Cluster Computing (2025) 28:529
https://doi.org/10.1007/s10586-025-05308-x

Blockchain-based access control and privacy preservation in healthcare: a comprehensive survey

Ahmed M. Tawfik[1] · Ayman Al-Ahwal[2] · Adly S. Tag Eldien[3] · Hala H. Zayed[1,4]

Received: 3 November 2024 / Revised: 14 March 2025 / Accepted: 25 April 2025 / Published online: 19 August 2025

Abstract

In recent years, blockchain technology has emerged as a promising solution for securing electronic health records (EHRs) while preserving patient privacy. Traditional e-health systems facilitate EHR sharing among healthcare providers but also introduce significant privacy risks, such as unauthorized access and data breaches. Blockchain, when integrated with privacy-preserving techniques, enhances transparency, integrity, and availability in EHR management. Smart contracts further strengthen security by enabling automated authentication and access control. This paper provides a comprehensive survey of blockchain-based access control frameworks in healthcare, categorizing them into permissioned and permissionless approaches. It also explores cryptographic privacy-preserving techniques designed to mitigate privacy risks. Additionally, blockchain platforms and consensus protocols commonly used in these frameworks are analyzed. The methodology follows a structured paper selection process, leading to the final inclusion of 45 research papers focusing on blockchain-based privacy preservation and access control in healthcare. Furthermore, it presents real-world case studies that illustrate the practical implementation of blockchain-based access control in healthcare settings, highlighting their strengths and challenges. Finally, it identifies privacy-related challenges, open research issues, and future directions to guide further research in this evolving domain.

Keywords Blockchain · Security · Privacy · Electronic health records · Access control methods

Abbreviations

ABE	Attribute-based encryption
AI	Artificial intelligence
BFT	Byzantine fault tolerance
CP-ABE	Ciphertext-policy attribute-based encryption
CSP	Cloud service provider
DApps	Decentralized applications
DBFT	Delegated Byzantine fault tolerance
DPoS	Delegated proof of stake
EHR	Electronic health record
FHE	Fully homomorphic encryption
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
IoT	Internet of things
IPFS	InterPlanetary file system
MSP	Membership service provider
NIZKP	Non-interactive zero-knowledge proof
PBFT	Practical Byzantine fault tolerance
PoA	Proof of authority
PoAc	Proof of activity
PoAh	Proof of authentication
PoC	Proof of conformance
PoET	Proof of elapsed time
PoS	Proof of stake
PoV	Proof of vote

✉ Ahmed M. Tawfik
ahmed.tawfek@fci.bu.edu.eg

Ayman Al-Ahwal
dr.ayman.hiet@gmail.com

Adly S. Tag Eldien
adlytag@feng.bu.edu.eg

Hala H. Zayed
hala.zayed@fci.bu.edu.eg

[1] Computer Science Department, Faculty of Computers and Artificial Intelligence, Benha University, Benha, Egypt

[2] Communication and Electronics Department, Pyramids-Institute for Engineering and Technology, 6th of October City, Egypt

[3] Electrical Engineering Department, Faculty of Engineering at Shoubra, Benha University, Benha, Egypt

[4] Faculty of Engineering, Egypt University of Informatics (EUI), Cairo, Egypt

PoW	Proof of work
SGX	Software guard extensions
SMPC	Secure multi-party computation
SSharing	Secret sharing
TEE	Trusted execution environment
TTP	Trusted third party
ZKP	Zero-knowledge proof

1 Introduction

The majority of healthcare providers worldwide are now interested in using smart technologies to replace traditional healthcare systems with e-health systems. Efficiently managing and improving the electronic transmission and distribution of healthcare data to physicians is a top priority for enterprises and healthcare providers. The Electronic Health Record (EHRs) are the primary component of e-health systems, digitizing a patient's paper file and providing authorized parties with easy and secure access to this information [1]. EHRs may include all relevant patient information, such as medical history, diagnoses, images (e.g., CT scans, X-rays), laboratory results, and treatments. As EHRs are distributed across various medical organizations, the benefits of transitioning toward e-health are increasingly recognized [2]. However, the lack of interoperability between different medical organizations' data standards presents a significant challenge. Additionally, the sharing of health records and their transfer outside medical organizations are often restricted due to privacy concerns [3].

Privacy is a major concern in shared environments and must be carefully considered. In recent decades, privacy and security issues in the healthcare industry have become increasingly significant [4]. These challenges make exchanging medical data extremely difficult, severely limiting its practicality. One of the key features of EHRs is their ability to create and manage electronic health information that can be accessed by multiple authorized healthcare providers. Despite global efforts to enhance EHR security, patients' private data remains vulnerable to breaches. Since most medical information is stored centrally within medical institutions, it is exposed to risks such as hacking, natural disasters, and malicious tampering, all of which can lead to data breaches or loss of medical information. For instance, about 47 GB of health data stored by medical institutions on an Amazon database was accidentally leaked to the public, affecting an estimated 150,000 patients [5]. Blockchain technology has been proposed as a potential solution to mitigate these issues [6].

Blockchain is a decentralized system that combines a hash chain and a consensus mechanism to establish a common "truth" regarding the data stored on the chain. This system relies on a network for communication and storage, distributing data across participants without the need for a central server. While blockchain technology is resistant to tampering, it can be altered if consensus is reached among participants [7]. Permissionless blockchains allow anyone with an internet connection to participate, while permissioned blockchains restrict access to certain individuals or groups.

Unlike traditional databases controlled by central entities such as governments and banks, blockchain decentralizes data storage across nodes within the network. It acts as a tamper-resistant ledger, recording transactions in a sequence that, while difficult to alter, can be modified through consensus. The features of transparency, decentralization, and verifiability make blockchain technology a promising tool for managing EHRs in medical organizations, enabling secure data sharing across different entities while ensuring its integrity [8].

There are two primary types of blockchains: permissionless and permissioned. In a permissionless blockchain, any participant can write to the ledger and engage in the consensus mechanism, although not all implementations are fully anonymous. In contrast, permissioned blockchains restrict these activities to authorized participants [9]. To ensure proper access control in healthcare systems, healthcare providers must develop reliable methods to validate permissions and securely distribute EHRs.

Blockchain technology can play a key role in access control by recording and verifying access-related information through a decentralized ledger. This ensures transparency, accountability, and a tamper-resistant record of access events, which can be audited and traced back to specific users or devices. Moreover, blockchain eliminates the need for a central authority, reducing the risk of a single point of failure and enhancing security against malicious actors.

Access control in healthcare systems relies on three foundational services, commonly referred to as AAA: Authentication, Authorization, and Accounting [10]. (1) Authentication: To safeguard patient data and prevent identity theft, healthcare providers must authenticate the identity of users attempting to access electronic health information. Methods of authentication include passwords, biometric verification, two-factor authentication, and more. (2) Authorization: After authentication, users are granted or denied access to specific resources or functions based on predefined access control policies, ensuring that only authorized individuals can access sensitive patient data. (3)

Accounting: Accounting involves tracking and logging user activity within the healthcare system, including who accessed patient data, when it was accessed, and what actions were taken. This is crucial for auditing and ensuring compliance with healthcare regulations. By incorporating these services into an access control system, healthcare organizations can enhance data security and prevent breaches or unauthorized access.

In fact, enabling authentication, authorization, and accounting is critical for adopting a good EHR access control approach [11]. Access control methods should be employed to ensure that only authorized users are granted access to patients' EHRs. The survey's main contributions are:

1. The categorization of recent EHR access control methods based on blockchain into two categories: permissionless and permissioned. Each category includes a summary of publication year, blockchain type, consensus protocol, blockchain platform, EHR location, privacy/access control technique, and weaknesses.
2. Classifying access control methods from privacy and security perspectives provides readers with a concise understanding of various factors, including confidentiality, integrity, availability, accountability, revocability, scalability, and access control.
3. Outlining blockchain-based privacy-preservation cryptographic techniques in healthcare to protect the privacy of patients' EHRs.
4. Introducing the most popular blockchain platforms and consensus protocols used in access control methods, as well as summarizing the consensus protocols in terms of publication year, blockchain type, mining technique, blockchain platform, decentralization, computing overhead, benefits, and drawbacks.
5. Representing the smart contract mechanisms in the development of access control methods in healthcare and providing an in-depth explanation of the blockchain's main characteristics.
6. Identify prevalent privacy challenges, address open research issues, and outline potential future directions.

The organization of this survey is as follows: Sect. 2 reviews relevant survey papers on blockchain-based security and privacy in healthcare. Section 3 provides a comprehensive overview of blockchain technology. Section 4 discusses the key elements of blockchain, including consensus algorithms, blockchain platforms, and smart contracts. Section 5 defines privacy-preserving cryptographic techniques using blockchain in the healthcare domain. Section 6 covers blockchain-based EHR access control methods. Section 7 highlights privacy challenges and issues that arise in the healthcare domain when utilizing blockchain technology. Section 8 discusses open research issues and potential future directions. Section 9 presents case studies of blockchain-based access control in healthcare. Finally, Sect. 10 concludes the survey. The organization of the paper is also illustrated in Fig. 1.

2 Related work

In this section, we examine various survey papers related to blockchain-based security and privacy approaches in healthcare. Kassab et al. [12] surveyed 52 papers based on blockchain technology and published between 2015 and 2018, reviewing several blockchain-based healthcare applications for patients, healthcare providers, and insurance companies. Syed et al. [13] surveyed 143 papers based on blockchain technology and published between 2015 and 2018, with a focus on their relevance to the healthcare domain, including the challenges, scenarios, and benefits associated with using blockchain in healthcare, and discussing security and privacy issues relevant to EHR methods.

Hussien et al. [14] conducted a survey of 58 papers related to blockchain technology, published between 2016 and 2019. Their primary focus was on blockchain solutions within the healthcare sector, particularly classifying them, identifying challenges, and outlining security objectives. Agbo et al. [15] surveyed 65 blockchain-based papers published between 2016 and 2018, focusing on multiple studies in various use cases for implementing blockchain technology in the healthcare sector. Tandona et al. [16] surveyed 42 blockchain-based papers published between 2016 and 2019 related to the handling and sharing of healthcare data, including EHRs. Soltanisehat et al. [17] surveyed 62 papers based on blockchain technology and published between 2016 and 2020, reviewing the applications, challenges, and future directions in healthcare. Hasselgren et al. [18] reviewed 39 blockchain-based papers in the healthcare domain published between 2018 and 2020, focusing on healthcare data integrity, interoperability, and access control challenges. Farouk et al. [19] conducted a survey of 11 blockchain-related papers published between 2016 and 2019, with a primary focus on healthcare systems. Their survey encompassed an investigation into the participation of start-up companies in this domain and the identification of potential research directions. Qadri et al. [20] conducted a survey of 99 blockchain-based papers published between 2016 and 2019, with a primary focus on reviewing blockchain as an emerging technology for the future of healthcare internet of things (IoT).

Shi et al. [21] conducted a survey of 33 blockchain-based papers published between 2016 and 2019. Their

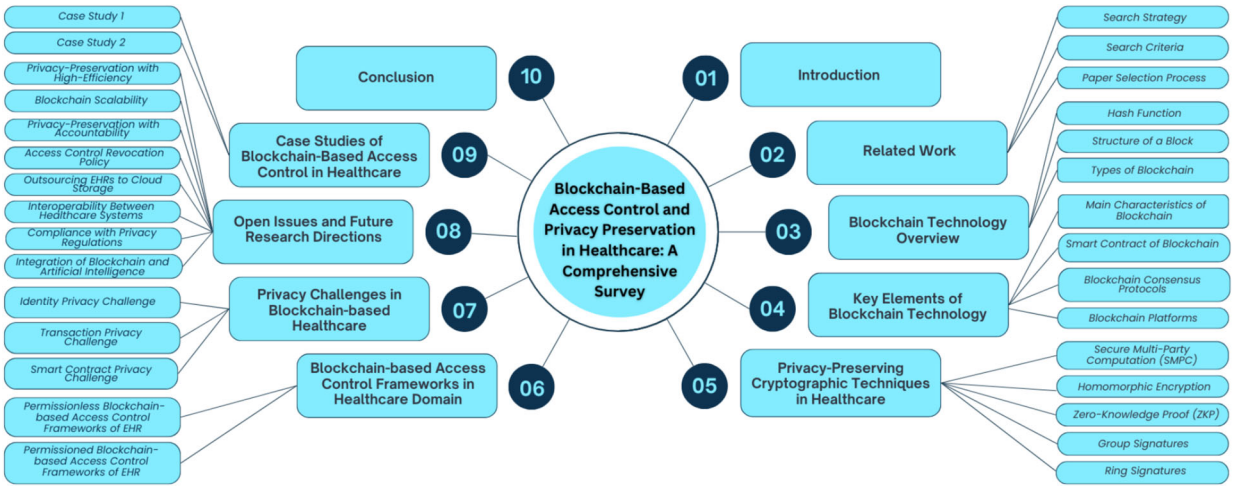

Fig. 1 The organization of this survey paper

primary focus was on reviewing healthcare systems, including requirements, applications, limitations, and potential research directions. Chukwu et al. [22] conducted a survey of 61 blockchain-based papers published between 2017 and 2019, with a primary focus on applications in Healthcare Systems, along with a consideration of potential research directions. Khatri et al. [23] reviewed 50 blockchain-based papers in the healthcare sector published between 2016 and 2020, discussing a systematic review of blockchain trends and healthcare challenges. Hussien et al. [24] surveyed 940 blockchain-based papers related to the healthcare domain and published between 2016 and 2020, conducting a bibliometric analysis of healthcare data systems to improve privacy and security in this domain. Arbabi et al. [25] reviewed 45 papers on blockchain in healthcare published between 2016 and 2021. They focused on analyzing interactions among healthcare stakeholders and explored storage systems' functional components and non-functional requirements, addressing aspects such as health data collection, storage, and sharing.

Villarreal et al. [26] surveyed 21 papers on blockchain technology published between 2017 and 2022, focusing on blockchain interoperability and security solutions. They classified these papers to identify architectural mechanisms used in healthcare environments and highlighted the architectural elements supporting these solutions. The study outlined seven architectural approaches for implementing blockchain in healthcare, providing an overview of the problems addressed, analyzing interoperability and security, and discussing related tactics for each scenario. Popoola et al. [27] conducted a critical literature review on security and privacy in smart home healthcare schemes that adopt IoT and blockchain technologies. The study surveyed 38 papers published between 2016 and 2023, examining the problems, challenges, and solutions associated with these systems, focusing on vulnerabilities such as cyber-attacks, data breaches, and privacy concerns due to the sensitive nature of health data. The authors highlighted the potential of blockchain to enhance security and privacy through decentralized and tamper-proof data management. They analyzed existing solutions and proposed improvements, emphasizing robust encryption, secure data-sharing mechanisms, and user-centric privacy controls. The paper provides a comprehensive overview of current research and suggests directions for future work in this domain. Lastly, Reshi et al. [28] conducted an in-depth examination of the challenges, contributing technologies, and alternatives in blockchain systems. The study surveyed 30 papers published between 2016 and 2023, analyzing critical issues such as scalability, energy consumption, interoperability, and security, alongside the role of consensus mechanisms and cryptographic techniques in addressing these challenges. The authors also explored emerging alternatives, including Directed Acyclic Graphs (DAGs), sharding, and hybrid architectures, which aim to overcome the limitations of traditional blockchain systems. By highlighting the trade-offs between decentralization, security, and efficiency, the paper provides valuable insights into adapting blockchain for various applications, including healthcare, and suggests future research directions to address these challenges.

Table 1 compares our survey with other existing surveys in the healthcare domain based on various factors such as year of publication, main contributions, EHR frameworks, blockchain types, consensus protocols, privacy techniques, access control, and covered years.

Our survey surpasses existing reviews by providing a comprehensive and up-to-date analysis of blockchain-based EHR access control, privacy-preservation techniques, and consensus protocols in healthcare. Unlike prior

works, we systematically categorize access control methods into permissionless and permissioned blockchains, evaluate critical privacy and security factors, and analyze widely used blockchain platforms. Furthermore, we address open research issues, propose potential solutions, and outline future directions up to 2024. While recent studies offer valuable insights, they often lack a holistic comparison of blockchain-based access control frameworks from both privacy and security perspectives-a gap our work thoroughly addresses. As a result, our survey serves as a more comprehensive and actionable resource for researchers and practitioners seeking a well-rounded understanding of blockchain-based EHR access control.

2.1 Search strategy

This study reviews blockchain-based research papers related to healthcare, privacy, and access control that were published between 2016 and 2024. We defined the search space for this study by utilizing multiple scientific databases, including Google Scholar, ResearchGate, IEEE, Science Direct, Elsevier, Springer, ACM, MDPI, Wiley, and Hindawi.

2.2 Search criteria

To obtain a comprehensive understanding of the topic and answer our research questions, we used specialized search keywords to conduct our search. The selected papers were obtained using the search keywords ("EHR" OR "Healthcare" OR "EMR" OR "Electronic Health Record" OR "Electronic Medical Record") AND ("Privacy" OR "Access Control") AND "Blockchain".

2.3 Paper selection process

Following the established search strategy and criteria, we queried papers using the selected search keywords, as illustrated in Fig. 2, and as outlined below:

- Step 1: In the first step, we collected papers based on the selected search keywords, resulting in 296 papers being collected.
- Step 2: In the second step, we continued the paper selection process by removing duplicates and focusing on the titles and abstracts. At the end of this step, 164 papers remained.
- Step 3: In the third phase, we thoroughly studied the entire contents of the papers and removed any unsuitable ones. This led to a selection of 129 papers related to blockchain technology in the healthcare domain.
- Step 4: Lastly, we analyzed and examined the papers remaining from the third phase. This resulted in a final selection of 45 papers related to the use of blockchain in healthcare, specifically focusing on providing privacy-preservation and access control methods for inclusion in this review.

In this survey, our main focus is on privacy-preserving techniques based on blockchain for implementing access control methods in the healthcare sector. To ensure a comprehensive understanding, we will begin by presenting an overview of blockchain technology in the following section, prior to diving into the access control techniques being discussed.

3 Blockchain technology overview

Blockchain is a technology introduced by the pseudonymous entity known as Satoshi Nakamoto [29]. It has become one of the most popular research areas and has the potential to revolutionize applications across various fields. Transactions on the blockchain are publicly visible yet become immutable once recorded. Any attempt to modify a transaction would require updating the hash values of all subsequent blocks. The blockchain stores data indefinitely through a network of decentralized and distributed nodes. Each node maintains an instance of the blockchain, which is continuously updated to ensure consistency across all nodes. The blockchain consists of a series of interlinked blocks, with each block pointing to its predecessor. Every valid transaction is recorded within a block on the blockchain.

3.1 Hash function

A *hash function* [30] is a deterministic mathematical algorithm that maps data of arbitrary size to a fixed-size bit string, known as the hash value. Formally, let H be a hash function defined as:

$$H : \{0,1\}^* \rightarrow \{0,1\}^n, \tag{1}$$

where $\{0,1\}^*$ denotes the set of all binary strings of arbitrary finite length and $\{0,1\}^n$ represents the set of binary strings of fixed length n. Hash functions are designed to satisfy the following essential properties:

- **Pre-image resistance:** Given a hash value h, it is computationally infeasible to find any input x such that $H(x) = h$.
- **Second pre-image resistance:** Given an input x, it is computationally infeasible to find a different input x' such that $H(x) = H(x')$.
- **Collision resistance:** It is computationally infeasible to find any two distinct inputs x and x' such that $H(x) = H(x')$.

Table 1 A comparison between this survey and other surveys in the healthcare domain

Survey authors	Publication year	Main contributions	EHR frameworks	Blockchain types	Consensus protocols	Privacy techniques	Access control	Covered years
Kassab et al. [12]	2019	Review the blockchain-based challenges, benefits, and scenarios in healthcare	✓	x	x	x	x	2015–2018
Syed et al. [13]	2019	Review of several blockchain based healthcare applications	✓	✓	✓	x	x	2015–2018
Hussien et al. [14]	2019	A review of blockchain solutions in healthcare and their classifications, problems, and security objectives	✓	✓	x	x	✓	2016–2019
Agbo et al. [15]	2019	A review of various use cases for implementing blockchain technology in the healthcare sector	✓	✓	x	x	x	2016–2018
Tandona et al. [16]	2020	Review of the handling and sharing of healthcare data, including EHRs	✓	✓	x	x	x	2016–2019
Soltanisehat et al. [17]	2020	Review of the blockchain-based applications, challenges, and future directions in healthcare	✓	✓	✓	x	x	2016–2020
Hasselgren et al. [18]	2020	A blockchain review of healthcare data integrity, interoperability, and access control challenges	✓	✓	✓	x	✓	2018–2020
Farouk et al. [19]	2020	A review of blockchain in healthcare systems, including an exploration of start-up companies involved	✓	✓	✓	x	x	2016–2019
Qadri et al. [20]	2020	Review of Blockchain as an emerging technology for the healthcare IoT	✓	x	x	✓	x	2016–2019
Shi et al. [21]	2020	A review of healthcare systems requirements and limitations, and potential research directions	✓	✓	✓	x	✓	2016–2019
Chukwu et al. [22]	2020	Review of applications in Healthcare Systems, along with a consideration of potential research directions	✓	✓	✓	x	x	2017–2019
Khatri et al. [23]	2021	A systematic review of blockchain trends and healthcare challenges	✓	x	x	x	x	2016–2020
Hussien et al. [24]	2021	Review the bibliometric analysis of healthcare data systems to improve privacy and security	✓	✓	✓	x	✓	2016–2020
Arbabi et al. [25]	2022	Analyze interactions among healthcare stakeholders and explored storage systems' functional components and non-functional requirements	✓	✓	✓	x	✓	2016–2021
Villarreal et al. [26]	2023	Review blockchain applications in healthcare, focusing on blockchain interoperability and security solutions	✓	✓	✓	x	x	2017–2022
Popoola et al. [27]	2024	Review security and privacy challenges in IoT-based smart home healthcare, proposing blockchain solutions and future directions	✓	✓	✓	x	✓	2016–2023

Table 1 (continued)

Survey authors	Publication year	Main contributions	EHR frameworks	Blockchain types	Consensus protocols	Privacy techniques	Access control	Covered years
Reshi and Sholla [28]	2024	Review blockchain applications in healthcare, focusing on blockchain energy consumption, interoperability and security solutions	✓	✓	✓	✓	x	2016–2023
Our Survey	2025	A review of EHR access control methods, privacy preservation tech- niques and challenges, open research issues, and future directions	✓	✓	✓	✓	✓	2016–2024

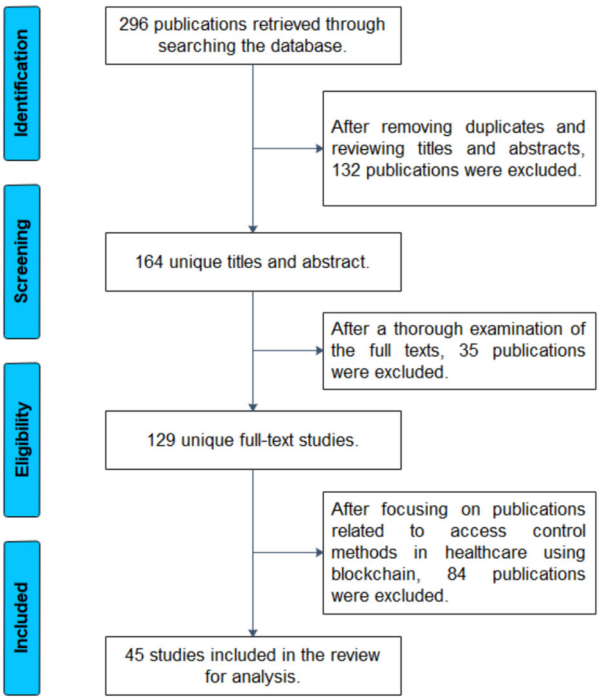

Fig. 2 A flow diagram of the study selection process

These properties are critical for ensuring data integrity and security in blockchain systems.

