Chapter 1
Blockchain and 5G-Enabled Internet of Things: Background and Preliminaries

Shweta Kaushik

1 Introduction

1.1 Blockchain

Blockchain is generally known as the fundamental innovation of the cryptographic money Bitcoin [1]. The centre feature of a blockchain is decentralization. This implies it does not store any of its databases in a pivotal area. Rather, the data is replicated and distributed over a system of members. At whatever point any block is added to the blockchain, each computer on the system refreshes its blockchain to mirror the change. This distributed engineering guarantees a robust and secure procedure on the blockchain with the upsides of alter obstruction and no single-point weaknesses. Specifically, blockchain can be available for everybody and is not constrained by any system element. This is enabled by an instrument called accord, which is a set of rules to guarantee the understanding between all members on the position of the blockchain top. The overall idea on how blockchain works is shown in Fig. 1.1. Blockchain, a circulated record innovation empowers clients to connect and execute (store and recover information) with guaranteed information legitimacy, changelessness and non-disavowal. The appropriated idea of blockchain permits the mechanical elements and different 5G/IoT gadgets to trade information, to and from their friends, removing the necessity for concentrated operation.

The blockchain-assisted 5G biological system is suitable for building up responsibility, information provenance, and non-denial for each client. The principal hinder in a blockchain is alluded to as the beginning block, which does not contain any exchange. Each block from that point contains various approved exchanges

S. Kaushik (✉)
ABES Engineering College, Ghaziabad, Uttar Pradesh, India
e-mail: shweta.kaushik@abes.ac.in

S. Tanwar (ed.), *Blockchain for 5G-Enabled IoT*,
https://doi.org/10.1007/978-3-030-67490-8_1

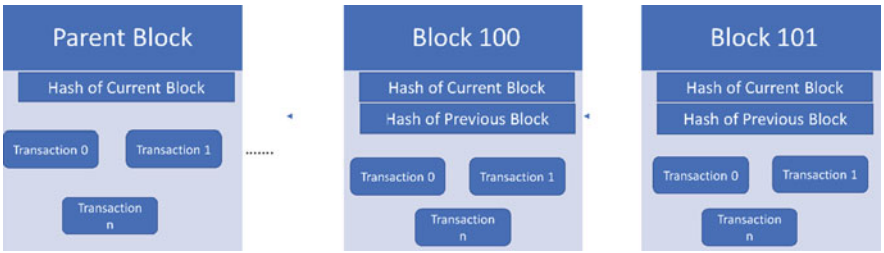


Fig. 1.1 How blockchain works

and is cryptographically connected with past blocks. When all is said and done, blockchains can be named either an open (permission-less) or a private (permissioned) blockchain [2]. An open blockchain is available for everybody and anybody can join and cause exchanges but only some can decide the agreement procedure. The most popular open blockchain applications are used in Bitcoin and Ethereum. Private blockchains have an access control system overseen by a focal element. A member must be permissioned to utilize an approval component. To understand the capability of blockchain in 5G systems, it is important to comprehend the activity idea, principle components of blockchain, and how blockchain can bring opportunities to 5G-enabled applications. Moreover, blockchain is unique in relation to other disseminated frameworks dependent on agreement and the following properties [3], as shown in Fig. 1.2:

- Trust-less: The elements associated with the system are obscure to one another. However, they can convey, coordinate and work together without realizing one another, which implies there is no prerequisite of guaranteed advanced character to carry out any exchange between the substances.
- Permission-less: There is no limitation of who can or cannot work inside the system, that is, there is no sort of consent.
- Restriction safe: Being a system without supervisors, anybody can communicate or execute on the blockchain. Additionally, any affirmed exchange cannot be altered or blue-pencilled. Notwithstanding the previously mentioned legitimacies, blockchain innovation has four fundamental segments [4], which are referred to as:
- Consensus: The PoW convention is mindful to check each activity in the system which is fundamental to avoid a solitary excavator hub from commanding the whole blockchain system and to control the exchanges history.
- Register or Ledger: It is a common and conveyed database that encompasses data exchanges performed inside the system. It is commonly changeless, where data once put away cannot be erased using any means. It ensures that each exchange is checked and afterwards acknowledged as a legitimate one, by the greater part of the customers required at a specific moment [5].

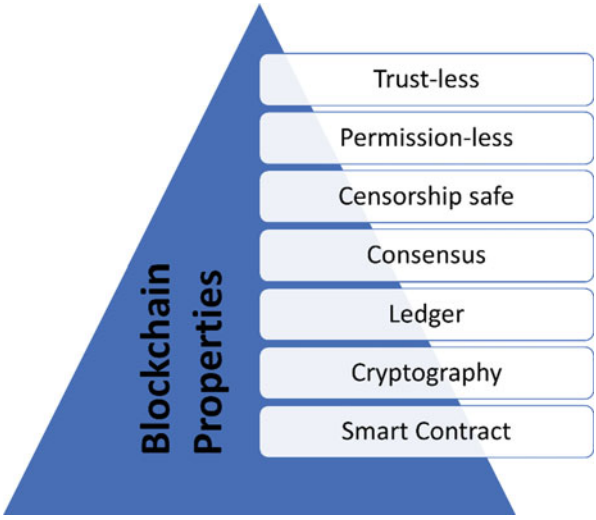


Fig. 1.2 Blockchain properties

- Cryptographic operations: It guarantees that all the information in the system is verified with a solid encryption process. Only approved clients are permitted to unscramble the data.
- Smart Contract: It is utilized to approve and confirm the members of the system.

1.2 5G Technology

In the course of recent decades, the world has seen a consistent improvement of correspondence systems, beginning with the original and moving towards the fourth era. The worldwide correspondence traffic has demonstrated an extraordinary increment as of late and is continuing to proceed, which has triggered the emergence of the prospective age of media transmission systems, to be specific 5G that aims to address the constraints of past cell guidelines and scope with ever-expanding system limits. The 5G system can surpass previous adaptations of remote correspondence innovation and offer assorted assistance capacities as well as support full systems administration among nations all-inclusive. Likewise, 5G presents answers related to the effective and financially smart dispatch of a huge number of new administrations, customized for various vertical markets with a wide scope of administration prerequisites. Specifically, the advances in 5G correspondence are imagined as inaugural of new submissions in different areas through extraordinary effects on almost all parts of our lives, for example, IoT, smart medical services [11], vehicular systems [12], smart frameworks [13] and smart cities [14]. Blockchain innovation promises the possibility for various specialized advantages regarding 5G

systems and administrations. We sum up the potential applications that blockchain can provide to 5G in Table 1.1.

The 5G organization engineering must help to organize the security systems and capacities (for example, virtual security firewalls) at whatever point required in any system border. The most conspicuous innovation for streamlining management arrangement is Software-Defined Networking (SDN). SDN isolates the framework control from the data-sending plane. The control plane is configured to administer the entire system and control organization of assets through programmable Application Programming Interfaces (APIs). System Functions Virtualization (NFV) executes Network Functions (NF) for all intents and purposes by decoupling equipment machines (for example, firewalls, entryways) from the capacities that are running on them to give virtualized entryways, virtualized firewalls and, indeed, even virtualized segments of the system, prompting the arrangements of adaptable system capacities. In the meantime, cloud processing/cloud RAN underpins boundless information stockpiling and information preparing to adapt to the developing IoT information traffic in 5G. The variety of 5G empowering innovations guarantee to encourage portable systems with recently accelerating administrations such as smart information investigation and huge information handling. Contrary to past system ages (for example, 3G/4G), 5G promises to offer portable types of assistance with incredibly low inertness of vitality investment funds because of adaptability (for example, arrange cutting edge processing), which will improve quality of service (QoS) for the system and guarantee from top to bottom quality of experience (QoE) aimed at clients.

