The integration of blockchain technology in 5G-enabled IoT

Honar Mohammed Taha[1*], *Marwan* Aziz Mohammed[2], *Yousif* Sufyan Jghef[2], *Sazan* Kamal Sulaiman[2], *and Twana* Saeed Mustafa[3]

[1] Dept. of Software and Informatics Engineering, College of Engineering, Salahaddin University, Erbil 44001, Iraq.
[2] Dept. of Computer engineering, College of Engineering, Knowledge university, Erbil 44001, Iraq.
[3]Department of Software Engineering, Firat University, Elazig, Turkey.

Abstract. By linking billions of electronic devices and gadgets, the Internet of Things (IoT) has completely changed the digital landscape by extending the Internet to the various application deployments in different areas within a centralized network, these devices need high data rates and low latency to perform well and to be secure due to the nature of the application necessity, the fifth generation (5G) network solves most of the issues related to the network due to its excellent characteristics in term of high quality of service. However, because of the centralization, IoT devices with 5G support suffer several security-related problems. This paper examines the security, performance, and network issues in 5G-IoT devices and the integration of Blockchain. Technology in these devices or gadgets with the recent blockchain applications in 5G with the Internet of Things is being explored in various fields like smart home, smart city, healthcare, industry, supply chain, smart grid, and smart transportation.

1 Introduction

IoT, 5G technology, and blockchain are three separate but related technologies that together possess the power to influence the direction of the future [1]. The Internet of Things, or IoT, is a network of intelligent devices and gadgets that can interact with other machines online, collect data from their environment through sensors, and operate independently without requiring human intervention [2]. Wireless Sensor Networks and Radio Frequency Identification (RFID) are examples of Internet of Things technologies. (WSN) [3]. The number of IoT devices has significantly increased as a result of the technology's quick acceptance in many different applications; by 2023, it is predicted that the number of connected objects will surpass 43 billion [4]. Health care, smart homes, smart automobiles, smart TVs, smart furniture, smart cities, smart farms, and vacuum cleaners are among the industries where the Internet of Things is most widely used. At this point, the Internet of Things (IoT) offers a way to link practically any type of physical object to the Internet. The Internet of Things (IoT) is rapidly expanding the worldwide network area by facilitating the connecting of objects ranging from massive industrial machinery to small consumer products, Therefore, IoT has the power to fundamentally alter how automation is understood at the level of individual (physical) objects

* Corresponding author: honarmohammedtaha@gmail.com

[5]. The fifth generation of technology, or **5G**, is distinguished by three primary qualities, its capacity to handle Enhanced mobile broadband, ultra-reliable low latency communication, and massive machine-type communication [6] To fulfill the constant increasing needs of user traffic and developing services, the primary goal of future 5G services is to offer a personalized and sophisticated value focused on the user, enabling the connectivity of almost every element of human existence to communication networks [7]. To achieve these objectives, a 5G network order SDN, network function virtualization (NFV), edge computing, cloud computing, cloud computing, network slicing, and D2D communication have all been proposed [8]. Still, there are additional security concerns, such as network dependability, data immutability, and privacy, brought about by the explosive growth of 5G wireless services in terms of size, speed, and capacity[9]. By combining **blockchain** technology with 5G and IoT, security concerns with IoT devices can be resolved [10]. Blockchain is an open technology that builds trust amongst untrustworthy parties [11]. Without intervention from a third party, safe information transfer is ensured by this decentralized technology [12]. Blockchain is a distributed, decentralized ledger that keeps track of a constantly expanding collection of data entries known as blocks. A set of transactions made by blockchain participants may be found in every block. A transaction on the blockchain is a bit of data that should be kept in a secure database. Numerous features of blockchain technology include its decentralized, immutability, and lack of a single point of failure.

This research primarily analyzes and discusses the integration of blockchain technology in 5G-enabled IoT devices. Section 2, talked in brief about the fifth-generation (5G) mobile networks. Section 3 listed the importance of 5G with IoT, Section 4 blockchain technology and decentralization are briefed, Section 5 blockchain categories are analyzed, Section 6, is about blockchain with 5G-enable IoT, Section 7 discuss the Blockchain Applications in 5G enabled IoT, In Section 8 all the challenges listed and reviewed, In Section 9 future direction of the research is mentioned, in the last section 10, the conclusion is made up for the study.