3.2 Structure of a block

Each block in a blockchain is secured through hash functions, which ensure data integrity and block chaining, and digital signatures [30], which prevent unauthorized modifications. When a block is generated, a unique hash value is produced based on its content, including transaction data. The block is then added to the blockchain, where its hash value is referenced by the subsequent block to ensure the integrity of the chain. The Genesis block is the first block in the chain and, as it has no previous hash, it is considered the foundational block of the blockchain. Transactions in subsequent blocks are validated using a combination of cryptographic methods, ensuring the security and consistency of the blockchain network. Modifying a block's content is extremely difficult because it would require re-validating the affected block and potentially the hash values of connected blocks, depending on the consensus mechanism employed by the network. Hash functions enhance the security of blockchain systems in several ways:

- **Data Integrity:** Any modification to the data within a block results in a different hash value, immediately signaling tampering.
- **Linking Blocks:** Each block contains the hash of the previous block. This chaining ensures that altering one block would require recalculating and updating the hashes of all subsequent blocks, a process that is computationally prohibitive.
- **Resistance to Attacks:** The pre-image, second pre-image, and collision resistance properties make it practically impossible for an adversary to forge a block or alter transaction data without detection.

Block sizes and the number of transactions per block can vary significantly depending on the specific blockchain implementation. For example, Bitcoin limits block sizes to 1 MB, while other systems, such as Bitcoin Cash, allow larger blocks of up to 8 MB or more [31]. Larger blocks can process more transactions at once, but different blockchain systems impose their own limits on block size and transaction capacity.

Figure 3 represents the structure of a typical block, which includes fields such as the previous hash (the hash value of the preceding block), timestamp (the date and time

when the block was created), nonce (a unique number used in mining), the Merkle tree (a structure used to efficiently verify the integrity of the data), and the transaction data (information created by users that is stored in the block). A block is secured using a combination of hashing and, in many implementations, digital signatures [32]. Any attempt to modify a transaction in a block would require altering the corresponding hash values and, depending on the consensus mechanism, may require updating subsequent blocks-a computationally intensive process. Once validated, a new block is added to the blockchain, making it part of the permanent and secure record.

Figure 4 illustrates a blockchain architecture where participants are represented as nodes, though not all participants may function as full nodes. Each node maintains a copy of the blockchain, continuously updating it to reflect the latest transactions and blocks. Nodes can perform various activities, including transaction validation, mining, or executing transactions. Most blockchain implementations utilize decentralized consensus mechanisms to validate and add new blocks. The role and activities of a node depend on the specific blockchain architecture and design.

The distributed nature of the blockchain network allows it to function as a single, logical platform shared by all participants. One of the main advantages of a decentralized system over a centralized one is its resistance to failure-there is no single point of failure, as data is replicated across multiple nodes. Once a transaction is recorded on the blockchain, it becomes highly tamper-resistant due to the consensus mechanism and the cryptographic techniques in use. This ensures the integrity and transparency of the data across the network.

Different types of blockchain networks exist, each designed to meet the specific needs of various applications. Some blockchains require third parties for access control, while others manage confidentiality, integrity, and availability natively throughout the network. However, the adoption of blockchain in business networks is still in its early stages, and the technology continues to evolve [33].

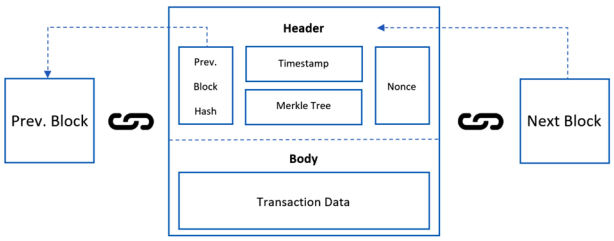

Fig. 3 A block structure

3.3 Types of blockchain

As shown in Table 2, blockchain technology can be classified into two main categories based on access control: permissionless and permissioned blockchains. These categories are further subdivided into public, private, and consortium blockchains, depending on the application requirements.

3.3.1 Permissionless (Public) blockchain

A public blockchain [34] is a type of permissionless blockchain, meaning it is open to all users of the network. Any user can connect to the network of public blockchains without needing prior permission. Participants have the ability to read, verify, and add transactions to the blockchain. Public blockchains have proven extremely useful in creating decentralized applications and cryptocurrencies like Bitcoin [29] and Ethereum [35]. Since any anonymous user can join, public blockchains offer high decentralization but may encounter scalability and privacy challenges.

3.3.2 Permissioned blockchain

A permissioned blockchain is a restricted type of blockchain in which only authorized users have access to the network. Permissioned blockchains can be either private or consortium-based.

Private Blockchain: A private blockchain [36] is a type of permissioned blockchain where only specific users, authorized by a central administrator, are allowed to participate in verifying and adding transactions. Unauthorized users cannot join the network. The administrator has control over the network's transactions and can implement

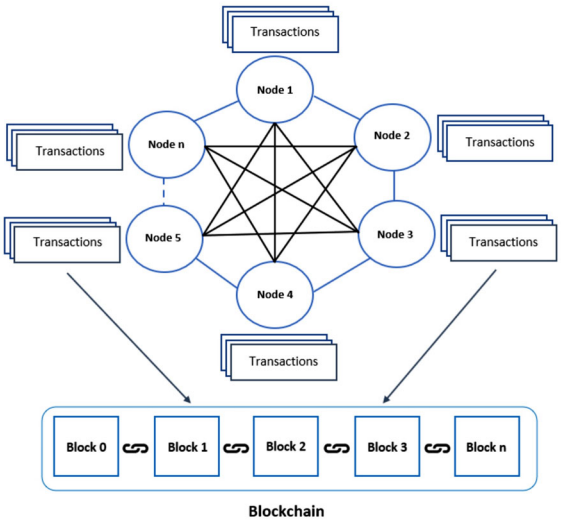

Fig. 4 A blockchain architecture

rules and policies. Private blockchains are commonly used by businesses and organizations for internal purposes. Examples include MultiChain [37] and Quorum [38].

Consortium Blockchain: A consortium blockchain [39] is another type of permissioned blockchain, but instead of being controlled by a single organization, it is governed by a group of organizations. These organizations collaborate to verify and add transactions, making the consortium blockchain a hybrid between public and private blockchains. Like a private blockchain, only authorized users can participate in the network, while other users are not allowed access. Examples of consortium blockchains include Hyperledger [40] and HydraChain [41].

Overall, understanding the different types of blockchain is crucial for selecting the right framework for various applications. In sectors like healthcare, the choice between permissioned and permissionless blockchains can significantly impact data privacy, scalability, and security, which are discussed in more detail in the following sections.

4 Key elements of blockchain technology

Blockchain technology is a distributed ledger system that stores transactions across a network of computers. Key elements of blockchain technology include: the main characteristics of blockchain, smart contracts, consensus protocols, and blockchain platforms.

4.1 Main characteristics of blockchain

Blockchain is a technology that provides secure and decentralized transactions. Here are some of the main characteristics of blockchain: transparency, integrity, and availability.

4.1.1 Transparency

Blockchain technology provides a high degree of transparency due to its decentralized and immutable nature [42]. Transactions on a blockchain are verified and stored on a distributed ledger, accessible to all participants in the network. Each block contains a hash of the previous block, creating a chain of blocks that cannot be altered or deleted without affecting the entire chain. This ensures that all data recorded on the blockchain is transparent, auditable, and tamper-resistant. Cryptographic techniques, such as hashing and digital signatures, further enhance the security of the recorded data. Transparency is one of the main advantages of blockchain, particularly in applications that require trust and accountability.

4.1.2 Integrity

Blockchain technology ensures data integrity through the hash function, linking each block to the previous one in an immutable chain. Any change in the data would alter the hash of the affected block, breaking the link to the next block and alerting participants to tampering. This mechanism ensures that data on the blockchain cannot be changed without detection. However, the integrity of the blockchain also relies on the consensus mechanism [43], which ensures agreement across participants regarding the validity of transactions and blocks. Without a reliable consensus mechanism, the blockchain's integrity could be compromised [44].

Merkle trees [45] are binary tree data structures used in blockchain systems to efficiently and securely verify the integrity of large datasets. Formally, a Merkle tree is constructed as follows:

- **Leaf Nodes**: Each leaf node contains the hash function $H(t_i)$ of a transaction t_i.

Table 2 A comparison of several types of blockchain

Parameters	Public blockchain [34]	Private blockchain [36]	Consortium blockchain [39]
Participant identity	Pseudonymous	Pre-approved identities	Pseudonymous
Block validation	All Nodes	Selected nodes	Selected nodes
Consensus protocol participation	Authentication is not needed	Authentication is needed	Authentication is needed
Throughput	Low	High	High
Read access	Public	Determined by organization	Determined by organization
Consensus protocol	Proof of Work (PoW), Proof of Stack (PoS), ...etc	Proof of Authority (PoA), Proof of Authentication (PoAh) ...etc	Practical Byzantine Fault Tolerance (PBFT), Proof of Elapsed Time (PoET), ...etc
Blockchain platforms	Bitcoin, Ethereum	Multichain, BlockStack, Quorum	Hyperledger, Hydrachain

- **Non-Leaf Nodes**: Each non-leaf node contains the hash of the concatenation of its child nodes. For example, if $H(L)$ and $H(R)$ are the hashes of the left and right child nodes, the parent node's hash is computed as:

$$H_{\text{parent}} = H(H(L) \parallel H(R))$$

  where $\parallel$ denotes concatenation.
- **Merkle Root**: The root of the tree, known as the Merkle root, is a single hash value that summarizes all transactions in the block. This root is stored in the block header and serves as a compact representation of the entire dataset.

As illustrated in Fig. 5, Merkle trees enable efficient and secure verification of individual transactions. To verify a specific transaction t_i, a user only needs the transaction's hash, the hashes of its sibling nodes along the path to the root (known as the Merkle proof), and the Merkle root. This eliminates the need to download and process the entire blockchain, significantly optimizing data integrity and validation. Merkle trees are a foundational component of blockchain systems like Bitcoin [29], ensuring scalability and security in transaction verification.

4.1.3 Availability

Traditionally, data is recorded in a centralized database, which poses security and privacy risks and makes it challenging to restore data once it has been compromised. In healthcare, this makes it difficult to establish a mutual trust network between providers. A blockchain system, on the other hand, allows each node to act as both a sender and a receiver, creating a fair and distributed peer-to-peer network. This approach eliminates transaction fees and power loss and enables data to be sent to nodes in various locations.

The blockchain's decentralization feature allows data to be stored and accessed from any node at any time with no issue of a single point of failure [46–48]. The decentralized nodes establish a peer-to-peer network with verification, propagation, and consensus methods where all nodes have equal responsibilities and tasks. The gossip protocol is used to synchronize data across nodes and achieve reliable data distribution and message consistency throughout the network [49].

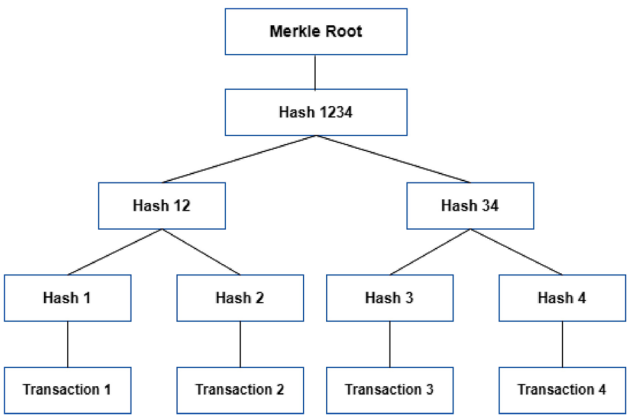

Fig. 5 An overview of Merkle tree

Blockchain technology is characterized by transparency, integrity, and availability, which are enabled through its decentralized and immutable nature. Transparency ensures that all transactions are publicly visible and auditable, while integrity is maintained through hash function and consensus protocols, preventing unauthorized alterations. Availability is achieved via decentralization, eliminating single points of failure and enabling peer-to-peer data sharing. These characteristics form the foundation for advanced blockchain applications, such as smart contracts, which automate and enforce predefined conditions for data transfers and access control. The next section will explore how smart contracts leverage these features to enable secure, decentralized, and automated agreements.

4.2 Smart contract of blockchain

A smart contract consists of a sequence of digitally defined conditions. A smart contract is a computer-assisted commitment mechanism from the user's perspective. The relevant data is automatically transferred by the smart contract when specific conditions are met. The smart contract is written as a stand-alone code with the aim of executing certain conditions and runs on the blockchain system. The smart contract transforms user transactions into code, which is then recorded on a blockchain and assigned a distinct address on the blockchain. As for blockchain technology, smart contracts could be self-managed and could have legal power. Users' trust relationships are enhanced via smart contracts [46, 50–52].

When the contract's requirements are satisfied, the smart contract's chain code can perform several automated tasks in sequence. Smart contracts provide automated legal rights, business logic, and duties, providing a basis for system security and privacy protection while also improving system efficiency. Smart contracts can apply multiple privacy protection techniques based on the level of private information provided by each user [53–55]. Due to the crucial needs of the systems of digital assets to design a programmable smart contract, The concept of smart contracts did not come into practical use until the development of blockchain technology. Indeed, smart contract development is based on the following requirements [56]: (1) the presence of digital asset systems that can be used to transfer assets between real-world parties automatically; (2) the development of law to ensure that

legal reasoning is automated in self-executing code in a way that respects regulations, bossiness, and contract rules; and (3) the creation of a secure environment suitable for contracts that are self-executive, with an emphasis on non-tampering and integrity, accuracy, and confidence, as well as availability and transparency.

According to blockchain technology, smart contracts can also be utilized among anonymous and untrusted parties with no dependence on a central authority, as shown in Fig. 6. The blockchain supports smart contracts by establishing connections between contracting parties in a logical programming language format, where the implementation of contract rules and conditions is recorded on the blockchain as an immutable transaction. Therefore, whenever a smart contract condition is met, a corresponding action can be automatically executed [57]. The smart contracts are developed using various programming languages, such as Java, JavaScript, Golang, and Solidity. The smart contract mechanisms also include a set of functions that allow the smart contract to interact with the blockchain and other contracts.

The smart contract mechanisms can be developed to facilitate the execution of transactions. For example, they can be utilized to facilitate the exchange of digital assets, such as EHRs. Smart contracts can be used to implement blockchain-based systems for access control. Rules can be encoded to enforce specific access control policies using smart contracts for different users or groups. These rules can define who is allowed to access certain data or perform certain actions on the blockchain network. By using smart contracts for access control, blockchain-based systems can enable only granted users to access sensitive data and perform sensitive operations. Additionally, smart contracts can track access history, providing an audit trail of who has accessed certain data or performed certain actions on the network. Ethereum [35] and Hyperledger are the most popular blockchain platforms that support smart contracts. This makes blockchain technology an attractive solution for many use cases and industries. Therefore, it is a promising tool for innovation and disruption in the future.

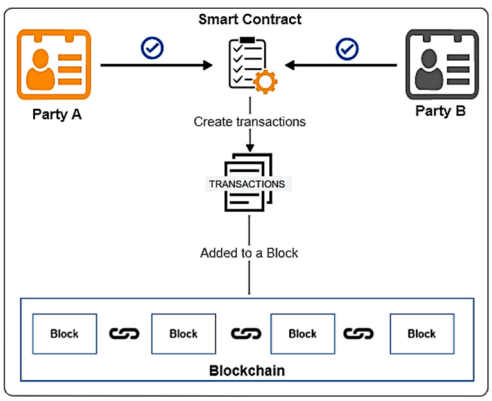

Fig. 6 An overview of smart contract

To summarize, smart contracts are self-executing agreements with predefined conditions encoded in code. Their execution relies on consensus protocols, which ensure that all nodes in the network agree on the outcome, making the process transparent and tamper-resistant. These protocols are essential for maintaining the integrity and trustworthiness of blockchain systems. The next section will explore consensus protocols in detail, focusing on how they enable nodes to collaboratively validate transactions and preserve the blockchain's integrity.

4.3 Blockchain consensus protocols

Consensus protocols ensure fairness and consistency among peers in a blockchain network, enabling the selection of trusted peers to validate transactions and maintain trust and security. Blockchain's immutability is based on the distributed management of nodes on a shared ledger with uniform data. A reliable consensus system is crucial for fault tolerance and preventing malicious nodes from disrupting the protocol. Several consensus protocols exist, each with varying degrees of performance efficiency and security, including some widely used protocols [58]:

Proof of Work (PoW) [29] achieved widespread adoption as a consensus protocol after being successfully implemented in Bitcoin [29], making it the first protocol to gain such acceptance. PoW enables the creation of a new block on the blockchain by solving a complex mathematical puzzle. Typically, the puzzle requires using a hash function to locate a specific hash that ends with a sequence of consecutive zeros. The difficulty of finding the hash increases over time and necessitates significant computational power. Peers in the network simultaneously attempt to solve the puzzle and obtain the hash, with the first peer to do so broadcasting the result to the remaining members of the network. In the case of the Bitcoin network, the node that solves the puzzle is compensated, usually with Bitcoin as a reward. The PoW algorithm offers decentralization and high security, but its primary drawback is the substantial amount of power required for mining blocks and its limited scalability.

Proof of Stake (PoS) [43] is the most commonly used alternative to PoW [29]. It is identified by the number of stakes a node has in the network. PoS allows peers to obtain coins before transactions take place. There is no competition for solving a complex mathematical puzzle in PoS; rather, the peer with the highest stake has a higher probability of submitting a new block to the blockchain. The way a block is recorded on the blockchain once it is created may vary. The advantage of PoS over PoW is that it does not require as much computational power to validate

transactions, so miners are only rewarded through transaction fees. PoS provides a fast block creation time, high throughput, independence from specialized hardware, and energy efficiency. However, since it relies heavily on peers with high stakes, the blockchain is likely to become centralized.

Delegated Proof of Stake (DPoS) [59] is an improvement to the PoS protocol [43], in which nodes vote for delegates to validate blocks. The delegates work together to generate the block rather than competing with each other. If a delegate makes a mistake or performs a malicious act, the other delegates can vote it out. The number of delegates is limited, allowing the network to be more efficiently organized. Each delegate can select the appropriate time for each block to be published. Scalability, energy efficiency, low-cost transactions, and solving the problem of double-spending are the most significant characteristics of this protocol. However, the limited number of delegates results in a semi-centralized network structure and the potential for delegate collusion.

Proof of Activity (PoAc) [60] is a hybrid of PoW [29] and PoS [43]. With this protocol, the process of recording a block to the blockchain begins similarly to PoW. Each node competes to solve the complex mathematical puzzle as quickly as possible. However, the newly generated block does not contain transactions; it only includes the header (block-related information) and the location of the node that initially generated the block. The system then switches to the PoS protocol to submit the block to the blockchain, where nodes with the highest stakes sign the block. After obtaining sufficient signatures, the transaction value is distributed among the nodes that created the block and the signing nodes. PoAc has the advantage of protecting the network from attacks such as the 51% attack, but it also has substantial drawbacks, including high energy consumption and limited scalability.

Practical Byzantine Fault Tolerance (PBFT) [61] is a mechanism utilized in distributed networks, including blockchains, to detect malicious nodes and make decisions. In PBFT, the block that is submitted to the chain is the one that receives the majority of votes (more than 2/3 of all peers' votes) validating it. The proposer in PBFT is selected in a round-robin fashion. This proposer gathers transactions to generate a block, which is then published to the network. After receiving the block, peers validate it and publish it to the blockchain. Its advantages include high throughput and low power consumption, but it lacks scalability and can cause delays due to the network waiting for all nodes' votes.

Delegated Byzantine Fault Tolerance (DBFT) [58] is based on the PBFT [61] principle but does not require all peers to vote to submit a new block. A group of peers is chosen as delegates based on specific criteria and a consensus protocol, such as PBFT. Several trusted nodes are elected to store data for all nodes in this mechanism. The NEO blockchain platform utilizes this protocol [62]. The advantage of DBFT is improved efficiency and scalability, while its drawbacks include a potential compromise of decentralization due to the restricted number of voters and reliance on trusted delegates.

Proof of Authority (PoA) [63] is a new class of permissioned blockchain-based Byzantine Fault Tolerant (BFT) consensus protocols. In the PoA protocol, authorities are a set of nodes in the network, each given a unique identification under the assumption that the majority of them are trusted. The PoA protocol uses a rotational mining mechanism to achieve consensus. Time is divided into slots, with a mining leader chosen for each slot. PoA was developed for the private Ethereum platform [35] and implemented in both the Clique and Aura versions. Geth [64] and Parity [65] are two well-known Ethereum clients that utilize PoA. PoA is suitable for distributed applications because it does not require high power consumption, generates blocks at predetermined intervals for increased transaction rates, and offers better scalability. However, its drawbacks include centralization risks and reliance on trusted authorities.

Proof of Elapsed Time (PoET) [66] was first proposed as a blockchain consensus protocol by Intel. Each miner must solve a mathematical puzzle, and a block approver (miner) is chosen at the earliest possible moment based on a hash function to create a block. The election process uses the Trusted Execution Environment (TEE) to randomly select miners across the network. Intel hardware presents TEE based on Secure Guard Extension (SGX), preventing malicious attacks by ensuring that only one instance of the chain runs on a single CPU. Strengths of PoET include high efficiency and fairness, while its drawbacks include reliance on specialized hardware and centralization risks.

Proof of Vote (PoV) [67] is a consensus protocol in which a voting authority verifies each block and grants nodes approval to create blocks. The distributed nodes, managed by consortium partners, coordinate consensus, resulting in decentralized arbitration by vote. The main objective is to provide separate, secure identities for network users so that block submission and verification can be chosen by the league's vote without a third-party mediator. PoV offers convergence reliability, controllable security, and low-delay transaction verification. However, it has centralization risks due to reliance on a limited number of voters.

Proof of Conformance (PoC) [68] is a consensus mechanism for both consortium and private blockchains, where the block generator requires the authorization of more than 2/3 of the existing participants. It enables keyword search within consortium blockchains to ensure

privacy preservation, access control, and secure searches of encrypted data, including user identities and keywords. Strengths include strong security and access control, while drawbacks include limited scalability and reliance on consortium-based validation.

Proof of Authentication (PoAh) [69] is a lightweight blockchain authentication protocol for resource-constrained devices in IoT and edge computing. It is suitable for private and permissioned blockchains, ensuring security, scalability, and sustainability. Miners, known as trusted nodes, use unique identification to validate block sources. PoAh has the benefits of low power consumption and suitability for IoT but poses centralization risks due to reliance on trusted nodes.

In summary, consensus protocols are a critical component of blockchain technology, ensuring trust, security, and global consistency across decentralized networks. These protocols vary in performance efficiency, security guarantees, and levels of decentralization, as outlined in Table 3. Key quantitative metrics such as transaction throughput, latency, and energy consumption play a crucial role in evaluating their efficiency. It is important to note that these metrics, as referenced in [70, 71], are **estimates** and can vary significantly based on specific implementations, network conditions, and environmental factors. The selection of an appropriate consensus protocol depends on the specific use case and the desired trade-off between performance, efficiency, and security. Additionally, the choice must align with the capabilities of the underlying blockchain platform. Understanding these variations is essential for making informed decisions when designing blockchain-based systems. Building on this foundation, the next section explores key factors to consider when selecting a blockchain platform for real-world applications.

4.4 Blockchain platforms

One of the most important steps in beginning to design and create real-world blockchain apps is to choose the appropriate underlying blockchain platform. The following are the main platforms:

Bitcoin [29] is the first and most widely used blockchain platform for performing digital financial transactions without involvement from a central authority such as a bank. Through a scripting language, Bitcoin makes it possible to construct smart contacts. Due to the programming language's limitations, Bitcoin, on the other hand, is an unsuitable choice for smart contract creation.