1.3 IoT

The Internet of Things (IoT) signifies the system of different unmistakable electronic or electrical gadgets that are competent to communicate with one another utilizing an open channel, for example, the Internet. This association is made utilizing remote innovations, for example, sensor systems, radio recurrence ID (RFID), close to handle correspondence (NFC), M2M and ZigBee [8]. The IoT has changed the domain of omnipresent registering with various mechanical applications working with different kinds of sensors. However, constraints exist regarding the use of the IoT, which should be addressed to advance it into a progressively effective framework [6], as shown in Fig. 1.3:

- Security: As the quantity of associated gadgets of the system expands, the odds to exploit weaknesses by outside assaults also increases. This occurs because of the usage of low standard gadgets.
- Privacy: The information gathered from IoT gadgets is sent to a focal distributed storage for investigation and handling, which involves an outsider. This sort of dissemination of information without the assent of the client can additionally cause information spills; thus, trading off the protection of the end clients.

Table 1.1 Blockchain characteristics and their possibilities for 5G

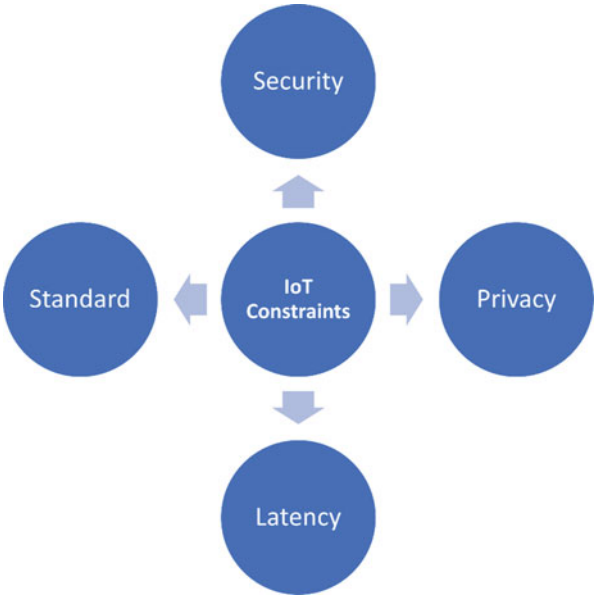
Blockchain characteristics	Description	Application for 5G
Data security and privacy	Blockchain hires uneven steganography for protection with excessive verification, truthfulness and nonrepudiation. Smart contracts to be had at the blockchain can aid records auditability, obtain entry to manage and records provenance for privacy.	Deliver excessive protection for 5G applications concerned with decentralized registers. It enables stability in the 5G networks with the aid of using supplying disbursed trust methods with excessive permissioned entry to authentication, in flip allowing 5G structures to shield themselves and ensure privacy. By loading facts statistics throughout a community of computers, the project of cooperating facts will become substantially more difficult for hackers. In addition, smart contracts, as trust-less third parties, probably assist 5G services, which include facts authentication, person verification and upkeep of 5G useful resources in opposition to attacks.
Immutability	It is very hard to regulate or alternate the records recorded within the blockchain.	Empower unbalanced unchanging nature for 5G administrations. Range sharing, records sharing, virtualized network helpful valuable asset arrangements, useful helpful asset looking for and advancing can be recorded permanently into the best-affixed blockchain. Also, D2D correspondences, pervasive IoT organizing, and wide-ranging human-driven interconnections should be possible through shared organizations of universal blockchain hubs without being adjusted or altered. The radical permanence can be exceptionally helpful for 5G organizations to call up and display bookkeeping entries, for example, logging of meeting information and utilization information for charging, helpful valuable asset use and style investigation.
Transparency	All data during transitions on blockchain (i.e. public ledgers) may be viewable to all public contributors.	Deliver better-localized perceptibility into 5G carrier utilization. The identical replica of information in blockchain banquets throughout a massive community for public verifiability. This permits carrier companies and customers to completely obtain right of entry to, verify and music transaction spots over the community with identical rights. Also, blockchains probably provide obvious ledger answers for open 5G architectures. Blockchain registers additionally assist truthful carrier buying and selling applications (i.e. useful resource buying and selling, payment) beyond the manipulation of all community entities.

(continued)

Table 1.1 (continued)

Blockchain characteristics	Description	Application for 5G
Decentralization	No principal authority and not dependent on a third party to carry out transactions. Users have complete access to their personal records.	Removes the need to rely upon the government in 5G environments, for example, range licenses, band chiefs and information base administrators are the executives; chief cloud/territory transporter manager in cell figuring and D2D networks; UAV control centre in 5G UAV networks; and convoluted cryptographic natives in 5G IoT structures. Decentralizing 5G networks most likely discards single-factor disappointments, ensures realities accessibility and amplifies transporter transport proficiency.

Fig. 1.3 IoT constraints



- Standards: Lack of guidelines and standards can cause unfortunate outcomes while managing the designed gadgets.
- Latency: The current correspondence principles utilized for cooperation between numerous IoT gadgets encounter dormancy issues. The continuous increase in the quantity of IoT-empowered gadgets causes a requirement for an innovation that can withstand this tremendous number of information transmissions effectively at an incredibly high data transfer capacity.

Additionally, the gadgets themselves must have the option to deal with these changes in setup, for example, enormous transfer speed limit, improved information rate and low latencies [7]. The appearance of quicker remote advancements, particularly the fifth era remote frameworks (5G), is a driver for the 5G-empowered

IoT applications. It likewise assists with managing an enormous number of IoT-empowered gadgets. The term 5G incorporates Massive-Input Massive-Output (MIMO), which helps to accomplish better arrangement capacities than the current 4G LTE, and "little cells," which permit a denser organization framework [9]. Contrasted with the current 4G innovation, which utilizes frequencies under 6 GHz, 5G systems use much higher frequencies which range from 30 to 300 GHz. 5G also empowers the making of another mechanical application that works outside of the current portable broadband range. This inescapable availability is the venturing stone to accomplish higher accessibility, which has been the focus since the initiation of cell framework [10]; thus, 5G innovation is a key empowering influence for IoT innovation. Along these lines, 5G supplements IoT to give higher information rates, diminished latencies, lower vitality prerequisites and higher versatility. The fast development of IoT innovation and 5G promises to carry substantial advantages to end clients, particularly purchasers and business companies. Purchasers are offered certain administrations dependent on their exercises. For instance, they can travel all the more proficiently by avoiding gridlocks and taking alterative driving routes when informed by the smart IoT-empowered gadget introduced in their vehicle. Furthermore, they can stay healthy by utilizing wearable gadgets that critique their wellbeing after monitoring their physical activity and body parameters for the duration of the day. Organizations can utilize the information of clients to give better administrations and items. Likewise, they can utilize area trackers and remote locking on certain hardware to verify their resources. Government and open specialists can bring about diminished medical services costs with the arrangement of better wellbeing support by remote wellbeing observing, particularly for senior individuals. In addition, street maintenance and smart road lighting can make the residents' life simpler by diminishing the general upkeep cost of the structures.

2 Adoption of Blockchain with IoT Systems

Blockchain can be used to follow the sensor data assessments and hinder duplication with some different malicious information. Positionings of IoT contraptions can be many-sided, and an appropriated record is fitting to give IoT device ID, approval and reliable secure data transfer. Rather than relying an outsider to set up trust, IoT sensors can trade information through a blockchain. All the possible advantages after adoption of blockchain in IoT systems are described in Fig. 1.4.

2.1 Trust Formation

The foundation of trust is one of the most critical prerequisites in the majority of enterprises. For the partners, including the hosts and buyers, of a specific service, such as electronic budgetary biological system or social insurance, management

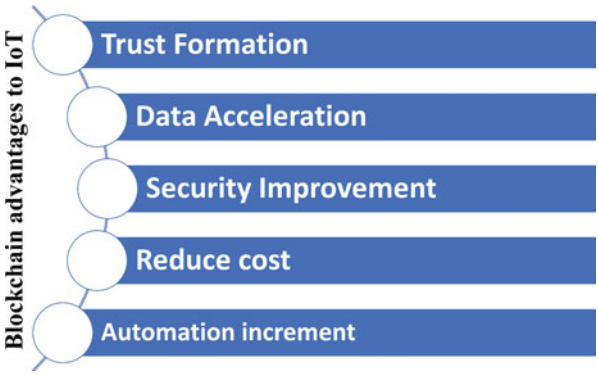


Fig. 1.4 Blockchain advantages for IoT

framework requires trust in various measurements. The measures of the trust are characterized as administrative requirements and internationally shared in the vast majority of the ventures. For example, Payment Card Industry-Information Security Standards (PCI-DSS) in a fund setting, Health Data Portability and Accountability Act (HIPAA) in a clinical setting and General Data Protection Regulation (GDPR) in a close to home information setting, are the instances of the guidelines for the foundation of trust. The smart agreements are recognizable as the trust delegates of the administrative definitions in real life. The smart agreements can be characterized as programming codes implementing the administrative standards and make them transparently available. The smart agreements completely rely upon transparency and integrity of all hubs involved.

