Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Blockchain for 5G-enabled networks in healthcare service based on several aspects

22

Garima Jain[a] *and Ankush Jain*[b]
[a]Department of Computer Science and Engineering, Noida Institute of Engineering and Technology, Greater Noida, India, [b]School of Computer Science Engineering and Technology, Bennett University, Greater Noida, India

1 Introduction

The advancement in healthcare diagnosis and healthcare practitioners' uses cutting-edge technologies. Fig. 1 explains the characteristics of 5G. The healthcare industry has undergone several transitions from Healthcare 1.0 to Healthcare 4.0. Healthcare 1.0 is more physician-centric with structural flexibility to keep manual records of their patient's medical histories. However, in Healthcare 2.0, these manual records were gradually supplanted by digital records. Wearable devices were used for the real-time monitoring of patient healthcare history in Healthcare 3.0 [1]. With resources lacking, the healthcare systems were constrained and not integrated with computer data throughout this time. On the other hand, biomedical machines had not yet been invented so were not integrated with networked electronic equipment. Paper-based medications and reporting were commonly employed in healthcare organizations during this time, resulting in higher costs and time [2, 3].

Electronic health records (EHRs) must frequently be exchanged across healthcare organizations, medical and pharmaceutical companies, pharmacies, health coverage organizations, researchers, and patients to deliver appropriate healthcare. This creates a significant problem in maintaining the security and accuracy of the patients' sensitive data. During treatment, a patient may be transported to/from other hospitals. According to the US Department of Health and Human Services [4], a patient in such a case owns the right to their medical information and may need to set access control limits. Blockchain technology is a distributed database that is replicated across multiple servers in the network. We cannot modify it because the data are kept in independent blocks. As a result, the blockchain can boost privacy, visibility, and confidence.

The authors of Ref. [5] believe that the blockchain applications in healthcare have full potential for manage the process, facilitating research, and installing EHRs after analyzing the economic effect of technology by examining the scalability and impact of use cases in various industries. Due to its decentralized nature and supposed immutability, blockchain can tackle data management concerns in the healthcare business.

Blockchain Applications for Healthcare Informatics. https://doi.org/10.1016/B978-0-323-90615-9.00018-9

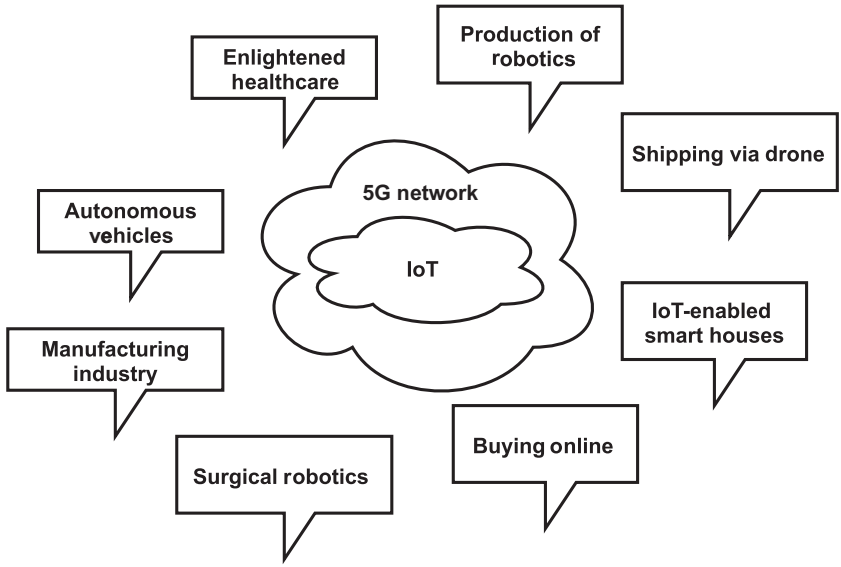

Fig. 1 Characteristics of 5G.

The system could simplify data sharing among numerous actors, improve effectiveness and efficiency, and provide anonymized academic file sharing [6].

With multiple taxonomies, this chapter will describe the leading technology and products for 5G security. It will detail a variety of attacks that have been detected in the 5G network as well as provide solutions. It examines whether we can use blockchain technology to transform our present healthcare system. Diverse healthcare participants (providers, users, patients, suppliers, producers, and academic institutions) play varied roles and have different requirements in the industry. This chapter aims to provide a deeper understanding by identifying the limitations of blockchain technology in the health field and determining the potential scope for blockchain for all health participants in a scientific test [7].

As far as healthcare is concerned, the urgency of development increases to more incredible speeds. The absence of systematic research on the topic and the separation of practice and academia make a detailed analysis of the new technologies' consequences for the healthcare sector difficult. By bringing study and practice together, both viewpoints may gain a better knowledge of critical issues. Reduced energy usage, lower latency, artificial intelligence (AI)-assisted programs, multimedia capability with AR/VR, increased security, and high data transmission rates are just a few of the benefits of 5G technology [7].

1.1 Motivation

As a result of the first stage of a comprehensive literature review, the following research objectives were generated to fill in the gaps, as shown in Table 1.

Table 1 Motivation and corresponding research objectives.

S. no.	Research question	Motivation
1	One of the most immediate issues among health professionals?	The goal is to bring attention to important challenges that are impeding the economic progress of the health sector.
2	How many blockchain features are being used to address the concerns that have been recognized?	The goal is to look into developing technology that helps to address problems and advance the area.
3	What are all the hurdles and difficulties with implementing blockchain?	The goal is to identify any concerns with blockchain deployment that have yet to be resolved.

1.2 Contribution

The following are the chapter's significant contributions:

- While the qualities of blockchain are appropriate for building a health service, these techniques are nonetheless costly in terms of runtime and data sent for record updates.
- Despite these costly methods, the blockchain paradigm can yield remarkable results, particularly in a measured approach. In this technique, patients and clinicians visit health records regularly to create a unified view from several hospitals for proper treatment or prediction of disorders using AI.

1.3 Structure of chapter

The rest of the chapter is organized as follows. The first section introduces technology and its role in the healthcare industry with contributions and research motivation. Section 2 delves into the characteristics of blockchain, including its features, architecture, and operation. The research approach in the healthcare system is described in Section 3. The implementation of 5G technology in the healthcare sector is summarized in Section 4. Section 5 discusses the likelihood of 5G in the blockchain. Section 6 explains how to use blockchain in healthcare records. Section 7 combines blockchain technology with the healthcare system. Section 8 ensures that blockchain technology in EHR is kept private and secure. Finally, Section 9 concludes the chapter.

2 Blockchain

The name "blockchain" was derived from the terms "chain" of "blocks" containing information, where the transactions made on a network are represented by a "block" and a string of blocks by a "chain" [8]. A blockchain is a decentralized, distributed, and public digital ledger. It is jointly maintained by multiple parties, using cryptography to ensure the security of transmission and access, achieve data storage

consistency, make data tamper-proof, and prevent repudiation. It is also known as distributed ledger technology (DLT).

2.1 Characteristics of blockchain

The blockchain has the following properties compared to regular data duplication: First, there is the transition from double entry to distributed accounting [9]. Each accountant records independently in a typical information system, and each reconciling involves numerous different ledgers. Second, "insertion, deletion, selection, and update" has been replaced with "insertion and selection." Third, the management shifts from unilateral to multilateral. Fig. 2 classifies the architecture of blockchain.

In a blockchain, every block comprises data, a hash of the current block, and a hash of the preceding block.

