Proof Central

Please use this PDF proof to check the layout of your chapter. If you would like any changes to be made to the layout, you can leave instructions in the online proofing interface. First, return to the online proofing interface by clicking "Edit" at the top page, then insert a Comment in the relevant location. Making your changes directly in the online proofing interface is the quickest, easiest way to correct and submit your proof.

Please note that changes made to the chapter in the online proofing interface will be added to the chapter before publication, but are not reflected in this PDF proof.

AUTHOR QUERY FORM

ELSEVIER	**Book:** DAS-9780323994811 **Chapter:** 05	**Please e-mail your responses and any corrections to:** **E-mail: s.pk@elsevier.com**

Dear Author,

Any queries or remarks that have arisen during the processing of your manuscript are listed below and are highlighted by flags in the proof. (AU indicates author queries; ED indicates editor queries; and TS/TY indicates typesetter queries.) Please check your proof carefully and answer all AU queries. Mark all corrections and query answers at the appropriate place in the proof using on-screen annotation in the PDF file. For a written tutorial on how to annotate PDFs, click http://www.elsevier.com/__data/assets/pdf_file/0007/98953/Annotating-PDFs-Adobe-Reader-9-X-or-XI.pdf. A video tutorial is also available at http://www.screencast.com/t/9OIDFhihgE9a. Alternatively, you may compile them in a separate list and tick off below to indicate that you have answered the query.

Please return your input as instructed by the project manager.

Location in Chapter	Query / Remark	
AU:1, page 1	Please check the chapter title and amend if necessary.	□
AU:2, page 1	Please verify and confirm the authorship details (author name and surname, affiliation, spelling of author’s name and author’s order) and amend if necessary.	□
AU:3, page 1	Please provide complete affiliation details (e.g., Institution or Organization, City, State (US, Canada, and Australia), and Country) for the authors “Ramchandra, Mangrulkar”	□

CHAPTER

5

c0005 [AU1] Enabling blockchain architecture for health information exchanges

[AU2] *Ramchandra Mangrulkar*[1] *and Nirali Parekh*[2]

[AU3] [1]&squf; [2]**Dwarkadas J. Sanghvi College of Engineering, Mumbai, India**

s0010 1. Introduction

p0010 Every day, terabytes of new data are created in the healthcare sector from laboratory reports, medical records, clinical trials, device monitoring, and other sources. They are all stored as electronic health records or EHRs. However, these are frequently buried in several distinct, isolated databases. The data are frequently outdated as a result of these discrepancies, resulting in diagnoses and treatments that are incorrect.[1] This problem has been solved through a health information exchange (HIE). An HIE is a secure central repository for patient data gathered from different facilities and EHR systems in the same geographic area. Through a secure, standardized system, the objective is to offer a holistic view of the patient's EHR.

p0015 An HIE allows medical institutions, clinicians, and patients to exchange health-related data electronically. Unlike traditional paper health records, electronic HIE allows healthcare providers and professionals, such as doctors and physicians, to securely access and exchange essential clinical data online.[2] An HIE stores previous medical history, clinical notes, lab reports and results, current medications, and other patient data. As a result, using an HIE streamlines a patient's data and connects a practitioner to all aspects of a patient's medical history. These centralized HIEs, despite restricted access and identity, cannot ensure data integrity or security. While information sharing between EHR systems and HIEs is HIPAA-compliant, the increasing frequency of cybersecurity breaches has raised concerns about the security of health data. Data breaches have exposed over 15 million health records, according to the U.S. Department of Health and Human Services Breach Report.[3] Furthermore, data breaches in healthcare are particularly costly compared to other industries. The flaws of the current system are critical and thus cannot be overlooked, necessitating the development of a new solution for sharing electronic medical records (EMRs) that is more secure, reliable, and capable of handling all the data privacy, data redundancy, and other security-related issues related to HIE system.[4]

https://doi.org/10.1016/B978-0-323-99481-1.00011-0

p0020 Blockchain offers several properties that make it appealing to any industry, particularly healthcare. Blockchain, according to a CBInsights' 2018 research study,[5] can help alleviate some of the healthcare industry's most pressing problems. One of the valuable applications of blockchain includes strengthening supply chain integrity. Every transaction between medicine producers, distributors, pharmacists, and patients may be verified using blockchain, and the process can be secured. Counterfeit drugs also have been addressed by some works[6–8] where authors propose an irreversible, robust, and trackable pharmaceutical supply chain based on blockchain to combat counterfeiting.

p0025 Another potential use of blockchain in healthcare is to design HIE systems to integrate a patient's medical data from several EHRs into a single, up-to-date, and tamper-resistant record. According to one research, full interoperability is predicted to save the US healthcare system $77.8 billion each year.[9] However, there are few studies on the practical implementation of blockchain in HIE. Furthermore, there has been minimal research strategy of its exposure to blockchain technology. From a practical standpoint, this chapter can be beneficial for HIE policymakers, healthcare specialists, and technical audiences to learn about the architectural designs, difficulties, and implementation of blockchain-based HIE models.

p0030 This chapter delves deeper into the use of blockchain-based HIE systems to enable national interoperability. The rest of the chapter is organized as follows: Section 2 discusses current HIE systems, their architecture models, and pitfalls. Section 3 provides an overview of blockchain as a technology, as well as its many types and properties. Section 4 describes the architectural basis for scalability and data flow in blockchain-based HIE systems. Section 5 discusses the difficulties and flaws in putting these concepts into effect. Our conclusions are presented in Section 6.

s0015 2. Traditional health information exchanges

p0035 The procedure of electronic transmission of patient health information and medical data across healthcare providers and institutions is used in traditional HIE systems (Fig. 5.1). Interoperability in HIE initiatives necessitates electronic communication across organizations to ensure that patient medical records from one healthcare institution are easily integrated into another.