The consistency is a fundamental reality for the trust foundation inside the system. Through the transparency of smart agreements, the trust is decentralized without being a "Black Box" in tasks. In the IoT setting, the arrangement of smart agreements makes the hubs reliable and consistent in the particular business biological system. Kuo et al. [15] clarified the advantages of utilizing blockchain-based smart agreements in the medical services space. Dagher et al. [16] clarified the utilization of blockchain for the entrance control of human services information. Yu et al. [17] depicted the establishment of trust in the IoT biological system utilizing blockchain.

2.2 Data Acceleration

The quickened information exchange with higher throughput and negligible inactivity is a key necessity to develop IoT biological systems. The presentation of the whole framework relies upon the quickened activity of information exchange in the IoT hubs. The appropriated idea of blockchain and smart contracts change the information exchange scene towards decentralization by lifting the presentation highlights. For example, the incorporated approval of specific information can be

supplanted by decentralized approval with the utilization of smart contracts conveyed on the IoT hub itself or close to the IoT hubs, for example, the edge or the fog registering hubs which go about as blockchain organized occupants. In this manner, the solicitation reaction full circle lead-time compared to information approval, control or access can be radically reduced utilizing blockchain. Manzoor et al. [18] proposed a blockchain stage which underpins the robotized IoT information trade. Androulaki et al. [19] introduced the ability to increase up to 3500 exchanges every second with lower inertness in Hyperledger Fabric along with different strategies.

2.3 Security Improvement

Privacy, Integrity and Availability are the head model of data security which is otherwise called the confidentiality integrity and accessibility (CIA) triangle. Keeping the classification aside, the integrity and accessibility are the key highlights in the blockchain-based smart contracts by structure. The blockchain-based smart agreements guarantee the integrity by applying hashing and reaching out to the advanced marks to the individual exchange and maintaining the chain of trust altogether inside the blockchain. In addition, the blockchain innovation uses cryptographic methods, for example, Merkle trees to guarantee the predictable respectability over the system. Yu et al. [20] researched the run of the mill security and protection issues in the IoT setting and further explained by developing a system for the combination of blockchain and IoT for the affirmation of different functionalities, including validation and adaptability. Khan et al. [21] clarified the critical security issues in the IoT and how the blockchain can address these issues. The accessibility is guaranteed by the disseminated operational nature of the blockchain arrangement. For example, Denial-of-Service assaults (DoS) assailants who endeavour to vanquish the blockchain arrangement need to survive computationally troublesome obstacles, for example, commandeering 51% of the mining intensity of the system. Blockchain's solid insurance against information altering prevents a rebel gadget from disturbing the cooperative nature of correspondence frameworks, including home, processing plant or transportation framework by infusing or transferring malicious data. In this manner, the blockchain innovation holds the possibility to safely open the business and operational estimations of 5G systems to bolster basic undertakings, for example, detecting, handling, storing and conveying data. Dwivedi et al. [22] proposed a novel system to empower highlights, for example, maintain control and uphold security for the IoT gadgets and clinical information in the medical services setting. Ramani [23] introduced an expansive clarification of blockchain in various settings, including the authorization of IoT security. Ramani et al. [23].

2.4 Reduce Cost

The operational expenses of an IoT environment can be limited in various viewpoints when the blockchain and smart contracts are used. The decentralized activity of smart agreements and the record remove the prerequisite of sending costly high quality registering framework, for example, multi-centre distributed computing hubs for simultaneous exchange handling. In addition, the incorporated information stockpiling can be eliminated by using the conveyed record rather than concentrated information bases. The information transmission overheads for the solicitation trips there and back to the incorporated hubs, for example, cloud occasions in the concentrated frameworks can be eliminated in the blockchain-based smart agreements related environments. Effective information use is an imperative necessity in any IoT-based framework, including the arrangements associated with 5G. However, the IoT framework requires some information overhead for the synchronization between the hubs. Clauson et al. [24] clarified a couple of utilization instances of blockchain featuring the cost-cutting advantages.

2.5 Automation Increment

Blockchain combined with IoT is ideal for the mechanization necessities of future industry. The smart agreements execute naturally when the conditions have reached the executable state without mediation of some other gathering. The blockchain and smart agreements sent in the IoT gadgets are equipped for executing the smart agreements and log the occasions in the appropriated record. For example, the temperature changes of the transitory payload can be executed through the smart agreements dependent on the outer temperature. In addition, the area-based traditions obligation count is operable through the smart agreements. Griggs et al. [25] proposed a framework which uses private Ethereum blockchain and a master–slave demonstrated clinical gadget organization model so that IoT-fuelled medication actuators function precisely. Gallo et al. [26] presented BlockSee, which is a blockchain-based video reconnaissance framework to approve and guarantee the permanence of camera settings similar to the observation recordings in the smart urban communities.

3 Challenge of Blockchain and IoT Integration

There is no uncertainty that the Internet of Things (IoT) and blockchain innovation will have a significant effect on the mechanized modern world. Despite the fact that the utilization of IoT is expanding quickly, it is filled with adaptability, security, protection and integrity issues. Although blockchain was originally made for

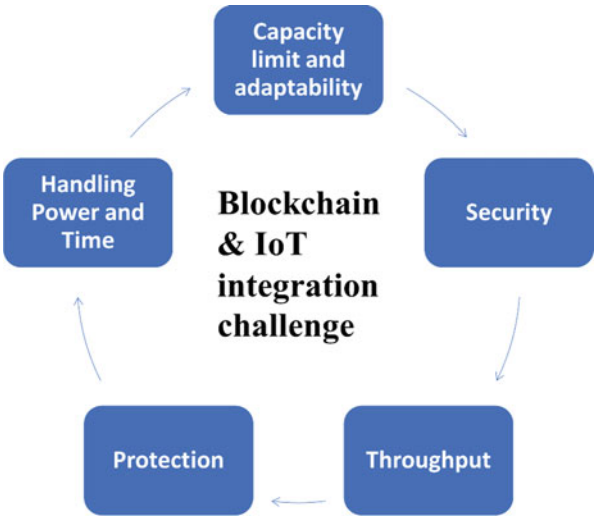


Fig. 1.5 Blockchain & IoT integration challenges

overseeing cryptographic forms of money, its decentralized nature, higher security and trustworthiness has prompted it to be incorporated with the IoT to improve the IoT. There are different difficulties emerging from this reconciliation which expands the complexities. It is important to examine the difficulties engaged with this joining before doing it. The various possible challenges are shown in Fig. 1.5.

A. Capacity Limit and Adaptability
The reliable stockpiling of exchanges and blocks is an essential necessity of the blockchain innovation. Hypothetically, every hub must contain a duplicate of the record which is developing with the exchanges. From an adaptability point of view, the effect on capacity for the IoT environment will influence the usefulness of the whole framework. Particularly, the advancing exchanges with scaling up the framework require noteworthy capacity.

B. Handling Power and Time
There are a couple of computational-asset serious tasks in the blockchain environment. These activities incorporate exchange confirmation and block age, which incorporate few cryptographic tasks. Because of the asset-limited nature of the IoT, there are certain constraints in calculation which will lead to security dangers. Therefore, use of the less asset-escalated choices must be applied explicitly when the blockchain is applied in the IoT setting. The Elliptic Curve Cryptography (ECC)-related advancements are one of the huge options, which bring about less computational overheads to the asset-confined IoT equipment. The cryptographic tasks in the limited equipment will lead to execution restrictions when scaling up the framework.

