Intelligent Medicine xxx (xxxx) xxx

Contents lists available at ScienceDirect

Intelligent Medicine

journal homepage: www.elsevier.com/locate/imed

Research Article

Blockchain for digital healthcare: Case studies and adoption challenges

Fei Zhou[1,2], Yue Huang[3], Chengquan Li[5], Xiaobin Feng[5], Wei Yin[5], Guoyan Zhang[1,2], Sisi Duan[4,*]

[1] School of Cyber Science and Technology, Shandong University, Qingdao, Shandong 250100, China
[2] Shandong Institute of Blockchain, Jinan, Shandong 250101, China
[3] Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China
[4] Institute for Advanced Study, Tsinghua University, Beijing 100084, China
[5] School of Clinical Medicine, Tsinghua University, Beijing 100084, China

ARTICLE INFO

Keywords:
Blockchain
Healthcare
Data sharing

ABSTRACT

Background The healthcare industry is significantly transforming toward digital and smart healthcare. Blockchain, as an emerging distributed collaborative paradigm, offers a promising solution for ensuring trustworthiness and high availability of services in the evolving healthcare sector. This study aimed to provide a comprehensive survey of blockchain-based applications in smart healthcare.

Methods We first present the real-world blockchain use cases in smart healthcare and related fields, outlining the motivations for this study. Next, we review the cutting-edge blockchain applications in various domains, including health data sharing, public health management, drug supply chains, insurance claims, and the Internet-of-Medical-Things. A detailed analysis of several blockchain-based healthcare data sharing scenarios is also included.

Results The findings illustrate the diverse applications of blockchain technology in enhancing healthcare systems, along with a detailed examination of the challenges related to technical implementation and adoption.

Conclusion We discussed the challenges encountered in blockchain integration in smart healthcare and propose potential solutions to guide future research in this area.

1. Introduction

The advancement in digital information technology has spurred rapid growth in the healthcare industry. Although digital services provide high-quality, efficient, and smart healthcare services, they also generate explosive growth in data volume. The International Data Corporation report estimates that the global healthcare data may exceed 50 zettabytes (ZB) [1]. Meanwhile, with the growing number of Internet-of-Medical-Things (IoMT) devices being deployed in the healthcare domain, the demand for efficient and large-scale data processing has grown significantly in recent years [2]. Conventional healthcare systems depend on centralized service for massive data storage and processing. This centralized system fails to accommodate efficient and massive data transmission and analysis. With respect to data sharing across healthcare institutions, it is often extremely expensive to share the data in real time. With the rapid development of electronic healthcare records (EHR) and interoperable healthcare data services, security and compliance in this area have attracted much research attention in recent years [3].

Blockchain has emerged as a promising solution for realizing a distributed and secure healthcare data management and sharing service. Conceptually, blockchain is a distributed collaborative system maintained by multiple parties in an untrusted environment. Blockchain achieves secure data processing among multiple parties without relying on trusted third parties. Blockchain has received extreme attention from academia and industry since Bitcoin was released in 2008 [4]. According to a report by Research and Markets [5], the global blockchain market will grow from an estimated USD 17.21 billion in 2023 to USD 29.35 billion in 2024 at a compound annual growth rate of 70.6.

Blockchain-based healthcare data management has been widely studied because of its excellent features, including data traceability, tamper-proof data storage, and availability of services. By incorporating access control mechanisms, blockchain-based solutions offer flexible data sharing, enforce accountability, and ensure data authentication. For instance, Patientory [6] uses blockchain to store and transfer healthcare data, ensuring secure and efficient data exchange. Chronicled [7] assists pharmaceutical companies in tracking the

* Corresponding author at: Sisi Duan, Institute for Advanced Study, Tsinghua University, Beijing 100084, China.
E-mail address: duansisi@mail.tsinghua.edu.cn (Sisi Duan).

https://doi.org/10.1016/j.imed.2024.09.001
Received 18 March 2024; Received in revised form 23 September 2024; Accepted 24 September 2024
Available online xxx

Please cite this article as: F. Zhou, Y. Huang, C. Li, et al., Blockchain for digital healthcare: Case studies and adoption challenges, Intelligent Medicine, https://doi.org/10.1016/j.imed.2024.09.001

production and distribution of their medicines, allowing law enforcement to monitor suspicious activities such as drug trafficking. Chronicled also developed the Mediledger [8] project, a ledger system dedicated to enhancing the safety, privacy, and efficiency of healthcare supply chains.

In the public health supply chain domain, blockchain-based data management has been well-studied. The secure data sharing and processing capabilities of blockchain make it a viable solution for data exchange among various organizations. This property is desirable in governmental and healthcare applications. A representative use case is the Accelerate project [9] by the U.S. Department of Health and Human Services (HHS). Accelerate stores HHS portfolio of 100,000 contracts. That portfolio is worth approximately $ 25 billion across approximately 50 systems. It was the first federal blockchain-based application that was granted the authorization to operate (ATO) by a designated approving authority, an internal senior management official.

Motivation and our contributions. Although several efforts have been made to study blockchain-based healthcare data management, existing solutions mainly focus on tackling one problem at a time (e.g., access control, anonymity). With respect to implementing and adopting blockchain in real-world applications, it is still unclear: 1) What are the killer applications of blockchain in the healthcare domain? 2) What technical challenges are yet to be resolved to support the massive adoption of blockchain-based data management solutions? To answer these questions, a thorough review and evaluation of blockchain-based healthcare data management solutions is required. To the best of our knowledge, although several survey articles have reviewed blockchain technology or blockchain-based solutions in general [10–12], no review has comprehensively summarized the real-world healthcare use cases, underlying techniques, and technical challenges.

Our study fills this gap by providing an overview of real-world use cases, the underlying cryptographic and blockchain solutions, and a summary of challenges. The key contributions of this review are outlined as follows:

- We introduce the blockchain concepts and core building blocks, aiming to describe blockchain from a technological perspective and the security properties that blockchain can achieve [Section 2].
- We present a review of the emerging blockchain-based applications in representative healthcare domains, including healthcare data sharing, public health management, drug supply chains, healthcare insurance claims, and IoMT. [Section 3].
- From the perspective of real-world use cases, we review and discuss how blockchain can be used to design a secure and efficient healthcare data sharing infrastructure in a decentralized, transparent, accessible, traceable, and auditable manner [Section 4].
- We discuss technical and adoption challenges and potential solutions for future blockchain research in smart healthcare [Section 5].

2. A technical overview of blockchain

2.1. System model

Blockchain is a distributed ledger maintained by multiple parties (often called nodes or validators). The ledger comprises a sequence of data blocks, each containing multiple transactions. The first ever block in the system is called a genesis block. As shown in Figure 1, each block, except for the genesis block, comprises two components: the block header and body. The body usually contains a batch of transactions. The block header includes metadata such as a timestamp, a hash [13] (to be defined shortly) of the parent block (i.e., the previous block in the chain), the hash of the block, and other data that might vary for different systems.

The cryptographic hash function is a one-way function that maps messages of arbitrary length to a fixed-length message digest. Most blockchain solutions rely on the collision resistance property of hash functions. Informally, collision resistance ensures that a computationally bound adversary cannot come up with two inputs that hash to the same value except for a negligible probability. With respect to the structure of the chain of blocks, it can be viewed as a cryptographic hash chain, where each block is linked to its parent block via the hash of the parent block. As the hash function is collision-resistant, we can ensure that the parent block is unique, so the chain clearly identifies a sequence of blocks (and transactions). Once the order of the hash chain is *finalized* on the blockchain, the order will never be reversed.

Notably, a cryptographic hash chain cannot guarantee that the chain order will never be reversed. Such a property (no reversed order) can only be guaranteed via the consensus mechanism of the blockchain (to be described shortly).