- *Data*: The type of blockchain determines the data stored. For example, the data maintained on a Bitcoin blockchain include information about the transaction, such as "sender," "receiver," and "amount."
- *Hash*: Each block in a blockchain includes a hash, which is similar to a finger print. It uniquely recognizes the block with all its data. When a block is formed, a hash is generated, and changes to the league will cause the hash value to change.
- *Preceding block's hash*: Every transaction also comprises the preceding block hash, producing a blockchain network with every block pointing to the previous block [10]. Finally, a plug-in contract transforms into a built-in contract. Historically, the financial capital flow and administrative flow of information were two distinct aspects of a commercial organization. Bitcoin is a new sort of peer-to-peer digital currency first proposed in a paper published in 2008 by the enigmatic and anonymous inventor Satoshi Nakamoto, whose true name is unknown, with speculation that the moniker refers to a group of developers rather than a single individual. With crypto algorithms, a digital currency was created that could be

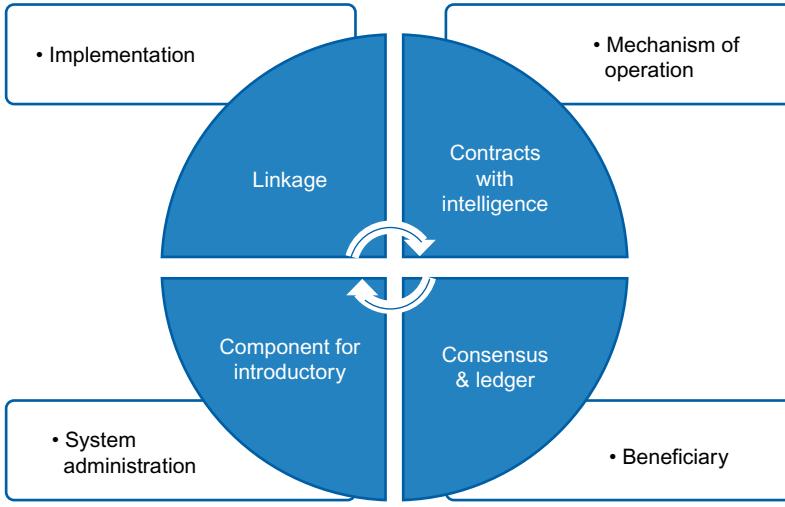

Fig. 2 Blockchain architecture.

utilized without any intermediaries or regulating authorities, allowing money to travel from one person to another without the need for a bank or other third-party middleman. Fig. 3 depicts the scenario of blockchain technology.

2.2 Working of blockchain technology

2.2.1 Technologies involved in blockchain cryptography

The workings of blockchain are complicated by several technologies, one of the most essential of which is cryptography, which uses public and private keys. The word "cryptography" comes from the Greek words "kryptos" (hidden) and "graphein" (writing). Cryptography is the art of writing in secret. It is a method of conveying a message from one person to another without allowing unwanted individuals access.

The public-key cryptography is one of the most popular technique among the various types of cryptography techniques. It consists of two keys: a "public key" and a "private key." Everyone can see the public key, but only the user who owns it can view the private key, which must be kept hidden [11, 12].

Fig. 4 depicts the working of a digital signature. In cryptography, the first stage is developing a private key, which is essentially a unique combination of letters (A through F) and integers. When a private key is generated, a sophisticated computational method is used to create its pair, known as the public key. The technological equivalent of the wax seal and stamp is a digital signature. The digital signatures are created using public and private key pairs [13]. The sender's private key is used to sign electronic communication before it is sent. Because the receiver knows the sender's public key, the recipient certifies that the sender's private key pair created the signature.

Nonce: A number that is used only once with a particular purpose and then is never used again is known as a once. One of its main applications is digital communication, which helps to avoid repeated operation that can be quite harmful and have bad repercussions.

Ledger: The ledger layer is in charge of the cryptocurrency system's storing information, which involves collecting user information, producing data blocks for local storage validity, and forwarding the patterned block to the blockchain. The ledger layer creates a blockchain data structure by embedding the preceding block's hashing into another block, ensuring the integrity of data and validity.

Consensus: The consensus layer is responsible for managing and ensuring the 10 Blockchain White Paper (2018) consistency of all end points in the data records of the channel. In blockchain technology, each node stores data independently. With the use of the consensus technique, the consensus layer synchronizes the books of each network, allowing it to execute functions such as node election, data integrity validation, and modern networking control.

Smart contract: The smart contract system is also responsible for constructing, installing, and executing the business processes of the blockchain network utilizing code as well as conditional triggers and automatic implementation of the established rules to reduce physical contribution.

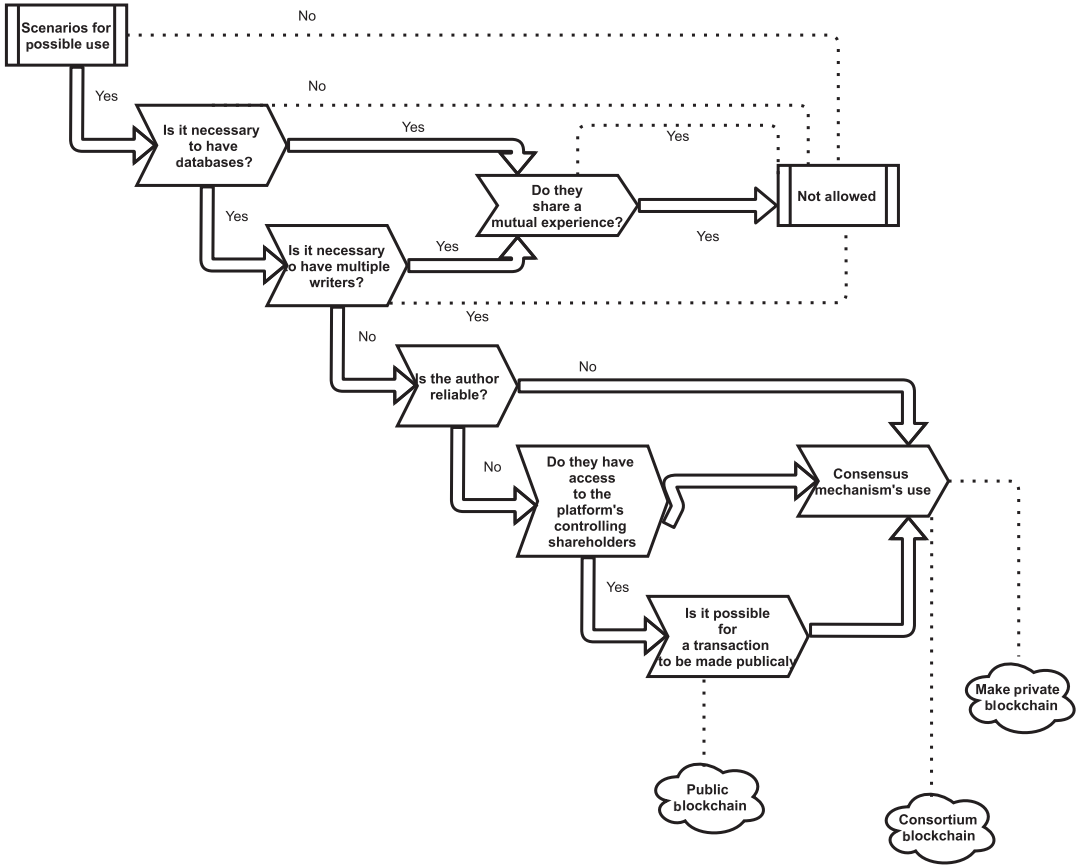

Fig. 3 Blockchain scenarios.