2 5G

The 5G and beyond generation of mobile networks have significantly improved network and service performance while enabling previously unthinkable levels of innovation that have transformed business and society [13]. 5G is distinguished by its extremely reduced round-trip latency (of the order of 1 ms), substantial data throughput (nearly 10 Gbps in speed), tremendous scalability (similar to the type of 100x connected devices), and other features, see below Fig. 1.

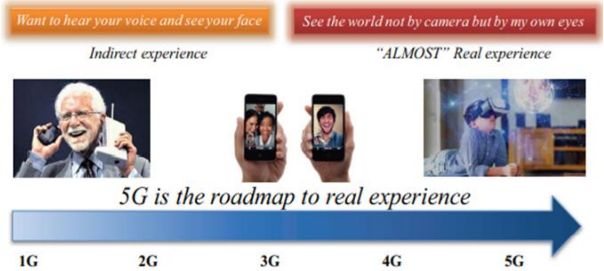

Fig. 1. Concepts and requirements for 5G mobile services.

3 5G and IoT

Device-to-device (D2D) connections, Network Slicing (NS), Software-Defined Networking (SDN), Network Function Virtualization (NFV), and MEC (Multiaccess Edge Computing) are the primary enabling technologies for 5G technology etc.

3.1 Software-Defined Networking (SDN):

Software-defined networks allow the network to be operated by software instead of hardware. It also considers dividing the control and data planes, which would allow 5G networks to be more agile and flexible [14].

3.2 Network Function Virtualization (NFV):

Network function virtualization (NFV) allows many network functions to be operated entirely by software on software-defined networks. Network function decoupling from proprietary hardware appliances is made possible by NFV, allowing the network to operate on standardized hardware.

3.3 Network slicing

Network slicing is a device scheme that allows users to configure the network type they need for their applications using SDN and NFV. This enables audio communications for one user with separate software and minimal latency for another. As a result, users can access a portion of the network with the performance they choose

3.4 Device to Device D2D

Base stations are used by modern cellular networks for communication, causing low spectral efficiency due to delay. 5G networks propose D2D communications, allowing close devices to communicate directly, creating multi-hop relays, increasing data rate, and improving QoS. This enhances flexibility, and energy efficiency, and eliminates unwanted traffic from the core network.

3.5 Multi-Access Edge Computing (MEC)

MEC improves network response by reducing congestion and enabling cloud computing near devices, reducing energy consumption and storage space. It also enhances QoS and network collaboration, improving user experience and overall network performance.

3.6 Cloud/Edge computing

Cloud computing is a solution for managing resources, storing data, and enabling mobile sensing in the 5G era, utilizing resourceful virtual computation centers for various application domains.

4 Blockchain

These days, most Internet of Things systems rely on centralized servers and databases for storage. The main problems with centralized systems are single points of failure and a lack of trust amongst the many parties. The decentralized design might be helpful for peer-to-peer communication across network nodes to get around such problems [15]. Decentralization is a blockchain's central concept. This indicates that no database on blockchain is kept in a single location. Rather, a network of participants copies and disseminates the blockchain. A distributed ledger known as blockchain is immutable and frequently used to record financial transactions. Blocks that are timestamped and joined by cryptographic hashes comprise its composition [16]. As seen in Fig. 2.