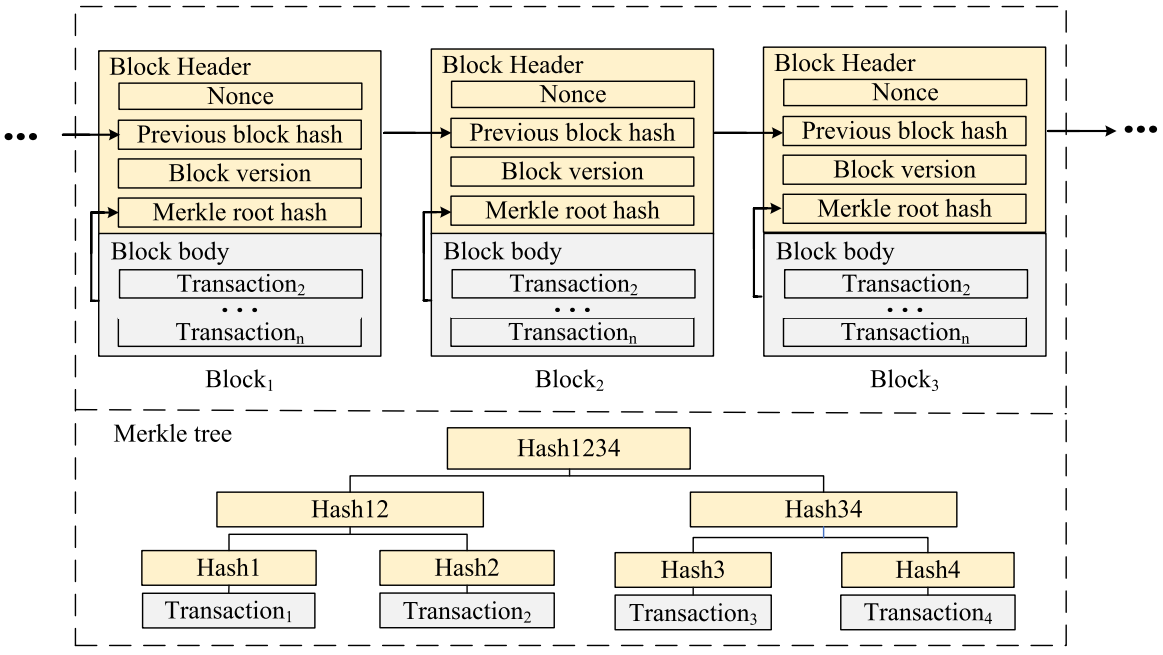

Figure 1. Blockchain structure.

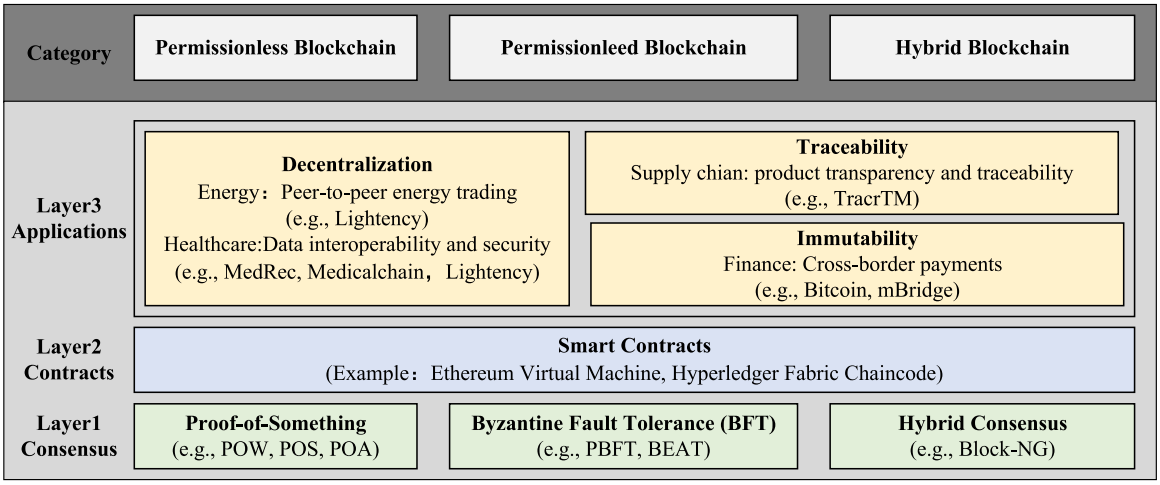

Figure 2. Overview of blockchains: a layered view and use cases.

2.2. Public key cryptography

Most blockchain platforms use public key cryptography [14] such as digital signatures. A digital signature scheme consists of three algorithms: key generation, signature signing, and signature verification. The key generation scheme outputs a pair of public/secret keys (pk, sk). Each party holds its secret key sk and makes its public key pk that is publicly available. Every party can query the key generation algorithm by themselves without relying on a trusted third party. In practice, a public key infrastructure (e.g., a trusted third-party certificate authority [15]) is sometimes needed to validate the key pair. A signature signing algorithm inputs a message and secret key and outputs a signature. Finally, a signature verification algorithm inputs a public key, message, and signature and outputs a $true/false$ (i.e., denoting whether the signature is verified). A secure digital signature scheme is unforgeable, where a computationally bound adversary cannot forge a valid digital signature (that passes the signature verification function) without obtaining a party's secret key.

The most commonly used digital signature scheme is the Elliptic Curve Digital Signature Algorithm (ECDSA) [16].

2.3. A layered view of blockchain

As illustrated in Figure 2, blockchain can be abstracted into three layers: consensus, smart contract, and application.

2.3.1. Layer 1: consensus

The consensus mechanism serves as the foundation of the blockchain system. An ideal blockchain consensus protocol tolerates Byzantine failures, i.e., software bugs, hardware errors, and malicious attacks. Therefore, blockchain consensus protocols are also called Byzantine fault-tolerant (BFT) protocols. Different Byzantine consensus protocols make different assumptions on the adversary model, including the threshold adversary, computational threshold adversary, and token threshold adversary models [11]. The threshold adversary model assumes that the adversary cannot corrupt a sufficiently large fraction of the nodes. Examples include standard BFT protocols, such as PBFT [17], Hotstuff [18], HoneyBadgerBFT [19], BEAT [20], and PACE [21]. The computational threshold adversary model assumes that the adversary cannot control a sufficiently large fraction of computational power. The most representative consensus solution in this category is Proof-of-Work [22] based consensus, the underlying consensus solution to Bitcoin and Ethereum 1.0 [23]. The token threshold adversary model assumes that the adversary cannot control more than a fraction of tokens. This type of consensus protocol is often used in cryptocurrencies, e.g., Polkadot [24] and Ethereum 2.0.

2.3.2. Layer 2: smart contracts

Smart contracts are self-executing computer programs. It enables automatically executing agreements based on predefined conditions on blockchains [25]. Smart contracts were originally introduced by Szabo [26], and the first instantiation of smart contracts in blockchains was by Ethereum [23]. Blockchain smart contracts offer automated execution of business logic. The smart contract layer offers an interface to implement new functions without the need to halt or restart the system. Depending on the platform, smart contracts can be developed using various programming languages. Popular platforms include Ethereum virtual machine (EVM) [27] and hyperledger fabric chaincode [28]. Smart contracts facilitate, verify, or enforce the execution of business transactions. Smart contract-enabled blockchain realizes state machine replication that allows honest nodes to maintain a consistent state of the transactions and execution results.

2.3.3. Layer 3: applications

The application layer allows blockchain-based applications to deliver services to the end-users. The application layer allows one to use blockchains in different use cases. To serve the purposes of concrete applications, developers may need to write new smart contracts to instantiate new application rules or provide APIs for the applications to query the data (e.g., web APIs).

2.4. Categories of blockchain

According to the parties that can participate in the blockchain, blockchains are categorized into permissionless, permissioned, and hybrid. The permissionless blockchain allows anyone to join the system. The permissioned blockchain only allows authorized parties to join the network. Additionally, the hybrid blockchain combines permissionless and permissioned blockchain features.

