trusted Cloud Radio over Optical Fiber Network for 5G Fronthaul,” www.osapublishing.org, Mar. 11, 2018. https://www.osapublishing.org/abstract.cfm?uri=OFC-2018-W2A.25 (accessed Jun. 04, 2021).

[9]H. Yang, H. Zheng, J. Zhang, Y. Wu, Y. Lee, and Y. Ji, “Blockchain-based trusted authentication in cloud radio over fiber network for 5G,” IEEE Xplore, Aug. 01, 2017. https://ieeexplore.ieee.org/abstract/document/8121598 (accessed Mar. 24, 2022).

[10]T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, “Federated Learning: Challenges, Methods, and Future Directions,” IEEE Signal Processing Magazine, vol. 37, no. 3, pp. 50–60, May 2020, doi: 10.1109/msp.2020.2975749.

[11]H. Kim, J. Park, M. Bennis, and S.-L. Kim, “Blockchained On-Device Federated Learning,” IEEE Communications Letters, vol. 24, no. 6, pp. 1279–1283, Jun. 2020, doi: 10.1109/lcomm.2019.2921755.

[12]J. Kang, Z. Xiong, D. Niyato, S. Xie, and J. Zhang, “Incentive Mechanism for Reliable Federated Learning: A Joint Optimization Approach to Combining Reputation and Contract Theory,” IEEE Internet of Things Journal, vol. 6, no. 6, pp. 10700–10714, Dec. 2019, doi: 10.1109/JIOT.2019.2940820.

[13]R. Doku, D. B. Rawat, and C. Liu, “Towards Federated Learning Approach to Determine Data Relevance in Big Data,” IEEE Xplore, Jul. 01, 2019. https://ieeexplore.ieee.org/abstract/document/8843451 (accessed Mar. 24, 2022).

[14]Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, “Blockchain and Federated Learning for Privacy-preserved Data Sharing in Industrial IoT,” IEEE Transactions on Industrial Informatics, pp. 1–1, 2019, doi: 10.1109/tii.2019.2942190.

[15]D. Chi-Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, “Secrecy Performance of the UAV Enabled Cognitive Relay Network,” IEEE Xplore, Dec. 01, 2018. https://ieeexplore.ieee.org/abstract/document/8644982 (accessed Mar. 24, 2022).

[16]J. Qiu, D. Grace, G. Ding, J. Yao, and Q. Wu, “Blockchain-Based Secure Spectrum Trading for Unmanned-Aerial-Vehicle-Assisted Cellular Networks: An Operator’s Perspective,” IEEE Internet of Things Journal, vol. 7, no. 1, pp. 451–466, Jan. 2020, doi: 10.1109/jiot.2019.2944213.

[17]A. Kapitonov, S. Lonshakov, A. Krupenkin, and I. Berman, “Blockchain-based protocol of autonomous business activity for multi-agent systems consisting of UAVs,” IEEE Xplore, Oct. 01, 2017. https://ieeexplore.ieee.org/abstract/document/8101648 (accessed Mar. 24, 2022).

[18]T. Rana, A. Shankar, M. K. Sultan, R. Patan, and B. Balusamy, “An Intelligent approach for UAV and Drone Privacy Security Using Blockchain Methodology,” 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Jan. 2019, doi: 10.1109/confluence.2019.8776613.

[19]A. Islam and S. Y. Shin, “BUS: A Blockchain-Enabled Data Acquisition Scheme With the Assistance of UAV Swarm in Internet of Things,” IEEE Access, vol. 7, pp. 103231–103249, 2019, doi: 10.1109/access.2019.2930774.

[20]A. Anjum, M. Sporny, and A. Sill, “Blockchain Standards for Compliance and Trust,” IEEE Cloud Computing, vol. 4, no. 4, pp. 84–90, Jul. 2017, doi: 10.1109/mcc.2017.3791019.

[21]Y. Zhang, C. Xu, X. Lin, and X. S. Shen, “Blockchain-Based Public Integrity Verification for Cloud Storage against Procrastinating Auditors,” IEEE Transactions on Cloud Computing, pp. 1–1, 2019, doi: 10.1109/tcc.2019.2908400.

[22]A. A. Monrat, O. Schelen, and K. Andersson, “A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities,” IEEE Access, vol. 7, pp. 117134–117151, 2019, doi: 10.1109/access.2019.2936094.

[23]S. Kim, Y. Kwon, and S. Cho, “A Survey of Scalability Solutions on Blockchain,” IEEE Xplore, Oct. 01, 2018. https://ieeexplore.ieee.org/document/8539529 (accessed Aug. 27, 2020).

[24]W. Wang et al., “A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks,” IEEE Access, vol. 7, pp. 22328–22370, 2019, doi: 10.1109/access.2019.2896108.

[25]X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, “A survey on the security of blockchain systems,” Future Generation Computer Systems, vol. 107, Aug. 2017, doi: 10.1016/j.future.2017.08.020.

[26]R. Cheng et al., “Ekiden: A Platform for Confidentiality-Preserving, Trustworthy, and Performant Smart Contracts,” 2019 IEEE European Symposium on Security and Privacy (EuroS&P), Jun. 2019, doi: 10.1109/eurosp.2019.00023.

[27]Y. Dai, D. Xu, S. Maharjan, Z. Chen, Q. He, and Y. Zhang, “Blockchain and Deep Reinforcement Learning Empowered Intelligent 5G Beyond,” IEEE Network, vol. 33, no. 3, pp. 10–17, May 2019, doi: 10.1109/mnet.2019.1800376.