Ethereum [35] is a platform based on blockchain technology that has greatly influenced the recent advancement of blockchain. Due to a built-in programming language called Solidity, Ethereum is widely recognized as the leading platform for facilitating smart contracts. The flexibility of smart contracts that can be created and executed on Ethereum enables blockchain technology to be used in a range of applications beyond cryptocurrency. As a result, Ethereum has become the most popular platform for creating blockchain applications. The two most popular Ethereum client implementations are Parity and Geth.

MultiChain [37] is a platform based on blockchain that allows participants to easily establish private blockchains within enterprises. It gives users a command-line interface to communicate with the network and uses a simple API to enhance the Bitcoin [29] API's fundamental functionality. Through the API, MultiChain allows multiple clients to connect with the network using PHP, Go, C#, Java, Ruby, Python, and Node.js.

HydraChain [41] is an extension of the open-source Ethereum [35] blockchain that enables the creation and implementation of permissioned blockchains. HydraChain supports the creation of smart contracts via Python and is fully consistent with the Ethereum platform. HydraChain's main benefit is that it allows different system components to be readily customized based on client requirements. Many tools are supported, allowing for a fast decrease in development time while also enhancing debugging capabilities.

Quorum [38] is an Ethereum-based platform for developing decentralized blockchain apps for enterprises easily. Quorum is an excellent choice for applications where transaction processing speed and throughput are important. In terms of functionality, Quorum is essentially identical to Ethereum. However, there are a few changes, such as voting-based consensus protocols, enhanced transaction and contract privacy, management of the network and peer permission, and improved performance. Quorum enables smart contracts, transaction confidentiality, privacy, and Byzantine fault tolerance consensus protocols.

Hyperledger Fabric [40] is a blockchain-based platform developed by the Linux Foundation, designed for enterprise applications and available as open-source software. Hyperledger Fabric provides the flexibility of using general-purpose programming languages such as Java, Node.js, and Go to create smart contracts. This makes it easier for businesses to use blockchain solutions, since developers don't have to learn another programming language to create smart contracts. Hyperledger Fabric has another important feature: it allows pluggable consensus mechanisms, which allow the platform to be customized for an organization, including use-cases.

In summary, selecting the right blockchain platform is critical for developing efficient, secure, and scalable blockchain applications. Factors such as scalability, security, decentralization, and compatibility with consensus protocols must be carefully evaluated. Popular platforms like Ethereum, Hyperledger Fabric, and Quorum offer

Table 3 A comparison of consensus protocols

Consensus protocol	Year	Appropriate blockchain	Mining technique	Blockchain platform	Decentr-alization	Estimated throughput	Estimated latency	Energy usage	Advantages	Disadvantages
Proof of work (PoW) [29]	2008	Public blockchain	Node solves hash puzzle. Based on power consumption	Bitcoin, Litecoin, Ethereum	High	7 TPS	10 min	Very High	High security. High decentralization	High power consumption. Vulnerable to 51% attack and Sybil attack
Proof of stake (PoS) [43]	2012	Public blockchain	Node with most stakes. Based on validation	Ethereum, Qtum, Wanchain, Stratis, NXT	Medium	30–100 TPS	10–60 sec	Medium	High throughput. Energy efficiency. Fast block creation time. Independence to the special hardware	Highly dependent on nodes with the most stakes, which makes the blockchain somewhat centralized. Vulnerable to DOS attack and Sybil attack. Problem called "nothing at stake"
Delegated proof of stake (DPoS) [59]	2013	Public blockchain	Nodes vote to choose delegates to validate blocks. Provide a democratic and fair way through the voting procedure	Bitshares, LSK, ARK, EOS, Nano, Cardano, Tezos	Medium	>1000 TPS	1–10 sec	Low	High scalability. Energy efficiency. Low-cost transactions. Solving the problem of double-spending	Limitation on the number of delegated stakeholders makes the network semi-centralized
Proof of activity (PoAc) [60]	2014	Public blockchain, Consortium blockchain	Solve a hash puzzle, then the node with the most stakes adds the block. Based on Pow and PoS	Bitcoin	High	15 TPS	10 min	High	Protecting the network from some potential attacks, such as the 51% attack	Consuming a lot of resources. Energy consumption. High latency. Vulnerable to double-spending attacks
Practical byzantine fault tolerance (PBFT) [61]	1999	Private blockchain, Consortium blockchain	The block will be recorded to the chain if it has at least 2/3 of the nodes agreeing upon it. Based on voting	Hyperledger Fabric, Hyperledger Sawtooth	Medium	10,000 TPS	1–5 sec	Low	High throughput. Low power consumption. Detection of malicious nodes	Lack of scalability parameters. Unscalable for large networks. High network overhead and potential delays. Vulnerable to Sybil attack
Delegated byzantine fault tolerance (DBFT) [58]	2017	Public blockchain	Some nodes are selected as delegates of the others to add blocks. Based on PBFT	NEO	Medium	1,000 TPS	15 sec	Low	Low latency than PBFT. More scalable than PBFT	Limiting the number of voters may compromise the network's decentralization
Proof of authority (PoA) [63]	2017	Public blockchain, Private blockchain	Time is split into several slots, and an authority mining leader is chosen for each slot. Based on BFT	Ethereum, Apla	Medium	1,000 TPS	5 sec	Low	Less computational power. High throughput and scalable due to authorized nodes generating blocks at specific time intervals	Relies on a set of authorities, which may affect the blockchain decentralization feature. By identifying the authorities, it is a centralized system

Table 3 (continued)

Consensus protocol	Year	Appropriate blockchain	Mining technique	Blockchain platform	Decentr-alization	Estimated throughput	Estimated latency	Energy usage	Advantages	Disadvantages
Proof of elapsed time (PoET) [66]	2015	Consortium blockchain, Private blockchain	Each miner has to solve a hash problem. The winning one is selected based on a random wait time where it finishes first. Based on Intel SGX	Hyperledger Sawtooth	Medium	1000 TPS	3 sec	Very Low	Protects against malicious attacks by preventing several instances of the chain from running on a single CPU. Lower energy consumption. Low latency. High throughput	Relies on Intel, which compromises the blockchain decentralization feature. Works only on dedicated hardware security
Proof of vote (PoV) [67]	2017	Consortium blockchain	A voting authority verifies each block and grants nodes' approval to add blocks. Based on Voting	Ethereum	Medium	500–1000 TPS	5–10 sec	Low	Convergence reliability. Controllable security. Low-delay transaction verification time	A limited number of voters may affect the network's decentralization. High latency of transactions if the number of nodes is increased
Proof of Conform-ance (PoC) [68]	2018	Private blockchain, Consortium blockchain	Dependent on the block generator's validity (authorization of more than 2/3 of the current participants)	JUICE	Medium	100-1,000 TPS	5–60 sec	Low	Keyword search to provide privacy preservation. Access control and secure search of all encrypted data	Does not handle the conjunctive keyword search
Proof of authenti-cation (PoAh) [69]	2019	Private blockchain	A trusted node is introduced to authenticate blocks based on a validation mechanism in blockchain	Proposed by author	Medium	500-1,500 TPS	3–5 sec	Low	Consuming very little power. Suitable for devices with limited resources	The presence of authenticating nodes within the network is necessary, which can result in increased traffic towards these nodes

unique features tailored to different use cases, from decentralized applications to enterprise solutions. In healthcare, blockchain technology has the potential to address key challenges such as access control, privacy, and data security. Its decentralized nature ensures transparent and secure data sharing, while cryptographic techniques protect sensitive patient information. Building on these foundations, the next section explores blockchain-based privacy-preserving techniques and their applications in healthcare.

5 Privacy-preserving cryptographic techniques in healthcare

Ensuring privacy in blockchain-based healthcare systems is critical due to the sensitive nature of EHRs. Traditional security measures often fail to provide strong guarantees against adversarial attacks, as evidenced by the compromise of over 112 million healthcare records in 2015 alone [72]. To address these challenges, advanced cryptographic techniques have been integrated with blockchain technology to enhance security and privacy. This section formally defines key privacy-preserving cryptographic techniques, presents their security models, and discusses their applications in healthcare.

5.1 Secure multi-party computation (SMPC)

Definition SMPC [73, 74] is a cryptographic technique that allows N parties to collaboratively compute a function $f(x_1, x_2, \ldots, x_N)$ over their private inputs x_i while ensuring that no party learns anything beyond the function output. Formally, an SMPC protocol satisfies the following security guarantee:

$$\forall i \in \{1, 2, \ldots, N\}, \text{Party } i \text{ learns nothing beyond } f(x_1, x_2, \ldots, x_N).$$

Secret Sharing (SSharing) in SMPC: SMPC fundamentally relies on *SSharing* [75], a technique that distributes a secret among multiple participants in such a way that only a subset of them can reconstruct it. The two primary secret-sharing schemes used in SMPC are:

- *Shamir's SSharing*: Based on polynomial interpolation, where a secret is divided into shares using a polynomial of degree $t-1$, requiring at least t shares to reconstruct the original secret.
- *Additive SSharing*: The secret is split into random shares that sum to the original value, commonly used in arithmetic SMPC protocols due to its efficiency in homomorphic operations.

By leveraging SSharing, SMPC enables computations over encrypted data without exposing individual inputs, making it ideal for privacy-preserving blockchain applications.

Security Model: SMPC ensures the following cryptographic properties [76]:

- *Privacy:* No party learns another participant's input beyond what is revealed by the function output.
- *Correctness:* The computed result is guaranteed to be accurate, even in the presence of dishonest participants.
- *Fairness:* Either all participants receive the output or none do, preventing selective disclosure.
- *Input Independence:* Each party chooses their input independently of others, ensuring no premature knowledge of input values.

Threat Model: The security of SMPC protocols is analyzed under two adversarial models [76]:

- *Semi-Honest Adversary (Passive Attack):* Follows the protocol but attempts to infer additional information from exchanged messages.
- *Malicious Adversary (Active Attack):* Deviates from the protocol to learn unauthorized information or manipulate computation results.

Applications in Healthcare: SMPC is particularly relevant in blockchain-based healthcare applications where privacy and security are critical. When integrated with smart contracts [77–81], SMPC enables secure computation on patient data without relying on a Trusted Third Party (TTP). For example, the HDG framework [78] utilizes SMPC to allow healthcare providers to process patient data securely while preventing data leakage. Despite its strong security guarantees, SMPC suffers from performance limitations, such as high computational overhead and communication complexity, requiring further optimization for practical deployment [82].

5.2 Homomorphic encryption

Definition Homomorphic encryption [83] is a public-key encryption scheme that enables computations directly on ciphertexts without requiring decryption. A homomorphic encryption scheme consists of the following core algorithms:

- $\mathsf{KeyGen}(1^\lambda) \rightarrow (pk, sk)$: Generates a public-private key pair.
- $\mathsf{Enc}(pk, m) \rightarrow c$: Encrypts plaintext m into ciphertext c.
- $\mathsf{Dec}(sk, c) \rightarrow m$: Decrypts ciphertext c to recover plaintext m.

Depending on its structure, a homomorphic encryption scheme can support either additive, multiplicative, or both types of homomorphic operations:

$$\mathsf{Dec}(sk, \mathsf{Enc}(pk, m_1) \cdot \mathsf{Enc}(pk, m_2)) = m_1 \cdot m_2 \quad \text{(Multiplicative Homomorphism)}$$

$$\mathsf{Dec}(sk, \mathsf{Enc}(pk, m_1) + \mathsf{Enc}(pk, m_2)) = m_1 + m_2 \quad \text{(Additive Homomorphism)}$$

A Fully Homomorphic Encryption (FHE) [84] scheme supports both addition and multiplication over encrypted data, making it suitable for privacy-preserving computations.

Security Model: The security of homomorphic encryption is defined under rigorous cryptographic assumptions [85]:

- *Indistinguishability under Chosen Plaintext Attack (IND-CPA)*: An adversary cannot distinguish between the encryptions of two plaintexts even when given the public key.
- *Adaptive Chosen-Ciphertext Attack (CCA) Security*: Fully homomorphic encryption models extend security under adaptive chosen-ciphertext attacks.

Threat Model: Homomorphic encryption ensures resilience against several attack vectors [86]:

- *Ciphertext Leakage:* No meaningful information is revealed about the plaintext.
- *Brute Force Decryption:* Security relies on hard mathematical problems, such as lattice-based cryptography.
- *Adaptive Adversaries:* Adversaries may adaptively choose inputs based on previous outputs.

Applications in Healthcare: Homomorphic encryption is another critical tool for privacy-preserving healthcare applications [87–91]. Homomorphic encryption enables statistical analysis on encrypted health data, ensuring privacy and precision. Despite its robust privacy guarantees, HE faces challenges such as high computational and memory overhead, limiting its scalability.

5.3 Zero-knowledge proof (ZKP)

Definition ZKP [92] is a cryptographic protocol that allows a prover P to convince a verifier V of the validity of a statement ϕ without revealing any additional information. A ZKP must satisfy:

- *Completeness:* If ϕ is true, an honest verifier is convinced by an honest prover.
- *Soundness:* A cheating prover cannot convince the verifier of a false statement.
- *Zero-Knowledge:* No additional information beyond the validity of ϕ is leaked.

Security Model: ZKP protocols are categorized based on interaction and computational assumptions [93]:

- *Interactive ZKP (IZKP):* Requires multiple rounds of interaction between the prover and verifier, ensuring security based on real-time challenge-response mechanisms.
- *Non-Interactive ZKP (NIZKP):* Achieved through a single-message proof, often using a shared reference string, eliminating the need for continuous interaction.

Threat Model: The security of ZKPs is analyzed under adversarial models [93]:

- *Adaptive Adversaries:* An adversary cannot extract useful knowledge from proof transcripts, even if they control computational resources.
- *Malicious Verifiers:* A verifier cannot infer private input data from the prover, even when deviating from the protocol.
- *Man-in-the-Middle Attacks:* Ensures that adversaries cannot tamper with proofs to forge valid statements.

Applications in Healthcare: ZKP are widely used in blockchain-based healthcare systems to enhance privacy and security [94–97]. For example, NIZKP technology in mHealth systems [94] ensures secure data sharing and transaction validation without requiring a TTP, improving healthcare outcomes.

5.4 Group signatures

Definition Group signatures [98] are a cryptographic primitive that enables a member of a predefined group to sign messages on behalf of the group while preserving anonymity. A designated group manager, however, has the capability to revoke anonymity and reveal the signer's identity if necessary. Group signatures provide a balance between privacy and accountability, making them useful in privacy-sensitive applications.

Security Model: A well-defined security model for group signatures ensures the following properties [99]:

- *Anonymity:* The identity of the signer remains hidden within the group unless explicitly revealed by the group manager.
- *Unlinkability:* Multiple signatures generated by the same signer are indistinguishable from those of other members.
- *Traceability:* The group manager can trace the origin of a signature and identify the signer in case of disputes or misuse.
- *Non-Frameability:* No entity, including the group manager or colluding members, can falsely accuse an honest member of signing a message they did not sign.

Threat Model: The security of group signatures is analyzed under various adversarial scenarios [99, 100]:

- *Forgery Resistance:* Only legitimate group members can generate valid signatures, preventing outsiders from forging signatures.
- *Collusion Resistance:* A subset of malicious group members cannot generate a valid signature that cannot be traced by the group manager.
- *Revocation Security:* A revoked group member should no longer be able to generate signatures, ensuring long-term security.

Applications in Healthcare: Group signatures are employed in healthcare frameworks [101, 102] to enable secure data sharing between institutions while maintaining patient confidentiality.

5.5 Ring signatures

Definition A ring signature [103] is a cryptographic scheme that allows a user to sign a message anonymously on behalf of a dynamically formed group of users, ensuring that the actual signer remains unidentifiable. Given a set of public keys, any member can generate a valid signature without revealing which specific key was used.

Security Model: A ring signature scheme must satisfy the following security properties [104]:

- *Anonymity:* The actual signer is computationally indistinguishable from the other members of the ring, preventing adversaries from determining the signer's identity.
- *Unforgeability:* Only a legitimate member of the ring can produce a valid signature, ensuring that unauthorized parties cannot create fraudulent signatures.

Threat Model: Ring signatures are subject to various attacks, including [105]:

- *Linkability Attack:* An adversary attempts to determine whether multiple signatures originate from the same signer, thereby compromising anonymity.
- *Forgery Attack:* A non-member attempts to generate a valid ring signature without access to any legitimate private key.
- *Key Exposure Attack:* If a participant's private key is compromised, an adversary might use it to generate unauthorized signatures while remaining undetected.

Applications in Healthcare: ring signatures allow anonymous message signing in blockchain-based health information exchange systems [106–109], though they may introduce latency and reduce throughput.

In summary, privacy-preserving cryptographic techniques such as SMPC, homomorphic encryption, ZKP, group signatures, and ring signatures play a vital role in securing blockchain-based healthcare systems. While each technique offers unique security and privacy guarantees, their individual limitations often hinder practical deployment in large-scale healthcare applications. To address these challenges, hybrid cryptographic approaches that combine multiple privacy-preserving techniques have emerged as a promising solution. By integrating complementary techniques, such as combining homomorphic encryption with SMPC for secure multi-party computations on encrypted data or leveraging ZKP alongside ring signatures for enhanced anonymity in transaction validation, hybrid cryptography enhances both privacy and security. These integrated approaches not only mitigate the computational overhead and scalability issues of standalone techniques but also provide stronger protection against evolving threats. Building on these cryptographic foundations, the next section explores blockchain-based access control frameworks, which leverage these advanced techniques to enforce secure and fine-grained access policies in healthcare applications.

6 Blockchain-based access control frameworks in healthcare domain

The data generated in the e-health domain includes a significant quantity of confidential patient information. If this confidential information was made public, patients would suffer significant data breaches. One of the most essential data security solutions is access control, which guarantees that data can only be read with the authorization of a patient or healthcare provider. To prevent unauthorized access and ensure permitted access, the access method relies on an approval policy that restricts access to specified resources. Auditing, authorization, and authentication are the main characteristics of the system's access control mechanism [110]. A decentralized personal data management system may be implemented on the blockchain-based e-health platform, which may differentiate between data access and data authority [111]. An application needs the owner's permission to access data [112]. The system verifies that the application can get the relevant data by checking the signature and all the records. The blockchain stores a complete record of the application's operations, and users can modify the data's access privileges at any moment [113]. Blockchain-based access control frameworks in the healthcare domain can be broadly categorized into permissionless and permissioned blockchain-based frameworks. Figure 7 illustrates this categorization and highlights the key characteristics of each type.

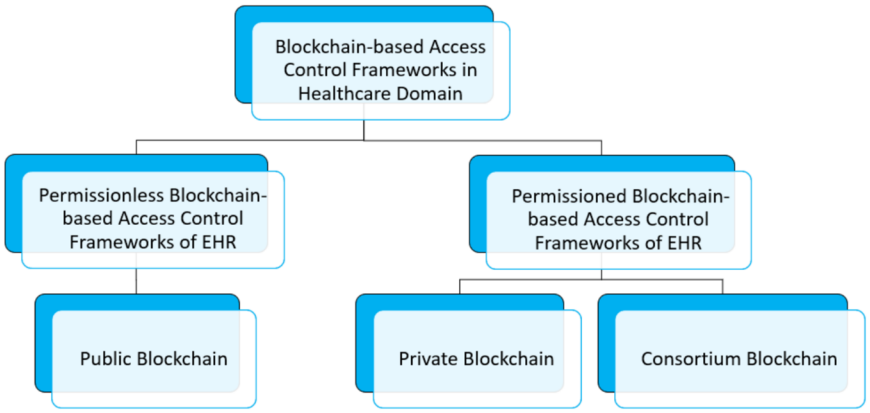

Fig. 7 Categlhcare Domain

6.1 Permissionless blockchain-based access control frameworks of EHR

Permissionless blockchains are developed using cryptographic protocols to prevent tampering while storing and sending data through P2P networks. Users of the blockchain can create personal addresses and use them to engage the network through the submission of each transaction to the ledgers. Although permissionless blockchains are public, and anybody may join the network, requests should only be made by authorized participants, who sign each transaction using their private keys. Furthermore, to validate transactions and store them in the blockchain as new blocks, all nodes should utilize a consensus protocol. Permissionless blockchains, such as Ethereum [35], enable smart contracts as self-executing transactions when certain conditions are met. As a result, the permissionless blockchain provides more frameworks for implementing an EHR access control method. The Ethereum blockchain is the most well-known permissionless blockchain that can be used in healthcare for access control [114].

MedRec [115] is an Ethereum-based blockchain framework that enables patients to transmit and access their EHRs with various healthcare providers. Due to the storage and capacity limitations of EHRs, MedRec will use smart contracts to define access controls rather than storing traditional EHRs. Three types of smart contracts were developed: (1) Register Contract (RC), which hides the identities of the patients by linking their identities to Ethereum addresses via the Domain Name System (DNS) [35]; (2) Patient-Provider Relationship Contract (PPR), which is developed to handle the data storage challenge in blockchain systems by defining a reference to healthcare providers' databases, which hold patients' EHRs and access rights; and (3) Summary Contract (SC), which maintains a collection of PPRs of patients and all current activities in the network to present a health record history.

HDG [78] is a blockchain-based framework that enables each patient to control access to EHRs stored in healthcare provider databases. HDG addresses the issue of data privacy by establishing an indicator-centric schema (ICS), where each data access request is categorized into two types: one for users who require raw data access and another for users who want to analyze data and obtain results. HDG utilizes the SMPC technique to allow an untrusted third party to perform computations on patient data while ensuring patient privacy.

BHEEM [116] is a blockchain-based framework designed to provide efficient and secure access to medical data for providers, patients, and third parties while preserving patient privacy. Built on the Ethereum platform [35] and utilizing a consensus process called proof of vote [67], BHEEM includes several smart contracts to manage EHR accessibility: a classification contract to divide nodes into healthcare providers, patients, and other parties; consensus contracts for voting permissions and approved participants; a service contract to track patients' access control; an owner contract to manage EHR ownership; and a permissions contract for granting, revoking, and altering permissions for each EHR. The framework categorizes blockchain network nodes into light nodes, full nodes, and archive nodes. It addresses the data storage challenge by connecting to patients' EHRs in local datasets through a database management entity and ensures privacy by employing a differential privacy model [117], which adds noise to transactions.

Most of the current EHR security mechanisms store patients' EHRs in local cloud storage or off-chain, lacking the decentralization necessary for robust access control and privacy preservation. The proposed methods for managing large-scale data often fail to address this need adequately. The Inter-Planetary File System (IPFS) [118] offers a significant solution by enabling secure data transfer within a blockchain system. IPFS allows clients to store their data on a decentralized file system and retrieve it without relying on a central server, thereby enhancing both access control and privacy preservation in healthcare data management.

A secure EHR sharing framework [119] is proposed to implement an access control mechanism using smart contracts to enable secure sharing of EHRs among patients and medical providers. The framework relies on the Ethereum platform [35], utilizing smart contracts to verify each request for adding EHRs and accessing existing ones. Patients' encrypted medical data is sent to the IPFS storage system [118], while the Ethereum platform stores only user addresses and hashes for access control management. On the blockchain, patients are identified by a combination of area IDs and patient IDs, with area IDs serving as a proxy for the patient's residence and used for classification.

Healthchain [120] is a hybrid blockchain-based access control framework designed to handle large-scale health data privacy preservation. It encrypts health data to implement fine-grained access control, allowing patients to dynamically revoke access permissions by updating keys and uploading them to the blockchain. To ensure data integrity and proper data mapping in IPFS storage, each EHR in Healthchain is encrypted and stored in the IPFS storage system [118], with corresponding hashes maintained on the blockchain network. Healthchain consists of two blockchains: (1) Userchain, which facilitates the sharing of patient EHRs on a public blockchain, and (2) Docchain, which stores doctor reports on a consortium blockchain. The Userchain is responsible for collecting and maintaining patient data, while the Docchain allows authorized physicians to monitor patients and record reports.