2.4.1. Permissionless blockchain

Permissionless blockchains allow anyone to join the network. Bitcoin [29] is a prime example. Bitcoin allows individuals to join the network using a pair of public and private keys. Most permissionless blockchains adopt a proof-of-something consensus protocol. For instance, Bitcoin employs a proof-of-work (PoW) [22] consensus mechanism. PoW involves solving a mathematical puzzle, an activity also known as mining. The blockchain node that solves the puzzle first successfully mines the

block and obtains some reward. The node also has the right to propose the next block, which includes a new puzzle. The major challenge of PoW is that it consumes high computing power and has low throughput (transactions are processed per second).

Other examples of consensus protocols for permissionless blockchains include proof-of-stake (PoS) and proof-of-authority (PoA). Although there is no clear definition of PoS, most PoS-based consensus protocols allow nodes to join the system and become eligible to vote by staking a certain amount of tokens. Most PoS-based consensus protocols are a hybrid of PoW and BFT, using some concepts in BFT for the finalization of the blocks. Additionally, PoA-based consensus usually selects a small group of nodes as representatives. The representatives reach an agreement on the order of the blocks and then convey the results to all the participants in the system.

2.4.2. Permissioned blockchain

Permissioned blockchains require participants to be permissioned, i.e., all nodes know the identities of each other. Hyperledger Fabric is a well-known, permissioned blockchain platform. Most permissioned blockchains are based on conventional BFT protocols. For instance, Aptos and Sui use HotStuff, VMware blockchain uses SBFT [30], and Tendermint uses the Tendermint BFT [31]. Compared to the consensus protocols used in permissionless blockchains, BFT protocols achieve higher throughput and lower latency among a smaller group of nodes.

2.4.3. Hybrid blockchain

Hybrid blockchains combine the characteristics of permissionless blockchains and permissioned blockchains, aiming for the best of both worlds. Most hybrid blockchains aim to build a system with higher throughput than conventional permissionless blockchains and higher scalability (scaling to a large number of nodes) than permissioned blockchains. Delegated PoS (DPoS) is an example. In DPoS, nodes can stake some of their tokens to some delegate who can vote for them. After the group of delegates are selected, the nodes can reach an agreement on the order of the blocks using PoS. In particular, this can also be viewed as a variant of PoS and PoA. The major challenge of protocols in this model is that it might be challenging to reason about their correctness. Other examples include bitcoin-NG [32], Ethereum 2.0 [24], and Omniledger [33].

3. Blockchain in healthcare

In this section, we first discuss the successful blockchain solutions in related healthcare domains, such as finance, supply chain, and energy [34]. We then explore how these can address similar challenges in the healthcare sector. We also examine representative use cases with insights on various healthcare scenarios, including data sharing, public health management, drug supply chains, healthcare insurance claims, the IoMT, and genomics.

3.1. Prevalent solutions in domains other than healthcare

Blockchain technology has been successfully implemented in the finance, supply chain, and energy sectors [35]. We present three representative domains related to healthcare applications: cross-border payments in the finance sector, traceability and tamper-proof in the supply chain sector, and data exchange and distribution in the energy sector. We discuss relevant use cases in these sectors and how some of the solutions are applicable to the healthcare domain.

3.1.1. Finance sector: cross-border CBDC

One representative use case in the finance sector is cross-border payment. Conventional cross-border payment often relies on a single trusted service such as SWIFT [36] and suffers from challenges such as high costs, low speed, lack of transparency, and operational complexities. Blockchain-based solutions can significantly simplify the complicated cross-border payment process, as transactions can be finalized relatively quickly. In recent years, several countries have started researching and implementing central bank digital currencies (CBDCs) and using cross-CBDC solutions for cross-border payments. For example, the Bank for International Settlements (BIS) launched the mBridge project [37], providing real-time, peer-to-peer, cross-border payments and foreign exchange transactions among multiple CBDCs.

Similar to cross-border payments, managing and processing data across healthcare institutions involves significant costs and complex procedures. It impacts the efficiency and sustainability of the system. Given the successful cross-border payment cases such as mBridge, the healthcare sector can similarly leverage blockchain technology to link various institutions in a decentralized manner. This streamlines healthcare transaction processing by reducing the reliance on centralized intermediaries [38].

3.1.2. Supply chain sector: tracing and tamper-proof

Blockchain transactions encompass the essential data to trace procurement, manufacturing, distribution, and logistics processes. These data are permanently recorded on the blockchain. Therefore, blockchain solutions can significantly benefit global supply chains by improving the traceability and transparency of products, particularly for high-end items. For example, diamond producer De Beers uses the TracrTM [39] blockchain to identify the source and production of the diamonds [40]; Ford uses the IBM blockchain to trace its cobalt supply [41].

In the healthcare domain, the pharmaceutical supply chain is related to the supply chain section. The pharmaceutical supply chain involves multiple parties, including manufacturers, distributors, wholesalers, retailers, and medical institutions. The data originating from various participants in the supply chain can be tampered with or distorted. It increases the risk of counterfeit drugs. Blockchain-based solutions can thus benefit such applications [42].

3.1.3. Energy sector: data exchange and distribution

Energy trading across regions and energy carriers are emerging topics in the energy sector. Blockchain facilitates peer-to-peer trading among distributed energy resources without a single trusted authority. Lightency [43], a French green-tech startup, established a blockchain-based peer-to-peer electricity trading platform. The production, consumption, and energy exchange events are stored on the platform, achieving transparency and traceability of the trades. Blockchain-based solutions can also achieve decentralized data exchange and remote control of the energy flow. For instance, Drone Energy provides sustainable blockchain-based energy management by building a decentralized, on-demand energy supply architecture [44].

In healthcare, the IoMT are related. IoMT devices, such as smart watches, blood glucose monitors, and heart rate monitors, can collect patients' health data in real time and transmit it to medical institutions through the network. This improves the efficiency of patients' health management and reduces the burden on hospitals. Modern medical equipment (such as MRI and CT scanners) usually consume considerable amounts of energy. It is crucial to manage their energy consumption [45] effectively. Various IoMT devices can achieve data interconnection and interoperability through peer-to-peer transactions on the blockchain. It improves the compatibility of different medical devices and systems.

3.2. Representative healthcare use cases

We explored six key areas: healthcare data sharing, public health management, drug supply chains, healthcare insurance claims, and IoMT. We have summarized the challenges in these scenarios, how blockchain can address the challenges, and representative projects in Figure 3.

Use cases	Healthcare challenges	Blockchain opportunities
Healthcare data sharing	Secure cross-domain data sharing	Distributed ledger and consensus protocol
Public health management	Complex intermediary processing flow	Distributed ledger and traceability
Drug supply chain	Drug traceability and anti-counterfeiting	Immutability and transparency
Health insurance claim	Efficiency improvement and fraud prevention	Distributed ledger and immutability
Medical Internet of Things	MIoT devices authentication and connection	Distributed ledger and consensus protocol
Genomics	Data security and privacy preservation	Immutability and encryption

Figure 3. Blockchain-based healthcare use cases.

3.2.1. *Healthcare data sharing*

In a real-world healthcare environment, data originates from various healthcare institutions and IoMT sensor devices. Healthcare data sharing across institutions raises security concerns, such as data leakage or violation of data compliance policies. Consequently, organizations are reluctant to share data with external parties.

Blockchain provides a solution for data sharing within the medical industry. It fosters collaboration and the flow of information among various healthcare institutions, patients, and researchers. The blockchain-based solution has five key features: governance, interoperability, privacy, scalability, and security. Specifically, governance is ensured through the transparency of blockchain records to authorized parties. Interoperability is accomplished by integrating blockchain with healthcare standards such as Health Level 7 (HL7). Privacy is maintained by incorporating data encryption and fine-grained access control into the blockchain framework. Finally, scalability and security are achieved by carefully selecting appropriate blockchain platforms.

Owing to these outstanding characteristics, numerous blockchain-based applications for healthcare data sharing have been developed.