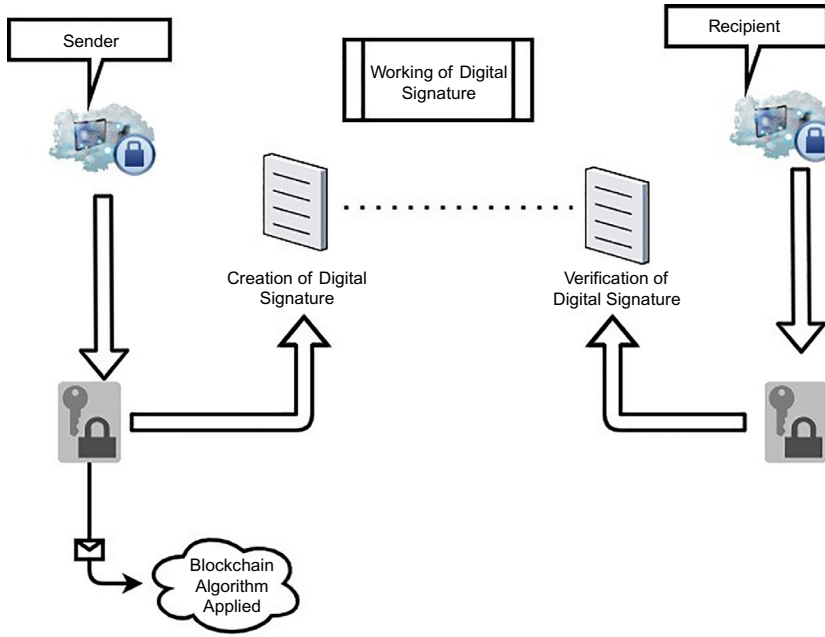

Fig. 4 Working of digital signature.

Interface layer: The major goal of the interface layer is to complete the encapsulating of opportunities for integration and provide a simple call to the application level. The remote procedure call (RPC) protocol is used to communicate with external networks at the application level, while the software development kit (SDK) toolbox is used to access and alter the private ledger data.

Application layer: The application layer is the part that the user sees in the end. The smart contract layer is called the primary purpose. The interface adjusts to numerous blockchain application scenarios to give consumers a variety of services and applications.

3 Healthcare system

Healthcare information needs to be more safe and private. Modification and destruction of stored data must be prohibited for this data. If an unauthorized individual has access to the data, it will be sold or misused. Because the amount of health records will grow due to 5G networks, security mechanisms to protect the data must also increase [14–16]. The field of healthcare encompasses a diversified set of tasks and procedures, and as a consequence, it confronts a wide range of issues. This review examines the difficulties that can be addressed by the literature through information technology, particularly blockchain. A healthcare scheme is a method of arranging healthcare in terms of finances, security, accessibility, data management, and retrieving.

Healthcare is the most critical factor in a country's overall development as it provides medical care to people worldwide to live healthy and prosperous lives.

As a result, as technology has advanced, the healthcare business has altered drastically. A healthcare system is based on accessible properties and public demands. Every patient's EHR could include critical information such as the patient's overall health, administrative data, and official papers. There has been significant progress in several fields of health, including telehealth, telesurgery, data collection, and diagnosis of illnesses.

3.1 Definition of healthcare

It is crucial to define the scope of the term "healthcare" to comprehend the context in which private blockchains can be applied. As stated earlier, several journals and definitions distinguish between the terms "health care" and "healthcare" as well as other terms such as "health system" and "healthcare business." Healthcare is a critical aspect in determining a region's or country's standard of living. The health sector is a collection of industries within the economy that provides services and products for the medicinal, preventative, curative, rehabilitative, and palliative care of patients [17].

4 5G in healthcare

This section highlights the clinical potential of 5G technology by presenting several clinically relevant use cases for 5G applications [18]. We will divide them into user groups and applications to standardize use cases and then identify the related goals and objectives, requirements, and timelines. Patients and caregivers, such as doctors, nurses, psychologists, companies, legislators, and legal organizations, are among the various users. The COVID-19 crisis exposed a vulnerability in many healthcare providers' processes, including hospitals and local/regional health authorities, which found themselves in the middle of the flood [19–21].

4.1 Need of 5G for future healthcare

Traditional healthcare systems are undergoing vast and ever-accelerating transformations. Enhanced or potentially developing information and communications technology (ICT) are driving these shifts.

More importantly, this technology suggests how 5G networks can evolve and enhance all the essential aspects of health insurance, a topic that is particularly relevant today given the propagation of the coronavirus, which has put immense strain on healthcare systems all over the world.

On multiple levels, the evolution of healthcare will occur in lockstep. In the start phase, the patient-care perspective evolves from the patient and illness to a decentralized physician healthcare setting, which is also overcoming healthcare providers' sector-specific barriers. Second, wellness data analysis results and treatment shift from inter-institutional to regional availability. In addition, health management is

evolving from a broad and basic approach to one that introduces to individual patient. Furthermore, the emphasis of healthcare systems is shifting away from cancer therapy and toward preventive care. 5G can achieve speeds that are 100 times faster than 4G, while also handling many more users [22]. These benefits are shown by ultralow delays, the time it takes for a request to be processed by the network. This novel strategy, known as "4P" medicine (personalized, preventative, predictive, and participatory), necessitates the development of breakthrough technology to provide additional value to patients. Advanced digitalization concepts and virtualization methods will be among these technologies based on principles adopted from Industry 4.0 standards. In turn, to support new health, both will heavily rely on sophisticated data transmission abilities, including those provided by 5G technology.

4.2 Cutting costs for the provision of health services

By delivering dispersed physician care, decentralized healthcare services remote from facilities yet individualized and instantaneously available everywhere, information technology can continue to lower costs in the health domain. Another goal is to improve consistency and reliability by increasing the complexity of patient data and enhancing the products and service levels. 5G also enables a shift toward digitalization of treatments, allowing for individualized and designed treatments in hospitals to be delivered in nursing homes or elsewhere. This finding increases the chances of extra payments, while also improving the lives of patients and families.

5 5G security with blockchain

Blockchain is a term used in 5G security to describe novel and transformational technologies that verify and authenticate transactions, preserve information, and manage identities across multiple entities in a decentralized and secure manner [23, 24]. From existing literature, it seems that there is a breakthrough for future communication technologies in 5G. To ensure security in a 5G network, blockchain, a peer-to-peer decentralized database technology for storing distributed ledgers connected in chains, has many qualities: decentralizing, distributing, and others. Because it is a decentralized and spreading technology, it needs numerous applications such as smart health, innovative finances, supply chain management, and driverless cars [25]. Combining 5G with a blockchain system can significantly increase the economic value of data sharing. Because of the strength of 5G coverage enabled by blockchains, delay, fast throughput, and bandwidth have decreased, allowing IoT devices to be widely used. At the same time, these devices can use blockchain technology as a foundation layer to benefit from its security, decentralization, integrity, and agreement mediation. While most IoT transactions and contracts occur on the network layer, blockchain can provide consensus and protection, with the ability to settle account management and transactional issues on a chain. 5G will immediately benefit blockchain technology by expanding node involvement and decentralization and lowering block times, on-chain scaling, and IoT economy support. Blockchain technology allows many parties to

share, transmit, and access data safely. The essential information is transferred to all parties via a distributed ledger in the blockchain. As a result, in the 5G network, blockchain technology delivers more security characteristics. In a transportation application, blockchain provides a secure data access system that allows relevant external bus transportation participants in the system to access a passenger's payment collection data.