C. Security

The trustworthiness, accessibility and access control are the essential security worries in any framework. Therefore, the blockchain implements respectability and accessibility characteristically by design. Each exchange is checked with the computerized signature and the blocks of exchanges connected with confirming advanced marks. The exchange confirmation is an asset-escalated activity due to the impediments of IoT registering framework. The exchange confirmation and block age will have adaptability impediments in cryptographic procedure on the blockchain execution. Kumar and Mallick [27] portrayed the security and protection issues in the IoT and examined the noteworthiness of blockchain in this specific situation. Novo et al. [28] proposed a blockchain-based access to management engineering for the IoT. The proposed design eliminates the correspondence overheads and improves versatility. The proposed arrangement joined Software-Defined Networking (SDN), haze processing and blockchain to empower easy and low latency access to the information in a verified way. Hu et al. [29] introduced a deferred open-minded Ethereum blockchain-based instalment plot for country zones.

D. Protection

The enormous volume of IoT gadgets is common in present day sending models. The IoT gadgets uncover more extensive danger surfaces and huge restrictions in protection implementation because of the asset-limited equipment. Particularly, when blockchain is thought of, the information protection is not inbuilt because the exchanges are affixed to the record openly upon confirmation. Security conservation is a critical challenge with broadly utilized encryption strategies. In any case, the lightweight cryptographic components produced for the asset-limited computational foundation will be the perfect answer for authorized information security in the IoT setting. Zhou et al. [30] proposed BeeKeeper, which uses homomorphic calculations on the information without uncovering any bits of knowledge regarding the clients who receive the information. The framework was assessed on the Ethereum blockchain stage.

E. Throughput

Other than the versatility issue of blockchain, the throughput is another task that is difficult to handle. The exchange throughput and inertness experience predictable difficulties, and as the size of exchanges increase, they present the difficult issues that the IoT framework cannot deal with. While hypothetical examination of a stage may give a thought regarding its presentation, only useful execution can give a real use examination. We can investigate the relevance of blockchain frameworks dependent on the objective use by considering the number of exchanges important to be served in an objective time outline. Concerning IoT gadgets, private blockchains might be appropriate, as the quantity of estimations for any single gadget will be small. Regardless, as we scale to bigger IoT-based smart world frameworks serving widely dispersed gadgets, or enormous information frameworks that follow up on an extraordinary amount of information, the capacity to apply blockchain becomes more troublesome.

4 Application of Blockchain in 5G-Enabled Services

Blockchain, when coordinated into the 5G organization, will offer numerous advantages at different levels in the whole 5G environment. Organizations incorporated with blockchain can be redone dependent on the spot and supporter needs and changed progressively to fulfil the flexibly and need. Blockchain can help to improve the interior activity in the centre organization, to lessen expenses and increment adaptability. The various possible application areas are as shown in Fig. 1.6.

4.1 Healthcare

Medical care is one of the significant components for the overall improvement of any country. It could be thought about as an outline of a general public's notable prosperity. With a development regarding people and logical conditions, the weight on contemporary-day medical services structures will also increase. 5G-empowered IoT contemplated a capacity choice to lighten the burden at the medical services devices [42]. One of the appropriate responses is remote wellness monitoring, which incorporates the utilization of IoT sensor contraptions to a degree and examines numerous wellness boundaries of a customer remotely. For instance, Baker et al. [43] perceived an IoT-based medical care device for remote monitoring of the wellness of significantly ill patients. Electronic wellness records (EHR) is the combined virtual model of patients' wellness realities, while non-public wellness

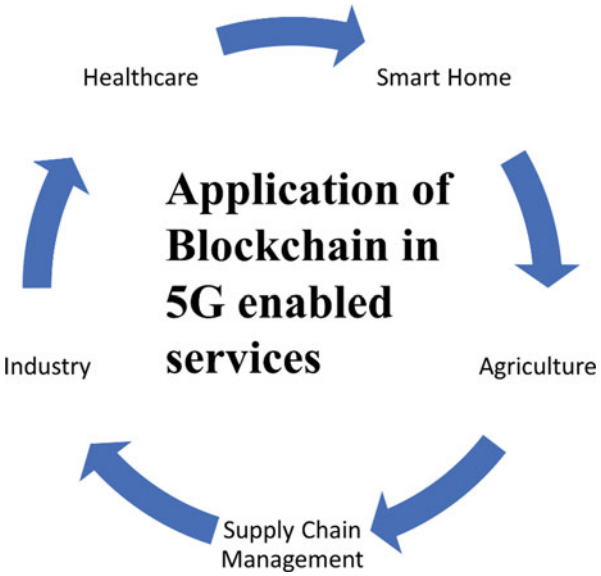


Fig. 1.6 Application of blockchain in 5G enabled services

record (PHR) is related to the virtual report of a character understanding. EHR permits consistent, continuous sharing of logical and cure accounts of patients to ensure a legitimate logical work force [44]. It handles non-public realities and oversees fundamental issues, including confirmation, privacy, responsibility and realities sharing. It empowers logical partners, including public wellness specialists, analysts and clinical specialists, to participate within the blockchain network as "miners" to offer sure motivating forces. Saravanan et al. [45] proposed a medical services worldview named Secured Mobile Enabled Assisting Device (SMEAD) to monitor diabetes. It is an offer up-to-surrender blockchain-based medical care contraption, which continuously monitors diabetic patients. In addition, it changed into fundamentally based at the guarantee that wearable devices have been presently not, at this point, suitable for crisis conditions and have been basically utilized for monitoring purposes. It helps patients who are looking for personal consideration and consistent management from specific clinical specialists.

The main aim of smart wellness applications is to organize wellness in the smart city (or society) in a green and manageable way. Capossele et al. [46] proposed a variant that encouraged the improvement of such s-wellness applications. It is assumed as an overhauled model of the existent e-wellness or m-wellness answers. It calls for realities accumulated from the various EHR and PHR, notwithstanding obtaining permission to the smart urban areas' realities and lays the foundation for the utilization of innovations such as IoT and 5G to flexibly provide appropriate continuous remarks to the residents. However, this strategy has a couple of security issues that need to be addressed. Substantially fewer environmental factors of the stage inferred that there has been a need for a consistent middleware to eliminate any third parties permissions. To address the previously mentioned issue, the creators of [46] proposed a blockchain-based on the absolute s-wellness stage to ensure security, protection, consistency, interoperability and concur with the use of 5G and IoT. Additionally, it allows the relationship of a few IoT devices with low dormancy and exorbitant unwavering quality.

Table 1.2 offers an in-depth contrast of the present procedures in healthcare, with regard to parameters, including utilization of blockchain, wearables, smart fitness, protection, open problems with possible challenges and merits/demerits of the prevailing procedures.