- Healthcare APIs provider PokitDok and Intel launched the DokChain medical blockchain project in 2016 [46]. DokChain is a distributed transaction processing network that processes financial and clinical data across the healthcare industry [47]. It connects all participants and stakeholders in the healthcare ecosystem, including endpoints such as electronic health records and devices such as heart monitors. Furthermore, DokChain automates payment processing and data exchange via smart contracts.
- The Patientory mobile app launched PTOYMatrix in 2020, one of the world's first blockchain-focused healthcare solutions [6]. Patientory keeps healthcare data on its native PTOYMatrix blockchain to facilitate healthcare service providers with superior accessibility and management of their patient's data (such as emergency room visits and medical images) [47]. To ensure data confidentiality, Patientory stores ciphertext on-chain for sensitive information and empowers data owners to define and manage their access permissions.
- Embleema launched PatientTruth in 2018, the first blockchain-based personal health record system [48]. As a patient-centered healthcare blockchain network, Embleema consolidates a secure repository by hosting it on a private Ethereum blockchain. This gives healthcare stakeholders a holistic view of a patient's medical history. Meanwhile, with blockchain and decentralized app (DApp), Embleema allows patients to assemble health history from dispersed health data originating from different resources such as healthcare providers' EHRs and connected health devices [49]. Embleema also exploits smart contracts to completely control data authorization and sharing.

3.2.2. *Public health management*

Public health encompasses vast amounts of data, such as epidemic surveillance, disease management, and vaccination records. The absence of a transparent and unified data sharing mechanism among various medical institutions, government departments, and international organizations hinders effective collaboration. For example, inconsistent information (e.g., due to delayed updates) may affect public health decision making. Similarly, public health entails extensive administrative tasks, including data reporting, auditing, and compliance verification. Current manual or semi-automated processes are inefficient and susceptible to data loss or delays.

Blockchain offers a unified, transparent, and real-time platform for data exchange. It enables all stakeholders to access reliable, tamper-proof health data in real time, ensuring consistency and transparency in public health information. To address cumbersome administrative management and processes, blockchain's smart contract technology can automate several tasks, minimizing errors and delays associated with human intervention.

- A healthcare blockchain startup, Coral Health, exploits blockchain to store patients' healthcare data and connects doctors, scientists, lab technicians, and public health authorities for data sharing [50]. To expedite the healthcare process, Coral Health also implements smart contracts for patients and healthcare professionals to streamline administrative procedures and guarantee the accuracy of patient data and treatment plans.
- The Estonian eHealth authority partners with GuardTime, a blockchain technology firm, to enhance transparency and audibility in healthcare [51]. Integrating blockchain with the Oracle database provides an independent audit trail for the entire lifecycle of patient records. That prevents tampering with data access history.

3.2.3. *Drug supply chain*

As mentioned previously, the pharmaceutical supply chain encounters several challenges, including inconsistent data, counterfeit drugs, data tampering, insufficient real-time monitoring, and complex compliance requirements. These challenges threaten the quality management, traceability, and safety of drugs.

Blockchain technology promotes transparency in the drug supply chain by maintaining traceability and tracking of drug data on the

chain. By providing a common blockchain-based collaboration platform, blockchain-based solutions integrate data from all parties for the drug supply chain. Meanwhile, with a tamper-proof log of blockchain, blockchain-based solutions properly monitor and track the whole supply chain process, from the acquisition of raw drug materials to production, storage, distribution, and sales of drugs. These guarantee the authenticity and quality safety of medicines and combat the market of counterfeit and inferior medicines.

Below, we discuss several solutions for drug supply chain management.

- FarmaTrust developed a blockchain-based solution called Zoi, a supply chain management platform. Zoi verifies and tracks pharmaceutical products through complete custody of the supply chain [52,53]. With the Ethereum blockchain network, FarmaTrust works with pharmaceutical companies, government agencies, and law enforcement to develop robust and smart data processes. The processes conduct security verification and tracking of authentic transnational drugs. Meanwhile, the Zoi platform can effectively prevent counterfeit and inferior drugs from entering the consumer market by integrating blockchain technology with machine learning and intelligent business logic. Besides, FarmaTrust encrypts data sets that circulate across the network. Additionally, it incorporates zero-knowledge proof [54] techniques for participants to verify data without revealing trade secrets.
- Blockpharma has developed a blockchain-based supply chain management system. This system aims at ensuring drug traceability and combating counterfeiting [55]. By scanning the supply chain and verifying each shipment point, the company's app enables patients to determine whether they are consuming counterfeit medications. According to builtin [56], Blockpharma says it helps to weed out the 15 percent of all drugs in the world that are fake.

3.2.4. Health insurance claim

Data sharing between insurers and alternative healthcare providers frequently suffers from a lack of transparency. It results in misunderstandings and disputes during the claims process. Blockchain's distributed ledger technology dismantles the data silos that exist between insurance companies, patients, and medical institutions. This approach alleviates the burden on policyholders to submit claim materials and evidence, eliminates lengthy reimbursement processes, and significantly enhances the efficiency of healthcare insurance claims. Meanwhile, the healthcare data maintained on the blockchain is accurate and immutable, which enhances the transparency and credibility of the insurance claim process and effectively avoids insurance fraud.

Below, we list a few blockchain-based solutions and their application scenarios.

- Change Healthcare launched the first enterprise-grade blockchain solution for healthcare in 2018 [57], i.e., Intelligent Healthcare Network^{TM}. The blockchain-based solution constructed a claims-processing network based on Hyperledger Fabric. Relevant institutions on the blockchain track the status of claim submissions and payment receipts throughout the claim process. This improves claims lifecycle throughput and transparency. Currently, Intelligent Healthcare Network^{TM} processes up to 50 million transactions daily, with a throughput of up to 550 transactions a second [58].
- Gem announced Gem Health, a network for developing blockchain applications for healthcare and health claims management, in 2016 [59]. Powered by Ethereum, Gem aims to create a healthcare ecosystem connecting universal data infrastructure. In this ecosystem, patients, providers, and insurers can securely access a patient's health timeline in real time, improving the speed and transparency throughout the claims process [47].

3.2.5. Internet-of-Medical-Things

IoMT devices are currently used in and out of clinics and hospitals. These devices can remotely monitor patients' vital signs, providing remote monitoring and virtual access to patients' symptoms. Conventional IoMT devices relied on a centralized agent or a cloud provider to store all the data. However, the cloud provider should be completely trustworthy. Moreover, different brands use different cloud providers, making data sharing difficult. Blockchain directly solves these challenges by providing a unified view of all IoMT data.

- Multinational Internet of Things supply chain manufacturer Ambrosus [60] combines high-tech sensors, blockchain, and distributed open-source software to build a universally verifiable, community-driven ecosystem to assure drug quality, safety, and origins. It uses Ethereum's smart contract into the drug supply chain for automated governance and data management. In this solution, product quality and device identities are verified according to predefined requirements written in smart contracts. Besides, Ambrosus uses the InterPlanetary File System, a distributed storage service, alongside the blockchain to store all sensors' data [61].
- Blockchain company Tierion cooperated with Philips on a blockchain-based medical project in 2015 [62]. Tierion [63] proposed the Chainpoint protocol to anchor data to the blockchain. A proof of the data with a timestamp from the blockchain was generated for verification. By using the decentralized real-time data monitoring solution provided by Tierion, Philips stores an audit trail of the maintenance, usage, and calibration history of the IoMT devices on the blockchain. This guarantees the integrity of data collected from IoMT devices and realizes real-time monitoring of patient healthcare data.

3.2.6. Genomics

Genetic data are extremely sensitive personal information, making it susceptible to leakage and misuse. To address this concern, blockchain-based solutions can often be integrated with cryptographic approaches such as encryption and privacy-preserving computing to ensure that only authorized users can access genetic information or information computed on top of genetic information.

- Genecoin [64] has leveraged blockchain technology in the field of genomics since 2014. Genecoin employs a decentralized blockchain network to store genetic data, ensuring immutability and traceability. It also allows users to receive tokens as rewards for sharing genetic data. This incentive encourages more people to contribute data and supports genomics research.