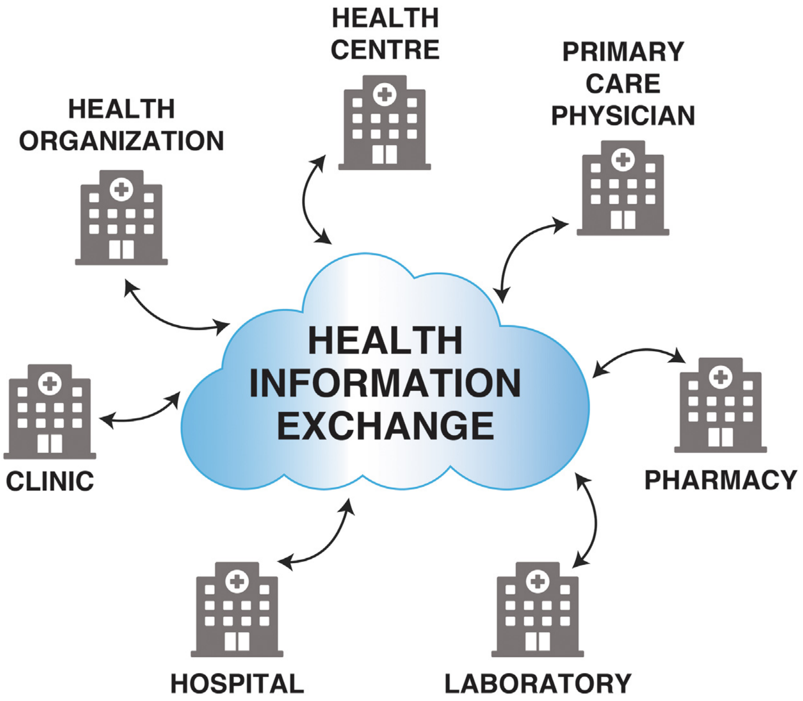
p0040 Essentially, in an ideal interoperable healthcare system, all medical information on a patient collected throughout their life could be safely incorporated into the patient's unique ID. This would contain diagnostics, past surgeries, laboratory tests, allergies, along with logs from smart wearable devices and third-party testing results. The advantages of HIE are numerous and varied. Some of them are:

o0010 **1.** It eliminates redundancy and unnecessary paperwork by streamlining the entire healthcare process.

o0015 **2.** It decreases medication errors and inaccurate diagnoses, hence improving patient care quality.

o0020 **3.** It reduces a country's or an institution's overall healthcare expenditures.

o0025 **4.** It enables healthcare professionals and academics to successfully deliver public health feedback and reports.



f0010 FIGURE 5.1 Traditional HIE system.

p0065 This section discusses the most prevalent architectural models used in HIE systems and healthcare, as well as their limits and drawbacks, which demand the use of other solutions. This summary will support the need for a forthcoming description of proposed blockchain architectures and their effectiveness.

s0020 2.1 Architectural models for an HIE system

p0070 In healthcare, three HIE architectural models are typically used.[10] Regardless of the data model used, the HIE system's degree of privacy and security must be robust and trustworthy.

s0025 2.1.1 *Centralized HIE system*

p0075 A centralized exchange design collects health data in a central repository such as a data warehouse. In this model, the entity that manages the exchange has complete control over data sharing. Controlling the exchange of data and records as well as the authorization and authentication procedure for accessing the data and records are all controlled centrally. Some of the challenges of centralized HIE systems are the implementation of an efficient patient matching algorithm and the risk of data emission leading to erroneous or incomplete data.

s0030 2.1.2 *Federated HIE system*

p0080 Federated HIE systems, also known as distributed or decentralized HIE systems, are comprised of several sources, such as separate healthcare organizations. Data collection and authorization are performed on a need-to-know basis, ensuring that the responses are always current and up-to-date. A single governing body administers a Record Locator Service to facilitate data transmission using conventional integration methods. This model avoids the risks of establishing a centralized database, which, if hacked, might reveal a massive quantity of data. This model is not ideal either. Patient matching algorithms, as well as maintaining a huge number of connections and ensuring that they are constantly operational, are among the problems it confronts. When compared to centralized systems, it is considered to be far more secure.

s0035 *2.1.3 Hybrid HIE system*

p0085 This model combines the advantages of both centralized and decentralized models. Storing critical parts in logically isolated ’vaults’ administered in a central place. The participants not only retain ownership of their data, but they also specify how that data can be utilized by the exchange. Data ownership and control can be retained by participating entities. In this architecture, the HIE database processes information requests, which are subsequently distributed across the network.

s0040 2.2 Pitfalls in traditional HIE systems

p0090 In this age of the internet, the most immediate risks are privacy and security concerns. Individuals rely on internet networks to store and share their private health data without robust security; thus they are susceptible to cyber-criminals, malevolent corporations. The domain’s primary issue is to ensure information availability while ensuring secrecy and integrity. Because any breach with one HIE would have a long-term impact on all HIE activities, all HIEs are acutely aware of the necessity of data security.[11]

p0095 The following are the various pain points of existing HIE systems:

o0030 1. **Varying data standards:** While transferring information via the internet, the various EHRs adhere to their own set of standards and guidelines.[12] Due to various standards, most providers are unable to comply with regulations mandating them to share patients’ health data with other doctors.

o0035 2. **High cost per transaction:** The purchase price, implementation, involvement in local or state healthcare units, and vendor transaction fees, all contribute to HIE’s overall costly affair.

o0040 3. **Unsynchronized records and multiple patient identifiers:** Due to similarities in patients having the same names, year of birth, and living in the same locations, it might be difficult to match patients’ identifiers with their accurate health information.

o0045 4. **Patient consent:** Patient rights and authorization can be important problems when it comes to health information. If the information is disseminated without the patient’s agreement, it may lead to legal action. Furthermore, patients frequently grant authorization for some platforms but not others, which again contributes to inconsistencies in data.

p0120 These are some of the ongoing issues that must be addressed by a system that can record digital transactions and build irreversible and deployable information while ensuring security against fraud. Given these shortcomings, a new solution must be developed to share medical records, keeping the confidentiality and integrity of the data in mind. In January 2018 alone, more than 4 lakh individuals were affected by data breaches of traditional HIE systems,[3] which could have been prevented by using more secure, reliable, and uncentralized solutions.

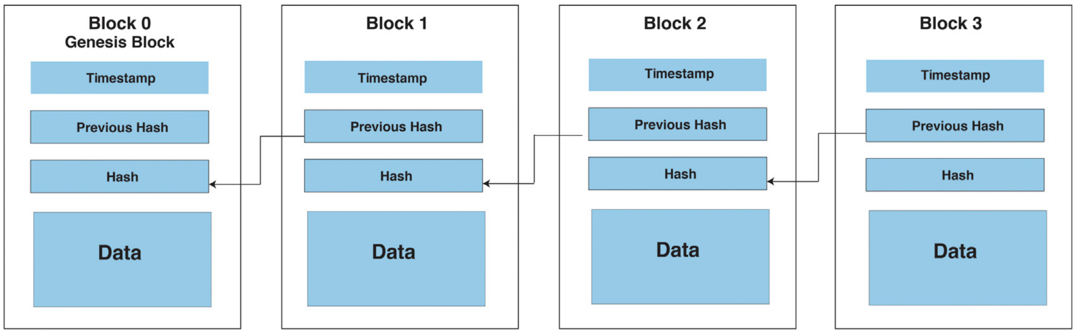
s0045 3. Blockchain technology—theory and philosophy

s0050 3.1 Blockchain basics

p0125 The word “Blockchain” has captivated many since the inception of Bitcoin in 2008 by Satoshi Nakamoto[13] since the possibilities of such technology are truly significant. For the first time in human history, individuals trust each other and transact within massive peer-to-peer networks without centralized administration. Trust is established not by centralized institutions but by rules, cryptography, and computer code.