4.2 Smart Home

A smart home is an exemplification of a mechanically improved dwelling, which has the objectives to upgrade the ways of life of the populace. It bears the cost of wellbeing, comfort and extravagance to the proprietors, by letting them adjust the settings in accordance with their decisions with the assistance of a smart phone program. Through the IoT, smart home devices organize with one another to robotize home functions in accordance with the clients' inclinations. The literature mentions a few designs for energy efficient green smart houses. A notable framework of a smart

Table 1.2 Comparative analysis of different approaches for healthcare applications

Model	Description	Advantages	Disadvantages	Blockchain usage	Wearable	Smart health	Security	Challenges
Islam et al. (2015)	Overviewed the advances in IoT-based medical services innovations.	Utilizations of IoT in medical care industry examined in detail.	A few utilizations of IoT were not talked about in detail.	No	Yes	No	Yes	Yes
Saravanan et al. (2017)	Proposed a medical care worldview for diabetes monitoring.	Employed prototype in disaster circumstances talked about.	Difficulties of the model, aside from crisis circumstances, not examined.	Yes	Yes	No	Yes	No
Baker et al. (2017)	Proposed a prototype for application in IoT medical services.	Widespread conversation about vesture medical care frameworks.	A noticeable effect of movement on sensors, which may obstruct the motivation behind these wearables.	No	Yes	Yes	Yes	Yes
Capossele et al. (2018)	Proposed a model for inspiring the improvement of wellbeing applications.	Nitty-gritty arrangements of fundamental difficulties in the wellbeing environment.	Security parts of s-wellbeing applications not delineated.	Yes	No	Yes	No	Yes

home incorporates the ensuing assets: network availability (for the most part Wi-Fi), IoT-empowered sensor devices, and cell programming for remote access. Some basic contributions outfitted through smart houses comprise smart lighting, smart entryway lock, smart indoor regulator, video reconnaissance and smart stopping [47]. To offer reasonable quality for the people living inside the home, the particular contributions should continually change depending on the desired outcome. A smart entryway lock device is a basic part of any smart home. Its main objective is to prevent any unapproved guests from entering the house. The data about the populace is kept in an important worker, which allows white-listed individuals to gain admission to the house. Nonetheless, the realities managed through such a device can be projected through an undesired individual who endeavours to avoid the lock contraption to attempt to gain unapproved admission to the device. To adapt to this issue, Han et al. [48] proposed a blockchain-based smart entryway lock device, which bears the cost of security capacities such as verification, realities integrity and non-renouncement. They utilized fixed Passive Infrared (PIR) sensors, ultrasonic sensors and a development sensor to find indoor/outside gatecrashers. The blockchain network blocks keep the information about exchanges which contain open/lock order. The changeless idea of the blockchain network makes it impractical for any interloper to gain unapproved admission to the contraption and make any adjustment to effectively finished exchanges. Notwithstanding, the inactivity of IoT contraptions (sensors) can presumably be an obstacle to find such an interruption. This issue may be addressed by utilizing 5G Wi-Fi innovation, which manages the cost of discernibly low inactivity, fast interruption recognition and block mining of the exchanges in the blockchain. Dorri et al. [49] proposed a blockchain-based smart home model, which incorporates three transparency levels: the smart home, overlay and distributed storage. In this model, IoT devices controlled midway through an excavator were put within the smart home level. The intersection network carried the designated nature to this structure and is essentially similar to the P2P group used in Bitcoin. In a practically identical line, Aung et al. [50] proposed a decentralized strategy of realities control to manage the smart home device wellbeing and prolateness issues. Table 1.3 presents an in-depth contrast of current strategies in smart houses with regard to parameters together with blockchain, conversation standards, domestic automation interfaces, demanding situations and issues, and pros, cons of the prevailing strategies.

4.3 Agriculture

Smart agribusiness uses present day affects, for example, IoT, GPS and big data, to enhance the standard and extent of the resultant plants. Information such as temperature, light, soil tenacity and moisture are often managed in a central system and broken down using certain AI counts [51]. The blend of assorted movements in agribusiness hopes to form an effective watchful cultivating chain with no compromise to quality. Appropriated Ledger Technologies (DLTs) are considered

Table 1.3 Comparative analysis of different approaches for smart home applications

Model	Explanation	Advantages	Disadvantages	Blockchain usage	Way of communication	Automation interface	Challenges
Lazaroiu et al. (2017)	A smart region model has been proposed, which is essential for constructing a smart city.	Discussed home automation interface more efficiently.	Difficulties and problems of the model not talked about.	Yes	KNX protocol	Yes	No
Aung et al. (2017)	An approach for blockchain implementation in a smart home system is presented, to survive with privacy and security problems.	Smart contract policies related to smart home system discussed very well.	Exchange season of 20s, not reasonable for time delicate circumstances.	Yes	Model and survey	No	Yes
Dorri et al. [49]	Blockchain-based smart home outline presented. Summarizes three main levels of smart homes.	Substantial security and privacy assistances.	Added energy and time overheads	Yes	IPv6 over low power WAN	No	No

to have the most potential to deliver efficiency and simplicity in these common productivity chains [52]. The foremost advantage that DLTs provide is improved prominence. They will ceaselessly follow any trades that happen throughout the productivity chain. The employment of blockchain relies upon the food productivity chain because agribusiness and the food chain are correlative centres, where the end products of cultivating are not any vulnerability used as obligations to varied multi-purpose scattered productivity chains. In such food productivity chains, the client is routinely the last customer. Hua et al. [53] proposed creating a blockchain-based provenance structure, which plans to focus on the trust issues in the productivity chain industry. It records all information associated with the creation of the productivity chain; therefore, everything taken under consideration will be seen by the included individuals. To address the complexities of storing information on the blockchain, they coordinated two related structures:

- Basic Planting Information: Information associated with a selected course of action of the productivity chain, for example, creation, gathering and various techniques, is managed.
- Provenance Record: Information associated with a specific creating improvement is managed.

Caro et al. [54] proposed a blockchain-based decentralized distinguishable quality structure for an agri-food productivity chain management, called AgriBlockIoT. It ensures transparency and auditable asset obviousness to store data from the IoT devices along the whole supply chain within the key blockchain. It uses present day devices as focal points of the layered blockchain to improve the facility of the structure. The vital modules of AgriBlockIoT were API, Controller and blockchain. Another essential part, aside from the agrarian productivity chain, is the smart water system, which provides a more efficient utilization of water. The variable access to open freshwater resources encourages the planning of a system to utilize water resources sensibly, given such advancement in science and headways, for example, IoT, spread enlisting and big data. Robotization of water framework structures together with warm imaging has been a probable response for staggering water structures, which evaluates the water levels within the earth and controls the actuators to flood. It is an improvement to the back-and-forth movement of previous water frameworks, therefore causing a more controlled use of water. Sushanth et al. [55] proposed a smart farming framework, in view of the ideas of IoT and distributed computing. It empowers a rancher to devise a productive, doable water system plan for their homestead dependent on their inclinations. According to the rancher's information sources, a computerized smart water system framework was created, which gave the appropriate timetable to them. At that point, with the assistance of significant sensors and actuators, a particular methodology was executed to control the water amount delivered. Table 1.4 gives the point-by-point examination of existing methodologies in horticulture, with reference to boundaries, for example, utilization of blockchain, smart agribusiness, food recognizability, calculation and professionals, and cons of the current methodologies.

Table 1.4 Comparative analysis of different approaches for agriculture applications

Model	Description	Advantages	Disadvantages	Blockchain usage	Smart Agriculture	Food Traceability	Algorithm
Lin et al. (2018)	A food recognizability framework identified with blockchain and IoT is introduced.	Talked about the information handling stream and structure.	Hard for law-agents to discover and handle issues in the framework.	Yes	Yes	Yes	No
Caro et al. (2018)	A blockchain-based discernibility answer for agri-food supply chain is talked about well overall.	"Ranch to-people" use case.	Utilizing a solitary language for actualizing smart agreements, may meddle while growing more refined business rationale.	Yes	No	Yes	No
Sushanth et al. (2018)	Brilliant farming dependent on IoT and WSN is portrayed.	Start to finish calculation for smart cultivating framework.	The necessity of consistent web availability, which may not be consistently accessible.	No	Yes	No	Yes
Hua et al. (2018)	Proposed a rural provenance framework dependent on blockchain.	Nitty-gritty utilization of information hubs clarified.	The information transferred by taking an interest in organizations will be obvious to all members, which implies there is an absence of access control.	Yes	No	Yes	No
Tripoli et al. (2018)	Investigated the chances of use of blockchain in the agri-food industry.	An exhaustive conversation about DLT in the rural areas.	Real models were excluded.	Yes	No	Yes	No