4. Two representative solutions in blockchain-based healthcare data sharing

As outlined in our discussion in Section 3, data sharing serves as a prominent use case for blockchain technology. Indeed, the nature of blockchain (e.g., data transparency and high availability of the service) makes it an excellent fit to facilitate EHR sharing and multimodal data sharing across organizations. The healthcare field has high standards for data privacy and security owing to its close connection to people's lives. Blockchain technology helps protect sensitive health information. Additionally, blockchain can support data sharing among medical institutions, enhancing treatment efficiency and patient experience. Therefore, in this section, we narrow down to blockchain-based data sharing and review the details of two representative projects: MedRec [65] and Medicalchain [66]. We summarize the architecture and module design of the two systems, aiming to demonstrate the use of blockchains in concrete applications.

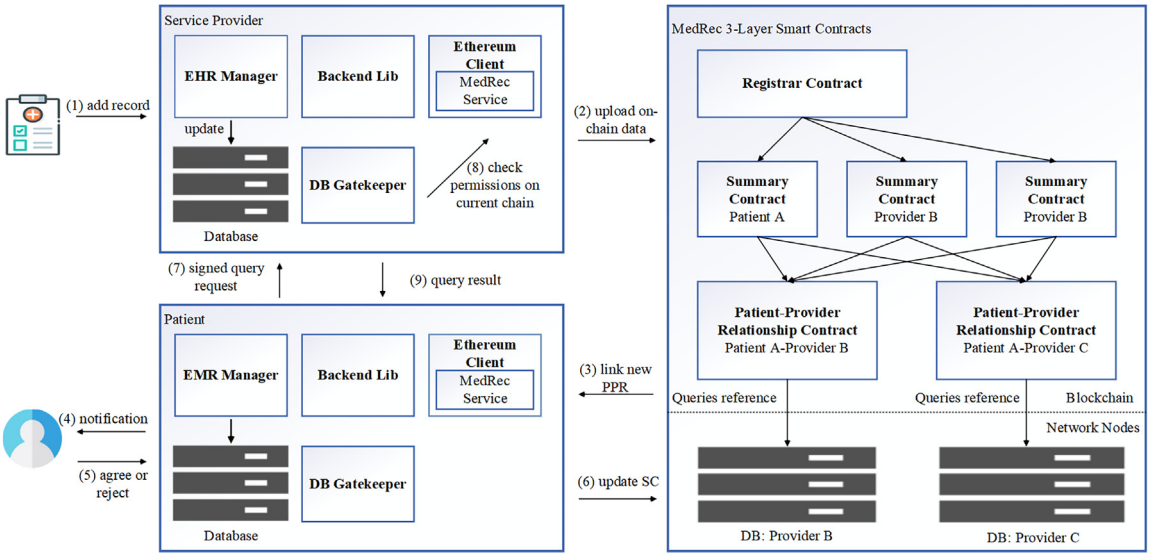

Figure 4. MedRec's system model.

4.1. MedRec: blockchain for healthcare data access and permission management

MedRec [65] is the first fully functional blockchain prototype designed for a patient-centric electronic health records management system. By recording access control logs for EHRs across multiple healthcare institutions on the blockchain, MedRec achieves traceability of patient medical data. To ensure flexibility and compatibility with the existing off-chain infrastructures (e.g., local databases), MedRec uses a modular API that enables seamless integration with diverse healthcare systems.

Given the massive volume of data typically handled in healthcare applications, MedRec uses a hybrid storage approach. Specifically, raw data are stored in local SQLite databases at healthcare institutions, while the blockchain retains only the hash values of these data. This protects the integrity and security of the original data while simultaneously enhancing the scalability of MedRec's data storage.

Furthermore, to promote a sustainable ecosystem within healthcare information systems, MedRec incorporates an incentive mechanism inspired by Bitcoin. In this model, stakeholders such as researchers and public health authorities act as miners. The miners uphold the integrity of the blockchain network, facilitate the exchange of healthcare data, and receive mining rewards as compensation.

MedRec exploits Ethereum's smart contracts to keep track of medical records' ownership and access permissions. To achieve efficient, flexible, fine-grained access control and secure data sharing, it deploys a 3-layer smart contract, as shown below.

- The registrar contract (RC) maps entity identification to a blockchain address to complete the data requester's identity authentication and maintain anonymity.
- The patient-provider relationship contract (PPR) maintains data ownership, stewardship, and views permissions between patients and healthcare service providers.
- Summary contract (SC) contains a list of references to PPRs to maintain data history.

MedRec modularizes system components to integrate with existing healthcare infrastructures. It proposes four software components on the servers: Backend Library, Ethereum Client, Database Gatekeeper, and EHR Manager.

- The Backend Library abstracts the communication between the applications and blockchain. It provides a function-call API for managing the applications and data that need to be stored on-chain.
- The Ethereum Client is responsible for all the functionalities required to join and participate in the Ethereum blockchain network.
- The Database Gatekeeper interacts with the off-chain databases and handles data access requests.
- The EHR Manager connects all the above components and provides a visualization interface to the users via user interfaces.

We have summarized the workflow of MedRed in Figure 4. The system involves nine steps for submitting data on-chain.

- In steps 1 and 2, the service providers add new patient records to the off-chain database via the EMR Manager. By querying the Backend Library's APIs and using the RC on the blockchain, the patient's identity is resolved to their matching ethereum address, and the corresponding SC is located. Later, the provider uploads the new PPR to the blockchain. The contract aims to define the data access rules.
- From steps 3 to 6, the ethereum client component continuously monitors its SC. Once a new PPC is linked to SC, the ethereum client notifies the patients. The patients agree to or reject the provider's PPR contracts. The SC is also updated accordingly.
- From steps 7 to 9, after the provider's PPR request is agreed upon, the patient sends query requests to the provider's Database Gatekeeper server to retrieve the EHRs and attains query results.

4.2. Medicalchain: blockchain for healthcare data storage and secure sharing

The EHR platform Medicalchain [66] uses blockchain technology to securely store and manage EHR, achieving secure, transparent, fast, and cross-domain healthcare data sharing. The Medicalchain announced a partnership with The Groves Medical Group [67] in 2018. The Groves Medical Group is the first medical practice in the UK to use blockchain technology and to accept cryptocurrency as the payment for health services [68]. It allows patients to take full control of their healthcare records through blockchain technology and will provide access to flexible telemedicine services.

The Medicalchain developed a dual blockchain architecture that uses Hyperledger Fabric and ethereum [69] (in particular, ERC20 token [70]) with three layers: ethereum, fabric, and storage layers (Figure 5)

The ethereum layer is used to manage participants in the system and make transactions. Its function includes account services, cross-layer

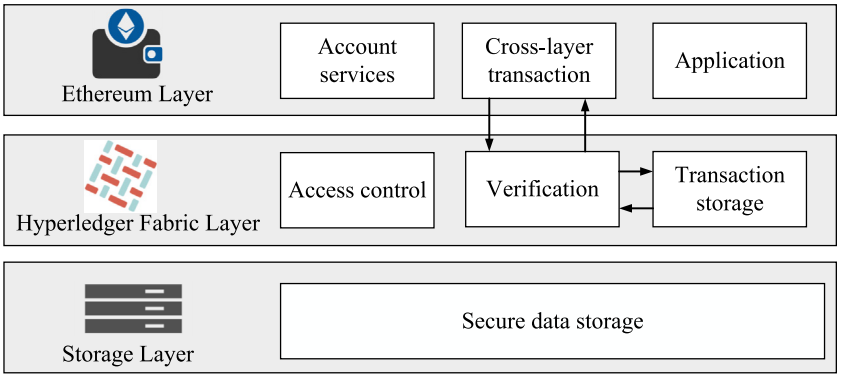

Figure 5. Medicalchain's system model.

transactions, and applications. This layer's account service manages all ethereum network nodes, maintaining the account details and balances. Medical cross-layer transactions on the Medicalchain (i.e., storing or retrieving an EHR) are powered through a newly created cryptocurrency on ethereum ERC20, called MedTokens, powered by the consensus proof of stake [71]. Medicalchain preserves and verifies all token transactions. For example, MedToken enables patients to receive telemedicine consultations and rewards doctors for telemedicine services. Meanwhile, to form a fully automated network, it exploits smart contracts to allow users to program processes. The application function also supports other applications and upper-level services.