A blockchain-based framework for clinical trails (CT) data management [42] utilizes Ethereum as an underlying platform and smart contracts to address the issue of CT data control where patient EHR is stored in the IFPS storage system, as shown in Fig. 8. To simplify operations and data transmission across CT stakeholders, the model uses IPFS [118] as a file storage system. Tampering with CT documents in the IPFS is very hard because they are assigned unique cryptographic hashes and the IPFS storage is decentralized. The framework includes algorithms for managing CT data at various phases.

An Ethereum-based blockchain framework [121] was proposed to provide patients with authority over their EHRs in a confidential and verifiable manner. The proposed model uses decentralized IPFS [118] storage and a trusted reputation-based re-encryption oracle to securely retrieve, store, and exchange patients' EHRs for the purpose of encrypting the patient's key with the symmetric key of the physicians. When patients receive an access request from an authorized doctor, they are responsible for creating the re-encryption keys. Oracle re-encryption gets the required EHRs and encrypted symmetric keys from IPFS, which they then re-encrypt and send to the doctor. The oracle also produces hashes of the ciphered symmetric keys and delivers them to the smart contracts of the patient for analysis. However, the patient is not able to delegate access to doctors in emergency cases.

SecureRx [122] is a framework based on blockchain and built on top of the Ethereum blockchain [35] that enables participants to access prescription information in a safe, interoperable, and efficient manner. It enables healthcare providers to double-check the medical history of the patient and make informed decisions about whether to prescribe opioids. SecureRx is composed of three major software elements, i.e., a JavaScript-based web application, an Ethereum smart contract, and a database simulator. SecureRx addresses the major flaw in the current prescription system and allows appropriate authorities to monitor and track patients' prescription information across many states in a secure manner. The Ethereum smart contracts were intended to make tracking all the requests for data and comments easier using the Solidity high-level language. The proposed framework has the advantage of high scalability and throughput when the number of nodes is decreased. However, in high workload conditions, there is no clear approach for evaluating this framework's throughput and scalability.

SPChain [123] is a blockchain-based framework for privacy preservation and medical data transfer in the e-health system, as shown in Fig. 9. The system was designed to achieve fast retrieval of patients' EMRs by using specific keyblock and microblock blockchains. Keyblocks store register transactions, while label transactions and medical transactions are linked to the microblocks of the patients. SPChain was able to share medical data with patients while preserving their privacy using proxy re-encryption techniques. It employs chameleon hash functions [124] to develop a structure in the block that store each patient's entire medical history. EHRs can only

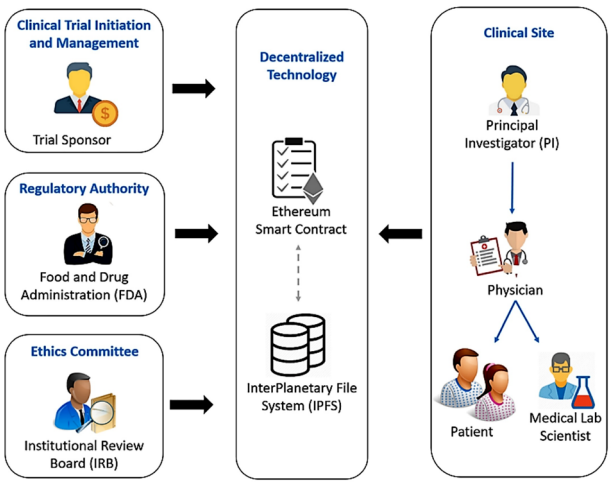

Fig. 8 An overview of clinical trails (CT) framework [42]

be queried by authorized healthcare providers. SPChain has three kinds of transactions in the system, namely: register-transaction, label-transaction, and medical-transaction. The indexes of the bonded microblocks are stored in the key-block as register transactions. SPChain's consensus protocol is a hybrid of Pow [29] and BFT. SPChain has low storage overhead, high throughput, and a high level of resistance against blockchain attacks. However, it should decrease communication overhead and improve throughput.

HealthLock [91] is a blockchain-based solution aimed at enhancing privacy preservation in IoT-based healthcare applications through the utilization of homomorphic encryption techniques. It integrates smart contracts into the blockchain network to enforce access control and define data-sharing policies. The framework also generates a comprehensive audit trail of all data transactions, enhancing accountability and transparency. Furthermore, deep learning techniques have been implemented for predictive data analytics in the medical field. Nevertheless, it's essential to acknowledge certain limitations of the framework, such as constrained scalability and performance concerns, as homomorphic encryption is a computationally intensive technique.

Peng et al. [125] introduced a privacy-preserving framework for sharing EHRs based on a dual-blockchain system. They devised an identity-based tripartite authentication key agreement (TAKA) scheme, offering patients precise control over their EHR access. In this setup, the dual blockchain fosters trust between patients and healthcare institutions, ensuring the immutable storage of EHR digests, and overseeing doctors whose identities have expiration constraints. However, the framework's reliance on bilinear pairing operations for authentication impacts system efficiency and lacks scalability. Lax et al. [126] proposed utilizing blockchain to obscure the link between patients' identities and their e-health records, providing exclusive access to entities authorized by patients. Key aspects involve employing a digital identity for access control and implementing it on the Ethereum blockchain. However, the framework expects patient authentication

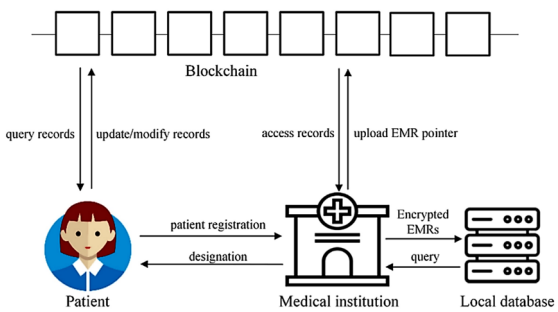

Fig. 9 An overview of SPChain framework [123]

before each EHR operation, and the use of a public blockchain, like Ethereum, introduces an average delay of 10 s. Additionally, the framework is not fully implemented.

An Ethereum-based blockchain framework [127] was proposed to enable a distributed application for an IoT-based healthcare system. It controls unauthorized access and manipulation of medical certificates, effectively preventing fraud in healthcare documents. The distributed application serves as an interface between the blockchain network and system entities, including healthcare centers, verifiers, and regulatory authorities, streamlining the generation and issuance of medical documents. Nevertheless, the framework has drawbacks, such as its exclusive focus on medical certificates and the fact that the PoW protocol requires substantial energy resources.

Chinnasamy et al. [128] proposed a smart contract-enabled access control framework for secure sharing of EHRs in mobile cloud-based e-health systems. The framework leverages blockchain technology to replace centralized systems with a decentralized, trustworthy architecture, ensuring the privacy, security, and accessibility of healthcare data. It supports continuous data streams from sensors and monitoring devices, addressing the limitations of traditional cloud-based platforms. The system was implemented on the Ethereum blockchain and evaluated using AWS cloud, demonstrating lightweight access control and low latency. However, its reliance on cloud infrastructure may partially compromise the decentralization benefits of blockchain.

6.2 Permissioned blockchain-based access control frameworks of EHR

Permissioned blockchains are restricted systems in which users must be identified and registered in order to access and submit transactions. Like private networks, they are often managed by centralized entities. Permissionless blockchains might not have been fully trusted by healthcare providers such as Ethereum [35], due to their privacy requirements, which prevent anonymous participants from accessing private data. There is also a storage overhead issue in permissionless blockchains, where all data and transactions are stored by full nodes, necessitating a large capacity of storage and substantial maintenance costs for such enterprises.

The Hyperledger Fabric is the best-known permissioned blockchain [40], which is utilized in permissioned blockchains where all participants should be identified. The transactions of Hyperledger Fabric are classified into two categories: code-deploying transactions, which are used to deploy, alter, or terminate a portion of a smart contract; and code-invoking transactions, which are utilized to execute

smart contract functionalities for performing blockchain transactions. There are three phases to a Hyperledger transaction: (1) Phase of Execution: The request for transactions will be verified and sent out to participants, who will be in charge of validating the transactions using smart contract functions based on existing policies. (2) Phase of Ordering: Blocks are formed by grouping transactions and subsequently hashing them together. (3) Phase of Validation: Check the proposed blocks' validity and add them to the recorded ledgers if they do not violate any of the smart contract's existing rules.

ChainAchor [95] proposed the first permissioned blockchain system for access control and management of EHR that used the EPID zero-knowledge proof technique [129] to anonymize the data owners' identities. In actuality, the EPID zero-knowledge proof scheme enables the participant to verify transactions with diverse EPID secret keys while only validating them with one EPID public key. Permissions Verifier (PV) and Permissions Issuer (PI) are the two essential parts of ChainAchor. In order to receive the transaction's public key, the PI is responsible for providing user-specific keys that each user may use to confirm his or her participation in the PV by utilizing the ZKP technique [130]. In a PV database, the public key of the transaction should be specified. Since a participant may have a numerous public keys, the PV is not able to validate the identities of the participants. ChainAchor utilizes consensus nodes to validate transactions that use the PV database's current public keys, where access control is implemented. Unknown transactions may be readily discarded using the proposed scheme, since the PV database lacks a public key. The proposed framework has a drawback in that it lacks performance justification.

A permissioned blockchain-based framework [131] was proposed to allow EHR transmission by keeping the original data off-chain, utilizing Fast Healthcare Interoperability Resources (FHIR), and storing a reference on-chain. This framework proposes a consensus mechanism called the Proof of Interoperability (PoI) to ensure that each transaction is interoperable given a set of established semantic and structural constraints. The PoI consensus protocol allows the participants who make transactions to know which consensus nodes will be chosen as miners without publishing this information to the network. The blockchain may be queried by approved participants through a search in the encrypted transactions [132] to avoid data breaches by using some keywords to obtain the FHIR reference. The data referenced on the blockchain was utilized as a patient's identification to ensure anonymity, similar to the Bitcoin platform [29] due to the fact that each patient has several block addresses. The proposed framework has a drawback in that it lacks permission delegation and revocation, and the off-chain data storage is unknown.

MeDShare [133] is a permissioned blockchain-based framework that enables each patient to distribute and monitor their EHRs using smart contracts. MeDShare manages access controls and tracks modifications to the EHRs. MeDShare is composed of three layers: (1) a data layer that classifies users; (2) a data query that handles access requests and translates instructions to and from the smart contract; and (3) a structural layer of data that uses smart contracts and datasets of permissions to authenticate, store, and verify data access and modification requests. The authenticator verifies the signature of the requester. The consensus nodes will get the access request, which will use smart contracts to check for potential violations based on the policies of the owners and store the information in the permissioned database. The data is subsequently transferred to the authenticator, which will record the request for auditing reasons on the blockchain and obtain the relevant data from the cloud storage. The data has been categorized into two types: high-sensitive data and low-sensitive data, with the purpose of discarding the need for breach reports for the low-sensitive data, while the high-sensitive data should be tracked and identified by the smart contract in order to detect probable violations that might result in the request for the requested data being revoked. The framework's performance is mainly evaluated based on network latency measures, which is a disadvantage.

BBDS [134] was proposed to enable an access control mechanism and secure EHR sharing by utilizing cloud storage as a repository for EHRs with a permissioned Ethereum blockchain [35] to record access duration. The following steps can be used to apply user membership authentication in BBDS: (1) using the identity-based authentication (IBA) protocol [135] to generate a shared key for confidentially communicating with the issuer, who is in charge of producing a verification key for the membership reliant on the user's identification; and (2) using the authentication protocol of change-response [135] to generate the private keys dependent on the verification keys. After joining the blockchain, users have access to the data and create the transaction key pair (public and private keys) based on the issuer's parameters. The users may then use their private keys to produce access requests for EHRs, sign them with their transaction public keys, and send them to the unprocessed requests pool. Unprocessed blocks are validated using the PoW consensus mechanism before being added to the blockchain and granted permission to the cloud storage system. The proposed framework has a drawback in that it lacks detailed solutions for users and data owners.

An EHR access control framework [136] was proposed to establish access control over EHRs where access to data

is allowed to approved users reliant on smart contract policies. The proposed framework protected the patients' privacy by hashing the concatenation of the personally identifiable information (PII) and the patients' symmetric keys. Membership service is a vital part of the proposed framework, as users must first register in order to submit data or request access to off-chain data that has been outsourced to cloud storage. The membership service creates a pair of keys for verifying and validating the signatures after the user registers, as well as a pair of keys for securely distributing the blocks. Patients will also be required to encrypt EHRs using a symmetric encryption key before they are stored in the cloud. When the patient wants to share data with a physician, the physician's public key can encrypt the patient's encryption key. If a blockchain node gets requests from users via role-based APIs, the leader node uses the PBFT consensus protocol [137] to validate the transaction. The transaction may then be executed on these nodes utilizing the established smart contract policies. The smart contract's patient metadata contains (1) clinical metadata, which contains a hash of the record and a reference to an off-chain EHR that is stored in the cloud, and (2) permissions, which define the levels of physicians' access control. The proposed framework's drawback is that it relies on a central patient authentication process.

Ancile [138] was proposed as a secured access control method on the EHR that uses a permissioned blockchain (a private Ethereum [35]), with links to EHR hashes recorded on the blockchain and actual EHRs kept in healthcare providers' datasets. Ancile makes it easier to send EHRs to a TTP by re-encrypting them with the requester's public key, as described in the proxy re-encryption protocol [139]. Ancile uses six smart contracts to apply access control to the EHRs: (1) the consensus contract, which uses the QuorumChain consensus protocol to ensure block mining responsibilities [38]; (2) the classification contract, which divides nodes into three categories: patients, providers, and third parties; (3) the service history contract, which is used to ask a patient for permission to access his or her EHRs before enabling a healthcare provider to establish a connection with him or her; (4) an ownership contract (OC), which keeps track of the EHRs that are created by healthcare providers; (5) a permission contract, which is produced by the OC for each EHR to indicate each node's level of access control; and (6) a re-encryption contract, which re-encrypts the symmetric of data owners through proxy nodes, making it easier to provide EHRs to a TTP. The proposed framework has the drawback of being vulnerable to DoS attacks.

A permissioned blockchain-based access control framework [140] was proposed to authenticate users for establishing access control over EHRs, based on Shamir's SSharing [75]. The EHRs were stored on off-chain cloud-based storage. After the EHRs are outsourced, authorized users may send queries to receive permissions through an agent layer, which aggregates the queries using SSharing. The agent then forwarded the request to the layer of storage to get the required data after validating it. Furthermore, the agent ciphers the data received with the AES algorithm and provides it to the user along with a random value that the user can use to recreate the key to decrypt the EHR through SSharing. The proposed framework's drawbacks are that it has a significant storage cost and uses a centralized approach because it is being built in the cloud.

MediChain^{TM} [141] was proposed as a permissioned blockchain based on the Hyperledger [40] to gain access control over data, wherein the original EHRs are kept in cloud storage while the hashes of these data are recorded on the blockchain. Through the Hyperledger blockchain's Business Network Archive (BNA) feature, MediaChain^{TM} allows data owners to create a smart contract called Discretionary Access Control (DAC) for data that has been outsourced. The proposed method utilizes the PBFT consensus protocol to add a new block to the blockchain [61]. The proposed framework has drawbacks in that it doesn't handle essential requirements for access control, like delegation and revocation.

A BSPP [68] was proposed to address privacy concerns while securely sharing EHRs. The framework is used to establish a private blockchain for recording data as well as a consortium blockchain to store the relevant indexes for transferring EHRs between healthcare providers, as shown in Fig. 10. The system manager component of the BSPP is responsible for enrolling users and physicians, as well as storing their public keys and creating a consensus vector to confirm indexes. Whenever a patient connects to healthcare providers, the protected indexes of these blocks are published to the consortium blockchain, while a new block is recorded on the private blockchain with encrypted EHR and the patient's pseudo ID. To allow patients' data to be searchable by approved users, the public encryption with keyword search (PEKS) technique [142] is utilized to encrypt EHRs along with the necessary indexes. It may also be utilized to create a unique pseudo-ID for users by ciphering their actual identification to protect their privacy. A POC [68] as a novel consensus protocol is developed to submit new blocks to these blockchains based on the structure of the indexes and the tokens created for each patient upon enrollment with the healthcare providers. The created block will be recorded on the blockchain, according to the POC by the physician, if the block generator's identity is approved by more than 2/3 of the current physicians or healthcare providers. The proposed framework has a drawback in that it has high communication and storage overhead.

A secure EHR access control framework [143] was proposed to utilize a consortium blockchain to provide insurance firms with an EHR sharing system. Authorized users encrypt and decrypt data using cipher-text-policy attribute-based encryption (CP-ABE) [144] to provide authentication, confidentiality, and access control. The proposed framework creates the needed keys for healthcare providers, patients, and insurance companies through a single key generation center. If patients decide to publish their EHRs with an insurance firm, they should submit a letter of permission and send it to both the healthcare provider and the blockchain data pool, along with their secret keys. The hospital then ciphers the EHRs of the patients according to the permission regulations and transmits them to the data pool of the blockchain after signing the cipher text. The consensus nodes should match the permission letter and encrypted EHR before utilizing the consensus protocol to process the data and validate the provider's signature. The ciphered data should then be transferred to the cloud, with the associated addresses being stored on the blockchain. The proposed framework has a drawback in that it requires performance justification.

An EHR access control framework based on blockchain [145] was proposed with two types of blockchain: sidechain and mainchain, to provide access control management for efficiently distributing EHRs. The network's nodes are also classified into 2 groups: (1) trusted nodes, which are responsible for validating transactions and include trusted physicians who have access to both the mainchain and the sidechain; and (2) untrusted nodes, which include other organizations seeking to gain access to the EHRs of patients. Only trusted nodes may add new blocks to the mainchain, while the other nodes may submit requests and view the chain. The mainchain provides two kinds of transactions: (1) storage transactions, which are generated by physicians when they visit patients and provide temporary patient IDs that are stored in the sidechain; and (2) policy transactions, which enable patients to define access permission blocks for their EHRs to provide a certain degree of access control. It's vital to understand that the sidechain's purpose is to utilize transaction links given by authorized healthcare providers to construct a mapping between a transient ID of patients and their actual IDs. Therefore, the proposed framework protects the patient's privacy and data security by enabling patient anonymity via sidechains and signing transactions with the RSA algorithm. This framework uses a novel consensus protocol that requires the permission of 50% of the participating nodes to create a new block. The framework has a drawback in that it has a high storage overhead.

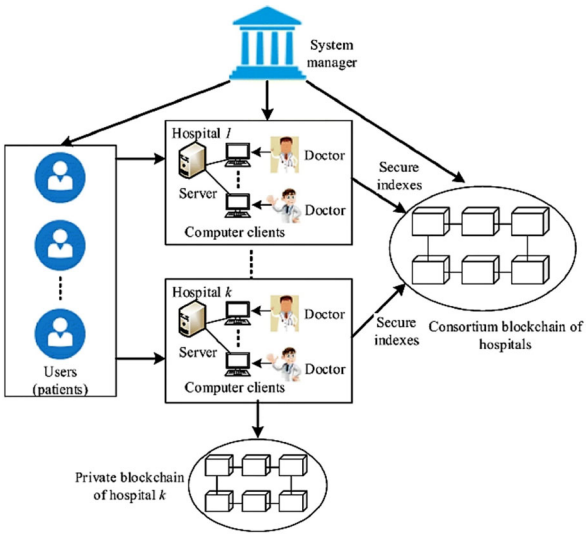

Fig. 10 An overview of BSPP framework [68]

An XACML-based access control management framework [146] was proposed for the secure sharing of EHRs, utilizing the eXtensible Access Control Markup Language (XACML) standard, to address the issues raised by the MediChain proposed method [141], in which smart contract access control policies should be kept in a consortium blockchain. If patients want access to EHRs, the miners evaluate the request according to the blockchain's existing smart contract. If the blockchain does not have any predefined policies, the data owner will get the access request and will either establish new access control policies or refuse this request. The proposed framework has a drawback in that it does not provide enough performance justification.

A Hyperledger-based Access Control Framework [147] was proposed for securely managing and controlling EHRs. To allow or deny access from a user, the proposed framework uses multiple smart contracts based on the Hyperledger platform [40], such as Grant Access and Revoke Access. A Membership Service Provider (MSP) is the core component of the developed framework, and it is responsible for enrolling healthcare providers and patients as well as creating public and private keys. The proposed framework has the drawback of having a high storage overhead and relying on MSP, so it lacks a decentralized feature.

A secure EHR access control framework [148] was proposed to handle the retrieval of multiple users' needs for access management of EHRs by utilizing the attribute-based encryption (ABE) technique [149] and enabling access control of patients. This framework's main concept is to keep ciphered medical data in the cloud, with extracted keywords distributed on a permissioned blockchain. Therefore, users may only access the EHRs of patients through their search metadata and by using the blockchain to execute keyword searches. The proposed framework's drawback is that the system's performance is

evaluated solely based on specific attributes and the time taken for searching.

GuardHealth [150] is a blockchain-based framework designed to enable users to dynamically grant and revoke data access permissions. It ensures confidentiality, authentication, and secure data sharing when handling sensitive information. Utilizing a consortium blockchain and smart contracts, GuardHealth protects data storage and transfer, preventing unauthorized data sharing. The framework separates raw data storage from data storage indexes, meaning that data is encrypted and stored in the cloud, while storage indexes are kept on the blockchain. GuardHealth employs proxy re-encryption [151] to manage access and revocation permissions. It supports two types of smart contracts: GH-IS (data sharing law) and GH-DS (data storage law). Built on the Ethereum blockchain platform [35], GuardHealth uses the DPoS [59] consensus protocol, where the stake represents the amount of health data collected. While the proposed scheme may meet security criteria and offer improved efficiency, its accuracy in detecting malicious activity does not significantly improve with a low number of participating nodes, and network latency increases with the number of nodes.

BCHealth [152] is an architecture based on blockchain that allows data owners to specify their preferred access permissions for their EHRs. The data of the patient is not distributed on the blockchain network without the patient's approval under the BCHealth architecture. BCHealth utilizes two distinct chains: the data chain and the access control chain. In a private blockchain, the data chain contains the patient's EHRs, while the access control chain keeps the patient's predefined access rules. BCHealth employs a novel clustering technique to improve the blockchain network's capacity and scalability. BCHealth might assist by alerting physicians as soon as the symptoms of the disease are identified, allowing them to take the best action. To enhance the system's efficiency and scalability, it employs a consensus protocol called Proof-of-Authority [63]. It establishes a permissioned blockchain in which only authorized nodes may join. It provides convenient computation and processing times and is resistant to a variety of security threats, but it has a little delay in retrieving health information and more storage overhead than the centralized solution. The number of nodes in each cluster and their clusters has not been optimized.

A blockchain-based medical information framework [153] was designed for secure access control and data transfer. It uses proxy re-encryption and cloud servers to anonymize data transfers. Built on Hyperledger Fabric [40] with Kafka as ordering service [154], the framework includes medical chaincode for access management. The system has five layers: management, data collection, blockchain network, cloud service, and application. It provides high throughput and efficiency but relies on semi-trusted cloud servers for encrypted data storage, which lacks blockchain decentralization features.

SmartMedChain [155] is a framework based on blockchain for privacy-preserving and sharing medical data in a smart healthcare environment. The framework uses smart contracts for secure data sharing and provides data usage auditing techniques and access control management for health data. The IPFS [118], a decentralized data storage system with high reliability and scalability, is utilized to record encrypted EHRs, and the blockchain is established on the Hyperledger Fabric platform [40]. SmartMedChain proposed an innovative privacy agreement management scheme to ensure that healthcare providers follow patients' preferences as well as any privacy standards and policies. It simply stores the health records' hash on the blockchain, with the real data being kept in the distributed storage platform IPFS after encryption to ensure health data scalability. The Hyperledger Fabric platform's Kafka ordering service [154] is utilized. This framework secures health data sharing amongst many participants by combining several blockchains: the data chain, the service chain, and the log chain. SmartMedChain provides efficient confidentiality, privacy, scalability, and integrity of health data while involving several blockchains that require a significant amount of computing resources.