In the 5G network, centralized and scalable IoT systems are also a big issue. Blockchain-based techniques, in this scenario, provide decentralized security and privacy mechanisms for various IoT applications in 5G. The taxonomies for several applications of 5G networks are shown in Fig. 5. Blockchain can efficiently access numerous users in the ultra-dense network (UDN) ecosystem for 5G, and it also provides a simple, secure authentication mechanism to solve the access-point group (APG) trusted generation and security problems. They DLT [26] states that multiple UDN systems generate a consortium blockchain and sensor node accessibility to the APG, which comprises various access points (APs). The UE (local support) service center manages the AP clusters (LSC). In the 5G environment, UE, on the other hand, employs blockchain technology to give secure and dependable access.

5G security applications and services for healthcare: The most significant claim in the 5G network is healthcare. Blockchain technology has a significant effect on decentralized systems that depends on several factors. The secure transmission of a patient's medical information is the most important criterion for providing advanced analysis in the healthcare domain because information leakage is a concern [27].

Big data analytics: In big data applications, the 5G network is critical for network data centers. Big data can successfully transfer massive volumes of complex information to data centers by utilizing the core features of 5G networks, cognitive radio

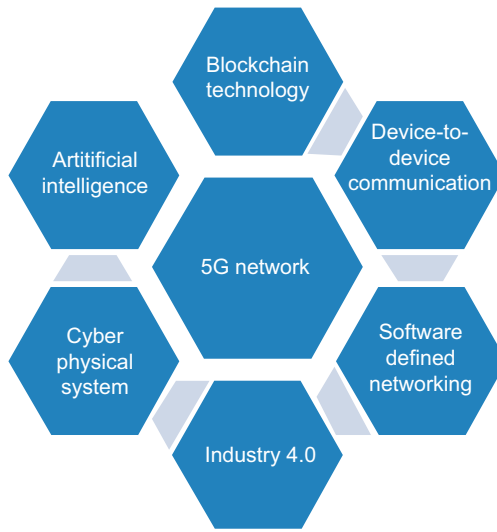

Fig. 5 Applications associated with a 5G network.

systems, and network infrastructure sections. One advantage of large datasets in 5G is the ability to detect anomalies quicker and in real time using a vast amount of data gathered from linked devices.

Internet of things: Every day, IoT devices generate massive volumes of data, necessitating efficient data transfer and huge quantities of throughput, something 4G-based networks have struggled to provide. Sensor nodes need more capacity, reduced latency, and faster data rates, which 5G networks can supply [21].

Automotive driving: Automotive driving is being examined in the context of the 5G network, such as completely autonomous car steering and mapping, as modern logistics milestones. Others may provide economic rewards or disincentives for adopting forms of conduct that reduce congestion.

Smart grid: It is part of Industry 4.0, which employs 5G technology to enable tailored solutions, flexibility, and cost savings in the manufacturing process.

Smart drones: With large number of links, 5G can significantly speed up the implementation of unmanned aerial vehicles (UAV) area networks, also known as drone access points.

5.1 Current technical and societal challenges

5G also brings with its several new issues. The use of this modern innovation establishes new benchmarks for infrastructure components. Even though 5G is commonly referred as a new technology, several features have been in use for years. For example, the radio-access technology (RAT) is quite similar to the widely used 3G and 4G technologies. The frequencies used by 5G devices, ranging from 450 MHz to 3.8 GHz, have been used since the early 1990s. It was first introduced when smartphone technologies incepted.

A mix of existing technologies and development areas of the network is used to provide novelty and additional value. For example, one of the most creative characteristics of the network infrastructure is "network slicing," which exploits the current frequency to develop new commercial services through virtualized channels of communication. Even though much of this technology was in use in recent decades, the demands on infrastructure have increased [28]. Many of the newest features have an increasing demand for processing power that older architectures cannot meet. As a result, additional expenditures in 5G infrastructure are required.

We must, however, invest in cutting-edge transmitter technology. On the other hand, many present communications are unsuitable for 5G applications. We feel that high investment costs and complex conversion stages are inhibiting the advancement of 5G technology. Governments will have to license all medical equipment, particularly software connected via 5G, and transferring patient data. Organizations will have to obey the relevant legislation for medical sensors and data protection. As a result, patients can rest assured that their information is secure. The hospital sector, in particular, has a high requirement for data security and safety. Indoor transmission within hospitals, for example, is tightly controlled and supervised in important application settings. In medical equipment factory, the functional interconnection is now getting difficult. New use cases and application possibilities are enabled by 5G as a

high-performance communication link between medical equipment. Until they can benefit patients, these innovative applications must be researched and verified on a medical and technological level.

6 Blockchain for healthcare records

A total of 135 of the 150 publications (90%) emphasize the necessity for a blockchain-based implementation aimed at a specific type of EHR. A blockchain design can be considered a virtually incorruptible cryptographic database for storing crucial medical information.

Information technology has long been a part of a wide range of businesses, including healthcare. Technology has advanced by leaps and bounds in comparison to a few millennia ago. Fig. 6 depicts the architecture of medical record storage.

Patients, allied health professionals (e.g., doctors, nurses, and pharmacies), and executives are among the participants inside the bitcoin healthcare system model. To complete a healthcare transaction on the developed platform, the transaction is transferred to the public blockchain by the patient and allied health providers.

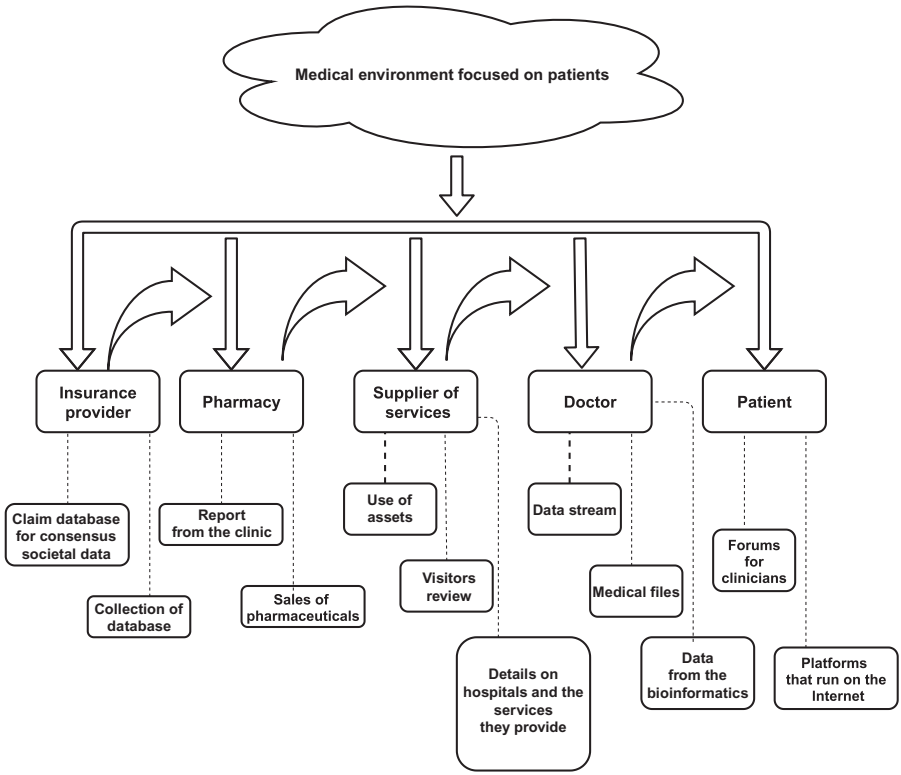

Fig. 6 Architecture of medical record storage.

Physicians and researchers authenticate the transaction, then transmit it to the administration, which acts as a miner. The transaction's block will be generated by the administrator and sent to all other institution administrators for repetition.