The hyperledger fabric layer is designed based on a consortium blockchain model to manage the storage and access of EHRs. As a permissioned blockchain, the Hyperledger Fabric establishes decentralized trust in a network of known participants (patients and practitioners) rather than an open network of anonymous participants. This layer has three main functions: access control, verification, and transaction storage.

- The access control technology used in this study is built upon Medical-chain's access control language (ACL), where access permissions are determined using specific elements and predefined rules. Through ACL, this layer can efficiently govern participants' access to resources within the network's domain mode.
- During the verification, the authenticated data structure (ADS) is generated by hashing the metadata of a new transaction, resulting in a hash value that is typically derived from the Merkle root of the Merkle tree. This hash value acts as a unique identifier. By comparing the metadata hash values between the ethereum and fabric layers, the system guarantees the integration of transactions.
- In this layer, transactions involving EHRs are initially stored in the transaction storage for temporary retention. Once verified, these transactions are securely transferred to the storage layer.

The storage layer provides secure storage functionality, storing all transactions transmitted from the fabric layer. Data are permanently stored within the secure storage consistent with the fabric layer to ensure traceability.

To prevent unauthorized data access and maintain data safety, MedicalChain uses symmetric cryptography techniques to encrypt the patients' EHRs, ensuring the privacy of data. Additionally, MedicalChain also employs asymmetric cryptography methods to encrypt these symmetric keys to prevent malicious attackers from stealing symmetric keys.

5. Technical and adoption challenges

Despite the increasing number of blockchain-based projects, technical and adoption challenges persist. In this section, we summarize the challenges based on our survey results.

5.1. Technical challenges

5.1.1. Performance and scalability

Performance is a primary consideration when implementing real-world blockchain applications. Throughput and latency are critical performance indicators for assessing the efficiency of the consensus mechanism. Throughput is defined as the number of transactions processed within a specified timeframe, typically measured in transactions per second (TPS) [72]. Latency refers to the time taken for each transaction to be finalized on the blockchain after submission. Additionally, scalability usually denotes the number of blockchain nodes that can participate in the system without significant performance degradation.

For instance, Bitcoin's throughput is approximately 7 TPS, whereas Ethereum generally has 15-30 TPS [73]. Recent research has explored the concept of layer *2* to enhance the performance of the blockchains. The idea of layer 2 solutions is to execute some transactions off the chain (i.e., layer 1 blockchain or simply mainchain) and store the execution results on the chain. Examples include bitcoin's lightning network [74] and Ethereum's plasma [75]. Additionally, Zilliqa [76] and Ethereum 2.0 [77] leverage sharding to optimize the data storage. Finally, some solutions also explore the scalability of conventional BFT protocols [78–80] to provide more efficient solutions for the blockchain consensus.

5.1.2. Storage limitation

Blockchain requires all parties to store all the data (i.e., transactions), functioning in an append-only manner. The storage costs grow over time. As the data volume increases, the storage capacity of the blockchain becomes a critical challenge. As of July 2023, Bitcoin has 799,579 blocks, with tens of thousands containing millions of transactions accumulated over the past decade. In contrast, Ethereum boasts 17,738,278 blocks and approximately 700 GB of transaction data [81].

Multiple solutions have been proposed to address the storage limitations. Some blockchain Layer 2 models process transactions off-chain and submit the final state to the blockchain. This off-chain processing increases data processing speed and efficiency while ensuring the main chain's security [75,82]. Additionally, BigchainDB [83] integrates erasure coding, a commonly used technique in reducing the storage cost for databases, with blockchain to reduce the storage cost.

5.1.3. Adaption to existing relational databases and verifiable query

Verifiable data query refers to a mechanism that ensures the correctness and integrity of query results, particularly in an untrusted environment such as cloud services. Most healthcare information systems focus on efficient relational queries. However, they do not consider the integrity and correctness of these results. In contrast, blockchain uses key-value pairs to store the data, so blockchain-based solutions fail to support rich and complex relational queries. Significant efforts have been undertaken to enable relational data support on blockchains [84–86].

Several solutions have been studied for verifiable data queries leveraging the authenticated data structure (ADS). For instance, vChain [87] leverages the Merkle tree as its ADS, enabling the blockchain to support verifiable Boolean and numeric range queries. The ADS solution broadens the range of blockchain data queries by optimizing the Merkle tree structure. However, ADS continues to face challenges, such as long construction delays. Meanwhile, blockchain remains insufficient for supporting comprehensive, flexible, and complex relational queries. Consequently, the blockchain continues to have limitations in addressing more advanced query requirements.

5.2. Adoption challenges

5.2.1. Data security

Healthcare data often contain sensitive information. To protect the security and privacy of healthcare data, countries worldwide have implemented various data protection laws and regulations. For instance, the United States has enacted the Health Insurance Portability and Accountability Act [88]. It aims to regulate the transmission and utilization of EHR and protect citizens' personal health information. Thus, blockchain-based solutions should be developed to comply with these regulations. Several solutions achieve such a need. For example, Ancile [89] exploits smart contracts in an ethereum-based blockchain for patient-centric access control, achieving HIPAA compliance.

5.2.2. Data interoperability

Data interoperability refers to different systems and organizations' ability to exchange and collaborate using data and information. It ensures that the exchanged data are accurately interpreted and seamlessly integrated. Meanwhile, the meaning and context of the exchange data should be preserved [90]. Blockchain-based healthcare systems have various characteristics, such as governance rules and data standards. Current healthcare interoperability standards, such as integrating the healthcare enterprise and HL7 fast health interoperability resources [91], facilitate healthcare data exchange and collaboration. However, interoperability between multiple blockchain systems introduces another challenge. Several healthcare systems are based on different blockchain platforms. There is currently no universal standard that defines blockchain and data interoperability.

5.2.3. Data ownership

Data ownership generally refers to the control and responsibility of an individual or organization over their data. The control includes the rights to create, manage, use, and share data [92]. As healthcare providers become more reliant on data, the issue of data ownership transcends mere technical concerns [93]. Moreover, healthcare data often undergoes intricate processes of transmission and transformation [93]. In this context, data ownership is shaped by various factors. For instance, personal data, especially personally identifiable information, is typically owned by patients, though the service providers generate it.

Modern healthcare data applications are increasingly adopting patient-centric access control mechanisms. MediBloc [94] is one of the leading examples of healthcare applications. In MediBloc, patients take ownership of their data. They have the ability to control and manage their health data and securely share specific information with medical institutions or researchers. However, in certain healthcare settings, data generated by the providers cannot be easily shared with other institutions. Consequently, the healthcare sector continues to face logistical and technological challenges.

6. In summary

In this study, we reviewed blockchain-based solutions for digital and smart healthcare applications. We reviewed the technical building blocks of blockchains and representative use cases of blockchain-based solutions in smart healthcare, including health data sharing, drug supply chains, healthcare insurance claims, and IoMT. By comprehensively considering some solutions, we summarized the key challenges that are left unaddressed and potential solutions.

Conflicts of interest statement

The authors declare no conflicts of interest.

Fundings

This work was sponsored by the Tsinghua-Toyota Joint Research Institute Inter-disciplinary Program.

Author contributions

Fei Zhou: Conceptualization, Methodology, Writing – original draft, Writing – review & editing, Visualization. **Yue Huang:** Conceptualization, Methodology, Writing – original draft, Writing – review & editing, Visualization. **Chengquan Li:** Conceptualization, Writing – review & editing. **Xiaobin Feng:** Conceptualization, Writing – review & editing. **Wei Yin:** Conceptualization, Writing – review & editing. **Guoyan Zhang:** Conceptualization, Writing – review & editing. **Sisi Duan:** Conceptualization, Methodology, Writing – original draft, Writing – review & editing, Visualization.