PTBM framework [156] uses 5 G technology to track the current paths of patients with pandemic infections like COVID-19 and to monitor the public's locations without intruding on their privacy or identification. To achieve public location monitoring, supervised data storage, and tracing, permissioned and permissionless blockchains are utilized. PTBM achieves privacy protection while maintaining decentralization and accountability by integrating the blockchain's hierarchical design with robust cryptographic techniques. The proposed method enhances its privacy-preserving feature through the utilization of a public-key cryptosystem with strong key decryption (PCSD) [156] and hash functions. PTBM utilizes the Hyperledger Fabric [40] as the underlying blockchain platform, as well as flexible smart contract programmability and effectiveness. PTBM enables patient privacy protection and authentication with a low delay and a high communication cost. While the users' number increases, the average execution time of the system's registration process also increases, which causes high computational costs.

A blockchain-assisted SABE framework [157] was proposed to provide access control management for e-health systems, as shown in Fig. 11. The proposed framework uses a hidden access policy to provide a search keyword feature using the ABE technique [149]. In this framework, each participant is identified by a group of

related attributes, which are stored as health metadata. The framework, which combines numerous transaction rules and enables fair transactions, utilizes blockchain to avoid suspicious attacks and ensure search efficiency. Each hospital in the system creates its own private blockchain, while this framework creates a consortium blockchain that holds all the keywords for the EHRs created by each hospital. A blockchain consists of a set of authorized consensus nodes for managing medical data in this framework. For auditing purposes, the access requests and actions may be stored on the blockchain, while the encrypted EHRs are recorded in cloud storage. This framework allows for fast searches of health data, as well as lightweight data decryption for users. It also preserves the privacy of attributes and increases the efficiency of cloud service provider (CSP) searches, resulting in a low-cost technique with little communication and computation cost. In this framework, most of the decryption processes are outsourced to the CSP, which significantly reduces the user's computation overhead. However, depending on the CSP, it may eliminate the decentralization feature.

A blockchain-based IHT framework [158] was proposed to enhance the access control and privacy of data communication using the combination of smart contracts and blockchain with the information hiding technique (IHT), as shown in Fig. 12. It uses an enhanced steganography technique that hides the required data in other kinds of data, such as images. The smart contracts are deployed to automatically create a one-time hash for encryption operations, and the blockchain is used to establish trusted healthcare providers' clusters to interact. The private key is upgraded with each new communication initiation, removing the possibility of a cyberattacker and thereby improving the security and privacy of vital systems like smart healthcare. The framework has four tiers: (1) the healthcare IoT device tier; (2) the edge tier; (3) the fog tier; and (4) the cloud tier. The framework uses PBFT as a consensus protocol and the Hyperledger fabric as a private blockchain [40]. The framework tests the execution time of smart contracts using both the Hyperledger fabric and Ethereum [35], and the results show that the Hyperledger fabric-based smart contract provides a lower execution time. As compared to traditional techniques, this framework has a lower execution time and provides better security measurement. While the encryption and decryption phases of this framework have weaknesses, they are not discussed in detail.

Martínez et al. [159] presented a service-oriented framework leveraging blockchain technology. This framework implements fine-grained access control to safeguard health data based on consents, facilitates tamper-resistant and immutable storage of consents related to the subject of care, and incorporates auditing tasks for

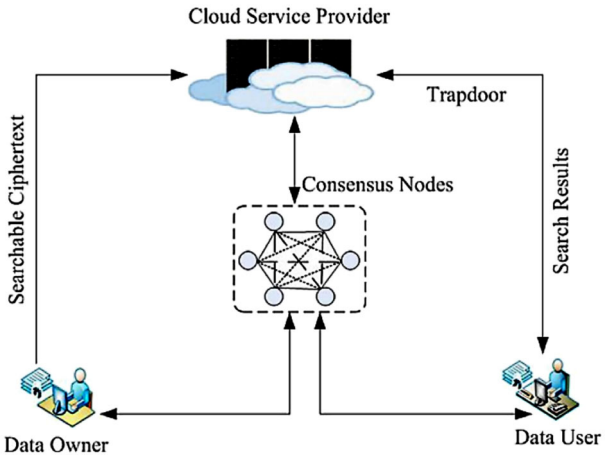

Fig. 11 An overview of SABE system [157]

supervisory authorities to evaluate healthcare organizations. It's worth noting that the blockchain network implementation has been confined to a single machine using Docker containers, posing limitations on the generalization of results.

Yang et al. [160] introduced an access control model that leverages the collaboration between the main and side chains of blockchain. In this model, a password-based authentication scheme is devised using doctors' identity information. The Polygon side chain is specifically designed to improve the storage scalability of the blockchain. Subsequently, access node information on the main Ethereum chain is situated on the side chain, and resources are acquired through the execution of Roll-up contracts deployed on the side chain. Nonetheless, the model overlooks the challenge of discerning the request type of Ethereum master chain nodes during periods of high concurrent access requests.

Mittal and Ghosh [161] introduced a two-tier access control system, incorporating the CP-ABE for authorization privileges and Proxy Re-encryption to secure data transfer, ensuring anonymity for the requester. While this method prevents unauthorized sharing of decryption keys,

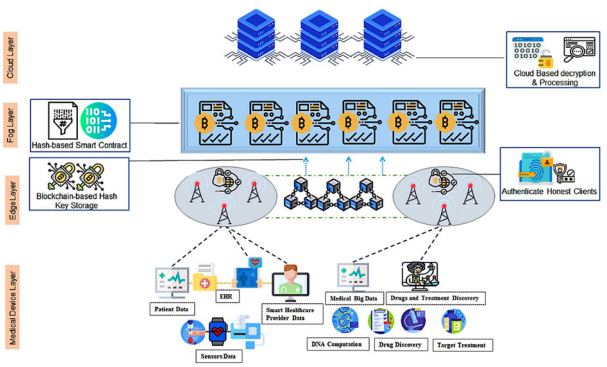

Fig. 12 An overview of blockchain-based IHT architecture. [158]

the use of CP-ABE introduces computational overhead proportional to the number of attributes in key generation, resulting in increased time costs. Alsuqaih et al. [162] presented a blockchain-based framework for enhancing privacy in e-health diagnostics. The framework offers an efficient access control mechanism, allowing data owners to define access preferences for their medical data. Users can employ their transactions for key generation, enabling the addition or revocation of authorized doctors. However, reliance on a local database may compromise decentralization.

Abutaleb et al. [163] introduced a framework for health record access control that allows patients to grant permissions to individuals accessing their health records. This framework uses blockchain and usage control to document activities, aiming for a user-centric and privacy-aware approach. However, blockchain may not be ideal for storing large volumes of health data.

Sutradhar et al. [164] developed an identity and access management framework using Hyperledger Fabric and OAuth 2.0 [165] to enhance security and privacy. This framework handles large data volumes, supports multiple applications, and employs role-based access control. It provides granular access to sensitive information, with OAuth 2.0 authorizing trusted third-party applications to access specific data on the Fabric network, ensuring interoperability. However, the framework has not been integrated with other blockchain platforms, such as Ethereum.

The AC-BMS framework [166] proposed an access control system that leveraged the collaboration between the main blockchain and side chains. In the model, the legitimate identity of a doctor is verified without the need for a trusted third party. Access authorization decisions are embedded in smart contracts, forming Roll-up contracts. These contracts use the access requests sent by doctors as trigger conditions to automatically execute smart contracts, granting access rights and corresponding resources stored on the side chain. The access node information on the main Ethereum chain is stored on the side chain, and resources are obtained by executing Roll-up contracts deployed on the side chains, which are based on Hyperledger Fabric. However, the AC-BMS does not account for the challenges in recognizing request types of Ethereum main chain nodes under high concurrent access requests.

Li et al. [167] introduced a hidden policy attribute-based access control scheme by leveraging the CP-ABE and ciphertext-policy attribute-based searchable encryption (CP-ABSE). Their solution also incorporated consortium blockchain and smart contracts for secure and reliable search and outsourced decryption. Using online/offline technology, the system executes the most computationally heavy tasks offline, requiring only minimal computation online to generate the final ciphertext and index. This method ensures flexible, fine-grained access and search control, allowing only authorized users to access private data. However, the scheme does not address the issue of revoked keys still being able to access blockchain data.

Kaur et al. [168] proposed a blockchain-based secure record-keeping system that uses the CP-ABE algorithm integrated with designed smart contracts for fine-grained access control. This system allows only authorized users to access specific EHR records based on their attributes. It enhances accountability and ensures that patients or owners can track and verify all actions taken on the data, making the system tamper-resistant and confidential. However, it suffers from high latency and low throughput.

Jakhar et al. [169] presented a privacy-preserving, access control framework based on blockchain that ensures the privacy, security, accessibility, and integrity of healthcare data using consensus-driven decentralized data management on peer-to-peer distributed computing platforms. This proposed framework is accessible to participants such as patients, doctors, chemists, and pathology labs. The permissioned blockchain network was systematically implemented using Hyperledger Fabric and Hyperledger Composer. However, its performance is mainly evaluated based on response time and memory usage, with high response time costs being a notable issue.

In summary, the reviewed access control frameworks are categorized from privacy and security perspectives, as shown in Table 5, comparing key factors such as confidentiality, integrity, availability, accountability, revocability, scalability, and privacy/access control. Frameworks like MedRec [115] excel in confidentiality and access control but lack revocability and scalability, while MeDShare [133] supports privacy and access control but has availability limitations. Most frameworks rely on popular blockchain platforms, such as Ethereum [35] and Hyperledger Fabric [40], utilizing smart contracts to manage EHR access permissions, as outlined in Table 4. To enhance scalability and efficiency, many methods store only EHR hash values on-chain while encrypting actual data in decentralized storage like IPFS [120]. Real-world implementations like MedRec [115] and FHIRChain [131], adopted in Boston-area hospitals, demonstrate blockchain's practical feasibility in secure, patient-centric EHR access control and FHIR-based interoperability. These frameworks bridge theoretical research and real-world deployment, reinforcing blockchain's role in privacy-preserving, scalable, and secure EHR management.

Blockchain technology provides a robust solution for decentralization, security, and privacy in healthcare, addressing challenges such as unauthorized access, identity theft, and medical errors. By leveraging smart contracts and cryptographic techniques, blockchain-based access

control methods ensure that EHRs are accessible only to authorized parties. The following sections explore privacy challenges, open research issues, and future directions in blockchain-based healthcare systems.

7 Privacy challenges in blockchain-based healthcare

Privacy is one of the primary concerns in the healthcare domain. While blockchain offers features that enhance security, such as transparency and immutability, it also introduces challenges related to safeguarding sensitive information from misuse or leaks. In the healthcare context, privacy challenges arise at multiple levels, and addressing these concerns is critical to the effective use of blockchain technology. This section identifies key privacy challenges, discusses potential solutions, and provides suggestions for future research and implementation.

7.1 Identity privacy challenge

Identity privacy focuses on protecting the identities of participants involved in blockchain transactions. Although blockchain provides some anonymity through cryptographic techniques, advances in technology make it possible for attackers to analyze transaction patterns and reveal personal information [171]. For example, adversaries can use transaction graphs to correlate public data with users' identities, exposing sensitive details such as location and personal identifiers [172].

Potential Solutions:

- **Privacy-Preserving Cryptographic Techniques:** Techniques such as ZKP [92] and Ring Signatures [103] can help enhance identity privacy. ZKP allows a party to prove knowledge of a value without revealing the value itself, ensuring anonymity.
- **Differential Privacy:** Adding noise to transaction data can prevent re-identification while preserving data utility [173].

Suggestions: Exploring hybrid approaches that combine differential privacy with cryptographic techniques could further enhance identity protection in blockchain-based healthcare systems.

7.2 Transaction privacy challenge

Blockchain transactions are published to all participants, creating potential risks of data leakage. Sensitive transaction details must be kept confidential to prevent unauthorized access and tampering. Ensuring that transactions remain secure and private, even when encryption isn't feasible, is critical.

Potential Solutions:

- **ZKP:** ZKP allows transactions to be verified without revealing sensitive details, ensuring privacy and integrity [92].
- **Ring Signatures:** Ring signatures obscure the sender's identity by mixing their transaction with others, enhancing anonymity [103].
- **Homomorphic Encryption:** Homomorphic encryption allows computations on encrypted data without decrypting it, ensuring transaction confidentiality while enabling verifiable operations [83].
- **SMPC:** SMPC enables multiple parties to jointly compute a function over their inputs while keeping those inputs private, ensuring secure processing of sensitive transactions [73].

Suggestions:

- Developing lightweight ZKP protocols tailored for healthcare applications could improve scalability and adoption.
- Hybrid privacy-enhancing approaches that combine ZKP and SMPC could be leveraged to enhance transaction confidentiality.
- Combining ring signatures with homomorphic encryption could provide a multi-layered approach to transaction privacy, addressing both identity and data confidentiality.

7.3 Smart contract privacy challenge

Smart contracts are integral to blockchain functionality but can pose privacy risks due to their public execution across all validating nodes [174]. During the validation process, nodes may access sensitive information, leading to potential privacy breaches.

Potential Solutions:

- **Privacy-Preserving Smart Contracts:** Frameworks like PPSC-BCAI [175] use artificial intelligence (AI) and cryptographic techniques to protect contract data.
- **TEEs:** TEEs, such as Intel SGX [66], enable secure execution of smart contracts without exposing sensitive data.
- **Homomorphic Encryption:** Allows computation on encrypted data, ensuring privacy during contract execution [83].

Suggestions: Integrating homomorphic encryption with TEEs could provide a hybrid approach, combining the privacy guarantees of encryption with the performance benefits of secure hardware.

Table 4 A comparison of blockchain-based frameworks for access control management and privacy-preservation in healthcare

Proposed method	Year	Blockchain type	Consensus protocol	Blockchain platform	EHR location	Access control technique	Drawbacks of the proposed methods
MedRec [115]	2016	Public	Proof of work	Ethereum	Local	Smart contract	Authentication and authorization are not completely supported
HDG [78]	2016	Public	Proposed by authors	Proposed by authors	Cloud	Role-Based Access Control (RBAC)	High storage costs. Authentication delays occur when expanding the number of users
ChainAchor [95]	2016	Private	Proposed by authors	Proposed by authors	Private blockchain	Anonymous Identity-Based Access Control (AIBAC)	Lacks performance justification
MeDShare [133]	2017	Private	Proposed by authors	Proposed by authors	Cloud	Smart contract	Performance is mainly evaluated based on network latency measures
BBDS [134]	2017	Private	Proof of work	Private Ethereum	Cloud	Identity-based authentication (IBA)	Lacks detailed solutions for users and data owners
Dubovitskaya et al. [136]	2017	Private	Practical byzantine fault tolerance	Hyperledger	Cloud	Smart contract (Chaincode)	Relies on a central patient authentication process
BHEEM [116]	2018	Public	Proof of vote	Ethereum	Local	Smart contract	More processing power caused by the differential privacy protection solution
Ancile [138]	2018	Private	Quorum-Chain	Private Ethereum	Local	Smart contract	Vulnerable to DoS attacks
FHIRChain [131]	2018	Private	Proof of Authority (PoA)	Ethereum	Off-Chain Storage	Smart contract	Scalability concerns due to smart contract execution overhead
Zhang and Poslad [140]	2018	Private	Proposed by authors	Proposed by authors	Cloud	Secret sharing	Expensive storage costs and utilizes a centralized approach since it is being developed via the cloud
MediChain™ [141]	2018	Private	Practical byzantine fault tolerance	Hyperledger	Cloud	Smart contract (Chaincode)	Most requirements of access control methods, like access revocation and delegation, are not addressed
BSPP [68]	2018	Private, Consortium	Proof of conformance	JUICE	Private blockchain	Public encryption with keyword search (PEKS)	High communication and storage overhead
Wang and Song [143]	2018	Consortium	Proposed by authors	Proposed by authors	Cloud	Attribute-based encryption (ABE)	Requires performance justification
Nguyen et al. [119]	2019	Public	Proof of work	Ethereum	IPFS	Smart contract	Performance is mainly evaluated based on network latency measures
Healthchain [120]	2019	Public, Consortium	PoW, PoS	Proposed by authors	IPFS	Smart contract	Doctors can still access the data even if the patient has canceled the doctor's authorization by making a new key to the userchain

Table 4 (continued)

Proposed method	Year	Blockchain type	Consensus protocol	Blockchain platform	EHR location	Access control technique	Drawbacks of the proposed methods
Hirtan et al. [145]	2019	Private, Consortium	50% approval	Hyperledger	Local	Policies in blockchain	High storage overhead
Omar et al. [42]	2020	Public	Proof of concept	Ethereum	IPFS	Smart contract	Has scalability issues
Madine et al. [121]	2020	Public	Proof of work	Ethereum	IPFS	Proxy re-encryption	In emergency cases, the patient is unable to delegate access to doctors
Dias et al. [146]	2020	Consortium	Proof of concept	Proposed by authors	Blockchain	Smart contract	Does not provide enough performance justification
Tanwar et al. [147]	2020	Consortium	Byzantine Fault Tolerance	Hyperledger	Blockchain	Smart contract	High storage overhead and relying on MSP, so it lacks a decentralized feature
Niu et al. [148]	2020	Private	Proof of work	Proposed by authors	Cloud	ABE	Performance is only measured in terms of some attributes and search time
GuardHealth [150]	2020	Consortium	Delegated proof of stake	Ethereum	Cloud	Smart contract	Network latency increases according to the number of nodes
SecureRx [122]	2021	Public	Proof of work	Ethereum	Local, Mongo DB	Smart contract	There is no clear mechanism for evaluating the framework's scalability and throughput in high workload situations
SPChain [123]	2021	Public	Pow and BFT	Bitcoin	Local	Proxy re-encryption	High communication overhead and low throughput
BCHealth [152]	2021	Private	Proof of authority	Proposed by authors	Private blockchain	Policies in blockchain	A little delay in retrieving EHR and more storage overhead
Chen et al. [153]	2021	Private	PBFT (Kafka)	Hyperledger	Cloud	Smart contract (Chaincode)	The EHRs are outsourced to cloud storage servers that lack the blockchain decentralization feature
SmartMedChain [155]	2021	Private	PBFT (Kafka)	Hyperledger	IPFS	Smart contract (Chaincode)	Involving several blockchains that require a significant amount of computing resources
PTBM [156]	2021	Public, Private	Proposed by authors	Hyperledger	Blockchain	Smart contract (Chaincode)	High computational overhead when the users' number increases
Xiang and Zhao [157]	2022	Private, Consortium	Proposed by authors	Proposed by authors	Cloud	ABE	Depending on the CSP, it may eliminate the decentralization feature
EL Azzaoui et al. [158]	2022	Private	Practical byzantine fault tolerance	Hyperledger	Cloud	Smart contract	The encryption and decryption phases of this framework have weaknesses, they are not discussed in detail
HealthLock [91]	2023	Public	Byzantine Fault Tolerance	Ethereum	Cloud	ABE	Constrained scalability and performance concerns. Homomorphic encryption is a computationally intensive technique

Table 4 (continued)

Proposed method	Year	Blockchain type	Consensus protocol	Blockchain platform	EHR location	Access control technique	Drawbacks of the proposed methods
Sharma et al. [127]	2023	Public	Proof of Work	Ethereum	Blockchain	Smart Contract	Exclusive focus on medical certificates. PoW protocol requires more energy resources
Chinnasamy et al. [128]	2023	Public	Proof of Work	Ethereum	IPFS	Smart Contract	Reliance on cloud infrastructure may partially compromise the decentralization benefits of blockchain
Peng et al. [125]	2023	Public Consortium	Proof of Work HotStuff [170]	Proposed by authors	Blockchain	Smart Contract	The bilinear pairing operations for authentication impact efficiency and lack scalability
Martínez et al. [159]	2023	Private	Practical byzantine fault tolerance	Hyperledger Fabric	Local	Smart Contract (Chaincode)	The blockchain is configured on a single machine that limits the generalization of results
Yang et al. [160]	2023	Private	Practical byzantine fault tolerance	Hyperledger Fabric	Blockchain	Smart Contract (Chaincode)	The model neglects to recognize master chain nodes during high access
Mittal and Ghosh [161]	2023	Private	Proposed by authors	Proposed by authors	Cloud	CP-ABE, Proxy re-encryption	CP-ABE usage leads to computational overhead proportional to the number of key attributes
Alsuqaih et al. [162]	2023	Private	Practical byzantine fault tolerance	Proposed by authors	Local	Policies in blockchain	Reliance on a local database may compromise decentralization
Abutaleb et al. [163]	2023	Consortium	Practical byzantine fault tolerance	Hyperledger Fabric	Blockchain	Smart Contract (Chaincode)	The blockchain is not an optimal solution for storing extensive health data
Sutradhar et al. [164]	2024	Consortium	Practical byzantine fault tolerance	Hyperledger Fabric	Blockchain	Role-based Access Control (OAuth 2.0 [165])	The framework lacks interoperability and scalability features
Lax et al. [126]	2024	Public	Proof of Stake	Ethereum	Blockchain	Smart Contract	The framework is not fully implemented. High computation overhead
AC-BMS [166]	2024	Consortium	PBFT	Ethereum Hyperledger Fabric	Blockchain	Smart Contract	The AC-BMS fails to recognize request types under high concurrent access
Li et al. [167]	2024	Consortium	PBFT	Hyperledger Fabric	Blockchain	CP-ABE CP-ABSE	The scheme does not prevent revoked keys from accessing blockchain data
Kaur et al. [168]	2024	Private	PoW	Ethereum	IPFS	CP-ABE Smart Contract	The framework suffers from high latency and low throughput
Jakhar et al. [169]	2024	Consortium	PBFT	Hyperledger Fabric	Blockchain	Smart Contract	The performance, mainly based on response time and memory usage, suffers from high response time costs

In conclusion, addressing privacy challenges in blockchain-based healthcare requires a combination of advanced cryptographic techniques, innovative frameworks, and regulatory alignment. Future research should focus on scalable, interoperable, and compliant solutions to unlock the full potential of blockchain in healthcare.

8 Open issues and future research directions

Blockchain technology has the capability to transform healthcare by enabling secure and transparent sharing of data, promoting interoperability, and facilitating patient-centered care. However, there remain some unresolved issues and areas for future research in the application of blockchain technology to healthcare.

8.1 Privacy-preservation with high-efficiency

Improving the efficiency of blockchain frameworks is challenging due to the high computational costs of cryptographic techniques like ZKP and FHE, often making them impractical for large-scale or real-time medical systems, especially when EHRs are acquired via IoT sensors. According to [176], IoT-based EHR systems face additional security and efficiency challenges, such as limited processing power, energy constraints, and vulnerability to unauthorized access. The FogBlock Connect framework, proposed by [177], addresses these challenges by integrating fog computing and blockchain to reduce latency and enhance data security while maintaining operational efficiency. While decentralized storage solutions like IPFS [120] improve data integrity and availability, they do not fully address latency or computational overhead.

Suggestions:

- **Academic Sector:** Develop lightweight cryptographic algorithms tailored for healthcare, balancing privacy and efficiency.
- **Industry Sector:** Implement hybrid systems combining on-chain and decentralized off-chain storage to improve scalability and reduce latency.

8.2 Blockchain scalability

Blockchain scalability refers to a system's ability to increase throughput while reducing latency and transaction costs [178]. In decentralized healthcare systems, where multiple providers collaborate, scalability becomes a critical requirement to ensure seamless data exchange and real-time access to patient records [119]. Extending traditional EHR methods for access control management is essential to enable a reliable and scalable medical system.