4.4 Industry

Currently, the total mechanization of industry and business is becoming a reality. Enormous improvements in innovation and their presentation into industry have brought about the development of a next generation of industry, known as Industry 4.0. It plans to join the ability of different innovative areas, for example, IoT, blockchain and Cyber-Physical Systems (CPS) [56]. In Industry 4.0, IoT is relied upon to offer promising ground-breaking answers for existing mechanical frameworks. Therefore, it is being viewed as a key empowering agent for the up and coming age of cutting-edge modern mechanization [57]. Because of the profoundly serious market, organizations plan to pick up business points of interest at any expense. This powers business processes management (BPM) frameworks in Industry 4.0 to digitize and mechanize business procedures to build their benefits. In any case, by adding independent specialists to these business forms, the exchange expenses and dangers related to them also increase. A potential answer for handling these dangers is that every operator should discuss transparently with one another. It tackled the issue of exchange costs for self-ruling operators. However, there emerges an issue of trust between those taking an interest specialist. To handle all previously mentioned issues, Kapitonov et al. [58] recommended the utilization of decentralized frameworks (blockchain innovation) for productive and secure correspondence between the self-sufficient operators in a multi-specialist system. Unlike other dispersed records such as Ethereum and Bitcoin, which experience high deferrals, being founded on the PoW, the QoS blockchain requires constant data updates. In this situation, the opportune execution of a smart agreement makes the anchoring of another block to the primary blockchain conceivable in real time. Moreover, customers that have additional registering force can get UNET tokens as remunerations, in the event that they distribute those unused assets into an unordered arrangement. The job of the "QoS chain" is to check the quality, throughput and dependability of the system suppliers. It improves administration quality, making unchained fit for wide reception. Table 1.5 gives the point-by-point examination of existing methodologies in Industry 4.0 regarding boundaries, for example, utilization of blockchain, BPM, QoS, smart agreements, utilization of AIRA convention, difficulties and issues, and experts, and cons of the current methodologies.

4.5 Supply Chain Management

A supply chain is the system of people, associations, assets and exercises that are engaged with the existence pattern of an item. It begins from item creation to its purchase, from the conveyance of crude materials from provider to producer, directly dependent upon its conveyance to the end client. The standard stream in a supply chain starts with the provider, followed by the producer, distributer,

Table 1.5 Comparative analysis of different approaches for Industry applications

Model	Description	Advantages	Disadvantages	Blockchain usage	BPM	QoS	Smart Contracts	AIRA protocol	Challenges
Viryasitavat et al. (2018)	Proposed an answer for coordinate blockchain with mechanized BPM frameworks.	Administration choice and arrangement in industry 4.0	The proposed QoS blockchain is unequipped for identifying exchange cheats.	Yes	Yes	Yes	Yes	No	Yes
Kapitonov et al. (2018)	Proposed a structure to sort out monetary communications between specialists utilizing a P2P network dependent on blockchain.	Proposed a structure to sort out monetary communications between specialists utilizing a P2P network dependent on blockchain.	Issues and challenges of the protocol were not discussed.	Yes	No	No	Yes	Yes	No
Xu et al. (2018)	Study of the cutting edge in industry 4.0 as it identifies with businesses.	Digital physical systems examined in detail.	Security angles identified with industry 4.0 were not investigated.	No	Yes	No	No	No	Yes

retailer and the buyer. Supply Chain Management (SCM) is the technique to oversee materials, data and funds as they travel through a procedure in the supply chain. Given the importance of supply chains, it likewise faces difficulties, some of which are as follows [59]:

1. Logistic blunder
2. Lack of perceivability and resources
3. Improper treatment of information
4. Inefficient treatment of stock
5. Ineffective hazard management

Kothari et al. [59] examined the effect of two advances on supply chains; blockchain and 5G-empowered IoT. 5G-empowered IoT expands the transfer speed limit to verify transmission of product-related information. Blockchain gives a changeless, conveyed record which enables secure capacity of information. Additionally, it may be utilized as a device to forestall malicious IoT gadgets from entering the system. In addition to the prudent effect of blockchain innovation on organizations as far as operational cost, it can conceivably assist with relieving lawful charges emerging from questions. The primary segment of blockchain innovation is smart agreements which can empower programmed instalment of products upon their receipt, and thus eliminate the requirement for an outsider affirmation. Another significant angle is to resolve debates with respect to whether a wholesaler is qualified for a volume motivation refund. This can be addressed by utilizing smart agreements combined with 5G to follow a shipment. Casado-Vara et al. [60] proposed a model of supply chain, where the purpose of blockchain is to give security to the data of organizations associated with the agrarian supply chain alongside multi-operator frameworks for viable coordination of inside exercises. It shows the theoretical design of a supply chain and the executives with blockchain. This model empowers another market model called circular economy. It utilizes the "Make–Use–Recycle" model, as opposed to the current "Take–Make–Dispose" model. It permits the economy to act naturally sufficient. Unlike physical resources, utilities do not have a stock of their basic digital resources. Also, they do not have the capacity to follow the various exercises related to programming and equipment, for example, their turn of events, shipment and establishment, which sometimes make the frameworks vulnerable to outside digital assaults. The utilization of blockchain for this situation helps to review and track the subtleties of the product and equipment supply chain. Table 1.6 gives the point-by-point examination of existing methodologies in supply chains regarding boundaries, for example, utilization of blockchain, sort of industry, difficulties and issues, and professionals, of the current methodologies.

Table 1.6 Comparative analysis of different approaches for supply chain management

Model	Description	Advantages	Disadvantages	Blockchain usage	Industry	Challenges
Dewey et al. [9]	Explores the uses of blockchain, IoT, and 5G technology in supply chains and trade finance.	Detailed discussion on using blockchain with 5G/IoT.	Practical experiences not discussed in detail	Yes	General	Yes
Holland et al. [32]	Describes the use of DRM in additive manufacturing methods.	Discussion of business development by SAMPL ecosystem.	Implementation part was not explained in detail.	Yes	3D print	Yes
Mylrea et al. [61]	Software patch and configuration management using blockchain.	Detailed diagrammatic explanation of the research area.	Applied use case of the concept was not discussed.	Yes	Software development	Yes
Kothari et al. [59]	Explores how IoT addresses the challenges of current supply chain.	Conceptual model of IoT in SCM.	Challenges related to IoT were not discussed.	No	General	No
Casado-Vara et al. [60]	Presents the concept of circular economy.	Thorough comparison of current and blockchain-based supply chain.	Use case of circular economy was ignored	Yes	Alimentary	Yes

5 Future Research Direction

5.1 Blockchain with Big Data & 5G

In the time of information overload, large information is a hot topic in 5G [34]. A lot of interactive media information created from omnipresent 5G IoT gadgets can be abused to empower information related applications, for instance, information investigation and information extraction engaged by computerized reasoning programs. Distributed computing administrations can offer high stockpiling capacities to adapt to the increased volume of and decent variety of advanced IoT information. However, large information innovations can confront different difficulties, extending from information protection leaks, and they must maintain control over security weaknesses to prevent exceptionally complex information theft [35]. Further, huge information investigations on cloud/edge processing are profoundly helpless against cyberattacks in the complex operational business situations.

In such settings, blockchain shows up as the perfect up-and-comer to comprehend huge information related issues. To be sure, the decentralized executives related to validation and unwavering quality of blockchain can give high-security certifications to large information assets. In particular, blockchain can offer transparency and dependability for the sharing of enormous amounts of information among administration suppliers and information proprietors. By taking out the dread of security bottlenecks, blockchain can empower all-inclusive information trade which engages the wide range of 5G large information organizations. As of late, some huge information models empowered by blockchain have been proposed, for example, information offering smart agreements, maintaining control for huge information security [36], or protection safeguarding for huge information investigations [37]. Such fundamental outcomes show that blockchain can acquire different points of interest in terms of security and execution improvement to large information applications in the time of 5G.

5.2 Blockchain with Machine Learning in 5G

The fast advancements in blockchain innovation are opening new doors for computerized reasoning applications. The unrest of AI or ML innovation changes current 5G administrations by empowering its capacity to gain from information and give information driven bits of knowledge, choice help and forecasts. These focal points of AI would change the way information examinations are performed to help smart administrations in the time of 5G. For instance, ML has the capacity to associate with the remote condition to encourage executives and client correspondence [31]. ML also shows incredible potential regarding information highlight disclosure to foresee information use conduct to create control calculations, such as information traffic estimation to organize clog shirking or client monitoring for security protec-

tion [33]. Currently, there is a developing pattern of coordinating AI with blockchain in 5G applications. For instance, deep fortification learning [23] has been examined and joined with blockchain to empower secure and insightful assets for management and organization in 5G systems.