References

[1] Idc futurescape: Worldwide healthcare industry 2024 predictions. Avaiable from https://www.idc.com/getdoc.jsp?containerId=US50105223&pageType=PRINTFRIENDLY.
[2] Kraus S, Schiavone F, Pluzhnikova A, et al. Digital transformation in healthcare: analyzing the current state-of-research. J Bus Res 2021;123:557–67.
[3] Nowrozy R, Ahmed K, Kayes A, et al. Privacy preservation of electronic health records in the modern era: a systematic survey. ACM Comput Surv 2024;56(8):1–37.
[4] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. Decentralized business review 2008:21260.
[5] Blockchain global market report 2024. Available from https://www.researchandmarkets.com/reports/5735144/blockchain-global-market-report.2024.
[6] Meet patientory's blockchain solution protecting healthcare data. Available from https://bitcoinist.com/meet-patientorys-blockchain-solution-protecting-healthcare-data/.
[7] Chronicled. Available from https://www.chronicled.com/.
[8] Mediledger. Available from https://www.mediledger.com/.
[9] Report: Hhs obtains authority to operate ai, blockchain-based acquisition tool. 2018. Available from https://www.executivegov.com/2018/12/report-hhs-obtains-authority-to-operate-ai-blockchain-based-acquisition-tool/.
[10] Clavin J, Duan S, Zhang H, et al. Blockchains for government: use cases and challenges. Digital Government: Research and Practice 2020;1(3):1–21. doi:10.1145/3427097.
[11] Wang X, Duan S, Clavin J, et al. Bft in blockchains: from protocols to use cases. ACM Comput Surv 2022;54(10s):1–37.
[12] De Aguiar EJ, Faiçal BS, Krishnamachari B, et al.. A survey of blockchain-based strategies for healthcare, 53. ACM Computing Surveys (CSUR); 2020. p. 1–27.
[13] Pub F. Secure hash standard (shs). Fips pub 2012;180(4).
[14] Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Commun ACM 1978;21(2):120–6.
[15] Buchmann J, Karatsiolis E, Wiesmaier A, et al. Introduction to public key infrastructures. Springer; 2013.
[16] Johnson D, Menezes A, Vanstone S. The elliptic curve digital signature algorithm (ecdsa). Int J Inf Secur 2001;1:36–63.
[17] Castro M, Liskov B, et al. Practical byzantine fault tolerance. In: OsDI; 1999. p. 173–86.
[18] Yin M, Malkhi D, Reiter MK, et al. Hotstuff: bft consensus with linearity and responsiveness. In: Proceedings of the 2019 ACM symposium on principles of distributed computing; 2019. p. 347–56.
[19] Miller A, Xia Y, Croman K, et al. The honey badger of bft protocols. In: Proceedings of the 2016 ACM SIGSAC conference on computer and communications security; 2016. p. 31–42.
[20] Duan S, Reiter MK, Zhang H. Beat: asynchronous bft made practical. In: Proceedings of the 2018 ACM SIGSAC conference on computer and communications security; 2018. p. 2028–41.
[21] Zhang H, Duan S. Pace: Fully parallelizable bft from reproposable byzantine agreement. Cryptology ePrint Archive 2022 Paper 2022/020.
[22] Gervais A, Karame GO, Wüst K, et al. On the security and performance of proof of work blockchains. In: Proceedings of the 2016 ACM SIGSAC conference on computer and communications security; 2016. p. 3–16.