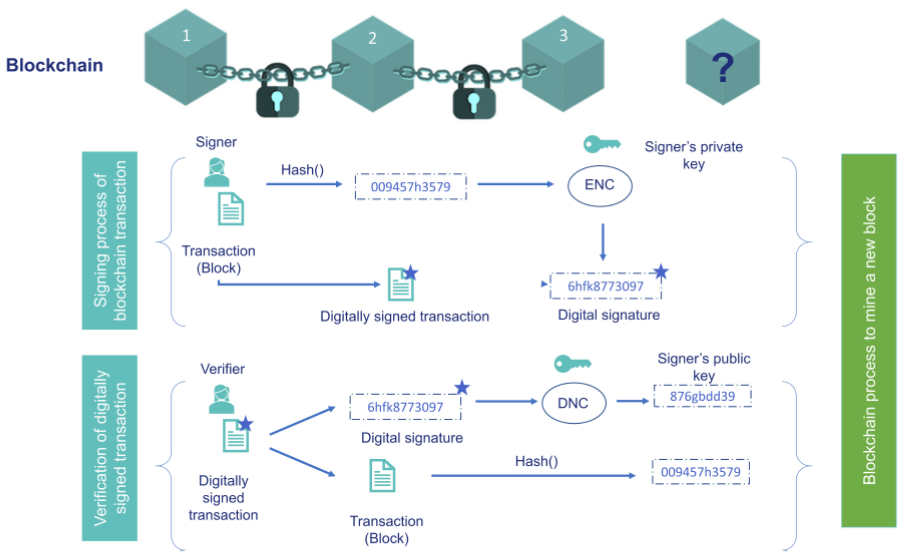

Fig. 2. Blockchain workflow.

The following are the four main parts of blockchain technology:

4.1 Ledger Distributed:

A distributed database is what blockchain is, which ensures the immutability and security of information by using replicated copies from the ledger. New blocks are added only after verification by the network's major portion.

4.2 Smart Contract:

The Smart Contract system is utilized to validate and verify the network's participants. Blockchain smart contracts are non-modifiable, non-changeable programs that automatically execute actions according to a contract's terms. They are implemented permanently on the Ethereum blockchain, coded using Solidity, and can be used for system management or network access control. These contracts can run dynamically within the network.

4.3 Consensus:

Consensus algorithms in blockchains enable nodes to agree on decisions, which are crucial for adding new blocks under specific rules and agreements. Blockchain consensus comes in a variety of forms. The four most popular consensus algorithms are Practical Byzantine Fault Tolerance (PBFT), Proof of Work (PoW), Proof of Stake (PoS), and Proof of Activity (PoA).

4.4 Cryptography:

is a secure method that encrypts all network data, ensuring only authorized users can decrypt it.

5 Blockchain Categories

This section provides the strengths and weaknesses of current authentication methods That nowadays used on various systems and environments, as in Table 1.

5.1 Public Blockchain

A permission-less blockchain, sometimes referred to as a public blockchain, is one in which everyone may join the consensus process and view all transactions [17]. Bitcoin is the most well-known example of this type of blockchain.

5.2 Private Blockchain

Private blockchains, like Ripple, are permission and suitable for single organizations or enterprise solutions. They do not require processing fees or tokens, and organizations can roll back to previous points, making them not completely decentralized.

5.3 Consortium

or federated blockchains are closed systems governed by a group of businesses, based on common interests. They operate as semi-decentralized systems, relying on a few verified nodes for agreement.

Table 1. Blockchain categories properties.

Properties	Public Blockchain	Private Blockchain	Consortium Blockchain
Access	Public	Restricted	Restricted
Permissioned	No	Yes	Yes
System Throughput	Slow	Fast	Fast
Consensus participants	All nodes	An Organization	Multiple Organization

Transparency in open data is crucial, but privacy concerns inferring private and sensitive information. Blockchain technology, based on smart contracts, offers privacy-preserving data provenance for open data protection. This technology is a promising candidate for

5G networks and services due to its technical benefits. The potential applications of blockchain in 5G are summarized in Table 2.

Table 2. Main characteristics of blockchain and their potential to 5G.