p0130 Blockchain is a combination of protocols and encryption methods for keeping data securely over a distributed network. Blockchain is simply a distributed secure database made up of a series of blocks, each of which contains a record of data that has been encrypted.[14] Every computer on the blockchain network has a copy of the block database, which is referred to as a ledger (Fig. 5.2). This block relies on a distributed consensus method to make an entry into the blockchain because there is no centralized component to validate the modifications to the database. The blockchain is made up of multiple such blocks linked together in a chain in a linear chronological sequence, with each block consisting mostly of three elements: data, the block’s hash, and the preceding block’s hash. Because each block has a hash value that is reliant on the hash of the preceding block, they are all linked together, which means that if one is modified, all subsequent blocks connected to it will be changed as well. A hash, like a fingerprint, identifies all of the contents of a block and is always unique. The hash of a block is determined after it is generated and it will change if something inside the block is changed. In other words, hashes are quite effective for detecting changes in a block.

p0135 When a single block is tampered with, all subsequent blocks become invalid. However, this is not enough to make a blockchain entirely secure. Due to today’s enormous processing



f0015 FIGURE 5.2 **Basic structure of a blockchain.**

capacity, instantly calculating the hashes of all subsequent blocks in a blockchain is relatively simple. Proof-of-work[15] has been implemented to slow down the production of new blocks to alleviate this. Calculating proof-of-work takes longer; for example, calculating proof-of-work for a bitcoin takes around 10 min. Because recalculating proof-of-work for all blocks and each node in the network takes time, this technique makes it exceedingly difficult. This is why it is nearly difficult to tamper with data after it has been stored in a blockchain.[16] The blockchain's security stems from its innovative use of hashing and the proof-of-work method.

s0055 3.2 Taxonomy of blockchain systems

p0140 There are three types of blockchain systems currently in use: public blockchain, consortium blockchain, and private blockchain.[17] A comparison of these forms of blockchain from various aspects[18] is given in Table 5.1.

s0060 3.3 The three principles of blockchain

s0065 3.3.1 *Immutability*

p0145 The inability to change or alter something is referred to as immutability. This is one of the most essential elements of Blockchain technology for guaranteeing that it remains what it is—a permanent, immutable network.[19] Rather than relying on centralized authority, it ensures blockchain functionality through a network of nodes.[20] Each node must first validate the transaction's legitimacy before adding it. It is recorded in the ledger if the majority agrees

t0010 **TABLE 5.1** Blockchain systems comparison between private, public, and consortium blockchain.

Attribute	Public blockchain	Consortium blockchain	Private blockchain
Structure	Decentralized	Semidecentralized	Centralized
Consensus process	Permissionless	Permissioned	Permissioned
Consensus determination	All miners	A selected set of nodes	One organization
Bias among nodes	None	Present	Present
Immutability	Almost impossible	Difficult to tamper	Easier to tamper than consortium blockchain
Centralized	No	Partial	Yes
Read permission	All nodes	A selected set of nodes	A selected set of nodes
Transparency	High	Low	Low
Examples	Ethereum, bitcoin	Quorum, hyperledger, and corda	Internal business operations

that it is correct. This improves openness while also making the system resistant to corruption. As a result, no transaction blocks may be added to the ledger without the consent of the majority. After the transaction blocks have been added to the ledger, no one can change them, which means that no one on the network will be able to modify, remove, or update them.

s0070 3.3.2 *Decentralization*

p0150 Blockchain is decentralized, which implies there is no governing authority or one individual in charge of the infrastructure.[21] The network is not centralized, instead maintained by a collection of nodes. We can access the system straight from the web and keep our assets there because it does not require any regulating authority. The decentralized system restores the individuals' power and rights over their assets. Users now have power over their data, thanks to blockchain and decentralization. There is no additional danger because there is no third party involved.

s0075 3.3.3 *Security*

p0155 Authentication and authorization can be used to ensure security in the blockchain. To manage and restrict access, rules and permissions can be defined. Every transaction that takes place between entities in a network may be digitally signed and validated using a private/public key to secure the transaction's identity. To preserve confidentiality, the transaction's payload, or actual data, is encrypted using crypto hash techniques. A private blockchain can only be viewed and updated through access control restrictions, whereas in a public blockchain, such as bitcoin and Ethereum,[22] every node in the network has visibility and access to the transaction and block generation. Cryptography adds another degree of security to users' protection. Changing or attempting to tamper with the data will result in all hash IDs being changed. And correcting all the hashes is nearly impossible owing to the distributed nature of blockchain.

s0080 3.4 Blockchain-based HIE as an alternative

p0160 Traditional HIE systems' shortcomings lead us to innovations that guarantee total immutability and consensus. The security, dependability, data privacy, and redundancy of the blockchain-based solution will benefit the healthcare information exchange system.[23] These features of blockchain can be extremely beneficial in improving the efficiency of HIEs. The following are some of the advantages and enhancements that blockchain provides.

s0085 3.4.1 *Security enhancing*

p0165 The ledger would be impossible to compromise due to the immutable nature of the transactions, which is based on cryptography. This revolutionary technology is said to be impenetrable.[24]

s0090 3.4.2 *Interoperability enabling*

p0170 Due to the blockchain, healthcare units, patients, insurers, and researchers can tackle data sharing and availability issues due to a network of nodes in a blockchain. It makes the promotion of data access and operation simpler across organizations.[25]

s0095 3.4.3 *Trust*

p0175 Blockchain eliminates the need for a central authority due to its decentralized nature and distributed ledger structure.[10] As a consequence, patients' trust and security are enhanced because no single authority has access to all of the data.

s0100 3.4.4 *Traceability and transparency*

p0180 Healthcare organizations can constantly maintain track of financial information and have accurate information on each transaction. Because of the immutability of blockchain, accountability is possible.

s0105 3.4.5 *Opt-out intention*

p0185 When providers begin to join, they must give each patient notice of health information practices, including their choice to opt-out of having their information shared through the HIE, as required by law. Patients can then either confirm the notification or opt-out of having their information shared through the HIE. If a patient opts out, no provider, even in an emergency, can access any of the patient's information from HIE.