Several studies have used blockchain in therapeutic diagnostics to enable reliable health information preservation, processing, and exchange due to the decentralization and flexibility of the blockchain. Simonov et al. [29] examine the difficulties and possibilities for integrating blockchain into e-healthcare systems in depth. Liu and colleagues developed a blockchain-based data-sharing system to address the privacy issues of electronic medical records (EMR) sharing [30]. Fig. 7 defines the health data transfers using blockchain.

In the proposed system, the content extract signature approach and ciphertext-policy attribute-based encryption (CP-ABE)-based accessibility are introduced. To achieve human rights and verifiable health information storage, Li et al. [10] designed cryptocurrency medical data together. Ginn et al. [31] presented a confidentiality picture retrieval method for medical IoT devices that stored the feature representation for every image using modified digital ledger structures. Privacy-preserving image retrieval is based on feature vector extracts via smart contracts. The nature of the data contained in the EHRs is the fundamental cause of the concerns raised in the healthcare sector. Hussein et al. [32] said, "Data related to the diagnosis and treatment of a patient is considered extremely sensitive and private." Therefore, safeguarding and updating such information is a serious challenge and leads to barriers in adopting healthcare-related data systems [33]. Even if a sufficient amount of data is gathered in the system, the variety of sources and formats in which it is available extend the problem. While patient privacy must be assured, data should also be easily manageable and transferable [34]. Newly arising areas such as remote patient monitoring, telemedicine, and mHealth pose new challenges due to the need for speedy data manipulation and gathering based on the requirement of short reaction times.

Moreover, data can be exposed in an adequately safe facility to nasty user attacks [35]. Although storage modes may differ, cloud service providers, according to Kullo et al. [36], have difficulty persuading hospitals to employ their solutions due to concerns about third-party exploitation.

Interoperability is a critical factor that influences the development of new EHR management paradigms. While EHR and connectivity might be separate use cases in some ways, all focus on connection in the current level of blockchain development in healthcare. Hence, they will be examined together in the framework of this chapter. The definition of interoperability is, "The ability of healthcare systems to work together inside and across company boundaries in order to promote the successful delivery of healthcare for persons and communities." While some previously stated EHR-focused solutions address consistency, Pirtle and Ehrenfeld [37] raise an essential point. It introduces many new, blockchain-based solutions that address the EHR and integration use instances without issuing a concomitant standard. Agreeing on a unified system can result in a new interoperability issue. A new shift toward "patient-centered interoperability" is visible, in addition to interoperability among commercial entities such as hospitals, research institutes, and so on. The aim of giving clients

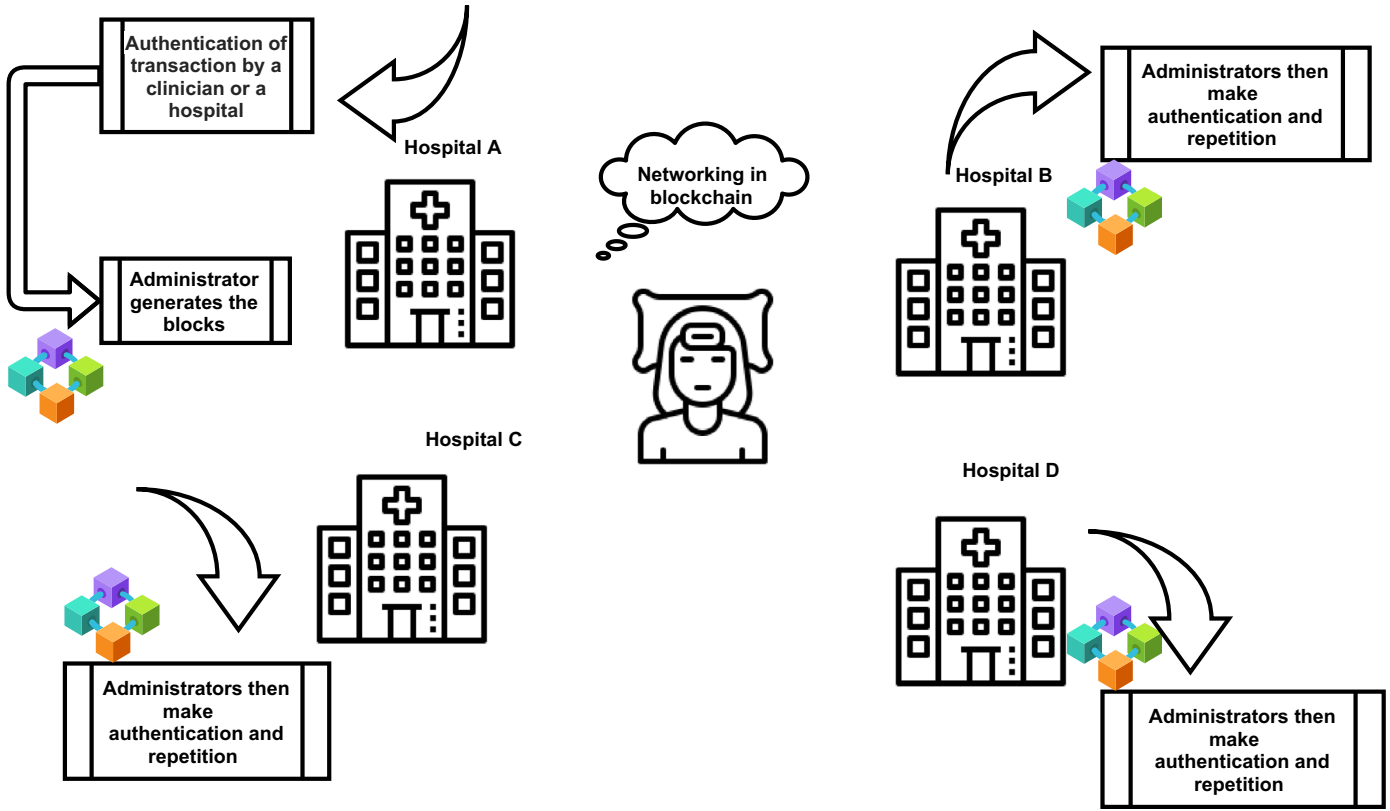

Fig. 7 Flow of health data transfers using blockchain.

information with their medical information, which goes hand in hand with EHR, brings significant privacy and security problems.

7 Healthcare system and blockchain technology

The blockchain is the Internet of the future. We believe that innovation will revolutionize the way that technology facilitates confidence in any system. In any transaction, we believe blockchain would be the most significant single "chain of trust." By eliminating intermediaries from the process, blockchain has the potential to increase the quality of our digital transactions. According to Forrester's "Top 10 Technology Trends to Watch: 2018 to 2021" research, "a viable distributed ledger business will be established" by 2020.

In the healthcare business, a blockchain is a collection of records known as blocks used to keep track of a growing number of online transactions, such as electronic health data (EHR) or EMR. A time stamp and a digital signature are included in each block and link to prior blocks. Several beginning businesses have been researching and developing blockchains for use in the healthcare sector. This shows that people are becoming more aware of the new technology's potential. It is critical to ensure that it is implemented on a large scale rather than simply in one system. However, cloud technology has vastly improved over time, which is excellent news for blockchain enthusiasts because a blockchain needs a lot of electricity to run. A high-end public cloud can assist in overcoming this constraint in the future. In the last few decades, the health sector has remained one of the most popular research areas. Researchers are constantly looking for new and more dependable ways to assist society and the health insurance industry.