Role of Third-Layer Blockchains in Scalability: Third-layer blockchains (Layer 3) are protocols or frameworks built on top of Layer 2 solutions (e.g., rollups, sidechains) to further enhance scalability, interoperability, and functionality. They address scalability challenges through the following mechanisms:

- **Offloading Computational Workload:** By managing complex computations off-chain, third-layer blockchains reduce congestion on the main blockchain, improving overall scalability.
- **Data Indexing and Query Optimization:** These solutions provide efficient data retrieval mechanisms, minimizing the need for full-node storage and enhancing query response times.
- **Cross-Chain Communication:** They enable seamless interaction between different blockchain networks, allowing healthcare providers to share data across platforms without compromising security or performance.
- **Resource Optimization:** By allocating computational resources efficiently, third-layer blockchains reduce latency and transaction costs, which are critical for real-time healthcare applications.

Third-layer blockchains can significantly enhance healthcare systems by improving throughput to handle a higher volume of transactions, reducing latency to ensure timely access to critical patient data, and enabling interoperability to facilitate seamless data sharing across different healthcare providers and systems. This ensures continuity of care and enhances the overall efficiency of healthcare delivery. As highlighted in [179], third-layer blockchains, combined with Layer 2 scaling solutions, offer a promising approach to achieving the scalability required for modern healthcare systems.

Suggestions:

- **Academic Sector:** Development of novel consensus mechanisms and Layer 3 protocols to enhance scalability without compromising security.
- **Industry Sector:** Implementation of Layer-3 blockchain solutions in real-world medical data systems.

8.3 Privacy-preservation with accountability

Balancing privacy and accountability is challenging, as malicious participants may exploit anonymity to engage in illegal activities (e.g., drug trading) without detection. While privacy preservation is essential, revealing the identities of malicious actors in certain cases conflicts with this goal. Blockchain's decentralized nature, which eliminates the need for a TTP, further complicates the design of systems that require both privacy and accountability.

As a potential solution, [180] proposed a blockchain-based platform that enables accountability without mutual trust or a central authority. By maintaining an immutable ledger of interactions, this approach provides a verifiable indicator of unusual behavior, helping identify malicious nodes while preserving the privacy of legitimate participants. Addressing this trade-off remains a significant future research direction.

Suggestions:

- **Academic Sector:** Development of cryptographic techniques to enable accountability without compromising privacy.
- **Industry Sector:** Implement blockchain-based auditing tools to detect and mitigate malicious activities in healthcare systems.

8.4 Access control revocation policy

Access control policies in blockchain-based systems are often implemented using smart contracts. However, revoking user access is computationally expensive, requiring the data owner to modify the smart contract and add new blocks to the blockchain. Most systems lack attribute-based revocation, where access is revoked entirely based on user attributes. While methods like ABE and identity-based encryption (IBE) [33, 143, 148, 181] enable revocation based on attributes, they may suffer from forward and backward security issues. For example, new users might access previously encrypted EHRs without the data owner's consent. A promising solution is the use of lazy revocation schemes [182], which efficiently update keys to address these challenges.

Suggestions:

- **Academic Sector:** Development of efficient attribute-based revocation mechanisms for smart contracts to minimize computational overhead.
- **Industry Sector:** Develop user-friendly access control frameworks with built-in revocation capabilities for healthcare providers.

8.5 Outsourcing EHRs to cloud storage

EHRs can be stored either on-chain or off-chain, such as in cloud storage. However, outsourcing EHRs to cloud service providers (CSPs) introduces security and patient privacy risks, as CSPs may be vulnerable to data breaches, insider threats, or misconfigurations that expose sensitive information. Additionally, the centralized nature of cloud storage can introduce latency and may not seamlessly integrate with blockchain's decentralized architecture. As highlighted in [183], traditional cloud-based access control mechanisms, such as Role-Based Access Control (RBAC) and certain centralized Attribute-Based Access Control (ABAC) implementations, often struggle to address these challenges due to their reliance on central authorities, which can become single points of failure.

To mitigate these risks, EHRs can be anonymized before outsourcing using K-Anonymity techniques [184], though additional privacy-preserving mechanisms (e.g., differential privacy) may be necessary to prevent linkage attacks. The HCAC-EHR framework [185] proposes a hybrid cryptographic access control scheme for secure storage and retrieval of EHRs in healthcare cloud environments. Alternatively, decentralized storage solutions such as the IPFS [120] or edge computing [181] can be employed to enhance security and reduce latency. IPFS facilitates tamper-resistant, distributed file storage, while edge computing allows processing closer to the data source, minimizing dependence on centralized cloud infrastructure. These decentralized approaches align more closely with blockchain's principles, offering improved privacy, scalability, and resilience against attacks.

Suggestions:

- **Academic Sector:** Research hybrid storage solutions combining blockchain and decentralized storage for enhanced security and scalability.
- **Industry Sector:** Deployment of blockchain-integrated decentralized storage solutions for healthcare.

8.6 Interoperability between healthcare systems

Interoperability challenges arise from the lack of standardized blockchain frameworks, cross-border data transfers, and varying national regulations. These barriers hinder communication between healthcare systems, especially when patients interact with multiple systems across different countries. Regulatory constraints, such as the General Data Protection Regulation (GDPR) [186], further complicate data sharing and transfer. Additionally, interoperability between blockchain platforms (e.g., Ethereum and Hyperledger) and non-blockchain systems is particularly challenging [187]. A potential solution is to use shared off-chain data, but ensuring its authenticity and integrity remains a critical concern.

Suggestions:

- **Academic Sector:** Design interoperability frameworks for seamless data exchange between heterogeneous blockchain platforms.
- **Industry Sector:** Develop middleware solutions to bridge blockchain and legacy healthcare systems, ensuring compliance with regulations.

8.7 Compliance with privacy regulations

The development of blockchain-based healthcare solutions faces challenges due to the lack of standardized regulations. Recent health data breaches have highlighted vulnerabilities, prompting a reassessment of existing systems. Regulatory bodies like GDPR [186] in the EU and the Health Insurance Portability and Accountability Act (HIPAA) [188] in the USA mandate robust security and privacy measures for healthcare providers. These regulations require securing patient data while ensuring accessibility for data owners and authorized third parties. Compliance with these evolving guidelines is essential for all participants in the system.

Suggestions:

- **Academic Sector:** Explore regulatory-compliant blockchain designs that balance privacy and accessibility.
- **Industry Sector:** Create compliance tools and frameworks to help healthcare providers implement blockchain solutions that meet regulatory standards.

8.8 Integration of blockchain and artificial intelligence

AI involves creating intelligent systems capable of performing tasks without human intervention, leveraging machine learning and deep learning algorithms [189]. The integration of blockchain and AI has the potential to revolutionize healthcare by enhancing threat detection, improving data privacy and integrity, and increasing resistance to attacks [190]. Recent advancements in large AI models, such as Large Language Models (LLMs) and transformer-based architectures like GPT, have improved diagnostic accuracy and treatment recommendations. However, challenges remain in ensuring the reliability and adoption of these models in clinical settings.

Blockchain integration enhances security by ensuring data integrity and access control, particularly for training and deploying AI models in privacy-sensitive environments. Centralized AI platforms, which store patient data in provider data centers, raise concerns about data breaches [191]. Federated learning, combined with blockchain, offers a solution by enabling collaborative training of shared AI models without exposing underlying data, significantly enhancing privacy [192]. For example, [193] proposed a blockchain-based reinforcement federated learning framework for scalable Internet of Medical Things (IoMT) applications. Their approach uses federated learning to train machine learning models on decentralized medical data without transferring raw data, ensuring privacy, while blockchain secures the aggregation of model updates and maintains data integrity. This framework addresses scalability challenges while preserving patient privacy, making it a promising solution for real-time health data analysis and remote patient monitoring.

Suggestions:

- **Academic Sector:** Investigate privacy-preserving AI training methods (e.g., federated learning) combined with blockchain for secure data sharing.
- **Industry Sector:** Develop blockchain-based platforms for training and deploying AI models in healthcare, ensuring data integrity and access control.

9 Case studies of blockchain-based access control in healthcare

This section presents two case studies that demonstrate the practical implementation of blockchain-based access control and privacy preservation in healthcare. Each case study highlights unique challenges, solutions, and outcomes, providing insights into the real-world applicability of blockchain technology.

9.1 Case Study 1: blockchain-based EHR access control in a hospital network

In a real-world application, a large hospital network implemented a blockchain-based access control system to securely manage EHRs across multiple branches and affiliated clinics. This case study demonstrates the practical implications of blockchain technology for access control and privacy preservation in healthcare.

9.1.1 Scenario

The hospital network, consisting of multiple branches and affiliated clinics, faced challenges in securely sharing EHRs among healthcare providers while ensuring patient privacy and compliance with regulations such as the HIPAA. To address these challenges, the network adopted a blockchain-based solution.

9.1.2 Implementation

The implementation involved the following key components:

- **Blockchain Platform**: The hospital chose **Hyperledger Fabric**, a permissioned blockchain platform, due to its scalability, privacy features, and support for smart contracts.

- **Access Control**: Smart contracts were used to define access policies. For example:
  - Only authorized doctors and nurses could access specific patient records.
  - Patients could grant temporary access to specialists or external healthcare providers.
  - Access logs were immutably recorded on the blockchain for auditing purposes.
- **Privacy Preservation**: To protect patient privacy, the system integrated privacy-preserving techniques such as:
  - **ZKPs**: Used to verify access permissions without revealing sensitive patient information.
  - **Data Encryption**: EHRs were encrypted and stored off-chain, with only metadata (e.g., access logs) stored on the blockchain.
- **Consensus Protocol**: The hospital employed the **PBFT** consensus protocol to ensure fast transaction processing and fault tolerance.

9.1.3 Outcome

The implementation yielded the following outcomes:

- **Improved Security**: Unauthorized access to EHRs was prevented, and data breaches were minimized.
- **Enhanced Privacy**: Patients had control over who accessed their records, and sensitive data was protected using cryptographic techniques.
- **Regulatory Compliance**: The immutable audit trail on the blockchain ensured compliance with healthcare regulations.
- **Efficiency**: Healthcare providers could securely access patient records in real-time, improving care coordination and reducing administrative overhead.
- **Challenges**: Increased computational overhead due to ZKP verification and encryption schemes.

9.1.4 Discussion

This case study demonstrates the effectiveness of blockchain-based access control frameworks in hospitals. However, scalability, interoperability with legacy systems, and computational efficiency of cryptographic techniques remain challenges for future research.

9.2 Case Study 2: decentralized patient data sharing in a telemedicine platform

Building on the success of blockchain-based access control in hospital networks, the next case study explores the application of blockchain technology in telemedicine platforms. Telemedicine, which relies heavily on secure and decentralized data sharing, presents unique challenges and opportunities for blockchain integration. The following case study highlights how blockchain can address these challenges while ensuring patient privacy and regulatory compliance.

9.2.1 Scenario

A telemedicine platform aimed to facilitate secure and decentralized sharing of patient data between healthcare providers and patients. The platform needed to ensure data integrity, patient privacy, and compliance with regulations like the GDPR.

9.2.2 Implementation

The platform implemented the following:

- **Blockchain Platform**: The platform used **Ethereum** (with a private network) to leverage its smart contract capabilities and support for decentralized applications (dApps).
- **Access Control**: Smart contracts were deployed to manage access permissions. For example:
  - Patients could grant or revoke access to their data for specific healthcare providers.
  - Access requests were logged on the blockchain for transparency and auditing.
- **Privacy Preservation**: To ensure privacy, the platform integrated:
  - **Data Anonymization**: Ring Signatures ensured anonymity in access requests.
  - **Off-Chain Storage**: Sensitive data was stored off-chain in a secure, encrypted database, with only hashes stored on the blockchain.
- **Consensus Protocol**: The platform used **PoA** for consensus, ensuring fast transaction processing and energy efficiency.

9.2.3 Outcome

The implementation resulted in:

Table 5 A comparison of access control frameworks from privacy and security perspectives

Reference	Confidentiality	Integrity	Availability	Accountability	Revocability	Scalability	Access Control
MedRec [115]	x	x	x	✓	x	x	✓
HDG [78]	x	✓	x	x	x	x	✓
ChainAchor [95]	✓	✓	✓	x	x	x	✓
MeDShare [133]	✓	✓	x	x	✓	✓	✓
BBDS [134]	✓	✓	x	✓	x	✓	✓
Dubovitskaya et al. [136]	✓	✓	x	x	x	✓	✓
BHEEM [116]	✓	x	x	x	✓	✓	✓
Ancile [138]	✓	x	x	x	x	x	✓
FHIRChain [131]	✓	✓	✓	✓	✓	x	✓
Zhang and Poslad [140]	✓	✓	x	x	x	x	✓
MediChain^{TM} [141]	✓	✓	x	x	x	✓	✓
BSPP [68]	✓	✓	✓	x	x	x	✓
Wang and Song [143]	✓	✓	x	x	x	x	✓
Nguyen et al. [119]	✓	✓	✓	✓	✓	x	✓
Healthchain [120]	✓	✓	✓	✓	x	✓	✓
Hirtan et al. [145]	✓	x	x	x	x	x	✓
Omar et al. [42]	✓	✓	✓	x	x	x	✓
Madine et al. [121]	✓	✓	✓	x	x	x	✓
Dias et al. [146]	✓	✓	✓	✓	✓	x	✓
Tanwar et al. [147]	✓	✓	x	x	✓	✓	✓
Niu et al. [148]	✓	✓	x	x	x	x	✓
GuardHealth [150]	✓	✓	x	x	✓	x	✓
SecureRx [122]	✓	x	x	✓	x	✓	✓
SPChain [123]	✓	✓	x	x	x	x	✓
BCHealth [152]	✓	x	x	x	✓	x	✓
Chen et al. [153]	✓	✓	x	x	x	x	✓
SmartMedChain [155]	✓	✓	✓	✓	✓	x	✓
PTBM [156]	✓	✓	✓	x	x	x	✓
Xiang and Zhao [157]	✓	✓	x	x	x	x	✓
EL Azzaoui et al. [158]	✓	✓	x	x	x	x	✓
HealthLock [91]	✓	✓	x	✓	x	x	✓
Sharma et al. [127]	✓	✓	✓	x	x	x	✓
Chinnasamy et al. [128]	✓	✓	✓	x	✓	x	✓
Peng et al. [125]	✓	✓	✓	✓	✓	x	✓
Martínez et al. [159]	✓	✓	✓	✓	x	x	✓
Yang et al. [160]	✓	✓	✓	✓	x	✓	✓
Mittal and Ghosh [161]	✓	✓	✓	x	✓	x	✓
Alsuqaih et al. [162]	✓	✓	✓	x	✓	x	✓
Abutaleb et al. [163]	✓	✓	✓	✓	✓	x	✓
Sutradhar et al. [164]	✓	✓	✓	x	✓	x	✓
Lax et al. [126]	✓	✓	✓	x	x	x	✓
AC-BMS [166]	✓	✓	✓	✓	x	✓	✓
Li et al. [167]	✓	✓	✓	✓	x	x	✓
Kaur et al. [168]	✓	✓	✓	✓	✓	x	✓
Jakhar et al. [169]	✓	✓	✓	x	✓	x	✓

- **Secure Data Sharing**: Patients retained control over their data, and healthcare providers could access it securely.
- **Regulatory Compliance**: The platform met GDPR requirements for data protection and patient consent.
- **Improved Trust**: Patients were more willing to share data, knowing it was protected by blockchain technology.
- **Challenges**: SMPC computations introduced slight delays in data processing, requiring optimization.

9.2.4 Discussion

This case study highlights blockchain's role in decentralized patient data sharing and telemedicine. However, optimizing cryptographic computations, reducing latency, and ensuring seamless interoperability remain critical future directions.

10 Conclusion

This survey paper highlights research trends by presenting the most significant access control methods in state-of-the-art healthcare applications. It provides a comprehensive overview of healthcare DApps based on blockchain technology, focusing on privacy-preserving access control methods for EHRs. We categorized blockchain-based access control methods into permissioned and permissionless systems, summarizing them based on publication year, blockchain type, consensus protocol, platform, EHR location, privacy/access control techniques, and weaknesses. Our analysis confirms that blockchain is one of the most widely adopted solutions for decentralization, security, access control, and privacy in healthcare, addressing numerous challenges related to health data privacy. This paper also provided an overview of blockchain technology, emphasizing its main characteristics, such as confidentiality, transparency, integrity, and availability. We discussed the structure of blockchain systems, their types, and the critical role of consensus protocols in ensuring network equality and security. Additionally, we defined smart contracts and highlighted their importance in access control and healthcare system management. Furthermore, we outlined the most common blockchain-based privacy preservation techniques used in EHR access control methods. Our survey reveals that most proposed methods rely on established blockchain platforms like Ethereum and Hyperledger Fabric, which support smart contracts. These smart contracts, often developed in general-purpose programming languages, serve as a key access control mechanism. To improve the efficiency, decentralization, and scalability of access control methods, we recommend storing only the hash value of healthcare data on the blockchain ledger while encrypting and storing the actual data in off-chain systems like IPFS, which handles large files by dividing them into 256 KB chunks. Finally, we highlighted privacy challenges in blockchain-based healthcare systems and presented open research issues and future directions. This survey underscores the potential of blockchain technology to revolutionize healthcare access control while identifying areas for further exploration and innovation.

List of Notations H: Hash function; $\{0,1\}^*$: Set of all binary strings of arbitrary finite length; $\{0,1\}^n$: Set of binary strings of fixed length n; h: Hash value; x, x': Inputs to a hash function; $H(x)$: Hash of input x; t_i: Transaction in a blockchain; $H(t_i)$: Hash of transaction t_i; $H(L)$, $H(R)$: Hashes of left and right child nodes in a Merkle tree; $\|$: Concatenation operator; H_{parent}: Hash of a parent node in a Merkle tree; N: Number of parties in secure multi-party computation (SMPC); $f(x_1, x_2, \ldots, x_N)$: Function computed by N parties in SMPC; x_i: Private input of party i in SMPC; $\mathsf{KeyGen}(1^\lambda)$: Key generation algorithm in homomorphic encryption; pk, sk: Public and private keys in homomorphic encryption; $\mathsf{Enc}(pk, m)$: Encryption of plaintext m using public key pk; $\mathsf{Dec}(sk, c)$: Decryption of ciphertext c using private key sk; m, m_1, m_2: Plaintext messages; c: Ciphertext; ϕ: Statement in a zero-knowledge proof (ZKP); P: Prover in a ZKP protocol; V: Verifier in a ZKP protocol; t: Threshold in Shamir's secret sharing scheme; λ: Security parameter

Author Contributions All authors contributed to the study conception and design. Material preparation, data collection, and analysis were performed by Ahmed M. Tawfik; the first draft of the manuscript was written by Ahmed M. Tawfik, and all authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.

Funding Open access funding provided by The Science, Technology & Innovation Funding Authority (STDF) in cooperation with The Egyptian Knowledge Bank (EKB). No funding was received to assist with the preparation of this manuscript. The authors have no relevant financial or non-financial interests to disclose.

Data Availability Not applicable.

Declarations

Conflict of interest The Author declares that there is no Conflict of interest.

Ethics Approval Not applicable.

References

1. Mettler, M.: Blockchain technology in healthcare: The revolution starts here. In 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), pp. 1–3, (2016). https://doi.org/10.1109/HealthCom.2016.7749510
2. Mayer, A.H., André da Costa, C., da Rosa Righi, R.: Electronic health records in a blockchain: a systematic review. Health Inform. J. **26**(2), 1273–1288 (2020). https://doi.org/10.1177/1460458219866350. (**PMID: 31566472**)
3. Zhang, R., Xue, R., Liu, L.: Security and privacy for healthcare blockchains. IEEE Trans. Serv. Comput. (2021). https://doi.org/10.1109/TSC.2021.3085913
4. Badve, O., Gupta, B.B., Gupta, S.: Reviewing the security features in contemporary security policies and models for multiple platforms. handbook of research on modern cryptographic solutions for computer and cyber security, pp. 479–504 (2016). https://doi.org/10.4018/978-1-5225-0105-3.ch020
5. Chen, Y., Ding, S., Xu, Z., Zheng, H., Yang, S.: Blockchain-based medical records secure storage and medical service framework. J. Med. Syst. **43**, 1–9 (2019)
6. Gupta, M., Jain, R., Kumari, M., Narula, G.: Securing healthcare data by using blockchain, pp. 93–114. Springer, Singapore (2021). ISBN 978-981-15-9547-9. https://doi.org/10.1007/978-981-15-9547-9_4
7. Griggs, K.N., Ossipova, O., Kohlios, C.P., Baccarini, A.N., Howson, E.A., Hayajneh, T.: Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. J. Med. Syst. **42**(7), 1–7 (2018)
8. Yan Zhuang, Lincoln R. Sheets, Yin Wu Chen, Zon Yin Shae, Jeffrey J.P. Tsai, and Chi Ren Shyu. A patient-centric health information exchange framework using blockchain technology. *IEEE Journal of Biomedical and Health Informatics*, 24 (8):2169–2176, 2020. ISSN 21682208. https://doi.org/10.1109/JBHI.2020.2993072
9. Esther Mengelkamp, Benedikt Notheisen, Carolin Beer, David Dauer, and Christof Weinhardt. A blockchain-based smart grid: towards sustainable local energy markets. *Computer Science - Research and Development*, 33 (1-2):207–214, 2018. ISSN 18652042. https://doi.org/10.1007/s00450-017-0360-9
10. Singh, A., Chatterjee, K.: Trust based access control model for securing electronic healthcare system. J. Ambient Intell. Hum. Comput. **10**, 4547–4565 (2019)
11. Ausanka-Crues, R.: Methods for access control: advances and limitations, pp. 1–5. Harvey Mudd College, Claremont (2001)
12. Kassab, M., DeFranco, J., Malas, T., Laplante, P., Destefanis, G., Neto, V.V.G.: Exploring research in blockchain for healthcare and a roadmap for the future. IEEE Trans. Emerg. Top. Comput. **9**(4), 1835–1852 (2021). https://doi.org/10.1109/TETC.2019.2936881
13. Syed, T.A., Alzahrani, A., Jan, S., Siddiqui, M.S., Nadeem, A., Alghamdi, T.: Problems and recommendations: a comparative analysis of blockchain architecture and its applications. IEEE Access **7**, 176838–176869 (2019). https://doi.org/10.1109/ACCESS.2019.2957660
14. Hassan Mansur Hussien, Sharifah Md Yasin, SNI Udzir, Aws Alaa Zaidan, and Bilal Bahaa Zaidan. A systematic review for enabling of develop a blockchain technology in healthcare application: taxonomy, substantially analysis, motivations, challenges, recommendations and future direction. *Journal of medical systems*, 43:1–35, 2019
15. Agbo, C.C., Mahmoud, Q.H., Eklund, J.M.: Blockchain technology in healthcare: a systematic review. Healthcare **7**(2), (2019). ISSN 2227-9032. https://doi.org/10.3390/healthcare7020056. URL https://www.mdpi.com/2227-9032/7/2/56
16. Tandon, A., Dhir, A., Islam, A.N., Mäntymäki, M.: Blockchain in healthcare: a systematic literature review, synthesizing framework and future research agenda. Comput. Ind. **122**, 103290 (2020)
17. Soltanisehat, L., Alizadeh, R., Hao, H., Choo, K.K.: Technical, temporal, and spatial research challenges and opportunities in blockchain-based healthcare: a systematic literature review. IEEE Trans. Eng. Manag. **70**(1), 353–68 (2020)
18. Hasselgren, A., Kralevska, K., Gligoroski, D., Pedersen, S.A., Faxvaag, A.: Blockchain in healthcare and health sciences-a scoping review. Int. J. Med. Inform. **134**, 104040 (2020)
19. Farouk, A., Alahmadi, A., Ghose, S., Mashatan, A.: Blockchain platform for industrial healthcare: vision and future opportunities. Comput. Commun. **154**, 223–235 (2020)
20. Qadri, Y.A., Nauman, A., Zikria, Y.B., Vasilakos, A.V., Kim, S.W.: The future of healthcare internet of things: a survey of emerging technologies. IEEE Commun. Surv. Tutor. **22**(2), 1121–1167 (2020)
21. Shi, S., He, D., Li, L., Kumar, N., Khan, M.K., Choo, K.-K.R.: Applications of blockchain in ensuring the security and privacy of electronic health record systems: a survey. Comput. Secur. **97**, 101966 (2020)
22. Chukwu, E., Garg, L.: A systematic review of blockchain in healthcare: frameworks, prototypes, and implementations. Ieee Access **8**, 21196–21214 (2020)
23. Khatri, S., Alzahrani, F.A., Ansari, M.T., Agrawal, A., Kumar, R., Khan, R.A.: A systematic analysis on blockchain integration with healthcare domain: scope and challenges. IEEE Access **9**, 84666–84887 (2021)
24. Hussien, H.M., Yasin, S.M., Udzir, N.I., Ninggal, M.I., Salman, S.: Blockchain technology in the healthcare industry: trends and opportunities. J. Ind. Inf. Integr. **22**, 100217 (2021)
25. Arbabi, M.S., Lal, C., Veeraragavan, N.R., Marijan, D., Nygård, J.F., Vitenberg, R.: A survey on blockchain for healthcare: challenges, benefits, and future directions. IEEE Commun. Surv. Tutor. **25**(1), 386–424 (2022)
26. Villarreal, E.R., García-Alonso, J., Moguel, E., Alegría, J.A.: Blockchain for healthcare management systems: a survey on interoperability and security. IEEE Access **12**(11), 5629–5652 (2023)
27. Popoola, O., Rodrigues, M., Marchang, J., Shenfield, A., Ikpehai, A., Popoola, J.: A critical literature review of security and privacy in smart home healthcare schemes adopting IoT & blockchain: problems, challenges and solutions. Blockchain Res. Appl. **5**(2), 100178 (2024)
28. Reshi, I.A., Sholla, S.: The blockchain conundrum: an in-depth examination of challenges, contributing technologies, and alternatives. Concurr. Comput. Pract. Exp. **36**(8), e7987 (2024). https://doi.org/10.1002/cpe.7987
29. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system. Bitcoin Whitepaper, p. 9 (2008). ISSN 1556–5068. https://doi.org/10.2139/ssrn.3440802
30. Gligoroski, D.: Cryptographic hash functions. Multidisc. Introd. Inf. Secur. **5**(4), 49–72 (2011). https://doi.org/10.1587/essfr.4.57