5.3 Blockchain for 6G

Past the fifth-age (B5G) systems, or purported 6G, will develop to give prevalent execution to 5G and meet the inexorably high prerequisites of future versatile administrations and applications during the 2030s. The key drivers of 6G will be the union of all the past highlights, for example, arrangement densification, high throughput, high dependability, low vitality utilization and monstrous network. As per [38], 6G remote systems are common to help huge client availability and multi-gigabits information transmissions with super-high throughput, incredibly low inactivity interchanges (roughly 10 s), and backing submerged and space correspondences. The 6G systems are additionally imagined to make new human-driven qualities [39] empowered by various imaginative administrations with the expansion of new innovations. The new administrations may incorporate smart wearables, inserts, autonomous vehicles, processing reality gadgets, 3D planning, smart living, space travel, Internet of Nano-Things, remote ocean touring and space travel [40]. To fulfil such applications for the 2030 smart data society, 6G should meet various rigid specialized necessities. Following this method of reasoning, high security and versatility are the significant highlights of 6G, which will be given exceptional consideration from the remote exploration network. With the promising security capacity, blockchain is expected to assume a significant role in future 6G systems. Blockchain conceivably gives a wide range of security administrations, from decentralization, protection, transparency to security and recognizability without requiring any outsiders, which will not only upgrade the security of 6G arranges but also guarantee to advance the change of future versatile administrations. The Federal Communications Commission (FCC) likewise proposes that blockchain will be a key innovation for 6G administrations. For instance, it is accepted that blockchain-based remote sharing [41] is a promising innovation for 6G to give secure, more intelligent, minimal effort and profoundly productive decentralized remote sharing. Blockchain can likewise empower security and protection of quantum correspondences, such as processing, atomic interchanges and the Internet of Nano-Things, through secure decentralized records. All the possible future research directions are shown in Fig. 1.7.

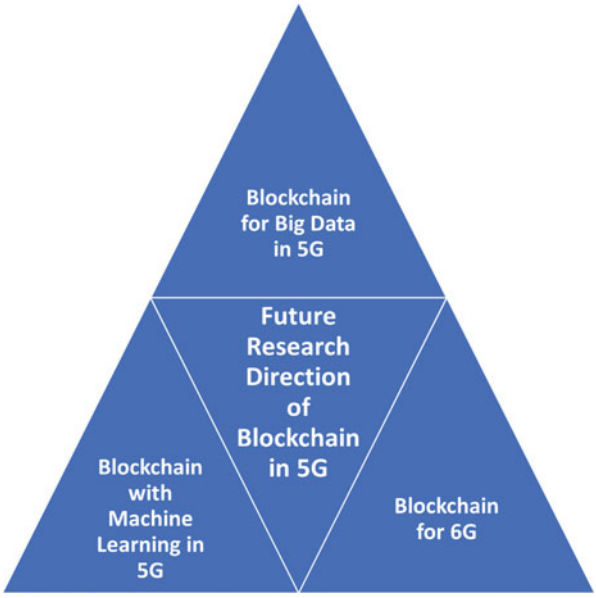


Fig. 1.7 Future research direction of blockchain in 5G

6 Conclusion

Blockchain has moved past the domain of digital currency and is currently reforming a few businesses. The intrigue goes past the promotion as a few ventures have begun embracing the blockchain-based answer for improved business measures. Similarly, 5G organization and past 5G networks are no special case as a few examinations have been directed to carry the advantages of blockchain to 5G organizations. As future 5G networks are required to be exceptionally appropriated and decentralized in nature, network management and security issues become more common and difficult contrasted with prior times. Blockchain, because of its protected plan ideas, addresses centre security issues, for example, integrity, verification, trust and accessibility, in a dispersed style. Likewise, the smart agreements can empower start to finish asset portion/sharing, network management and coordination conveying wanted administrations imagined by 5G. Moreover, blockchain will empower a few new plans of action, diminish the issue related to collaboration among network administrators and consistently handle a few cycles.

References

1. S. Nakamoto et al., Bitcoin: A Peer-to-Peer Electronic Cash System, 2008
2. W. Wang, D.T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, D.I. Kim, A survey on consensus mechanisms and mining strategy management in blockchain networks. IEEE Access **7**, 22328–22370 (2019)

3. A. Panarello et al., Blockchain and IoT integration: A systematic survey. Sensors **18**(8), 2575 (2018)
4. M. Singh, A. Singh, S. Kim, Blockchain: A game changer for securing IoT data, in *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, pp. 51–55
5. S.Z. Khan, S.R. Kamble, A.R. Bhuyar, A review on BIoT: Blockchain IoT. IJREAM **04**(03), 808–812 (2018)
6. E.P. Yadav, E.A. Mittal, H. Yadav, IoT: Challenges and issues in indian perspective, in *2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU)*, IEEE, pp. 1–5
7. J.M. Khurpade, D. Rao, P.D. Sanghavi, A survey on IOT and 5G network, in *2018 International Conference on Smart City and Emerging Technology (ICSCET)*, pp. 1–3
8. M.H. Miraz, M. Ali, Blockchain enabled enhanced IoT ecosystem security, in *International Conference for Emerging Technologies in Computing*, (Springer, Cham, 2018), pp. 38–46
9. J.N. Dewey, R. Hill, R. Plasencia, Blockchain and 5G-enabled internet of things (IOT) will redefine supply chains and trade finance, in *Proc. Secured Lender*, 2018, pp. 43–45
10. A.Y. Ding, M. Janssen, Opportunities for applications using 5G networks: Requirements, challenges, and outlook, in *Proceedings of the Seventh International Conference on Telecommunications and Remote Sensing*, ACM, 2018, pp. 27–34.
11. A. Ahad, M. Tahir, K.-L.A. Yau, 5G-based smart healthcare network: Architecture, taxonomy, challenges and future research directions. IEEE Access **7**, 100747–100762 (2019)
12. D. Garcia-Roger, S. Roger, D. Martin-Sacristan, J.F. Monserrat, A. Kousaridas, P. Spapis, C. Zhou, 5G functional architecture and signalling enhancements to support path management for ev2x. IEEE Access **7**, 20484–20498 (2019)
13. T. Dragičević, P. Siano, S. Prabaharan, et al., Future generation 5G wireless networks for smart grid: A comprehensive review. Energies **12**(11), 2140 (2019)
14. M. Usman, M.R. Asghar, F. Granelli, 5G and d2d communications at the service of smart cities, in *Transportation and Power Grid in Smart Cities: Communication Networks and Services*, (2018), pp. 147–169
15. T.-T. Kuo, H.-E. Kim, L. Ohno-Machado, Blockchain distributed ledger technologies for biomedical and health care applications. J. Am. Med. Inform. Assoc. **24**(6), 1211–1220 (2017)
16. G.G. Dagher, J. Mohler, M. Milojkovic, P.B. Marella, Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using Blockchain technology. Sustain. Cities Soc. **39**, 283–297 (2018)
17. B. Yu, J. Wright, S. Nepal, L. Zhu, J. Liu, R. Ranjan, IoTChain: Establishing trust in the internet of things ecosystem using Blockchain. IEEE Cloud Comput. **5**(4), 12–23 (2018)
18. A. Manzoor, M. Liyanage, A. Braeke, S.S. Kanhere, M. Ylianttila et al., Blockchain based proxy re-encryption scheme for secure IoT data sharing, in *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, IEEE, 2019, pp. 99–103
19. E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich et al., Hyperledger fabric: A distributed operating system for permissioned blockchains, *in Proceedings of the Thirteenth EuroSys Conference*, ACM, 2018, p. 30
20. Y. Yu, Y. Li, J. Tian, J. Liu, Blockchain-based solutions to security and privacy issues in the internet of things. IEEE Wirel. Commun. **25**(6), 12–18 (2018)
21. M.A. Khan, K. Salah, IoT security: Review, blockchain solutions, and open challenges. Futur. Gener. Comput. Syst. **82**, 395–411 (2018)
22. D. Dwivedi, G. Srivastava, S. Dhar, R. Singh, A decentralized privacy-preserving healthcare blockchain for IoT. Sensors **19**(2), 326 (2019)
23. V. Ramani, T. Kumar, A. Bracken, M. Liyanage, M. Ylianttila, Secure and efficient data accessibility in blockchain based healthcare systems, in *2018 IEEE Global Communications Conference (GLOBECOM)*, IEEE, 2018, pp. 206–212
24. K.A. Clauson, E.A. Breeden, C. Davidson, T.K. Mackey, Leveraging blockchain technology to enhance supply chain management in healthcare. Blockchain Healthc. Today **1**, 1–12 (2018)