s0110 3.4.6 *Data ownership*

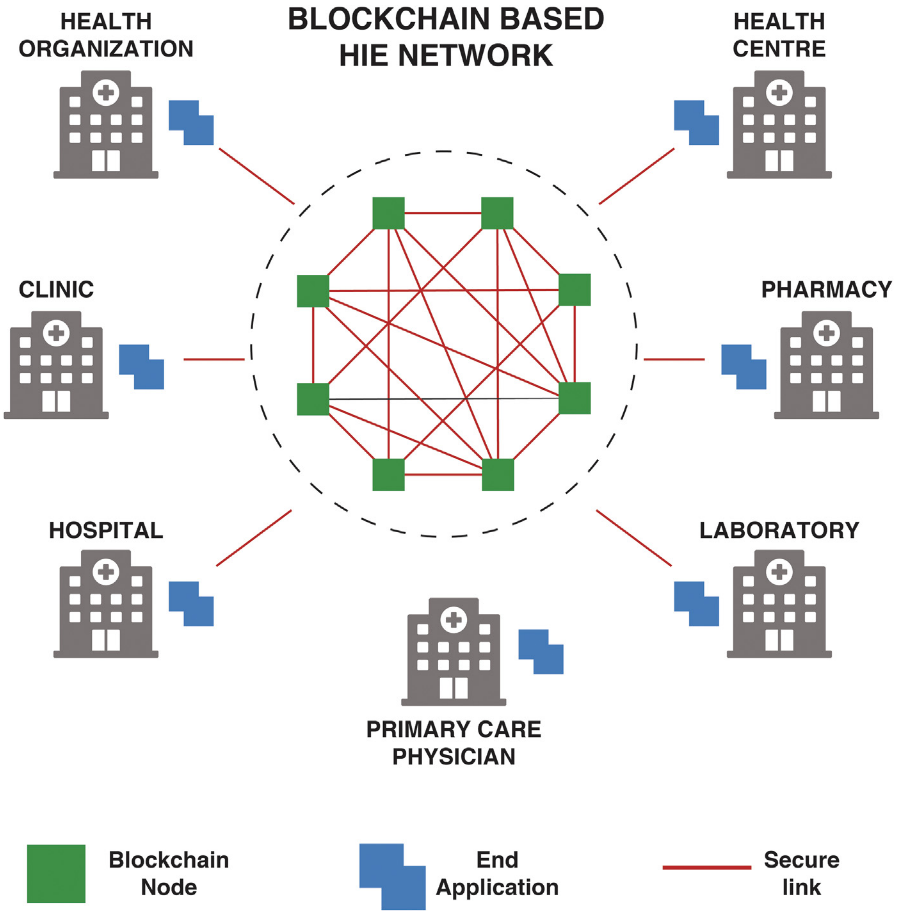
p0190 In a blockchain-based HIE system, healthcare providers would require encrypted keys to acquire information from patients, and patients would be able to choose who gets access to their medical records and when. Patients may preauthorize data sharing with authorized providers in the case of an emergency, as well as select research entities to lend their data to, without actually delivering the data.

s0115 3.4.7 *Business value*

p0195 Blockchain eliminates the need for intermediaries in the data exchange process. It protects data and makes managing insurance claims, personal health information, and other medical papers much easier.[26] It will also reduce the cost of present intermediaries and improve information flow efficiency.

s0120 4. Health information exchange architectures based on blockchain

p0200 One of the primary requirements of enterprise architecture for HIEs to adopt blockchain technology is that they should store and exchange clinical data smoothly among patients, health organizations, and healthcare providers (Fig. 5.3). For example, HIE systems can leverage enterprise Blockchain as a Service (BaaS) to manage comprehensive health data. The three architectural levels described by the Zachman Framework[27] represent different degrees of abstraction at which the enterprise can be modeled. This section will first outline some of the essential components of blockchain in the context of an HIE. Later, it explores how medical data are created and accessed in a blockchain-based architecture from the three architectural levels—conceptual, logical, and physical level.



f0020 FIGURE 5.3 **Blockchain-based HIE systems.**

s0125 4.1 Components in a blockchain-based HIE architecture

p0205 The following are the main building blocks that can be thought of as the architectural cornerstones of a business blockchain.

s0130 *4.1.1 Distributed ledger*

p0210 A blockchain is essentially a distributed ledger that records immutable digital data in discrete packets known as blocks. It's a database that stores all of the transactions in a specific business network in chronological order. As a result, in an HIE, a blockchain would act as a ledger that could be shared with patients and healthcare providers. They have access to the data because they have the required permissions and roles. Because of the immutability and distributed nature of blockchain, it is difficult to change data contained in the HIE architecture. Furthermore, once the health records are stored in the ledger, tampering, stealing, or altering them is impossible.[28] It also saves money on healthcare management by eliminating the costs of reconciling medical data from various sources. Consensus helps the network members in preserving control over their personal health information.

s0135 *4.1.2 Nodes*

p0215 Nodes are the most important crucial component and the backbone of this HIE Blockchain model. When a new medical record entry is added, all nodes in the HIE network create a peer model and collaborate to reach a consensus. As a result, they validate and execute transactions to maintain the network's integrity. Miners, validators, monitoring nodes, and other responsibilities are assigned to each node in a blockchain-based HIE system. As a consequence, by performing their duty, they help to make the blockchain more resilient, consistent, and secure.