31. Mohanta, B.K., Jena, D., Panda, S.S., Sobhanayak, S.: Blockchain technology: a survey on applications and security privacy challenges. Internet Things **8**, 100107 (2019)
32. Gilbert, H., Handschuh, H.: Security analysis of SHA-256 and sisters. In: International Workshop on Selected Areas in Cryptography 2003, pp. 175–193. Springer, Berlin
33. Guo, R., Shi, H., Zhao, Q., Zheng, D.: Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems. IEEE Access **6**, 11676–11686 (2018)
34. Luu, L., Narayanan, V., Zheng, C., Baweja, K., Gilbert, S., Saxena, P.: A secure sharding protocol for open blockchains. In: Proceedings of the ACM Conference on Computer and Communications Security, 24-28-October-2016:17–30, (2016). ISSN 15437221. https://doi.org/10.1145/2976749.2978389
35. Buterin, A.V.: Ethereum Whitepaper. (2013). URL https://ethereum.org/en/whitepaper/
36. Min, X., Li, Q., Liu, L., Cui, L.: A Permissioned Blockchain Framework for supporting instant transaction and dynamic block size. Proceedings—15th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 10th IEEE International Conference on Big Data Science and Engineering and 14th IEEE International Symposium on Parallel and Distributed Processing with Applications, IEEE TrustCom/BigDataSE/ISPA 2016, pp. 90–96 (2016). https://doi.org/10.1109/TrustCom.2016.0050
37. Greenspan, G.: MultiChain Private Blockchain—White Paper. White Paper, pp. 1–17 (2015). ISSN 0093-7754. http://www.multichain.com/download/MultiChain-White-Paper.pdf
38. Baliga, A., Subhod, I., Kamat, P., Chatterjee, S.: Performance evaluation of the quorum blockchain platform (2018)
39. Dib, O., Brousmiche, K., Durand, A., Thea, E., Hamida, B.: Consortium blockchains: overview, applications and challenges. Int. J. Adv. Telecommun. **11**(1 &2), 51–64 (2018)
40. Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolić, M., Cocco, S.W., Yellick, J.: Hyperledger fabric: A distributed operating system for permissioned blockchains. In: Proceedings of the Thirteenth EuroSys Conference, EuroSys '18, New York, NY, USA, (2018). Association for Computing Machinery. ISBN 9781450355841. https://doi.org/10.1145/3190508.3190538
41. Ethereum and Bot B.: Hydrachain open source code. https://github.com/HydraChain/hydrachain (2015)
42. Ilhaam A. Omar, Raja Jayaraman, Khaled Salah, Mecit Can Emre Simsekler, Ibrar Yaqoob, and Samer Ellahham. Ensuring protocol compliance and data transparency in clinical trials using Blockchain smart contracts. *BMC Medical Research Methodology*, 20(1): 1–17, 2020. ISSN 14712288. https://doi.org/10.1186/s12874-020-01109-5
43. Sriman, B., Ganesh Kumar, S., Shamili, P.: Blockchain technology: Consensus protocol proof of work and proof of stake. In Dash, S.S., Das, S., Panigrahi, B.K. (eds.), Intelligent Computing and Applications, pp. 395–406, Singapore (2021). Springer, Singapore. ISBN 978-981-15-5566-4
44. Zhu, H., Guo, Y., Zhang, L.: An improved convolution merkle tree-based blockchain electronic medical record secure storage scheme. J. Inf. Secur. Appl. **61**, 102952 (2021)
45. Merkle, R..: A digital signature based on a conventional encryption function. In Conference on the Theory and Application of Cryptographic Techniques, pp. 369–378. Springer (1988)
46. Lu, Y.: The blockchain: state-of-the-art and research challenges. J. Ind. Inf. Integr. **15**, 80–90 (2019)
47. Song, J.C., Demir, M.A., Prevost, J.J., Rad, P.: Blockchain design for trusted decentralized iot networks. In: 2018 13th Annual Conference on System of Systems Engineering (SoSE), pp. 169–174 (2018). https://doi.org/10.1109/SYSOSE.2018.8428720
48. Zarrin, J., Wen Phang, H., Babu Saheer, L., Zarrin, B.: Blockchain for decentralization of internet: prospects, trends, and challenges. Clust. Comput. **24**(4), 2841–2866 (2021)
49. Demers, A., Greene, D., Hauser, C., Irish, W., Larson, J., Shenker, S., Sturgis, H., Swinehart, D., Terry, D.: Epidemic algorithms for replicated database maintenance. In Proceedings of the sixth annual ACM Symposium on Principles of distributed computing (pp. 1–12) (1987). https://doi.org/10.1145/41840.41841
50. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.*, 14(4):352-375, 2018. ISSN 1741-1106
51. Rahulamathavan, Y., Phan, R. C. W., Rajarajan, M., Misra, S., Kondoz, A.: Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption. In: 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS) (pp. 1–6). IEEE. https://doi.org/10.1109/ANTS.2017.8384164
52. Agrawal, R., Verma, P., Sonanis, R., Goel, U., De, A., Kondaveeti, S.A., Shekhar, S.: Continuous security in iot using blockchain. In 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 6423–6427, (2018). https://doi.org/10.1109/ICASSP.2018.8462513
53. Luu, L., Chu, D.-H., Olickel, H., Saxena, P., Hobor, A.: Making smart contracts smarter. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS '16, page 254-269, New York, NY, USA, (2016). Association for Computing Machinery. ISBN 9781450341394. https://doi.org/10.1145/2976749.2978309
54. Kosba, A., Miller, A., Shi, E., Wen, Z., Papamanthou, C.: Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In: 2016 IEEE Symposium on Security and Privacy (SP), pp. 839–858 (2016). https://doi.org/10.1109/SP.2016.55
55. Kouzinopoulos, C.S., Giannoutakis, K.M., Votis, K., Tzovaras, D., Collen, A., Nijdam, N.A., Konstantas, D., Spathoulas, G., Pandey, P., Katsikas, S.: Implementing a forms of consent smart contract on an iot-based blockchain to promote user trust. In: 2018 Innovations in Intelligent Systems and Applications (INISTA), pp. 1–6 (2018). https://doi.org/10.1109/INISTA.2018.8466268
56. Liu, J., Liu, Z.: A survey on security verification of blockchain smart contracts. IEEE Access **7**, 77894–77904 (2019). https://doi.org/10.1109/ACCESS.2019.2921624
57. Zheng, Z., Xie, S., Dai, H.N., Chen, W., Chen, X., Weng, J., Imran, M.: An overview on smart contracts: challenges, advances and platforms. Future Gener. Comput. Syst. **105**, 475–491 (2020)
58. Bamakan, S., Motavali, A., Bondarti, A.B.: A survey of blockchain consensus algorithms performance evaluation criteria. Expert Syst. Appl. **154**, 113385 (2020)
59. Larimer, D.: Delegated proof of stake (dpos): What is it? https://www.coinbureau.com/education/delegated-proof-stake-dpos/ (2013). Available: Online, Complete Beginners Guide
60. Bentov I, Lee, C., Mizrahi, A., Rosenfeld, M.: Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract]y. SIGMETRICS Perform. Eval. Rev. **42**(3), 34–37 (2014). ISSN 0163-5999. https://doi.org/10.1145/2695533.2695545
61. Castro, M., Liskov, B.: Practical byzantine fault tolerance. OSDI, pp. 173–186 (1999). cited By 99

62. Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H.: An overview of blockchain technology: Architecture, consensus, and future trends. In: 2017 IEEE International Congress on Big Data (BigData Congress), pp. 557–564 (2017). https://doi.org/10.1109/BigDataCongress.2017.85
63. Proof-of-authority consensus. https://openethereum.github.io/Proof-of-Authority-Chains#:~:text=Proof%2Dof%2DAuthority%20is%20a,blocks%20and%20secure%20the%20blockchain, 2017
64. A. team of engineers. Go ethereum. https://geth.ethereum.org/, 2013-2019
65. A. team of engineers. Parity technologies. https://www.parity.io/, 2019
66. Bowman, M., Das, D., Mandal, A., Montgomery, H.: On Elapsed Time Consensus Protocols. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 13143 LNCS:559–583, (2021). ISSN 16113349. https://doi.org/10.1007/978-3-030-92518-5_25
67. Li, K., Li, H., Hou, H., Li, K., Chen, Y.: Proof of vote: A high-performance consensus protocol based on vote mechanism & consortium blockchain. In: 2017 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), pp. 466–473 (2017). https://doi.org/10.1109/HPCC-SmartCity-DSS.2017.61
68. Zhang, A., Lin, X.: Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain. J. Med. Syst. **42**(8), (2018). ISSN 1573689X. https://doi.org/10.1007/s10916-018-0995-5
69. Puthal, D., Mohanty, S.P., Nanda, P., Kougianos, E., Das, G.: Proof-of-authentication for scalable blockchain in resource-constrained distributed systems. In: 2019 IEEE International Conference on Consumer Electronics (ICCE), pp. 1–5 (2019). https://doi.org/10.1109/ICCE.2019.8662009
70. Bada, A.O., Damianou, A., Angelopoulos, C.M., Katos, V.: Towards a green blockchain: A review of consensus mechanisms and their energy consumption. In: 2021 17th International Conference on Distributed Computing in Sensor Systems (DCOSS), pp. 503–511 (2021). https://doi.org/10.1109/DCOSS52077.2021.00083
71. Xiao, Y., Zhang, N., Lou, W., Hou, Y.T.: A survey of distributed consensus protocols for blockchain networks. IEEE Commun. Surv. Tutor. **22**(2), 1432–1465 (2020)
72. Munro, D.: Data breaches in healthcare. https://www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-total-over-112-million-records-in-2015/?sh=72ad29e47b07, (2015). [Online; accessed 17-JAN-2022]
73. Cramer, R., Damgård, I.B., Nielsen, J.B.: Secure multiparty computation and secret sharing. Secure Multiparty Computation and Secret Sharing, pp. 1–373 (2015). https://doi.org/10.1017/CBO9781107337756
74. Tawfik, A.M., Sabbeh, S.F., El-Shishtawy, T.: Privacy-preserving secure multiparty computation on electronic medical records for star exchange topology. Arab. J. Sci. Eng. **43**, 7747–7756 (2018)
75. Adi, S.: How to share a secret. Commun. ACM **22**(11), 612–613 (1979). ISSN 0001-0782. https://doi.org/10.1145/359168.359176
76. David, E., Vladimir, K., Mike, R.: A pragmatic introduction to secure multi-party computation. *Foundations and Trends® in Privacy and Security*, 2 (2-3):70–246, 2018. ISSN 2474-1558. https://doi.org/10.1561/3300000019
77. Li, D., Liao, X., Xiang, T., Wu, J., Le, J.: Privacy-preserving self-serviced medical diagnosis scheme based on secure multi-party computation. Comput. Secur. **90**, 101701 (2020)
78. Yue, X., Wang, H., Jin, D., Li, M., Jiang, W.: Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. J. Med. Syst. **40**(10), (2016). ISSN 1573689X. https://doi.org/10.1007/s10916-016-0574-6
79. Zhou, J., Feng, Y., Wang, Z., Guo, D.: Using secure multi-party computation to protect privacy on a permissioned blockchain. Sensors **21**(4), 1540 (2021)
80. Yang, Y., Wei, L., Wu, J., Long, Ch.: Block-smpc: A blockchain-based secure multi-party computation for privacy-protected data sharing. In Proceedings of the 2020 The 2nd International Conference on Blockchain Technology, ICBCT'20, page 46-51, New York, NY, USA, (2020). Association for Computing Machinery. ISBN 9781450377676. https://doi.org/10.1145/3390566.3391664
81. Parthasarathy, S., Harikrishnan, A., Narayanan, G., Lohith J.J., Singh, K.: Secure distributed medical record storage using blockchain and emergency sharing using multi-party computation. In: 2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS), pp. 1–5 (2021). https://doi.org/10.1109/NTMS49979.2021.9432643
82. Liu, X.: Global blockchain technology and application innovation status, trend and inspiration. China Sci. Technol. Bus. **1**, 27–31 (2020). (**(in Chinese)**)
83. Rivest, R.L., Adleman, L., Dertouzos, M.L.: On data banks and privacy homomorphisms. Found. Secur. Comput. **4**(11), 169–180 (1978)
84. Gentry, C.: Fully homomorphic encryption using ideal lattices. In: Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing, STOC '09, page 169-178, New York, NY, USA (2009). Association for Computing Machinery. ISBN 9781605585062. https://doi.org/10.1145/1536414.1536440
85. Cramer, R., Shoup, V.: A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In: Krawczyk, H. (ed.), Advances in Cryptology—CRYPTO '98, pp. 13–25, Berlin, Heidelberg, (1998). Springer Berlin Heidelberg. ISBN 978-3-540-68462-6
86. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. J. ACM **56**(6), ISSN 0004-5411. https://doi.org/10.1145/1568318.1568324
87. Ghadamyari, M., Samet, S.: Privacy-preserving statistical analysis of health data using paillier homomorphic encryption and permissioned blockchain. In: 2019 IEEE International Conference on Big Data (Big Data), pp. 5474–5479 (2019). https://doi.org/10.1109/BigData47090.2019.9006231
88. Ali, A., Pasha, M.F., Ali, J., Fang, O.H., Masud, M., Jurcut, A.D., Alzain, M.A.: Deep learning based homomorphic secure search-able encryption for keyword search in blockchain healthcare system: A novel approach to cryptography. Sensors **22**(2), 528 (2022)
89. Neri da Silva Vanin, Fausto, Policarpo, Lucas Micol, da Rosa Righi, Rodrigo, Heck, Sandra Marlene, da Silva, Valter Ferreira, Goldim, José, da Costa, Cristiano André: A blockchain-based end-to-end data protection model for personal health records sharing: A fully homomorphic encryption approach. Sensors, 23(1), (2023). ISSN 1424-8220. https://doi.org/10.3390/s23010014. URL https://www.mdpi.com/1424-8220/23/1/14
90. Wibawa, F., Catak, F.O., Kuzlu, M., Sarp, S., Cali, U.: Homomorphic encryption and federated learning based privacy-preserving cnn training: Covid-19 detection use-case. In: Proceedings of the 2022 European Interdisciplinary Cybersecurity Conference, EICC '22, page 85-90, New York, NY, USA (2022). Association for Computing Machinery. ISBN 9781450396035. https://doi.org/10.1145/3528580.3532845

91. Ali, A., Al-rimy, B., Alsubaei, F.S., Almazroi, A.A., Almazroi, A.A.: Healthlock: Blockchain-based privacy preservation using homomorphic encryption in internet of things healthcare applications. Sensors **23**(15), 6762 (2023)
92. Goldwasser, S., Micali, S., Rackoff, C.: The knowledge complexity of interactive proof systems. SIAM J. Comput. **18**(1), 186–208 (1989). https://doi.org/10.1137/0218012
93. Sun, X., Yu, F.R., Zhang, P., Sun, Z., Xie, W., Peng, X.: A survey on zero-knowledge proof in blockchain. IEEE Network **35**(4), 198–205 (2021)
94. Tomaz, A.E., Do Nascimento, J.C., Hafid, A.S., De Souza, J.N.: Preserving privacy in mobile health systems using non-interactive zero-knowledge proof and blockchain. IEEE Access **8**, 204441–204458 (2020)
95. Hardjono, T.: Pentland. Verifiable anonymous identities and access control in permissioned blockchains, Alex (2016)
96. Sharma, B., Halder, R., Singh, J.: Blockchain-based interoperable healthcare using zero-knowledge proofs and proxy re-encryption. In: 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS), pp. 1–6 (2020). https://doi.org/10.1109/COMSNETS48256.2020.9027413
97. Bai, T., Hu, Y., He, J., Fan, H., An, Z.: Health-zkIDM: a healthcare identity system based on fabric blockchain and zero-knowledge proof. Sensors **22**(20), 7716 (2022)
98. Davies, D.W.: Group Signatures. Springer, 547 LNCS(iii):257–265, (1991). ISSN 16113349. https://doi.org/10.1007/3-540-46416-6
99. Bellare, M., Micciancio, D., Warinschi, B.: Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions. In Biham, Eli, editor, Advances in Cryptology—-EUROCRYPT 2003, pp. 614–629, Berlin, Heidelberg, (2003). Springer Berlin Heidelberg. ISBN 978-3-540-39200-2
100. Boneh, D., Shacham, H.: Group signatures with verifier-local revocation. In: Proceedings of the 11th ACM Conference on Computer and Communications Security, CCS '04, page 168-177, New York, NY, USA, (2004). Association for Computing Machinery. ISBN 1581139616. https://doi.org/10.1145/1030083.1030106
101. Zhang, S., Lee, J.-H.: A group signature and authentication scheme for blockchain-based mobile-edge computing. IEEE Internet Things J. **7**(5), 4557–4565 (2020). https://doi.org/10.1109/JIOT.2019.2960027
102. Wang, B., Li, Z.: Healthchain: a privacy protection system for medical data based on blockchain. Future Internet **13**(10), 247 (2021)
103. Rivest, R.L., Shamir, A., Tauman, Y.: How to Leak a Secret. In Springer, volume 2018, pp. 552–565. (2001). ISBN 978-3-540-39568-3. https://doi.org/10.1007/3-540-45682-1-32. URL http://link.springer.com/10.1007/3-540-45682-1_32
104. Bender, A., Katz, J., Morselli, R.: Ring signatures: stronger definitions, and constructions without random oracles. J. Cryptol. **22**(1), 114–138 (2009)
105. Herranz, J., Sáez, G.: Forking lemmas for ring signature schemes. In: Johansson, T., Maitra, S. (eds.), Progress in Cryptology—INDOCRYPT 2003, pp. 266–279 (2003). Springer, Berlin. ISBN 978-3-540-24582-7
106. Lee, D., Song, M.: Mexchange: a privacy-preserving blockchain-based framework for health information exchange using ring signature and stealth address. IEEE Access **9**, 158122–158139 (2021)
107. Lai, C., Ma, Z., Guo, R., Zheng, D.: Secure medical data sharing scheme based on traceable ring signature and blockchain. Peer-to-Peer Netw. Appl. **15**(3), 1562–1576 (2022)
108. Odoom, J., Huang, X., Zhou, Z., Danso, S., Nyarko, B.N.E., Zheng, J., Xiang, Y.: Blockchain-assisted sharing of electronic health records: a feasible privacy-centric constant-size ring signature framework. Int. J. Comput. Appl. **45**(9), 564–578 (2023)
109. Wang, L., Peng, C., Tan, W.: Secure ring signature scheme for privacy-preserving blockchain. Entropy, **25**(9), (2023). ISSN 1099-4300. https://doi.org/10.3390/e25091334. URL https://www.mdpi.com/1099-4300/25/9/1334
110. Cha, S.C., Yeh, K.H.: An ISO/IEC 15408-2 compliant security auditing system with blockchain technology. 2018 IEEE Conference on Communications and Network Security, CNS 2018, pp. 1–2, (2018). https://doi.org/10.1109/CNS.2018.8433185
111. Zaabar, B., Cheikhrouhou, O., Jamil, F., Ammi, M., Abid, M.: Healthblock: A secure blockchain-based healthcare data management system. Comput. Netw. **200**, 108500 (2021). ISSN 1389-1286. https://doi.org/10.1016/j.comnet.2021.108500. https://www.sciencedirect.com/science/article/pii/S1389128621004382
112. Zaabar, B., Cheikhrouhou, O., Ammi, M., Awad, A.I., Abid, M.: Secure and privacy-aware blockchain-based remote patient monitoring system for internet of healthcare things. In: 2021 17th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), pp. 200–205 (2021). https://doi.org/10.1109/WiMob52687.2021.9606362
113. Yin, W., Wen, Q., Li, W., Zhang, H., Jin, Z.: An anti-quantum transaction authentication approach in blockchain. IEEE Access **6**, 5393–5401 (2018). https://doi.org/10.1109/ACCESS.2017.2788411
114. Sookhak, M., Jabbarpour, M.R., Safa, N.S., Richard, Yu.: Blockchain and smart contract for access control in healthcare: a survey, issues and challenges, and open issues. J. Network Comput. Appl. **178**, 102950 (2021)
115. Azaria, A., Ekblaw, A., Vieira, T., Lippman, A.: MedRec: Using blockchain for medical data access and permission management. In: Proceedings—2016 2nd International Conference on Open and Big Data, OBD 2016, pp. 25–30, (2016). https://doi.org/10.1109/OBD.2016.11
116. Vora, J., Nayyar, A., Tanwar, S., Tyagi, S., Kumar, N., Obaidat, M.S., Rodrigues, J.J.P.C.: BHEEM: A Blockchain-Based Framework for Securing Electronic Health Records. 2018 IEEE Globecom Workshops, GC Wkshps- Proceedings, pp. 1–6, (2019). https://doi.org/10.1109/GLOCOMW.2018.8644088
117. Dwork, C.: Differential privacy: A survey of results. In: M. Agrawal, D. Du, Z. Duan, A. Li (eds), Theory and Applications of Models of Computation, pp. 1–19. Berlin, Heidelberg, (2008). Springer Berlin Heidelberg. ISBN 978-3-540-79228-4
118. Zheng, Q., Li, Y., Chen, P., Dong, X.: An Innovative IPFS-Based Storage Model for Blockchain. In: Proceedings—2018 IEEE/WIC/ACM International Conference on Web Intelligence, WI 2018, pp. 704–708 (2019). https://doi.org/10.1109/WI.2018.000-8
119. Nguyen, D.C., Pathirana, P.N., Ding, M., Seneviratne, A.: Blockchain for secure ehrs sharing of mobile cloud based e-health systems. IEEE Access **7**, 66792–66806 (2019). https://doi.org/10.1109/ACCESS.2019.2917555
120. Jie, X., Xue, K., Li, S., Tian, H., Hong, J., Hong, P., Nenghai, Yu.: Healthchain: a blockchain-based privacy preserving scheme for large-scale health data. IEEE Internet Things J. **6**(5), 8770–8781 (2019). https://doi.org/10.1109/JIOT.2019.2923525
121. Madine, M.M., Battah, A.A., Yaqoob, I., Salah, K., Jayaraman, R., Al-Hammadi, Y., Pesic, S., Ellahham, S.: Blockchain for giving patients control over their medical records. IEEE Access **8**, 193102–19315 (2020)
122. Alnafrani, M., Acharya, S.: Securerx: A blockchain-based framework for an electronic prescription system with opioids tracking. Health Policy Technol. **10**(2), 100510 (2021)