25. K.N. Griggs, O. Ossipova, C.P. Kohlios, A.N. Baccarini, E.A. Howson, T. Hayajneh, Healthcare Blockchain system using smart contracts for secure automated remote patient monitoring. J. Med. Syst. **42**(7), 130 (2018)
26. P. Gallo, S. Pongnumkul, U.Q. Nguyen, BlockSee: Blockchain for IoT video surveillance in smart cities, in *2018 IEEE International Conference on Environment and Electrical Engineering and 2018 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe)*, IEEE, 2018, pp. 1–6
27. N.M. Kumar, P.K. Mallick, Blockchain technology for security issues and challenges in IoT. Procedia Comput. Sci. **132**, 1815–1823 (2018)
28. O. Novo, Blockchain meets IoT: An architecture for scalable access management in IoT. IEEE Internet Things J. **5**(2), 1184–1195 (2018)
29. Y. Hu, A. Manzoor, P. Ekparinya, M. Liyanage, K. Thilakarathna, G. Jourjon, A. Seneviratne, A delay-tolerant payment scheme based on the Ethereum Blockchain. IEEE Access **7**, 33159–33172 (2019)
30. L. Zhou, L. Wang, Y. Sun, P. Lv, Beekeeper: A Blockchain-based IoT system with secure storage and homomorphic computation. IEEE Access **6**, 43472–43488 (2018)
31. D.C. Nguyen, P.N. Pathirana, M. Ding, A. Seneviratne, Privacy preserved task offloading in mobile blockchain with deep reinforcement learning. arXiv preprint arXiv:1908.07467 (2019)
32. M. Holland, J. Stjepandić, C. Nigischer, Intellectual property protection of 3D print supply chain with blockchain technology, in *2018 IEEE International conference on engineering, technology and innovation (ICE/ITMC)*, 2018, pp. 1–8
33. Y. Dai, D. Xu, S. Maharjan, Z. Chen, Q. He, Y. Zhang, Blockchain and deep reinforcement learning empowered intelligent 5G beyond. IEEE Netw. **33**(3), 10–17 (2019)
34. M.G. Kibria, K. Nguyen, G.P. Villardi, O. Zhao, K. Ishizu, F. Kojima, Big data analytics, machine learning, and artificial intelligence in next-generation wireless networks. IEEE Access **6**, 32328–32338 (2018)
35. K. Sultan, H. Ali, Z. Zhang, Big data perspective and challenges in next generation networks. Future Internet **10**(7), 56 (2018)
36. U.U. Uchibeke, K.A. Schneider, S.H. Kassani, R. Deters, Blockchain access control ecosystem for big data security, in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2018, pp. 1373–1378
37. K. Lampropoulos, G. Georgakakos, S. Ioannidis, Using blockchains to enable big data analysis of private information, in *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, 2019, pp. 1–6
38. W. Saad, M. Bennis, M. Chen, A vision of 6G wireless systems: Applications, trends, technologies, and open research problems. arXiv preprint arXiv:1902.10265 (2019)
39. S. Dang, O. Amin, B. Shihada, M.-S. Alouini, From a human-centric perspective: What might 6G be? arXiv preprint arXiv:1906.00741 (2019)
40. M.Z. Chowdhury et al., 6G wireless communication systems: Applications, requirements, technologies, challenges, and research directions. arXiv preprint arXiv:1909.11315 (2019)
41. Z. Zhang, Y. Xiao, Z. Ma, M. Xiao, Z. Ding, X. Lei, G.K. Karagiannidis, P. Fan, 6G wireless networks: Vision, requirements, architecture, and key technologies. IEEE Veh. Technol. Mag. **14**(3), 28–41 (2019)
42. S.M. Riazul Islam et al., The internet of things for health care: A comprehensive survey. IEEE Access **3**, 678–708 (2015)
43. S.B. Baker, W. Xiang, I. Atkinson, Internet of things for smart healthcare: Technologies, challenges, and opportunities. IEEE Access **5**, 26521–26544 (2017)
44. What is an electronic health record (EHR)? URL: https://www.healthit.gov/faq/what-electronic-health-record-ehr
45. M. Saravanan et al., SMEAD: A secured mobile enabled assisting device for diabetics monitoring, in *2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, pp. 1–6

46. A. Capossele et al., Leveraging blockchain to enable smart-health applications, in *IEEE 4th International Forum on Research and Technology for Society and Industry (RTSI)*, 2018, pp. 1–6
47. C. Lazaroiu, M. Roscia, Smart district through IoT and blockchain, in *2017 IEEE 6th International Conference on Renewable Energy Research and Applications (ICRERA)*, pp. 454–461
48. D. Han, H. Kim, J. Jang, Blockchain based smart door lock system, in *2017 International Conference on Information and Communication Technology Convergence (ICTC)*, pp. 1165–1167
49. A. Dorri, S.S. Kanhere, R. Jurdak, P. Gauravaram, Blockchain for IoT security and privacy: The case study of a smart home, *in 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)*, pp. 618–623
50. Y.N. Aung, T. Tantidham, Review of ethereum: Smart home case study, in *2017 2nd International Conference on Information Technology (INCIT)*, pp. 1–4
51. J. Lin et al., Blockchain and IoT based food traceability for smart agriculture, in *Proceedings of the 3rd International Conference on Crowd Science and Engineering*, ACM, 2018, p. 3
52. M. Tripoli, J. Schmidhuber, *Emerging Opportunities for the Application of Blockchain in the Agri-Food Industry* (FAO and ICTSD, Rome and Geneva. Licence: CC BY-NC-SA 3, 2018)
53. J. Hua et al., Blockchain based provenance for agricultural products: A distributed platform with duplicated and shared bookkeeping, in *2018 IEEE Intelligent Vehicles Symposium (IV)*, pp. 97–101
54. M.P. Caro et al., Blockchain-based traceability in Agri-Food supply chain management: A practical implementation, in *IoT Vertical and Topical Summit on Agriculture-Tuscany (IOT Tuscany)*, 2018, pp. 1–4
55. G. Sushanth, S. Sujatha, IOT based smart agriculture system, in *2018 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, IEEE, 2018, pp. 1–4
56. W. Viryasitavat et al., Blockchain-based business process management (BPM) framework for service composition in industry 4.0. J. Intell. Manuf **31**, 1737–1748 (2018)
57. L. Da Xu, E.L. Xu, L. Li, Industry 4.0: State of the art and future trends. Int. J. Prod. Res. **56**(8), 2941–2962 (2018)
58. A. Kapitonov et al., Blockchain based protocol for economical communication in Industry 4.0, in *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pp. 41–44
59. S.S. Kothari, S.V. Jain, A. Venkteshwar, The impact of IOT in supply chain management. Int Res. J. Eng. Technol. **5**(08), 257–259 (2018)
60. R. Casado-Vara et al., How blockchain improves the supply chain: Case study alimentary supply chain. Proc. Comput. Sci. **134**, 393–398 (2018)
61. M. Mylrea, S.N.G. Gourisetti, Blockchain for supply chain cybersecurity, optimization and compliance, in *2018 Resilience Week (RWS)*, 2018, pp. 70–76