[23] Wood G. Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper 2014:1–32.
[24] Wood G. Polkadot: Vision for a heterogeneous multi-chain framework. White paper 2016;21(2327):4662.
[25] Abraham I, Malkhi D. The blockchain consensus layer and bft. Bull EATCS 2017;123.
[26] Szabo N. Formalizing and securing relationships on public networks. First monday 1997.
[27] Ethereum virtual machine. Available from https://ethereum.org/en/developers/docs/evm/.
[28] Androulaki E, Barger A, Bortnikov V, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains. In: Proceedings of the thirteenth EuroSys conference; 2018. p. 1–15.
[29] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review 2008:21260.
[30] Gueta G, Abraham I, Grossman S, et al. Sbft: a scalable decentralized trust infrastructure for blockchains. 2018. 1804.
[31] Buchman E. Tendermint: Byzantine fault tolerance in the age of blockchains. University of Guelph; 2016.
[32] Eyal I, Gencer AE, Sirer EG, Van Renesse R. Bitcoin-ng: A scalable blockchain protocol. In: 13th {USENIX} symposium on networked systems design and implementation ({NSDI} 16); 2016. p. 45–59.
[33] Kokoris-Kogias E, Jovanovic P, Gasser L, et al. Omniledger: A secure, scale-out, decentralized ledger via sharding. In: Proceedings of 2018 IEEE Symposium on Security and Privacy (SP). IEEE; 2018. p. 583–98.
[34] Sunny FA, Hajek P, Munk M, et al. A systematic review of blockchain applications. IEEE Access 2022;10:59155–77.
[35] Sanka A, IIrfan M, Huang I, et al. A survey of breakthrough in blockchain technology: adoptions, applications, challenges and future research. Comput Commun 2021;169:179–201.
[36] Polillo S. Society for worldwide interbank financial telecommunication. The Wiley-Blackwell Encyclopedia of Globalization 2012.
[37] Project mbridge: Connecting economies through cbdc. 2022. Available from https://www.bis.org/about/bisih/topics/cbdc/mcbdc_bridge.htm.
[38] Attaran M. Blockchain technology in healthcare: Challenges and opportunities. International Journal of Healthcare Management 2022;15(1):70–83.
[39] Tracrtm-de beers group. Available from https://www.debeersgroup.com/sustainability-and-ethics/leading-ethical-practices-across-the-industry/tracr.
[40] De beers group introduces world's first blockchain-backed diamond source platform at scale. 2022. Available from https://www.debeersgroup.com/media/company-news/2022/de-beers-group-introduces-worlds-first-blockchain-backed-diamond-source-platform-at-scale.
[41] Ibm ford blockchain pilot targets cobalt supplies from democratic republic of congo. 2019. Available from https://finance.yahoo.com/news/ibm-ford-blockchain-pilot-targets-072400832.html.
[42] Ghadge A, Bourlakis M, Kamble S, et al. Blockchain implementation in pharmaceutical supply chains: a review and conceptual framework. Int J Prod Res 2023;61(19):6633–51.
[43] Lightency. Available from https://lightency.io/.
[44] 4 top blockchain startups impacting the energy industry. Available from https://www.startus-insights.com/innovators-guide/5-top-blockchain-startups-impacting-the-energy-industry/.
[45] Miglani A, Kumar N, Chamola V, et al. Blockchain for internet of energy management: review, solutions, and challenges. Comput Commun 2020;151:395–418.
[46] Dokchain by pokitdok-blockchain for healthcare. Available from https://ventures.mckesson.com/dokchain-pokitdok-blockchain-healthcare/.
[47] 5 blockchain startups working to transform healthcare. 2017. Available from https://www.cbinsights.com/research/healthcare-blockchain-startups-medicine/.
[48] Embleema closes $3.7m series a funding round and joins techstars alchemist blockchain accelerator program. 2022. Available from https://www.businesswire.com/news/home/20190206005103/en/Embleema-Closes-3.7M-Series-A-Funding-Round-and-Joins-Techstars-Alchemist-Blockchain-AcceleratorProgram:~:text=Hosted%20on%20a%20private%20Ethereum%20blockchain%2C%20Embleema%E2%80%99s%20consolidated%2C,with%20patients%20while%20maintaining%20the%20patient%E2%80%99s%20data%20sovereignty.
[49] Embleema launches the first health records blockchain to give patients complete control over their health data and be at the center of clinical research. 2023. Available from https://www.prweb.com/releases/embleema_launches_the_first_health_records_blockchain_to_give_patients_complete_control_over_their_health_data_and_be_at_the_center_of_clinical_research/prweb15635551.htm.
[50] Coral health: a case study for uses of blockchain in healthcare. 2022. Available from https://www.digitaljournal.com/pr/coral-health-a-case-study-for-uses-of-blockchain-in-healthcare.
[51] Partners with guardtime to accelerate transparency and auditability in health care. Available from https://guardtime.com/blog/estonian-ehealth-partners-guardtime-blockchain-based-transparency.
[52] Talking pharmaceuticals and blockchain with farmatrust. 2018a. Available from https://medium.com/quoineglobal/talking-pharmaceuticals-and-blockchain-with-farmatrust-9f9bc8616d37.
[53] Talking pharmaceuticals and blockchain with farmatrust. 2018b. Available from https://medium.com/quoineglobal/talking-pharmaceuticals-and-blockchain-with-farmatrust-9f9bc8616d37.
[54] Goldwasser S, Micali S, Rackoff C. The knowledge complexity of interactive proof-systems. In: Providing sound foundations for cryptography: on the work of shafi goldwasser and Silvio Micali; 2019. p. 203–25.
[55] Blockpharma. Available from https://www.blockpharma.com/.
[56] Blockpharma. Available from https://builtin.com/company/blockpharma.
[57] Case study change healthcare using hyperledger fabric to improve claims lifecycle throughput and transparency. Availabe from https://www.changehealthcare.com/about.
[58] Case study change healthcare using hyperledger fabric to improve claims lifecycle throughput and transparency. Available from https://www.hyperledger.org/learn/publications/changehealthcare-case-study:~:text=Change%20Healthcare%20using%20Hyperledger%20Fabric%20to%20improve%20claims,system%20in%20production%20...%204%20Future%20directions%20.
[59] The blockchain for healthcare: Gem launches gem health network with philips blockchain lab. 2016. Available from https://www.nasdaq.com/articles/the-blockchain-for-healthcare:-gem-launches-gem-health-network-with-philips-blockchain-lab.
[60] Ambrosus: Digitalising the global trade with blockchain. 2017. Available from https://www.openaccessgovernment.org/ambrosus-digitalising-global-trade-with-blockchain/39686/.
[61] Azzi R, Chamoun RK, Sokhn M. The power of a blockchain-based supply chain. Comput Ind Eng 2019;135:582–92.
[62] Tierion and philips bring blockchain technology to healthcare sector. 2015. Available from https://bitcoinist.com/tierion-philips-bring-blockchain-technology-healthcare-sector/.
[63] Tierion network. 2017. Available from https://www.cryptocompare.com/media/39501577/tieriontokensalewhitepaper.pdf.
[64] Yousuff M, Jayashree J, Vijayashree J, et al. Sharing and interpretation of genomic datasets using blockchain. Blockchain for. In: Healthcare, 4. CRC Press; 2024. p. 262–77.
[65] Azaria A, Ekblaw A, Vieira T, et al. Medrec: Using blockchain for medical data access and permission management. In: Proceedings of 2016 2nd International Conference on Open and Big Data (OBD); 2016. p. 25–30. doi:10.1109/OBD.2016.11.
[66] Medicalchain. Available from https://medicalchain.com/en/.
[67] The grove medical group. Available from https://thegrovemedicalgroup.nhs.uk/.
[68] Medicalchain announces a partnership with the groves medical group. Available from https://medicalchain.com/en/partnership/.
[69] Medicalchain. Available from https://golden.com/wiki/Medicalchain-R9DGJWW.
[70] Fabian V, Vitalik B. Eip-20: Erc-20 token standard. Ethereum Improvement Proposals 2015(20).
[71] Gaži P, Kiayias A, Zindros D. Proof-of-stake sidechains. In: Proceedings of 2019 IEEE Symposium on Security and Privacy (SP). IEEE; 2019. p. 139–56.
[72] Kuzlu M, Pipattanasomporn M, Gurses L, et al. Performance analysis of a hyperledger fabric blockchain framework: throughput, latency and scalability. In: Proceedings of 2019 IEEE international conference on blockchain (Blockchain). IEEE; 2019. p. 536–40.
[73] Xie J, Tang H, Huang T, et al. A survey of blockchain technology applied to smart cities: research issues and challenges. IEEE Commun Surv Tutor 2019;21(3):2794–830.
[74] Poon J, Dryja T. The bitcoin lightning network: Scalable off-chain instant payments. 2016.
[75] Poon J, Buterin V. Plasma: scalable autonomous smart contracts. White paper 2017:1–47.
[76] Xiao J, Liang W, Cai J, et al. An investigation of blockchain-based sharding. In: International conference on smart computing and communication. Springer; 2022. p. 695–704.
[77] Kim C. Ethereum 2.0: How it works and why it matters. Available from https://www.coindesk.com/wp-content/uploads/2020/07/ETH-20-072120.pdf 2020.
[78] Danezis G, Kokoris-Kogias L, Sonnino A, et al. Narwhal and tusk: a dag-based mempool and efficient bft consensus. In: Proceedings of the seventeenth european conference on computer systems; 2022. p. 34–50.
[79] Vilanova L, Maudlej L, Bergman S, et al. Slashing the disaggregation tax in heterogeneous data centers with fractos. In: Proceedings of the seventeenth european conference on computer systems; 2022. p. 352–67.
[80] Duan S, Zhang H, Sui X, et al. Dashing and star: Byzantine fault tolerance using weak certificates. Cryptology ePrint Archive 2022 Paper 2022/625.
[81] Heo JW, Ramachandran GS, Dorri A, et al. Blockchain data storage optimisations: a comprehensive survey. ACM Comput Surv 2024;56(7):1–27.
[82] Singh A, Click K, Parizi RM, et al. Sidechain technologies in blockchain networks: an examination and state-of-the-art review. J Netw Comput Appl 2020;149:102471.
[83] Mc Conaghy T, Marques R, Müller A, et al. Bigchaindb: a scalable blockchain database. White paper. BigChainDB 2016:53–72.
[84] Xu C, Zhang C, Xu J. Vchain: enabling verifiable boolean range queries over blockchain databases. In: Proceedings of the 2019 international conference on management of data; 2019. p. 141–58.
[85] Wang H, Xu C, Zhang C, et al. Vchain+ Optimizing verifiable blockchain boolean range queries. In: Proceedings of 2022 IEEE 38th International Conference on Data Engineering (ICDE). IEEE; 2022. p. 1927–40.
[86] Zhang C, Xu C, Xu J, et al. Gem 2-tree: A gas-efficient structure for authenticated range queries in blockchain. In: Proceedings of 2019 IEEE 35th international conference on data engineering (ICDE). IEEE; 2019. p. 842–53.
[87] Xu C, Zhang C, Xu J. Vchain: enabling verifiable boolean range queries over blockchain databases. In: Proceedings of the 2019 international conference on management of data; 2019. p. 141–58.
[88] Glenn T, Monteith S. Privacy in the digital world: medical and health data outside of hipaa protections. Curr Psychiatry Rep 2014;16(11):494. doi:10.1007/s11920-014-0494-4.
[89] Dagher GG, Mohler J, Milojkovic M, et al. Ancile: privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustain Cities Soc 2018;39:283–97.

[90] Kazemzadeh RS, Sartipi K. Interoperability of data and knowledge in distributed health care systems. In: Proceedings of 13th IEEE International Workshop on Software Technology and Engineering Practice (STEP'05). IEEE; 2005. p. 230–40.
[91] Peterson KJ, Deeduvanu R, Kanjamala P, et al. A blockchain-based approach to health information exchange networks; 2016.
[92] Asswad J, Marx Gómez J. Data ownership: a survey. Information 2021;12(11):465.
[93] Available from https://www.isaca.org/resources/isaca-journal/issues/2020/volume-2/data-ownership. 2020.
[94] Medibloc. Available from https://medibloc.com/.