Key Characteristics of Blockchain	Description	Potential application to 5G networks and services
Decentralization	No central authority or trusted third party is needed to perform transactions. Users have full control on their own data.	Eliminate the need of trusted external authorities in 5G ecosystems, i.e. spectrum licenses, band managers, and database managers in spectrum management; central cloud/edge service manager in mobile computing and D2D networks; UAV control center in 5G UAV networks, and complex cryptographic primitives in 5G IoT systems. Decentralizing 5G networks potentially eliminates single-point failures, ensures data availability and enhance service delivery efficiency.
Immutability	It is very difficult to modify or change the data recorded in the blockchain.	Enable high immutability for 5G services, Spectrum sharing, data sharing, visualized network resource provisions, resource trading can be recorded immutability into the only-appended blockchain. Besides, D2D communications, ubiquitous IoT networking and large-scale human-centric interconnections can be achieved via peer-to-peer networks of ubiquitous blockchain nodes without being modified or changed. The high immutability is very useful for 5G networks to performing accounting tasks, i.e. logging of session statistics and usage information for billing, resource utilization, and trend analysis.
Transparency	All information of transactions on blockchain (i.e. public ledgers) can be viewed to all network participants.	Provide better localized visibility into 5G service usage. The same copy of records of Blockchain spreads across a large network for public verifiability. This enables service providers and users to fully access, verify and track transaction activities over the network with equal rights. Also, blockchains potentially offer transparent ledger solutions for truly open 5G architecture (i.e. decentralized network visualization, distributed edge computing, distributed IoT networks). Blockchain ledgers also support fair service trading applications (i.e. resource trading, payment) under the control of all network entities.
Security and privacy	Blockchain employs asymmetric cryptography for security with high authentication, integrity, and nonrepudiation, smart contracts available on	Provide high security for 5G networks involved in decentralized ledgers. Blockchain helps secure the 5G networks by providing distributed trust models with high access authentication, in turn enabling 5G systems to protect themselves and

 https://doi.org/10.1051/itmconf/20246401001

	blockchain can support data auditability, access control and data provenance for privacy.	ensure data privacy. By storing data information (i.e. IoT metadata) across a network of computers, smart contracts, as trustless third parties, potentially support 5G services, such as data authentication, user verification, and preservation of 5G resource against attacks.

6 Blockchain-enabled for 5G beyond in IoT

IoT is transforming services by improving citizens' quality of life. Rapid growth has led to more access points, but centralized data storage systems like cloud computing can be opaque. Blockchain technology can improve privacy and security, particularly in industrial automation using 5G-enabled IoT [18]. Blockchain offers a secure, transparent, and auditable platform for IoT, ensuring reliable and traceable information exchange, offering numerous benefits, see **Fig. 3**.:

6.1 Security

Blockchain technology enhances security by using cryptographic hash functions to secure the exchange of information between nodes, making it difficult to hack authorization details in a decentralized network.

6.2 Autonomy

Blockchain technology in IoT enables autonomous devices, eliminating central authority, and permitting the processing of financial transactions in the absence of a central authority.

6.3 Trust

Decentralized blockchain technology, utilizing smart contracts and consensus algorithms, enhances trust and security in IoT devices by removing vulnerabilities and making transactions more affordable.

6.4 Tamper-free

Distributed ledgers use asymmetric encryption to store and date data in an immutable manner, protecting the decentralized Internet of Things from fraud and other tampering.

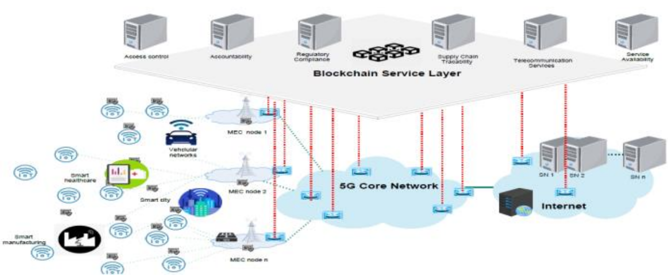

Fig. 3. Blockchain services for 5G-enabled IoT devices.

The integration of blockchain into IoT infrastructure requires deciding on the location of these interactions, either within the IoT, a hybrid design involving IoT and blockchain, or through blockchain. Fog computing has revolutionized IoT by introducing a new layer between cloud computing and IoT devices, which could facilitate this integration. Alternatives as shown in Fig. 4., including fog computing, are described with their advantages and disadvantages.