s0140 *4.1.3 Smart contract*

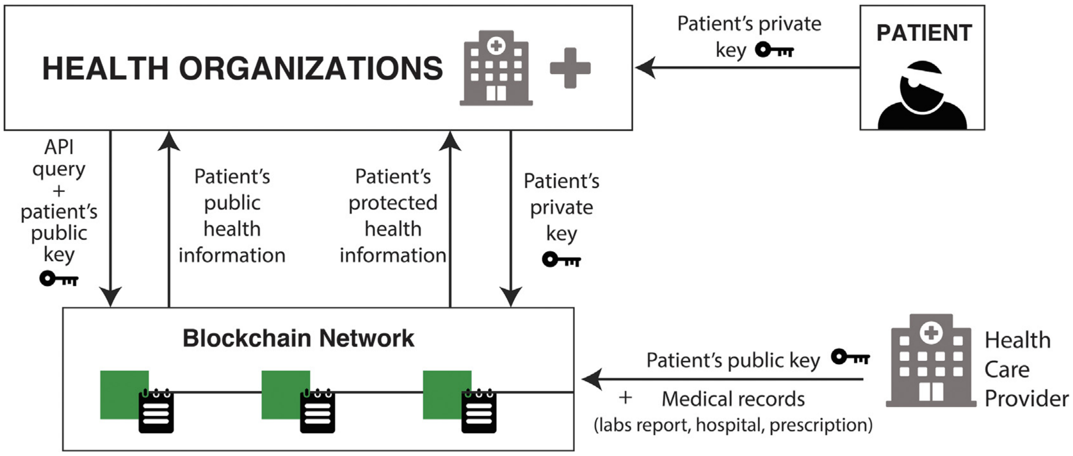
p0220 Smart contracts were introduced in Blockchain 2.0, a newer version of the blockchain.[29] It's a contract in which software code written in a programming language like Java or NodeJS specifies and executes transactions. It's the sum of the real driving business logic and conditional rules that determines how this transaction will be carried out. The patient's authorization for accessing and sharing his or her medical data will be stored in a blockchain-based HIE architecture. More healthcare companies are putting a premium on trustworthy automation and cutting-edge security. Smart contracts are used to securely store patient data on a blockchain, which can only be accessed with the patient's private key. Patients may be confident that their medical providers will always have access to the information they need and that their data will be kept safe. Smart contracts are secured via encryption and digital signature.

s0145 *4.1.4 Consensus*

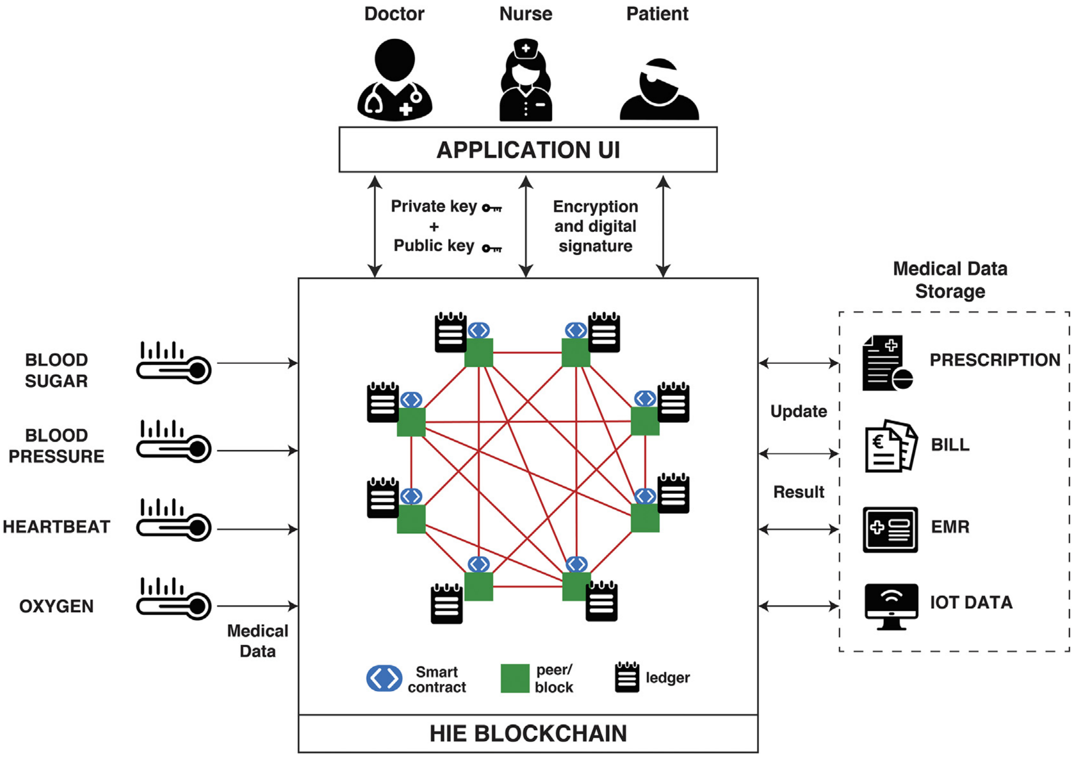
p0225 The term "consensus" indicates "majority agreement." Each node in a blockchain has its copy of the ledger, which is synced when a new transaction occurs. When all nodes in the network validate and approve a new transaction, the blockchain is considered to be in consensus.[30] Consensus ensures the integrity of the HIE network. The agreement cannot be broken by any type of corruption or hacking of protected medical data. As a result, they give the HIEs a level of confidence. Some of the most often used consensus protocols are Proof-of-Work,[15] Proof-of-Stake,[31] and Byzantine General's Problem.[32]

s0150 4.2 Conceptual and logical architecture

p0230 The conceptual architecture is the most abstract of the three architectural levels. This model highlights the high-level relationships between entities like patients, health organizations, and medical data. Conceptual architecture creates a concise image of the HIE architecture using blockchain and its strategic objectives, without going into the technical details. The conceptual design of an HIE system based on blockchain is shown in Fig. 5.4 built on the work by Hang et al.[33] In terms of function and logical information, logical architecture defines how a solution operates. The abstraction given in the conceptual view is scrutinized further in this level (Fig. 5.5), which includes information on the blockchain architecture, medical health data, and storage.



f0025 FIGURE 5.4 **Conceptual architectural model—medical data creation, access, and flow in a blockchain-based HIE architecture.** *Modified from Hang, L., Choi, E. and Kim, D. H. (2019). A novel EMR integrity management based on a medical blockchain platform in hospital.* Electronics*, 8(4).* *https://doi.org/10.3390/electronics8040467*



f0030 FIGURE 5.5 **Logical architectural model: a closer look at the interactions between blockchain network and medical data flow for HIE systems.**

4.2.1 Data creating and updating

p0235 The patient shares their private key to health organizations. This key is used to access confidential health data of the patient further from the blockchain network. Also, the healthcare providers like laboratories and hospitals send the clinical data to the blockchain network using the patient's public key.

s0160 *4.2.2 Transaction processing and storage*

p0240 After the creation of the record in the blockchain, each new update and modification to the patient's medical history is logged on the blockchain (without any personal information) using their public ID.