The following are some of the blockchain systems that are already in use in various medical systems:

- Medical data are already kept on a blockchain, which makes them safer.
- The healthcare industry has been impacted by several software companies.
- Blockchain technology is already being used in several medication production processes and controls, including recording and storing parameters and providing services and shipments with automated judgments.
- Smart contracts have already been used to establish the stability of medical supplies by storing their temperature histories and monitoring them along the supply chain, including storage, shipping, and administration.
- Doctors might study the drug or treatment in different doses, or with other drugs or treatments.
- Using a blockchain to store and maintain medical data.

Distributed ledgers are all blockchains, but not all blockchain technology is a blockchain. Unlike conventional ledger systems, blockchain does not include a node with special permissions to amend or delete transactions. Blockchain technology is not new; it is a hybrid of numerous existing technologies combined in a novel way. The majority of blockchains rely on six primary technologies:

- Asymmetric encryption, which uses a two-way method of secret keys to secure data.
- Hash functions, which use an integer to validate the integrity of data.
- Merkle trees, which efficiently check data.

The following are some of the ways that blockchain can help healthcare:

Management of complaints and billing: All stakeholders will be aware of their portion of the predicted cost for services if blockchain is used in the claims adjudication and billing management processes. It can cut operating expenses even more by automatic invoicing and health coverage tasks.

Management of medical data: The use of blockchain technology can aid in promoting connectivity and securing healthcare data sharing. The ability to track patients instantaneously improves patient care, which is an important part of providing value-based and profitable care.

Fraud reduction: Fraud costs the healthcare industry more than $95 billion each year. Blockchain can help validate whether a contribution is real by securely collecting data from numerous sources at each step in the transaction, preventing fraudulent behavior. Clinical studies and medical research are two types of things while considering clinical trials. Clinical trials are predicted to go unreported in 70% of cases.

Blockchain improvements can address selective reporting and result manipulations using time-stamped data and results, reducing fraud and inaccuracies in clinical trial records; it is also known as counterfeit medication detection. Counterfeit pharmaceuticals cost medical businesses an estimated $500 billion each year. By documenting each step of the pharmaceutical supply chain at the particular medication level, blockchain might create a "single source of truth" around the flow of commodities and assist in maintaining integrity. They were securing confidential health data Protected Health Information. Between 2015 and 2021, 210 million patient records were compromised, impacting around 38 million patients.

Apart from hackers and malware, internal errors or misconduct accounted for 45% of breaches (220 occurrences). It is possible that the current healthcare IT architecture would not be enough to manage and safeguard linked devices (Internet of medical things [IoMT]). Concerns about privacy and reliability can be alleviated by using cryptocurrency.

7.1 How the blockchain's smart contract can change healthcare

The most powerful feature of blockchain implementation is smart contracts in a blockchain network. Smart contracts, which are part of a blockchain's consensus system, act as a portal for storing essential data on the network. Because most corporate blockchain implementations will be permitted, companies with sufficient permissions will access the data on the blockchain using an application interface (API) without difficulty. While using the API, businesses can request a specific block from the blockchain at any moment. Smart contracts can be thought of as the blockchain's business logic. They are specialized to a business or industry and are unique to each blockchain. Smart contracts, when properly configured, will be able to validate or reject a transaction on the blockchain system. Blockchains are being used in various

settings and can address some of the healthcare industry's most pressing concerns. However, further research is required before real-time implementations of this technology can be deployed. There are four stages to the base classifier into the healthcare sector. The healthcare providers get direct access to the blockchain in the initial stage, and all clinical data are tracked and maintained in existing health IT systems. Patient IDs are used to provide various data connected to patients to the blockchain network via API. Inner transactions are then executed using a consensus protocol on blockchain technology.

All transactions are recorded in the public blockchain using patient public IDs that do not contain any personally identifiable information. The immutable ledger is used to build and chain the blocks. After that, all operations are completed and assigned a unique identifier. As a result, query processing or reverse mining begins with the health provider via APIs. Only semipatient data, such as ethnicity, age, and ailments, are stored in the block database. To gain in-depth knowledge, clinical data are evaluated. Finally, the patient can disclose their private key with the healthcare professional if they desire to share their identity. It is how the provider may have access to the patient's information and offer remedies or treatment for the complaints that have been recognized. To people who do not have the patient's private key, the information is private.

8 Blockchain applications to ensure the privacy and security of EHR

Blockchain technology is an innovation used to address privacy and security issues with EHR data in the cloud in a secured environment. Governments and relevant industrial sectors are becoming increasingly interested in digitalizing health systems, as indicated by various efforts taking place in many nations and industries. The possible advantages of EHR systems (e.g., public healthcare administration, online patient access, and patient medical data exchange) have attracted academic organizations' interest.

Blockchain is a peer-to-peer network-based distributed database that are organized in a chronological sequence. They can mitigate for a single point of failure with blockchain-based technologies. Furthermore, data stored in the distributed ledger and all nodes in the blockchain network have ledger backups that can retrieve this information. From any location, such a system promotes information sharing and aids in developing distributed node trust. It also makes data auditing and transparency easier by allowing users to track tamper-proof historical records in the ledger.

Data in the ledger can be stored in encrypted form using various cryptographic approaches, depending on the actual implementation, ensuring data privacy. Users can also use pseudoanonymity to conceal their true identities. To improve resilience, we can use smart contracts to enable various tasks for various application situations. Users can specify the criteria of the smart contract and will only perform the smart contract if the terms are met or fulfilled.

8.1 Blockchain

The success of Bitcoin helped popularize blockchain, enabling reliable and verified communications through an untrustworthy system without relying on a centralized third party.

In a chronological succession of blocks, a blockchain is a collection of detailed and legal transaction data. Each block is linked to the one before it by a reference (hash value), producing a lengthy chain. The genesis block is the parent block of a given block. The block body is derived from authenticated transactions from a specific time frame. The Merkle tree, in which every leaf node is a transaction, and every nonleaf node is indeed the hash of its two convolutional current nodes, is used to store all transaction details. Because any node could confirm the validity of any payment by the cipher value of the current branches instead of the whole Merkle tree, such a decision tree seems to be efficient for verifying transaction existence and integrity. Meanwhile, any changes to the contract will cause a new hash value to generate in the upper layer, resulting in a fraudulent root hash. Furthermore, the maximum number of users in a block is determined by the size of each money transfer and the block size.

These blocks are then tethered together in an encrypted configuration using a cryptographic hash function. Because it is impossible to change or delete recently identified data, new data are added in increased blocks chained with the preceding block. Any change to one of the blocks, as previously stated, will result in a different hash value and a different link similarity. As a result, integrity and protection are achieved.

8.2 Digital signature

In an unreliable environment, for transaction validation, asymmetric cryptography has well defined the use of storing data. Blockchain uses an asymmetric cryptographic mechanism to send transactions and validate transaction authenticity. It will verify the transfer and the sender's encryption key before being sent via the P2P network. In most extant blockchains, the symmetric encryption electronic signature technique (ECDSA) is used.

8.3 Consensus algorithms

The blockchain network has no central authority. As a result, attaining consensus for these operations among untrustworthy nodes in a distributed system is a major task, as highlighted by the Byzantine generals (BG) challenge. The Byzantine army is circling the area under the direction of a group of generals. According to the BG, they have no chance of success in the battle until they all assault at the exact moment. They are unsure, however, whether there would be traitors in a dispersed context. As a result, they must decide whether to assault or retreat. The blockchain network has the same problem.

8.4 Hashing

When evaluating the authenticity and appropriateness of blocks in consideration, the blockchain uses a consensus algorithm. Blocks are approved or rejected accordingly when a consensus is reached. There are several consensus techniques to choose from,

including proof of work, proof of stake [38], proof of elapsed time, and Kafka [39]. A description of each is beyond the scope of this paper, and we direct the reader to the evidence given for more information.