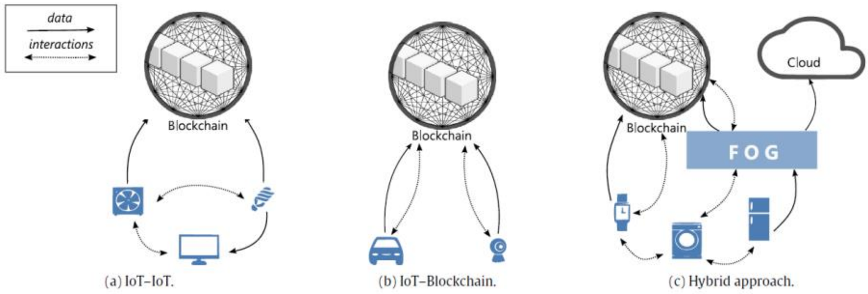

Fig. 4. Blockchain interaction.

Companies like the Trusted IoT Alliance are collaborating to bridge the gap between IoT and blockchain. Increasingly, devices with integrated blockchain capabilities are available, such as EthEmbedded, Raspnode, and Ethraspbian, which enable Ethereum full nodes on embedded devices like Raspberry Pi. Antrouter R1-LTC is a Wi-Fi router that supports mining Litecoin, making it suitable for smart homes. However, mining on IoT devices is currently a specialized task for certain hardware, making it unsuitable for IoT devices. There is still much research to enable a wide integration of IoT devices as blockchain components. The integration of IoT and cloud computing has been used to overcome IoT limitations in processing, storage, and access. Cloud computing's centralized architecture complicates reliable sharing with many participants. Fog computing, a distributed approach, aims to distribute computing closer to end devices, incorporating powerful devices like gateways and edge nodes. This could ease the integration of IoT with blockchain, ensuring reliable data and addressing previous limitations [18].

Table 3 compares blockchain platforms for creating IoT applications. Smart contracts enable application logic beyond cryptocurrency transactions. Blockchain deployments have a dualism, with established platforms like Ethereum providing infrastructure. Distribution is crucial for blockchain trustworthiness, while noncryptocurrency platforms like Hyperledger Fabric require consortium and infrastructure. Most platforms offer permissions and privacy, allowing for global applications. As shown in Table 3.

Table 3. Blockchain platforms for creating blockchain applications.

Platform	**Blockchain**	**Consensus**	**Crypto Currency**	**Smart contracts**
Ethereum	Public and permission-based	PoS	Ether(ETH)	Yes
Hyperledger Fabric	Permission-based	PBTF/SIEVE	None	Yes
Multichain	Permission-based	PBTF	Multi-currency	Yes
Litecoin	Public	Scrypt	Liteconin (LTC)	No

Lisk	Public and permission-based	DPoS	LSK	Yes
Quorum	Permission-based	Multiple	ETH	Yes
HDAC	Permission-based	ePoW, Trust-based	Multiasset	Yes

The study tested the feasibility of running blockchain platforms on IoT devices using a Raspberry Pi 3 model B with Raspbian Stretch OS and Linux kernel 4.9.59-v7+. The device was equipped with an SD card and connected to the internet via Ethernet. Energy consumption and task performance were measured, and a background process was run to evaluate CPU usage, memory requirements, and bandwidth consumption. The maximum CPU measurement was 400% for the quad core device [18]. As illustrated in Table 4.

Table 4. Blockchain nodes evaluation on Raspberry Pi v3 (Synchronizing (s), after synchronization (as))

	Avg energy(mA)	Avg %CPU	Avg %Mem	Avg VIRT(MB)	Total Sent MB	Total Received MB
Bitcoin light node	283.45	2.19	9.6	288	0.074	0.068
Litecoin light node	275.53	2.05	7.6	209	0.081	0.104
Ethereum full node(s)	599.72	256.82	85.96	1490	78.9	490
Ethereum full node (as)	371.26	47.39	29.36	1280	15.3	80.3
Bitcoin full node (s)	429.05	55.47	27.55	405	48	912
Litecoin full node (s)	437.62	117.80	19.36	341	17.1	546
Litecoin full (as)	280.04	7.01	51.7	679	1.22	2.06

7 Blockchain Applications in 5G enabled IoT

7.1 Smart Home

Smart homes have various features such as smart door locks, lighting, video surveillance, thermostats, and parking [19]. These systems require infrastructure like network connectivity, IoT-enabled sensor devices, and mobile applications for remote connection. Smart locks are crucial for protecting homes from unauthorized access. Central servers can cause security issues [20] proposed a blockchain-enabled smart lock system for integrity and non-repudiation. Low latency and quick intrusion detection are two further benefits of 5G-enabled IoT.
The SmartHome can help save money on household expenses by combining multiple Smart Homes with local objects connected and Cloud Computing for monitoring and managing

each case. High availability and security are not as important as Smart Healthcare, but access control and accounting may be required. OpenStack offers an extra level of service, including batch processing and querying large amounts of data. Apache HBase, Druid, OpenTS DB, Apache Hadoop, ApacheSpark, ApachePigand, Apache Hive, and Apache SparkSQL can be used for data storage [3].