s0165 *4.2.3 Data query*

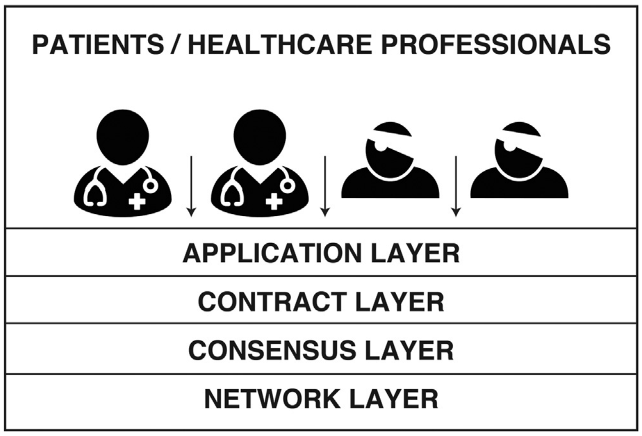
p0245 For patients who have opted-in for sharing their private data, health organizations can request that information using the patients' private key and get access to their confidential medical data. Also, patients whose public data are permitted to be accessed can be shared for research.

s0170 *4.2.4 Patient's data sharing*

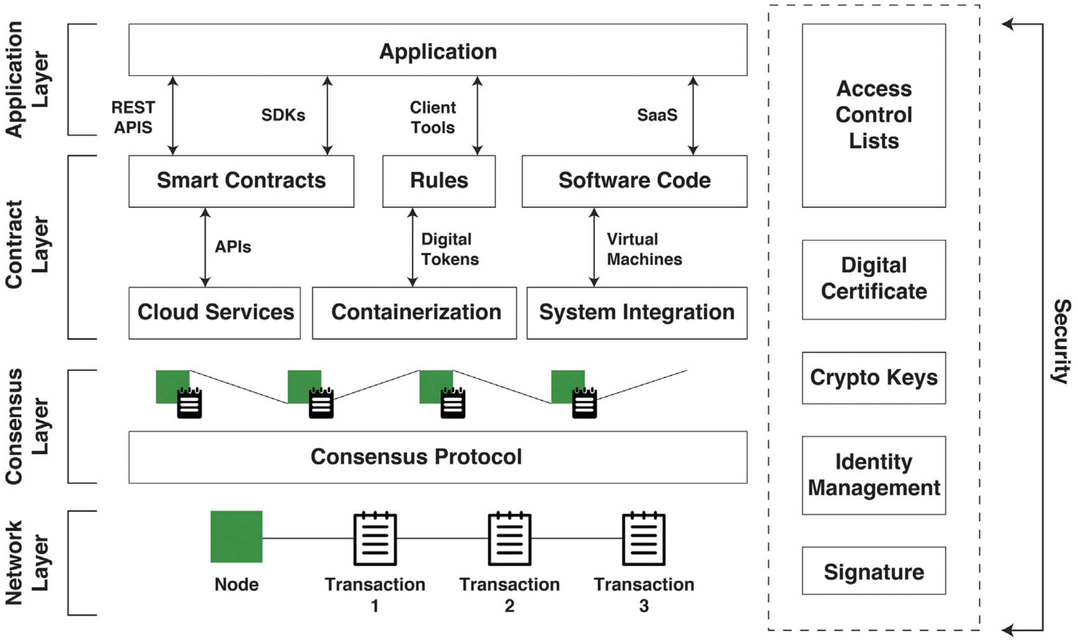
p0250 The patient might provide their authorization for data examination with the private key for this purpose. Hence, the private key can be shared to provide healthcare organizations and institutions access to all of your personal information. Those who do not have the key will be unable to access the secret information.

s0175 4.3 Physical architecture

p0255 This is the lowest level of abstraction, so it is very detail-oriented. It concerns itself with specific software, platforms, and data representations. Its purpose is to enable the real-life implementation of Blockchain technology solutions for the HIE system (Fig. 5.6 and Fig. 5.7).



f0035 FIGURE 5.6 **Physical architectural model: the physical layers stack of an HIE system based on blockchain.**



f0040 FIGURE 5.7 **Physical architectural model: layerwise detailed components in the blockchain-based HIE system.**

s0180 *4.3.1 Application layer*

p0260 The client or end-user application sits on the highest tier of the HIE blockchain architecture. It is made up of decentralized healthcare apps and browsers that communicate with the HIE. It usually initiates a transaction to start the workflow. The user interface (UI) is typically the preferred medium for widespread availability and accessibility of this program among patients, physicians, and nurses. It focuses largely on the advancement of Blockchain technology for use in several healthcare systems.

s0185 *4.3.2 Contract/service layer*

p0265 While the application layer is in charge of all user features and workflow modeling, the contract layer is responsible for the contract itself. Smart contracts consist of healthcare domain-specific logic for the HIE blockchain system. A smart contract is a piece of software that adds layers of information to digital transactions on a blockchain. To guarantee that the HIE system is dependable, safe, and verifiable, as well as devoid of any potential flaws, this layer must be carefully specified and implemented. This layer contains all crypto and digital assets, as well as sensitive data.

s0190 *4.3.3 Consensus layer*

p0270 This layer determines the consensus and associated participation mechanisms of the HIE system. It is made up of essential components that are required to keep the blockchain functioning. Participants are regulated, and cryptographic standards are implemented.

s0195 *4.3.4 Network layer*

p0275 In the blockchain architecture, it is the bottom layer. It's also the most important since it defines how data are delivered and received throughout a peer-to-peer HIE system. Peers communicate information about the state and security of the network in a blockchain through this layer. The Blockchain Distribution Network (BDN) is a network of computers devoted to providing data on a blockchain as rapidly as possible.[34] BDNs reside in this layer.

s0200 4.4 Data query workflow

p0280 The workflow is started by the patient or the health institution starting a transaction. This software communicates with the nodes via API or SDK.[35] Nodes execute smart contracts recorded in the blockchain consortium, which are then executed by them. The smart contract is a piece of software that depicts transactions and has preprogrammed rules and permissions for the patient and the health institutions. The nodes in blockchain networks invoke these business rules or conditions. Java, Golang, Scala, and other programming languages can be used as the execution runtime or virtual machine environment for smart contracts.

p0285 The integration layer allows data from within the blockchain network to be exchanged with data from outside the network. External event hubs are a typical approach in HIE systems for exchanging health information between various health centers and hospitals. Data are also sent between networks for use in analytics and AI applications to provide relevant insights. In the form of BaaS, blockchain can be delivered as a managed cloud service as well as embedded software for IoT devices (BaaS).[36]

p0290 Finally, the data are transferred to the distributed ledger. It is the core persistent layer in the blockchain architecture because it offers a decentralized and distributed database for transaction entities. The healthcare entries are hashed and stored in blocks that contain the patient's ID in the order that they appear.