123. Zou, R., Lv, X., Zhao, J.: SPChain: blockchain-based medical data sharing and privacy-preserving eHealth system. Inf. Process. Manag. **58**(4), 102604 (2021)
124. Khalili, M., Dakhilalian, M., Susilo, W.: Efficient chameleon hash functions in the enhanced collision resistant model. Inf. Sci. **510**, 155–164 (2020)
125. Peng, G., Zhang, A., Lin, X.: Patient-centric fine-grained access control for electronic medical record sharing with security via dual-blockchain. IEEE Trans. Netw. Sci. Eng. **10**(6), 3908–3921 (2023). https://doi.org/10.1109/TNSE.2023.3276166
126. Lax, G., Nardone, R., Russo, A.: Enabling secure health information sharing among healthcare organizations by public blockchain. Multimedia Tools and Applications, pp. 1–17 (2024)
127. Pratima Sharma, Suyel Namasudra, Naveen Chilamkurti, Byung-Gyu Kim, and Ruben Gonzalez Crespo. Blockchain-based privacy preservation for iot-enabled healthcare system. *ACM Transactions on Sensor Networks*, 19(3): 1–17, 2023
128. Chinnasamy, P., Albakri, Ashwag, Khan, Mudassir, Ambeth Raja, A., Kiran, Ajmeera, Babu, Jyothi Chinna: Smart contract-enabled secure sharing of health data for a mobile cloud-based e-health system. Appl. Sci. **13**(6), (2023). ISSN 2076-3417
129. Brickell, E., Li, J.: Enhanced privacy id: A direct anonymous attestation scheme with enhanced revocation capabilities. IEEE Trans. Depend. Secure Comput. **9**(3), 345–360 (2012). https://doi.org/10.1109/TDSC.2011.63
130. Micciancio, D., Goldwasser, S., Micciancio, D., Goldwasser, S.: The knowledge complexity of interactive proof systems. SIAM J. Comput. **18**(1), 186–208 (1989). https://doi.org/10.1007/978-1-4615-0897-7-9
131. Zhang, P., White, J., Schmidt, D.C., Lenz, G., Rosenbloom, S.T.: FHIRChain: applying blockchain to securely and scalably share clinical data. Comput. Struct. Biotechnol. J. **1**(16), 267–278 (2018)
132. Chang, Y.-C., Mitzenmacher, M.: Privacy preserving keyword searches on remote encrypted data. In: John Ioannidis, Angelos Keromytis, and Moti Yung, editors, Applied Cryptography and Network Security, pp. 442–455, Berlin, Heidelberg, (2005). Springer Berlin Heidelberg. ISBN 978-3-540-31542-1
133. Xia, Q.I., Sifah, E.B., Asamoah, K.O., Gao, J., Du, X., Guizani, M.: MeDShare: trust-less medical data sharing among cloud service providers via blockchain. IEEE Access **5**, 14757–14767 (2017)
134. Xia, Q., Sifah, E.B., Smahi, A., Amofa, S., Zhang, X.: Bbds: blockchain-based data sharing for electronic medical records in cloud environments. Information **8**(2), 44 (2017)
135. Wu, L., Zhang, Y., Xie, Y., Alelaiw, A., Shen, J.: An efficient and secure identity-based authentication and key agreement protocol with user anonymity for mobile devices. Wirel. Person. Commun. **94**, 3371–3387 (2017)
136. Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., Wang, F.: Secure and trustable electronic medical records sharing using blockchain. In: AMIA annual symposium proceedings (Vol. 2017, p. 650)
137. Miguel, C., Barbara, L.: Practical byzantine fault tolerance and proactive recovery. ACM Trans. Comput. Syst. **20**(4), 398–461 (2002). ISSN 0734-2071. https://doi.org/10.1145/571637.571640
138. Dagher, G.G., Mohler, J., Milojkovic, M., Marella, P.B.: Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustain. Cit. Soc. **39**, 283–297 (2018)
139. Zhou, L., Marsh, M.A., Schneider, F.B., Redz, A.: Distributed blinding for distributed elgamal re-encryption. In 25th IEEE International Conference on Distributed Computing Systems (ICDCS'05), pp. 824–824, (2005). https://doi.org/10.1109/ICDCS.2005.24
140. Zhang, X., Poslad, S.: Blockchain support for flexible queries with granular access control to electronic medical records (emr). In: 2018 IEEE International Conference on Communications (ICC), pp. 1–6, (2018). https://doi.org/10.1109/ICC.2018.8422883
141. Rouhani, Sara, Butterworth, Luke, Simmons, Adam D., Humphery, Darryl G., Deters, Ralph: Medichaintm: A secure decentralized medical data asset management system. In 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 1533–1538, (2018). https://doi.org/10.1109/Cybermatics_2018.2018.00258
142. Wang, Xu An, Huang, Xinyi, Yang, Xiaoyuan, Liu, Longfei, Wu, Xuguang: Further observation on proxy re-encryption with keyword search. Journal of Systems and Software, **85**(3), 643–654 (2012). ISSN 0164-1212. https://doi.org/10.1016/j.jss.2011.09.035. URL https://www.sciencedirect.com/science/article/pii/S0164121211002433. Novel approaches in the design and implementation of systems/software architecture
143. Wang, Hao, Song, Yujiao: Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain. Journal of Medical Systems, **42**(8), (2018). ISSN 1573689X. https://doi.org/10.1007/s10916-018-0994-6
144. Waters, Brent: Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In Dario Catalano, Nelly Fazio, Rosario Gennaro, and Antonio Nicolosi, editors, Public Key Cryptography – PKC 2011, pp. 53–70, Berlin, Heidelberg, (2011). Springer Berlin Heidelberg. ISBN 978-3-642-19379-8
145. Hirtan, Liviu, Krawiec, Piotr, Dobre, Ciprian, Batalla, Jordi Mongay: Blockchain-based approach for e-health data access management with privacy protection. In 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), pp. 1–7, (2019). https://doi.org/10.1109/CAMAD.2019.8858469
146. Dias, João Pedro, Ferreira, Hugo Sereno, Martins, Ângelo: A blockchain-based scheme for access control in e-health scenarios. In Ana Maria Madureira, Ajith Abraham, Niketa Gandhi, Catarina Silva, and Mário Antunes, editors, Proceedings of the Tenth International Conference on Soft Computing and Pattern Recognition (SoCPaR 2018), pp. 238–247, Cham, (2020). Springer International Publishing. ISBN 978-3-030-17065-3
147. Tanwar, Sudeep, Parekh, Karan, Evans, Richard: Blockchain-based electronic healthcare record system for healthcare 4.0 applications. Journal of Information Security and Applications, **50**, 102407, (2020). ISSN 2214-2126. https://doi.org/10.1016/j.jisa.2019.102407. URL https://www.sciencedirect.com/science/article/pii/S2214212619306155
148. Niu, S., Chen, L., Wang, J., Fei, Yu.: Electronic health record sharing scheme with searchable attribute-based encryption on blockchain. IEEE Access **8**, 7195–7204 (2020). https://doi.org/10.1109/ACCESS.2019.2959044
149. Goyal, Vipul, Pandey, Omkant, Sahai, Amit, Waters, Brent: Attribute-based encryption for fine-grained access control of encrypted data. In Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS '06, page 89-98, New York, NY, USA, (2006). Association for Computing Machinery. ISBN 1595935185. https://doi.org/10.1145/1180405.1180418
150. Wang, Ziyu, Luo, Nanqing, Zhou, Pan: Guardhealth: Blockchain empowered secure data management and graph convolutional network enabled anomaly detection in smart healthcare. Journal of Parallel and Distributed Computing, **142**, 1–12,

(2020). ISSN 0743-7315. https://doi.org/10.1016/j.jpdc.2020.03.004. URL https://www.sciencedirect.com/science/article/pii/S0743731519308470
151. Luo, Wei, Ma, Wenping: A secure revocable identity-based proxy re-encryption scheme for cloud storage. In Xingming Sun, Zhaoqing Pan, and Elisa Bertino, editors, Cloud Computing and Security, pp. 519–530, Cham, (2018). Springer International Publishing. ISBN 978-3-030-00009-7
152. Hossein, Koosha Mohammad, Esmaeili, Mohammad Esmaeil, Dargahi, Tooska, Khonsari, Ahmad, Conti, Mauro: Bchealth: A novel blockchain-based privacy-preserving architecture for iot healthcare applications. Computer Communications, **180**, 31–47, (2021). ISSN 0140-3664. https://doi.org/10.1016/j.comcom.2021.08.011. URL https://www.sciencedirect.com/science/article/pii/S0140366421003054
153. Chen, Zeng, Xu, Weidong, Wang, Bingtao, Yu, Hua: A blockchain-based preserving and sharing system for medical data privacy. Future Generation Computer Systems, **124**, 338–350 (2021). ISSN 0167-739X. https://doi.org/10.1016/j.future.2021.05.023. URL https://www.sciencedirect.com/science/article/pii/S0167739X21001734
154. Kreps, Jay, Narkhede, Neha, Rao, Jun et al.: Kafka: A distributed messaging system for log processing. In Proceedings of the NetDB, volume 11, pp. 1–7, (2011)
155. El Majdoubi, Driss, El Bakkali, Hanan, Sadki, Souad: SmartMedChain: A Blockchain-Based Privacy-Preserving Smart Healthcare Framework. Journal of Healthcare Engineering, 2021, (2021). ISSN 20402309. https://doi.org/10.1155/2021/4145512
156. Zhang, Can, Xu, Chang, Sharif, Kashif, Zhu, Liehuang: Privacy-preserving contact tracing in 5G-integrated and blockchain-based medical applications. Computer Standards and Interfaces, 77(August 2020), 103520 (2021). ISSN 09205489, https://doi.org/10.1016/j.csi.2021.103520
157. Xiang, Xinyin, Zhao, Xingwen: Blockchain-assisted searchable attribute-based encryption for e-health systems. Journal of Systems Architecture, **124**, 102417 (2022). ISSN 1383-7621. https://doi.org/10.1016/j.sysarc.2022.102417. URL https://www.sciencedirect.com/science/article/pii/S1383762122000194
158. EL Azzaoui, Abir, Chen, Haotian, Kim, So Hyeon, Pan, Yi, Park, Jong Hyuk: Blockchain-based distributed information hiding framework for data privacy preserving in medical supply chain systems. Sensors, **22**(4), (2022). ISSN 1424-8220. https://doi.org/10.3390/s22041371. URL https://www.mdpi.com/1424-8220/22/4/1371
159. Román-Martínez, I., Calvillo-Arbizu, J., Mayor-Gallego, V.J., Madinabeitia-Luque, G., Estepa-Alonso, A.J., Estepa-Alonso, R.M.: Blockchain-based service-oriented architecture for consent management, access control, and auditing. IEEE Access **11**, 12727–12741 (2023). https://doi.org/10.1109/ACCESS.2023.3242605
160. Yang, Liang, Jiang, Rong, Pu, Xuetao, Wang, Chenguang, Yang, Yue, Wang, Meng, Zhang, Lin, Tian, Feifei: An access control model based on blockchain master-sidechain collaboration. Cluster Computing, pp. 1–21, (2023)
161. Mittal, Shweta, Ghosh, Mohona: A novel two-level secure access control approach for blockchain platform in healthcare. International Journal of Information Security, pp. 1–19, (2023)
162. Alsuqaih, Hanan Naser, Hamdan, Walaa, Elmessiry, Haythem, Abulkasim, Hussein: An efficient privacy-preserving control mechanism based on blockchain for e-health applications. Alexandria Engineering Journal, **73**, 159–172 (2023). ISSN 1110-0168. https://doi.org/10.1016/j.aej.2023.04.037. URL https://www.sciencedirect.com/science/article/pii/S1110016823003186
163. Abutaleb, Rayan Anwar, Alqahtany, Saad Said, Syed, Toqeer Ali: Integrity and privacy-aware, patient-centric health record access control framework using a blockchain. Applied Sciences, **13**(2), (2023). ISSN 2076-3417. https://doi.org/10.3390/app13021028. URL https://www.mdpi.com/2076-3417/13/2/1028
164. Sutradhar, Shrabani, Karforma, Sunil, Bose, Rajesh, Roy, Sandip, Djebali, Sonia, Bhattacharyya, Debnath: Enhancing identity and access management using hyperledger fabric and oauth 2.0: A block-chain-based approach for security and scalability for healthcare industry. Internet of Things and Cyber-Physical Systems, **4**, 49–67 (2024). ISSN 2667-3452. https://doi.org/10.1016/j.iotcps.2023.07.004. URL https://www.sciencedirect.com/science/article/pii/S2667345223000470
165. Eugene Ferry, John O Raw, and Kevin Curran. Security evaluation of the oauth 2.0 framework. *Information & Computer Security*, 23(1): 73–101, 2015
166. Yang, L., Jiang, R., Xuetao, P., Wang, C., Yang, Y., Wang, M., Zhang, L., Tian, F.: An access control model based on blockchain master-sidechain collaboration. Cluster Computing **27**(1), 477–497 (2024)
167. Li, Peng, Zhou, Dehua, Ma, Haobin, Lai, Junzuo: Flexible and secure access control for ehr sharing based on blockchain. Journal of Systems Architecture, **146**, 103033 (2024). ISSN 1383-7621. https://doi.org/10.1016/j.sysarc.2023.103033. URL https://www.sciencedirect.com/science/article/pii/S1383762123002126
168. Kaur, J., Rani, R., Kalra, N.: Attribute-based access control scheme for secure storage and sharing of ehrs using blockchain and ipfs. Cluster Computing **27**(1), 1047–1061 (2024)
169. Jakhar, Amit Kumar, Singh, Mrityunjay, Sharma, Rohit, Viriyasitavat, Wattana, Dhiman, Gaurav, Goel, Shubham: A block-chain-based privacy-preserving and access-control framework for electronic health records management. Multimedia Tools and Applications, pp. 1–35, (2024)
170. Yin, Maofan, Malkhi, Dahlia, Reiter, Michael K., Gueta, Guy Golan, Abraham, Ittai: Hotstuff: Bft consensus with linearity and responsiveness. In Proceedings of the 2019 ACM Symposium on Principles of Distributed Computing, PODC '19, page 347-356, New York, NY, USA, (2019). Association for Computing Machinery. ISBN 9781450362177. https://doi.org/10.1145/3293611.3331591
171. Ron, Dorit, Shamir, Adi: Quantitative analysis of the full bitcoin transaction graph. In Ahmad-Reza Sadeghi, editor, Financial Cryptography and Data Security, pp. 6–24, Berlin, Heidelberg, (2013). Springer Berlin Heidelberg. ISBN 978-3-642-39884-1
172. Fleder, Michael, Kester, Michael S., Pillai, Sudeep: Bitcoin Transaction Graph Analysis. arXiv:1502.01657. [Online]., pp. 1–8, (2015). URL http://arxiv.org/abs/1502.01657
173. Dwork, Cynthia, McSherry, Frank, Nissim, Kobbi, Smith, Adam: Calibrating noise to sensitivity in private data analysis. In Theory of Cryptography Conference, pp. 265–284, (2006). https://doi.org/10.1007/11681878_14
174. Atzei, Nicola, Bartoletti, Massimo, Cimoli, Tiziana: A survey of attacks on ethereum smart contracts (sok). In Matteo Maffei and Mark Ryan, editors, Principles of Security and Trust, pp. 164–186, Berlin, Heidelberg, (2017). Springer Berlin Heidelberg. ISBN 978-3-662-54455-6
175. Deebak, B.D., AL-Turjman, Fadi: Privacy-preserving in smart contracts using blockchain and artificial intelligence for cyber risk measurements. Journal of Information Security and Applications, **58**, 102749, (2021). ISSN 2214-2126. https://doi.org/10.1016/j.jisa.2021.102749. URL https://www.sciencedirect.com/science/article/pii/S2214212621000028
176. Iraq Ahmad Reshi and Sahil Sholla: Challenges for security in iot, emerging solutions, and research directions. International

Journal of Computing and Digital Systems **12**(1), 1231–1241 (2022)
177. Iraq Ahmad Reshi and Sahil Sholla: Securing iot data: Fog computing, blockchain, and tailored privacy-enhancing technologies in action. Peer-to-Peer Networking and Applications **17**(6), 3905–3933 (2024)
178. Croman, Kyle, Decker, Christian, Eyal, Ittay, Gencer, Adem Efe, Juels, Ari, Kosba, Ahmed, Miller, Andrew, Saxena, Prateek, Shi, Elaine, Sirer, Emin Gün, Song, Dawn, Wattenhofer, Roger: On scaling decentralized blockchains. In Jeremy Clark, Sarah Meiklejohn, Peter Y.A. Ryan, Dan Wallach, Michael Brenner, and Kurt Rohloff, editors, Financial Cryptography and Data Security, pp. 106–125, Berlin, Heidelberg, (2016). Springer Berlin Heidelberg. ISBN 978-3-662-53357-4
179. Nasir, Muhammad Hassan, Arshad, Junaid, Khan, Muhammad Mubashir, Fatima, Mahawish, Salah, Khaled, Jayaraman, Raja: Scalable blockchains - a systematic review. Future Generation Computer Systems, **126**, 136–162 (2022). ISSN 0167-739X. https://doi.org/10.1016/j.future.2021.07.035. URL https://www.sciencedirect.com/science/article/pii/S0167739X21002971
180. Luciano Argento, Francesco Buccafurri, Angelo Furfaro, Sabrina Graziano, Antonella Guzzo, Gianluca Lax, Francesco Pasqua, and Domenico Saccà. Id-service: a blockchain-based platform to support digital-identity-aware service accountability. *MDPI*, 11(1):1–18, 2021. ISSN 20763417. https://doi.org/10.3390/app11010165
181. Guo, Hao, Li, Wanxin, Nejad, Mark, Shen, Chien-Chung: Access control for electronic health records with hybrid blockchain-edge architecture. In 2019 IEEE International Conference on Blockchain (Blockchain), pp. 44–51, (2019). https://doi.org/10.1109/Blockchain.2019.00015
182. Backes, Michael, Cachin, Christian, Oprea, Alina: Secure key-updating for lazy revocation. In Dieter Gollmann, Jan Meier, and Andrei Sabelfeld, editors, Computer Security – ESORICS 2006, pp. 327–346, Berlin, Heidelberg, (2006). Springer Berlin Heidelberg. ISBN 978-3-540-44605-7
183. Chinnasamy, P., Deepalakshmi, P., Shankar, K.: Chapter 6 - an analysis of security access control on healthcare records in the cloud. In Amit Kumar Singh and Mohamed Elhoseny, editors, Intelligent Data Security Solutions for e-Health Applications, Intelligent Data-Centric Systems, pp. 113–130. Academic Press, (2020). ISBN 978-0-12-819511-6. https://doi.org/10.1016/B978-0-12-819511-6.00006-6. URL https://www.sciencedirect.com/science/article/pii/B9780128195116000066
184. Sweeney, L.: Achieving k-anonymity privacy protection using generalization and suppression. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems **10**(05), 571–588 (2002). https://doi.org/10.1142/S021848850200165X
185. Chinnasamy, P., Deepalakshmi, P.: Hcac-ehr: hybrid cryptographic access control for secure ehr retrieval in healthcare cloud. Journal of Ambient Intelligence and Humanized Computing **13**(2), 1001–1019 (2022)
186. Council of the European Union. General data protection regulation (eu gdpr). https://gdpr-info.eu/, (2016)
187. Monika, Bhatia, Rajesh: Interoperability solutions for blockchain. In 2020 International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE), pp. 381–385, (2020). https://doi.org/10.1109/ICSTCEE49637.2020.9277054
188. Centers for Medicare & Medicaid Services. Health insurance portability and accountability act of 1996 (hipaa). https://www.cdc.gov/phlp/publications/topic/hipaa.html, 1996
189. Paul, D., Sanap, G., Shenoy, S., Kalyane, D., Kalia, K., Tekade, R.K.: Artificial intelligence in drug discovery and development. Drug discovery today **26**(1), 80 (2021)
190. Reshi, Iraq Ahmad, Sholla, Sahil: Leveraging AI and Blockchain for Enhanced IoT Cybersecurity, pp. 305–324. Springer Nature Singapore, Singapore, (2024). ISBN 978-981-97-1249-6. https://doi.org/10.1007/978-981-97-1249-6_14
191. Ilinca, Dragos: Applying Blockchain and Artificial Intelligence to Digital Health, pp. 83–101. Springer International Publishing, Cham, (2020). ISBN 978-3-030-12719-0. https://doi.org/10.1007/978-3-030-12719-0_8
192. Dinh C. Nguyen, Ming Ding, Quoc-Viet Pham, Pubudu N. Pathirana, Long Bao Le, Aruna Seneviratne, Jun Li, Dusit Niyato, and H. Vincent Poor. Federated learning meets blockchain in edge computing: Opportunities and challenges. *IEEE Internet of Things Journal*, 8(16): 12806–12825, 2021. https://doi.org/10.1109/JIOT.2021.3072611
193. Dhasaratha, Chandramohan, Hasan, Mohammad Kamrul, Islam, Shayla, Khapre, Shailesh, Abdullah, Salwani, Ghazal, Taher M., Alzahrani, Ahmed Ibrahim, Alalwan, Nasser, Vo, Nguyen, Akhtaruzzaman, Md.: Data privacy model using blockchain reinforcement federated learning approach for scalable internet of medical things. CAAI Transactions on Intelligence Technology, n/a (n/a). https://doi.org/10.1049/cit2.12287. URL https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/cit2.12287

Ahmed M. Tawfik holds a B.Sc. in Computer Science and an M.Sc. in Privacy and Security of EHRs from Benha University. He is currently pursuing a Ph.D. in Computer Science and serves as an Assistant Lecturer at the Faculty of Computers and Artificial Intelligence, Benha University. His research interests include privacy preservation in healthcare, security, and blockchain-based access control methods.

Ayman Al-Ahwal earned a B.Sc. in Electronics and Communication Engineering from Zagazig University (Benha Branch) in 1997, an M.Sc. from the same institution in 2003, and a Ph.D. in Electronics (Computer) from Benha University in 2008. His research focuses on computer network security, information security, IoT, VANET routing protocols, and cryptography.

Adly S. Tag Eldien received a B.Sc. in Electronics and Communication Engineering in 1984, an M.Sc. in 1989, and a Ph.D. in Electrical Engineering in 1993 from Zagazig University (Benha Branch). He is currently a professor in the Department of Electrical Engineering at Benha University. His research interests include communication networks, robotics, network security, privacy, and cryptography.

Hala H. Zayed earned a B.Sc. in Electronics and Communication Engineering from Zagazig University (Benha Branch) in 1985, an M.Sc. in 1989, and a Ph.D. in Electrical Engineering in 1995. She became an Associate Professor in Computer Engineering in 2005 and was promoted to Professor of Computer Science in 2012. Previously, she served as the Dean of the Faculty of Computers and Artificial Intelligence at Benha University. She is currently a Professor at the Faculty of Engineering, Egypt University of Informatics (EUI), Cairo, Egypt. Her research interests include artificial intelligence, neural networks, computer vision, feature extraction, pattern recognition, security, and healthcare.