7.2 Smart City

Smart cities utilize centralized services and interconnected networks, offering advantages but also potential security and privacy threats. Integrating blockchain technology with IoT is the most effective remedy for securing smart city applications [21]. proposes a security framework for blockchain-enabled IoT, addressing reliability, scalability, security, centralization, and efficiency.

The growing global population, resource scarcity, and environmental concerns have led cities to enhance their services and infrastructure to address these challenges. SmartCities aim to improve everyday life in areas such as transportation, public safety, urban consumption, tourism, and urban planning. These cities have diverse aims, utilizing IoT to optimize processes and improve aggregation. The proposed SmartCity scenario involves a strong orchestration of services to optimize city life. Key requirements include high availability, auto-scaling, and load balancing, as well as the OpenCloud Computing Interface (OCCI) for easier integrations and migrations between cloud infrastructures. New paradigms and machine learning algorithms are needed to enable efficient and emantic data processing [3].

7.3 Health-care

In the internet world, healthcare applications have advanced, allowing doctors to remotely monitor patients' health conditions using IoT-enabled smart devices. However, centralized IoT devices face disadvantages like unauthorized access and vulnerability, which can be dangerous for patients. The authors suggest blockchain-enabled IoT in healthcare applications as a solution to these security risks. The trend of reducing hospital resources and relocating healthcare services to homes is causing a need for more work on models and algorithms for decision-making in healthcare. Connected Health aims to reduce financial burden, provide a comfortable environment for patients, and quickly release hospital resources in emergencies. Real-time monitoring of vital signs is necessary for early detection and prediction of abnormal situations. The system also proposes personalized treatments based on patient history and genetic information [3].

7.4 Industry

Manufacturing companies face challenges like data fragmentation, interoperability, firmware upgrades, and security concerns in centralized systems. Blockchain enabled IoT and decentralization can transform the industry into a smarter, more secure, and privacy-protected one.

7.5 Supply chain

refers to the web of people, companies, assets, and activities that are engaged in the life cycle of a product, from its conception to its sale. Suppliers come first, followed by manufacturers, distributors, retailers, and, at the end, consumers. The practice of managing resources, data, and finances along the supply chain is known as supply chain management, or SCM. Blockchain offers an immutable distributed ledger for secure data storage, while 5G-enabled IoT expands bandwidth capability for safe data transport [22].

7.6 Smart grid

The increasing energy consumption of contemporary society demands substantial focus in the era of smart grids. The energy industry has transitioned from a centralized system to a decentralized mode, 5G technologies, including network slice, D2D communication, SDN, edge/cloud computing, and the Internet of Things [23].

7.7 Smart Transportations

IoV is a network connecting vehicles and the internet, with three main types, Vehicles to Infrastructure, Vehicles to Cloud, and Vehicles to Vehicles. The vehicle-to-cloud application centralized data storage, while the vehicle-to-vehicle application shared data among vehicles. Security challenges include data sharing and cloud storage. Blockchain-enabled 5G IoT can solve these issues through Proof of Work or smart contracts, enhancing security, integrity, authenticity, and decentralization. Integrating these technologies enhances security, integrity, authenticity, and decentralization.

8 Open challenges and security issues in blockchain-enabled 5G IoT

Researchers from academia and industry are showing a great deal of interest in integrating blockchain technology with 5G networks. Blockchain technology has the potential to revolutionize 5G infrastructure and industrial network topologies by providing decentralization, privacy, and security characteristics. However, a survey on blockchain's application in 5G networks highlights important unresolved problems and research gaps that should be taken into account when designing systems. Therefore, these difficulties need to be further researched before considering to implement this notion in current systems:

8.1 Storage and scalability

Blockchain were intended to displace the current client/server architecture. However, this data is kept in the nodes, which are typically Internet of Things gadgets, and its scalability rapidly is growing. The limited processing power and low storage capacity of these devices would be a significant obstacle to this technology's widespread implementation.