8.5 Smart contracts

Smart contracts are conscience programs implemented on the blockchain and used in various industries, including service industries, health, and administration. By delivering a contract-invoking transaction to the contractual address, such a system can achieve complicated programmable operations. The consensus mechanism will then automatically execute the specified parameters in a safe environment.

8.6 Motivations for blockchain-based EHR systems

Generally, EHRs often include patient history, personal information (such as age and weight), lab results, and other information. As a result, ensuring the privacy and security of sensitive data is critical. Furthermore, hospitals in countries are subject to stringent regulatory oversight. Implementing and deploying health services in practice also presents several problems. As previously mentioned, centralized server models are prone to single-point attack constraints and malevolent insider assaults. Fig. 8 determines the standard design for database storage in an EHR system.

Users (e.g., patients) who have their information exported or maintained in these EHR systems lose ownership of their data and have no means of understanding who is viewing the data and for what purposes (i.e., violation of personal privacy). Such data may also be in danger of being leaked to some other organization by malicious users; for example, an insurance provider may reject coverage to a patient based on informed medical history. We will now define the essential aims in developing secure blockchain-based EHR systems depending on the specification of the latest iteration of certain EHRs and the character traits of blockchain:

- *Confidentiality*: Personal information will be utilized in a private manner, and only authorized persons will have access to the required information.
- *Security in terms of privacy, authenticity, and accessibility*:
  - *Privacy*: data can be accessed by authorized users.
  - *Authenticity*: data in transit would have to be authentic and not tampered with by an unauthorized entity.
  - *Accessibility*: access to data and knowledge for lawful users is not unfairly withheld.
- Transparency is a crucial aspect of security. Audit records, for example, primarily collect details on who has access to which EHR, for what purpose, and the time stamps of any activity throughout the life cycle [40].
- *Responsibility*: a person or an organization will be audited and held accountable for their actions.
- *Legitimacy*: the capacity to verify requester identities before granting access to sensitive data.
- *Secrecy*: Ensure security; it means that the things have no apparent identity. Absolute anonymity is difficult to achieve, hence pseudoanonymity is more widespread.

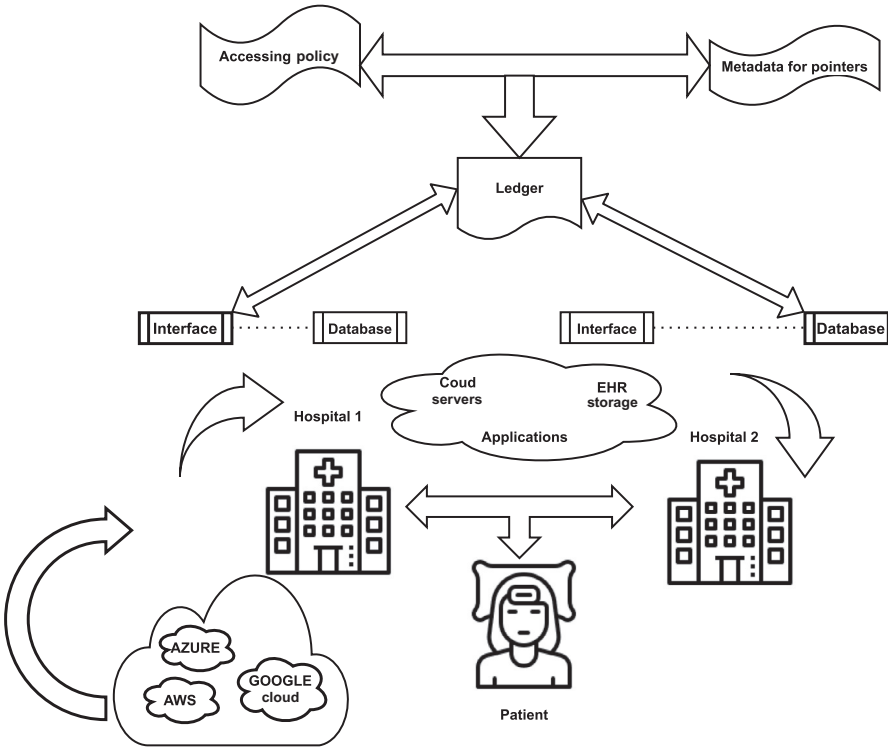

Fig. 8 Standard design for database storage in an EHR system.

9 Conclusion

Blockchain will have its own set of problems and difficulties. It is, nevertheless, a viable idea for allowing public and secured access to medical care data. In general public science and training, blockchain is still not developed enough, even for large-scale commercial adoption. This study discussed many technology products and benefits for 5G safety, such as availability, identification, authenticity, authentication, nonrepudiation, and secrecy, in light of recent developments and appropriate samples for 5G wireless networks.

Current trends such as globalization and digitalization, as stated in the chapter, necessitate change. The move from physical to untrusted virtual parties is one of the most significant adjustments brought about by these trends. The shift away from the old idea of trust necessitates a system that supports the new perspective. A distributed ledger device is expected to provide an additional degree of trust due to its architectural design. This layer establishes a standardized platform to make procedures more accessible around the globe. Healthcare data have value, especially given the vast amount of data available. It can reward data donors with a blockchain token.

It is critical to have an incentive program incorporated into the solution to keep the chain running smoothly. Create an interface that helps patients to contribute their

information anonymously. It must determine the valuation method for various types of data. Another fascinating topic is connectivity between different public blockchains. It is likely that numerous blockchain systems, including those for medicine, would interact with one another. We can agree that all parties benefit from information processing and research and that confidentiality should be preserved and improved as technology advances. This concept proposes using a distributed ledger in 5G networks to encrypt data in cognitive health services and avoid potential fraud. When it comes to application, blockchain technology has various issues that need to be addressed with more research. Challenges to the study's validity, as described earlier, could lead to improved future research work.

References

[1] E. Gökalp, M.O. Gökalp, S. Çoban, P.E. Eren, Analysing opportunities and challenges of integrated blockchain technologies in healthcare, in: Eurosymposium on Systems Analysis and Design, Springer, 2018, pp. 174–183.
[2] R. Gupta, U. Thakker, S. Tanwar, M.S. Obaidat, K.-F. Hsiao, Bits: a blockchain-driven intelligent scheme for telesurgery system, in: 2020 International Conference on Computer, Information and Telecommunication Systems (CITS), IEEE, 2020, pp. 1–5.
[3] R. Gupta, S. Tanwar, S. Tyagi, N. Kumar, M.S. Obaidat, B. Sadoun, HaBiTs: blockchain-based telesurgery framework for Healthcare 4.0, in: 2019 International Conference on Computer, Information and Telecommunication Systems (CITS), IEEE, 2019, pp. 1–5.
[4] R. Gupta, A. Shukla, S. Tanwar, Aayush: a smart contract-based telesurgery system for Healthcare 4.0, in: 2020 IEEE International Conference on Communications Workshops (ICC Workshops), IEEE, 2020, pp. 1–6.
[5] J. Hathaliya, P. Sharma, S. Tanwar, R. Gupta, Blockchain-based remote patient monitoring in Healthcare 4.0, in: 2019 IEEE ninth International Conference on Advanced Computing (IACC), IEEE, 2019, pp. 87–91.
[6] I. Mistry, S. Tanwar, S. Tyagi, N. Kumar, Blockchain for 5G-enabled IoT for industrial automation: a systematic review, solutions, and challenges, Mech. Syst. Signal Process. 135 (2020) 106382.
[7] A. Ismail, S. Abdelrazek, I. Elhenawy, IoT wearable devices for health issue monitoring using 5G networks' opportunities and challenges, in: Blockchain for 5G-Enabled IoT, Springer, 2021, pp. 521–530.
[8] R. Gupta, S. Tanwar, S. Tyagi, N. Kumar, Tactile-internet-based telesurgery system for Healthcare 4.0: an architecture, research challenges, and future directions, IEEE Netw. 33 (6) (2019) 22–29.
[9] L. Ismail, H. Materwala, Blockchain paradigm for healthcare: performance evaluation, Symmetry 12 (8) (2020) 1200.
[10] H. Li, H. Huang, S. Tan, N. Zhang, X. Fu, X. Tao, A new revocable reputation evaluation system based on blockchain, Int. J. High Perform. Comput. Netw. 14 (3) (2019) 385–396.
[11] C. Stergiou, K.E. Psannis, B.B. Gupta, Y. Ishibashi, Security, privacy & efficiency of sustainable cloud computing for big data & IoT, Sustain. Comput. Inf. Syst. 19 (2018) 174–184.
[12] A. Tewari, B.B. Gupta, Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework, Future Gener. Comput. Syst. 108 (2020) 909–920.
[13] S. Berenjian, S. Hajizadeh, R.E. Atani, An incentive security model to provide fairness for peer-to-peer networks, in: 2019 IEEE Conference on Application, Information and Network Security (AINS), IEEE, 2019, pp. 71–76.