p0295 In an HIE system, the ledger depicts a chain of hashed blocks containing medical data, each of which refers to the block before it. This ledger is shared across the whole blockchain network, which means that each node has its copy of the ledger and validates transactions independently. When every node agrees and verifies the transaction's authenticity, a consensus is achieved. Various HIE systems use different consensus techniques to achieve an agreement. This way the patients' data are permanently stored in the ledger, protected with enhanced security and immutability.

s0205 5. Implementation challenges and considerations

p0300 Blockchain technology has various applications in healthcare, but it is not yet fully mature enough to be used in the immediate future.[37] Before a healthcare blockchain can be implemented by businesses across the country, a number of technological, organizational, and behavioral economics hurdles must be overcome. While healthcare may not be the foremost industry to successfully implement blockchain technology at scale, it is an industry with one of the biggest opportunities to transform HIE and interoperability. This section delves into the problems of bringing blockchain solutions for HIE into practice. Some of them are described in the following sections.

s0210 5.1 Time-consuming transaction verification

p0305 The major drawback of Blockchain technology is that it requires the agreement of 51% of nodes to validate the blockchain's immutability. Mining these blocks can consume a lot of computing power as well as time, resulting in time-consuming block verification.

s0215 5.2 Compliance with Federal and local laws

p0310 While blockchains do not require a central authority to store data, they do not eliminate the requirement for any kind of authority.[38] Because of the personal and sensitive nature of healthcare data, blockchain applications will rely on regulation, monitoring, and standards and protocols. Any blockchain's consensus method is not dependent on technology, but rather on agreement among members. As a result, maintaining data distribution across the network while complying with existing HIPAA privacy laws is a key technological issue for blockchain's distributed ledger solutions.[23]

s0220 5.3 Lack of social support

p0315 The cultural adoption of blockchain, which is a relatively new technology, could prove difficult, since healthcare executives are hesitant about embracing the most recent healthcare trends.

s0225 5.4 Inadequate technical infrastructure

p0320 The biggest roadblock would be healthcare organizations' willingness to invest in the necessary technology infrastructure. Because blockchains are distributed systems, their operation has a significant storage cost.[39] As a result, vast amounts of data cannot be stored efficiently on the blockchain. While blockchains may be used for access control and data integrity, medical data and records must be stored somewhere else and may be subject to attacks.

s0230 6. Conclusion

p0325 HIE integrates the EHR systems from various health organizations, allowing them to securely communicate patient data and better coordinate treatment. The present centralized HIE models, on the other hand, have a number of security and scalability problems. Blockchain technology is one of the proposed methods for overcoming these obstacles. It makes use of a decentralized and distributed ledger to make use of the computing power of all participating nodes in the blockchain network, reducing latency and eliminating a single point of failure.

p0330 Integrating the HIE system with blockchain has numerous benefits. For example, it guarantees transparency and auditability, eliminates the need for mediation, and establishes confidence.

p0335 The chapter begins with a succinct introduction to HIE and the reasoning behind the emergence of Blockchain technologies for the healthcare landscape. The next section highlights the traditional HIE systems, emphasizing their limitations and need for a more secure solution. The next section covers essential components and the main principles behind Blockchain technology. The next section describes, in meticulous detail, the blockchain-based HIE architectures, underscoring the entities and interactions among them. The next section identifies the gaps present in the practical adoption of blockchain-based HIE systems at scale.

p0340 Future research can build on this work by identifying solutions to the constraints of blockchain-based HIE systems. It can also provide insight on large-scale software implementation and pave the way for more widespread use of such systems in the future. The cost-impact and investment implications can also be addressed by further research. In addition, beneficial elements such as payment for medical services may be incorporated with the HIE architecture to make the system more convenient for professionals while also keeping it safe and reliable. From medicines and improved payment choices to the decentralization of patient health records, blockchain can guarantee healthcare information exchange governance. While blockchain is not a panacea for all issues, it does provide a platform for study, investment, and proof-of-concept testing.

References

1. Roehrs A, da Costa CA, da Rosa Righi ROPHR. A distributed architecture model to integrate personal health records. *J Biomed Inf*. 2017;71:70–81. https://doi.org/10.1016/j.jbi.2017.05.012.
2. Murugan A, Chechare T, Muruganantham B, Kumar SG. Healthcare information exchange using blockchain technology. *Int J Electr Comput Eng*. 2020;10(1):421. https://doi.org/10.11591/ijece.v10i1.pp421-426.
3. B. Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf. Accessed October 1, 2021.
4. Zhuang Y, Sheets L, Shae Z, Tsai JJP, Shyu CR. Applying blockchain technology for health information exchange and persistent monitoring for clinical trials. *AMIA Annu Symp Proc*. 2018;2018:1167–1175.
5. How Blockchain Technology Could Disrupt Healthcare. https://www.cbinsights.com/research/report/blockchain-technology-healthcare-disruption/. Published 2018. Accessed October 1, 2021.
6. Bocek T, Rodrigues BB, Strasser T, Stiller B. Blockchains everywhere—a use-case of blockchains in the pharma supply-chain. In: *Proceedings of the IM 2017—2017 IFIP/IEEE International Symposium on Integrated Network and Service Management*. 2017:772–777. https://doi.org/10.23919/INM.2017.7987376.
7. Bryatov SR, Borodinov AA. Blockchain technology in the pharmaceutical supply chain: researching a business model based on Hyperledger Fabric. *CEUR Workshop Proc*. 2019;2416:134–140. https://doi.org/10.18287/1613-0073-2019-2416-134-140.
8. Sylim P, Liu F, Alvin M, Fontelo P. Blockchain technology for detecting falsified and substandard drugs in the pharmaceuticals distribution system. *JMIR Res Protoc*. 2018;7(10.2196):10163.
9. Walker J, Pan, Johnston D, Adler-Milstein J, Bates MB. The value of health care information exchange and interoperability: there is a business case to be made for spending money on a fully standardized nationwide system. *Health Aff*. 2005;(Suppl1):5–10.
10. Zhuang Y, Sheets LR, Chen YW, Shae ZY, Tsai JJP, Shyu CR. A patient-centric health information exchange framework using blockchain technology. *IEEE J Biomed Health Inform*. 2020;24(8):2169–2176. https://doi.org/10.1109/JBHI.2020.2993072.
11. Dagher GG, Mohler J, Milojkovic M, Marella PB. Ancile: privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustain Cities Soc*. 2018;39:283–297. https://doi.org/10.1016/j.scs.2018.02.014.
12. Takyar A. What is Health Information Exchange (HIE) And How Can Blockchain Transform It? https://www.leewayhertz.com/blockchain-health-information-exchange/. Accessed October 5, 2021.
13. Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. *Decent Bus Rev*. 2008:21260.
14. Peterson, D., Kanjamala, C.K. A Blockchain-Based Approach to Health Information Exchange Networks. Health-it.gov Accessed. 2021.