8.2 Lack of standardization

The absence of standardization and interoperability in ledgers prevents direct communication between them. To achieve full interoperability, stakeholders must compromise on data and policies, and international strategies for information security and collective trust are crucial.

8.3 Security

Blockchain, a secure database platform for 5G networks, faces security weaknesses, particularly in 51% of attacks. This vulnerability allows miners to control over Half of the network's hash rate for mining, preventing new transactions and halting payments between service providers and IoT users.

8.4 Throughput

The throughput of blockchain applications is far lower than that of non-blockchain ones; for example, Visa and PayPal process 1667–193 transactions per second, while Bitcoin and Ethereum process approximately 4–20 transactions per second. Block size limitations in blockchains cause long waiting times for transactions, limiting system throughput. Proper solutions are needed to sustain large transactions for 5G applications.

8.5 Consensus

IoT devices face challenges in mining due to limited resources, making popular consensus algorithms unsuitable. Despite proposals, more testing is needed for resource-constrained IoT models.

9 Future direction of research

9.1 Using blockchain technology with Machine Learning for 5G
9.2 Blockchain technology for big data and 5G
9.3 6G network and Blockchain integration

10 Conclusion

This paper discusses the integration of blockchain with IoT devices in 5G-enabled devices, highlighting its potential in industrial applications. The paper covers the background of blockchain, IoT, and 5G, their respective industrial applications, and open issues and challenges. The paper acknowledges that due to high-end hardware requirements and compatibility issues, the use of these technologies on a common platform is still not feasible. However, the paper focuses on maintaining security and faster data flow in industrial applications. It also suggests that further technological research is needed to address specific demands for collaboration between these technologies. The paper concludes by comparing existing blockchain-based industrial applications based on specific parameters. Blockchain technology, initially designed for cryptocurrency, has been proposed as a solution to 5G network challenges such as security, transparency, decentralization, and immutability. Researchers have shown the benefits of using blockchain solutions in 5G networks, such as secure design concepts, limited access control, and trust. Blockchain smart contracts, lightweight consensus and sharding concepts will enable new 5G business models to benefit from high data rates, secure communication, and reliable services. This chapter reviews blockchain integration opportunities for 5G network services and operations, proposing a scalable, secure, and lightweight blockchain architecture suitable for 5G requirements. It also summarizes open challenges and provides research directions for safe blockchain deployment in 5G networks.