[14] A. Naghizadeh, S. Berenjian, E. Meamari, R.E. Atani, Structural-based tunneling: preserving mutual anonymity for circular P2P networks, Int. J. Commun. Syst. 29 (3) (2016) 602–619.
[15] A. Naghizadeh, S. Berenjian, B. Razeghi, S. Shahanggar, N.R. Pour, Preserving receiver's anonymity for circular structured P2P networks, in: 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), IEEE, 2015, pp. 71–76.
[16] J.D. Halamka, A. Lippman, A. Ekblaw, The potential for blockchain to transform electronic health records, Harv. Bus. Rev. 3 (3) (2017) 2–5.
[17] J. Benet, IPFS-content addressed, versioned, P2P file system, arXiv preprint arXiv:1407.3561 (2014).
[18] V. Patel, A framework for secure and decentralized sharing of medical imaging data via blockchain consensus, Health Inf. J. 25 (4) (2019) 1398–1411.
[19] S. Kokolakis, Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon, Comput. Secur. 64 (2017) 122–134.
[20] N. Kshetri, Blockchain's roles in strengthening cybersecurity and protecting privacy, Telecommun. Policy 41 (10) (2017) 1027–1038.
[21] I. Lapowsky, How Cambridge analytica sparked the great privacy awakening, Wired (2019).
[22] R. Maull, P. Godsiff, C. Mulligan, A. Brown, B. Kewell, Distributed ledger technology: applications and implications, Strateg. Change 26 (5) (2017) 481–489.
[23] Q. Zhang, J. Liu, G. Zhao, Towards 5G enabled tactile robotic telesurgery, arXiv preprint arXiv:1803.03586 (2018).
[24] A. VishwaVidyapeetham, A blockchain and IPFS based framework for secure research record keeping, Int. J. Pure Appl. Math. 119 (15) (2018) 1437–1442.
[25] L. Lévêque, W. Zhang, C. Cavaro-Ménard, P. Le Callet, H. Liu, Study of video quality assessment for telesurgery, IEEE Access 5 (2017) 9990–9999.
[26] Y. Miao, Y. Jiang, L. Peng, M.S. Hossain, G. Muhammad, Telesurgery robot based on 5G tactile internet, Mobile Netw. Appl. 23 (6) (2018) 1645–1654.
[27] G.E. Simon, S.M. Shortreed, R.Y. Coley, R.B. Penfold, R.C. Rossom, B.E. Waitzfelder, K. Sanchez, F.L. Lynch, Assessing and minimizing re-identification risk in research data derived from health care records, eGEMs 7 (1) (2019), https://doi.org/10.5334/egems.270.
[28] M. Atzori, Blockchain technology and decentralized governance: is the state still necessary? Available at SSRN 2709713 (2015).
[29] M. Simonov, U. Ugwuowo, E. Moreira, Y. Yamamoto, A. Biswas, M. Martin, J. Testani, F.P. Wilson, A simple real-time model for predicting acute kidney injury in hospitalized patients in the US: a descriptive modeling study, PLoS Med. 16 (7) (2019) e1002861.
[30] J. Zhang, Y. Chen, S. Ashfaq, K. Bell, A. Calvitti, N.J. Farber, M.T. Gabuzda, B. Gray, L. Liu, S. Rick, Strategizing EHR use to achieve patient-centered care in exam rooms: a qualitative study on primary care providers, J. Am. Med. Inf. Assoc. 23 (1) (2016) 137–143.
[31] G.O. Ginn, J.J. Shen, C.B. Moseley, Hospital financial position and the adoption of electronic health records, J. Healthc. Manag. 56 (5) (2011) 337–352.
[32] S.A. Hussein, A.A. Al-Saboonchi, S.A. Al-Haji, Monthly variation in density of attached algae on solid plates in two lentic lotic localities from Basrah Province, Basrah J. Agric. Sci. 26 (1) (2013) 15–26.
[33] T.K. Mackey, T.-T. Kuo, B. Gummadi, K.A. Clauson, G. Church, D. Grishin, K. Obbad, R. Barkovich, M. Palombini, "Fit-for-purpose?"-challenges and opportunities for applications of blockchain technology in the future of healthcare, BMC Med. 17 (1) (2019) 1–17.

[34] A. Ozanne, D. Johansson, U. Hällgren Graneheim, K. Malmgren, F. Bergquist, M. Alt Murphy, Wearables in epilepsy and Parkinson's disease—a focus group study, Acta Neurol. Scand. 137 (2) (2018) 188–194.
[35] A. Ayadi, O. Ghorbel, A.M. Obeid, M. Abid, Outlier detection approaches for wireless sensor networks: a survey, Comput. Netw. 129 (2017) 319–333.
[36] I.J. Kullo, J. Olson, X. Fan, M. Jose, M. Safarova, C.R. Breitkopf, E. Winkler, D.C. Kochan, S. Snipes, J.E. Pacyna, The return of actionable variants empirical (RAVE) study, a Mayo clinic genomic medicine implementation study: design and initial results, in: Mayo Clinic Proc., vol. 93, Elsevier, 2018, pp. 1600–1610.
[37] C.J. Pirtle, J.M. Ehrenfeld, Information technology and patient protection, in: Precision Medicine for Investigators, Practitioners and Providers, Elsevier, 2020, pp. 511–517.
[38] F. Saleh, Blockchain without waste: proof-of-stake, Rev. Financ. Stud. 34 (3) (2021) 1156–1190.
[39] G. Wang, L. Chen, A. Dikshit, J. Gustafson, B. Chen, M.J. Sax, J. Roesler, S. Blee-Goldman, B. Cadonna, A. Mehta, Consistency and completeness: rethinking distributed stream processing in apache Kafka, in: Proceedings of the 2021 International Conference on Management of Data, 2021, pp. 2602–2613.
[40] M. Mashuri, M. Ahsan, M.H. Lee, D.D. Prastyo, PCA-based Hotelling's T2 chart with fast minimum covariance determinant (FMCD) estimator and Kernel density estimation (KDE) for network intrusion detection, Comput. Indus. Eng. 158 (2021) 107447.