15. Dwork C, Naor M. Pricing via Processing or Combatting Junk Mail. Springer Science and Business Media LLC; :139−147 https://doi.org/10.1007/3-540-48071-4_10.
16. Wu Y, Yan Z, Yu FR, Deng R, Varadharajan V, Chen W. Guest editorial: blockchain and healthcare computing. *IEEE J Biomed Health Inform*. 2020;24(8):2144−2145. https://doi.org/10.1109/JBHI.2020.3003767.
17. Buterin V. On Public and Private Blockchains. https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/. Published 2015. Accessed October 5, 2021.
18. Zheng Z, Xie S, Dai HN, Chen X, Wang H. Blockchain challenges and opportunities: a survey. *Int J Web Grid Serv*. 2018;14(4):352−375. https://doi.org/10.1504/IJWGS.2018.095647.
19. Jiang S, Cao J, Wu H, Yang Y, Ma M, He J. Blochie: a blockchain-based platform for healthcare information exchange. In: *Proceedings—2018 IEEE International Conference on Smart Computing, SMARTCOMP 2018*. 2018:49−56. https://doi.org/10.1109/SMARTCOMP.2018.00073.
20. Casino F, Dasaklis TK, Patsakis C. A systematic literature review of blockchain-based applications: current status, classification and open issues. *Telematics Inf*. 2019;36:55−81. https://doi.org/10.1016/j.tele.2018.11.006.
21. Wang H, Ma S, Guo C, Wu Y, Dai H-N, Wu D. Blockchain-based power energy trading management. *ACM Trans Internet Technol*. 2021;21(2):1−16. https://doi.org/10.1145/3409771.
22. Buterin V. A Next Generation Smart Contract & Decentralized Application Platform. Translatewhitepaper.com Accessed. 2021.
23. Esmaeilzadeh P, Mirzaei T. The potential of blockchain technology for health information exchange: experimental study from patients' perspectives. *J Med Internet Res*. 2019;21(6). https://doi.org/10.2196/14184.
24. Integrating Blockchain with ERP for a Transparent Supply Chain. https://www.infosys.com/oracle/white-papers/documents/integrating-blockchain-erp.pdf. Published 2018. Accessed October 5, 2021.
25. Bennett B. Blockchain HIE overview: a framework for healthcare interoperability. *Telehealth Med Today*. 2017. https://doi.org/10.30953/tmt.v2.14.
26. Mettler M. Blockchain technology in healthcare: the revolution starts here. In: *2016 IEEE 18th International Conference on E-Health Networking, Applications and Services, Healthcom 2016*. 2016. https://doi.org/10.1109/HealthCom.2016.7749510.
27. Nogueira JM, Romero D, Espadas J, Molina A. Leveraging the Zachman framework implementation using action-research methodology—a case study: aligning the enterprise architecture and the business goals. *Enterprise Inf Syst*. 2013;1:100−132.
28. Deborah A, Afolashade K, Lossan B, Adenrele A. Blockchain: a possible alternative to achieving health information exchange (HIE). *Int J Innov Res Comput Sci Technol*. 2020. https://doi.org/10.21276/ijircst.2020.8.3.23.
29. Fekih LM. Application of blockchain technology in healthcare: a comprehensive study. *Lect Notes Comput Sci*. 2020:268−276.
30. Acharya V. *Oracle Blockchain Quick Start Guide : A Practical Approach to Implementing Blockchain in Your Enterprise*. Birmingham: Packt Publishing, Limited; 2019.
31. Saleh F, Jiang W. Blockchain without waste: proof-of-stake. *Rev Financ Stud*. 2021;34(3):1156−1190. https://doi.org/10.1093/rfs/hhaa075.
32. Lamport L, Shostak R, Pease M. The byzantine generals problem. *ACM Trans Program Lang Syst*. 1982;4(3):382−401. https://doi.org/10.1145/357172.357176.
33. Hang L, Choi E, Kim DH. A novel EMR integrity management based on a medical blockchain platform in hospital. *Electronics*. 2019;8(4). https://doi.org/10.3390/electronics8040467.
34. Klarman, B., Kuzmanovic, Sirer EG. bloXroute: A Scalable Trustless Blockchain Distribution Network. Bloxroute.com Accessed. 2021.
35. Osei-Tutu K, Hasavari S, Song YT. Blockchain-based enterprise architecture for comprehensive healthcare information exchange (HIE) data management. In: *Proceedings—2020 International Conference on Computational Science and Computational Intelligence, CSCI 2020*. 2020:767−775. https://doi.org/10.1109/CSCI51800.2020.00145.
36. Xia Q, Sifah EB, Asamoah KO, Gao J, Du X, Guizani M. MeDShare: trust-less medical data sharing among cloud service providers via blockchain. *IEEE Access*. 2017;5:14757−14767. https://doi.org/10.1109/ACCESS.2017.2730843.
37. Heston F. Introductory T, chapter. Blockchain technology and smart healthcare. In: *Smart Healthcare*. IntechOpen; 2020.
38. *Opportunities and Challenges of Blockchain Technologies in Health Care*. Blockchain Policy Series; 2020. https://www.ospi.es/export/sites/ospi/documents/documentos/OECD_Opportunities-and-Challenges-of-Blockchain-Technologies-in-Health-Care.pdf. Accessed September 29, 2021.
39. Wood G. *Ethereum: A Secure Decentralised Generalised Transaction Ledger*. 2017.

DAS: 05

Non-Print Items

Abstract

Electronic health records (EHRs) have become an essential part of the healthcare system due to the digitalization of health records. The health information exchange (HIE) is a centralized system that enables healthcare providers to access and share these patient EHRs through the internet. They are intended to reduce medical errors and improve interorganizational collaboration of patient data across healthcare institutions. However, current HIEs suffer numerous complications, including privacy concerns, security threats, and lack of patient control. By putting security and immutability at the core of the system, blockchain has the potential to transform healthcare. Owing to its shared ledger structure, it has a permanent audit trail assuring immutability. Through its smart-contract standard, a blockchain-based HIE architecture may improve healthcare records' security, privacy, and interoperability while still ensuring data integrity. The blockchain-based HIE architecture seeks to guarantee data provenance and provide patients with complete ownership over their medical information.

Keywords:

Blockchain; Cryptography; Distributed ledger; Electronic health records; Health information exchange; Healthcare.