References

1. S. Hameed, S. A. Shah, Q. S. Saeed, S. Siddiqui, I. Ali, A. Vedeshin, and D. Draheim, “A scalable key and trust management solution for IoT sensors using SDN and blockchain technology,” IEEE Sensors Journal, vol. **21**, no. 6, pp. 8716–8733, (2021)
2. S. K. Dwivedi, R. Amin, S. Vollala, and P. Chaudhry, “Blockchain-based secured event-information sharing protocol in internet of vehicles for smart cities,” Computers & Electrical Engineering, vol. **86**, article no. 106719, (2020)
3. M. Díaz, C. Martín, B. Rubio, State-of-the-art, challenges, and open issues in the integration of internet of things and cloud computing, J. Netw. Comput. Appl. 67 (2016) 99–117
4. M. J. Islam, A. Rahman, S. Kabir, A. Khatun, A. I. Pritom, and M. Zaman, "Sdot-nfv: Enhancing a distributed sdn-iot architecture security with nfv implementation for smart city," GUB Journal of Science and Engineering, vol. **7**, (2020)
5. M. T. Hammi, B. Hammi, P. Bellot and A. Serhrouchni, "Bubbles of trust: A decentralized blockchain-based authentication system for iot", *Computers Security*, vol. **78**, pp. 126-142, (2018)
6. Agiwal, M., Roy, A., Saxena, N., 2016. Next generation 5G wireless networks: a comprehensive survey. IEEE Commun. Surv. Tutorials 18 (3), 1617–1655.
7. N. Panwar, S. Sharma, A.K. Singh, A survey on 5G: The next generation of mobile communication. Phys. Commun. **18**, 64–84 (2016)
8. Deborsi Basu, Vikash Kumar Gupta, Raja Datta, and Uttam Ghosh. 2021. Dynamic Cluster Based Control Plane Load Balancing in Large Scale vSDN-enabled 5G WAN. In 2021 IEEE 3rd PhD Colloquium on Ethically Driven Innovation and Technology for Society (PhD EDITS). 1–2. https://doi.org/10.1109/PhDEDITS53295.2021.9649455
9. Chin, W.H.; Fan, Z.; Haines, R. Emerging technologies and research challenges for 5G wireless networks. *IEEE Wirel. Commun.* **2014**, *21*, 106–112.
10. Jāmiʻat Qaṭar, Institute of Electrical and Electronics Engineers. Qatar Section. and Institute of Electrical and Electronics Engineers, (2017)
11. Z. Abou El Houda, A. S. Hafid, and L. Khoukhi. 2019. Cochain-SC: An Intra-and Inter-Domain Ddos Mitigation Scheme Based on Blockchain Using SDN and Smart Contract. IEEE Access 7 (2019), 98893--98907.
12. H. Moudoud, Z. Mlika, L. Khoukhi and S. Cherkaoui, "Detection and Prediction of FDI Attacks in IoT Systems via Hidden Markov Model," in *IEEE Transactions on Network Science and Engineering*, vol. **9**, no. 5, pp. 2978-2990, 1 Sept.-Oct. 2022, doi: 10.1109/TNSE.2022.3161479.
13. Nguyen, T.-M., Nham, T.P., Froese, F.J. and Malik, A. (2019), "Motivation and knowledge sharing: a meta-analysis of main and moderating effects", *Journal of Knowledge Management*, Vol. **23** No. 5, pp. 998-1016.
14. A. Gupta and R. K. Jha, "A Survey of 5G Network: Architecture and Emerging Technologies," in *IEEE Access*, vol. **3**, pp. 1206-1232, 2015, doi: 10.1109/ACCESS.2015.2461602.
15. Shiv Bharadwaj, Amit Dubey, Umesh Yadava, Sarad Kumar Mishra, Sang Gu Kang, Vivek Dhar Dwivedi, Exploration of natural compounds with anti-SARS-CoV-2 activity *via* inhibition of SARS-CoV-2 M^{pro}, *Briefings in Bioinformatics*, Volume **22**, Issue 2, March 2021, Pages 1361–1377,
16. Cohen JA, Mistry D, Kerr CC, Klein DJ. Schools are not islands: Balancing COVID-19 risk and educational benefits using structural and temporal countermeasures. medRxiv. 2020 Sep 10;2020.09.08.20190942.
17. Kaur, Baljinder, Santosh Kumar, and Brajesh Kumar Kaushik. "Recent advancements in optical biosensors for cancer detection." *Biosensors and Bioelectronics* 197 (2022): 113805.

18. Reyna, Ana, et al. "On blockchain and its integration with IoT. Challenges and opportunities." *Future generation computer systems* 88 (2018): 173-190.
19. Biswas, Kamanashis, Vallipuram Muthukkumarasamy, and Wee Lum Tan. "Blockchain based wine supply chain traceability system." *Future Technologies Conference (FTC) 2017*. The Science and Information Organization, 2017.
20. Jung, Geung-Sik. "Aspects of Nineteenth-Century Choson Society as Observed through a Legal Proceeding." *J. Korean L.* 5 (2005): 97.
21. El Makrini, Ilias, et al. "Working with walt: How a cobot was developed and inserted on an auto assembly line." *IEEE Robotics & Automation Magazine* 25.2 (2018): 51-58.
22. Villamor, P., et al. "Contribution of active faults in the intraplate area of Iberia to seismic hazard: The Alentejo-Plasencia Fault." (2012).
23. De Dutta, Sarmistha, and Ramjee Prasad. "Security for smart grid in 5G and beyond networks." *Wireless personal communications* 106 (2019): 261-273.